UNIVERSIDAD NACIONAL "PEDRO RUIZ GALLO"

FACULTAD DE CIENCIAS FÍSICAS Y MATEMÁTICAS

"Sistema de gestión de seguridad de la información y su automatización a través de herramientas Open Source para mejorar el control de la seguridad en la Dirección Desconcentrada de Cultura de Lambayeque"

Autora:

Bachiller Clara Patricia Cubas Penas

Asesora:

Msc. Ing. Jessie Leila Bravo Jaico

Lambayeque, Agosto del 2018

"Sistema de gestión de seguridad de la información y su automatización a través de herramientas Open Source para mejorar el control de la seguridad en la Dirección Desconcentrada de Cultura de Lambayeque"

Presentada a la Facultad de Ciencias Físicas y Matemáticas, Escuela Profesional Ingeniería En Computación e Informática de la Universidad Nacional Pedro Ruiz Gallo para obtener el Título Profesional de Ingeniero En Computación e Informática.

Bach. Clara Patricia Cubas Penas

Msc. Ing. Jessie Leila Bravo Jaico
Asesora

"Sistema de gestión de seguridad de la información y su automatización a través de herramientas Open Source para mejorar el control de la seguridad en la Dirección Desconcentrada de Cultura de Lambayeque"

Presentada a la Facultad de Ciencias Físicas y Matemáticas, Escuela Profesional Ingeniería En Computación e Informática de la Universidad Nacional Pedro Ruiz Gallo para obtener el Título Profesional de Ingeniero En Computación e Informática.

Mg. Ing. Carlos Alberto Valdivia Salazar
Presidente

Ing. Alejandro Chayan Coloma
Secretario

Ing. Denny John Fuentes Adrianzén
Vocal

DEDICATORIA

A Jorge, Miriam, Lisy y Mel, fuente de amor y energía en cada paso de mi vida. A Manuel y Norma, que celebrarían este momento con mucha alegría y orgullo. A ti, que nunca perdiste la fe en que podía lograrlo.

AGRADECIMIENTOS

A Jorge, Miriam, Lisy y Mel, por su incondicional amor, fuerza y motivación, su energía estuvo presente día a día.

A mi asesora Ing. Jessie Bravo Jaico por su paciencia, amistad y guía, gracias por sus consejos y profesionalismo.

A mi abuela Irma, mi tía Sarela y mis primos Sarita, Pamela y Alonso por su apoyo constante y su linda compañía en esta etapa.

A mis mejores amigos, por ser escucha y alegría en los momentos difíciles.

A ti, gracias por acompañarme con tu impulso en cada paso de este proyecto.

RESUMEN

Esta investigación se enfoca en el diseño de un sistema de gestión de seguridad de la información de la Dirección Desconcentrada de Cultura de Lambayeque, basándose en la norma ISO 27001 e integrándose al modelo PDCA y a la metodología de gestión de riesgos: Mehari, siendo el principal objetivo el aporte de herramientas de código abierto para automatizar los controles necesarios para el soporte del sistema.

La acción inicial fue identificar la situación problemática con respecto al manejo de la información en la institución, detectando bajos niveles de confidencialidad, integridad y disponibilidad. El método utilizado para la obtención de datos fue mediante encuestas a los colaboradores para luego realizar una evaluación de los procesos, utilizando diagramas de flujo y notación BPMN.

Se utilizó el modelo PDCA para construir una ruta que precise las fases importantes del sistema de gestión de seguridad y encamine la búsqueda de la mejora continua de los procesos junto a la metodología MEHARI, que tiene una base de conocimiento alineada a las normas ISO, con la que se realizó una evaluación detallada de los activos con el uso de herramientas que incluyen una lista de más de 200 escenarios de riesgos, adaptable a cualquier organización.

Después de la evaluación, se identificaron los riesgos más relevantes, se realizó el plan de tratamiento de riesgos y se definieron los controles aplicables en la institución según la norma ISO 27002. Como resultado, se han propuesto trece documentos entre políticas y procedimientos para la descripción de las tareas y la implementación de buenas prácticas en la institución, además de la configuración de tres herramientas de código abierto para los controles de gestión de activos, respaldo informático y gestión de incidentes. Cumpliendo con el objetivo establecido de mejorar el control de la seguridad en la Dirección Descentralizada de Cultura de Lambayeque.

Palabras clave: SGSI, Seguridad, Mehari, Código abierto, Procesos.

ABSTRACT

This research has focused on the design of an information security management system of the "Dirección Desconcentrada de Cultura de Lambayeque", based on ISO 27001 standards, integrating the PDCA method and the risk management methodology: MEHARI, with the main objective that is the contribution of open source tools to automate the necessary controls for the system support.

The first step was identified the critical situation, regarding with information management in the institution, where were found low levels of privacy, integrity, and availability. The chosen method of data collected was through surveys to institution's workers, and then to perform an evaluation of the processes, using flow charts and BPMN notations.

The PDCA method was used to build a route to accurate the phases on the safety management system, and to guide the search for continuous process improvement using the MEHARI methodology, which it has a knowledge base aligned to ISO standards. This method was used to provide a detailed evaluation of the assets with the use of tools that include a list of more than 200 scenarios of risk, all of them adaptable to any organization.

After the evaluation, the most relevant risks were identified, and the risk of treatment plan was implemented, and the applicable controls to the institution were defined according to ISO 27002. As a result, thirteen documents were proposed between policies and procedures to task descriptions and to enhanced good practices to the institution, as well as the configuration of three open source tools for asset management, IT backup and incident management controls. In compliance with the established objective that is to improve the control of security in "Dirección Desconcentrada de Cultura de Lambayeque".

Key words: SGSI, Security, Mehari, Open source, Process.

Índice de Contenido

Índice de Figuras:

Índice de Tablas:

Índice de Cuadros:

INTRODUCCIÓN

Toda unidad organizativa en busca de mejorar el desempeño de sus procesos y actividades, necesita generar cambios que le permitan adaptarse al entorno, un contexto que se actualiza constantemente gracias a la tecnología.

Los sistemas de información están cambiando la forma en que operan las organizaciones actuales. A través de su uso se logran importantes mejoras, pues automatizan los procesos operativos, proporcionan información de apoyo al proceso de toma de decisiones y, lo que es más importante, facilitan el logro de ventajas competitivas a través de su implantación. (Cohen & Asín, 2005)

Por ese motivo, la información se ha convertido en un activo de gran valor para las entidades, su flexibilidad nos permite tener mayor alcance a las necesidades de los usuarios, sin embargo esta accesibilidad también convierte a la información de cualquier empresa o institución en un elemento vulnerable, enfrentándose al riesgo de tener pérdidas significativas que afecten la productividad, el desempeño eficiente de los colaboradores y por lo tanto una debilidad para su crecimiento.

Para proteger la información, que en sí es algo inmaterial pero que reside en diferentes tipos de soportes, como pueden ser las personas, los documentos escritos o los sistemas informáticos, es necesario tomar las medidas de seguridad apropiada para garantizar el nivel de seguridad de la información que requiere nuestra organización. (Merino & Cañizares, 2011)

La Dirección Desconcentrada de Cultura de Lambayeque, organización gubernamental dependiente del Ministerio de Cultura, tiene un gran flujo de información en actividades como la gestión del patrimonio histórico, la difusión y desarrollo de eventos culturales, siendo importante el respaldo y soporte de su información, se ha considerado diseñar un sistema de gestión de seguridad de la información, realizar un plan de implementación adecuado para su contexto, a pesar de ser una institución pequeña, tiene procesos importantes y es necesario tener controles establecidos ante los riesgos.

La propuesta presenta como valor agregado una lista de herramientas open source ya existentes, usadas para automatizar los controles detallados en la declaración de

aplicabilidad, con la finalidad de analizar las que si pueden dar soporte al sistema de gestión de seguridad de la información de la institución, alineadas a sus políticas internas y con el propósito de mantener una evaluación constante del sistema y generar la mejora continua en sus procesos.

En el capítulo I, se realizó una descripción de la organización, comenzando por un análisis de la situación actual, su organigrama y las funciones de cada área de la dirección desconcentrada de cultura de Lambayeque.

En el capítulo II, se definió la problemática de la dirección, la importancia y justificación: teórica, académica, practica, económica y tecnológica. Además después de analizar la necesidad de la institución se establecieron los objetivos del proyecto, base esencial para su éxito y las limitaciones para determinar su alcance.

En el capítulo III, en el marco metodológico se fundamenta la hipótesis y el tipo de investigación definido como tecnológico formal.

El capítulo IV abarca el marco teórico, se analizaron antecedentes de otros sistemas de gestión de la seguridad de la información en contexto local, nacional e internacional, se determinó la base teórica iniciando por la decisión de alinear el proyecto a la ISO 27001 integrado al modelo PDCA, se realizó una comparación de diferentes metodologías de gestión de seguridad de la información, eligiendo la metodología francesa MEHARI y se propusieron herramientas open source tanto como para el análisis de riesgos como soporte de los controles de la ISO 27002.

En el capítulo V, se desarrolló la propuesta iniciando con el mapeo de procesos, la diagramación de flujos de las actividades con notación BPMN y utilizando el freeware Bizagi Modeler, luego se diseñó el SGSI con el apoyo de la herramienta Mehari PRO, comenzando con el análisis de riesgos, el inventario de activos, pasando por la identificación y definición de los riesgos más relevantes para obtener el plan de tratamiento y definir los controles necesarios con el objetivo de determinar medidas de mitigación, prevención, protección o disuasión, además se muestra la aplicación de las herramientas open source que se decidieron utilizar en la institución.

En la etapa de implementación se realizaron los acuerdos para la implementación, concretando a los participantes del comité de seguridad, sus roles y responsabilidades y la lista de políticas y procedimientos según la ISO 27001: política del SGSI, alcance,

procedimiento de control de acceso, de gestión de TI, gestión de incidentes, gestión de la continuidad entre otros. Finalmente en la etapa de revisión del SGSI se evaluaron los controles con indicadores y en la etapa de mejora continua, las correcciones que puedan servir para que el sistema de gestión de seguridad de la información sea sostenible con el tiempo.

En el capítulo VI, se analizó la rentabilidad de la propuesta, realizando un listado de costos de implementación, puesta en marcha y también los beneficios que obtendrá la institución después de poner en funcionamiento el SGSI, se ha precisado en la propuesta económica el VAR, TIR y PRI del proyecto.

Finalmente, después de lo mencionando, el diseño y la implementación del SGSI es esencial para preparar la institución ante futuras amenazas considerando que el aporte de esta investigación es otorgar un enfoque automatizado con herramientas open source de apoyo para el control de la seguridad en la Dirección desconcentrada de cultura de Lambayeque.

Capítulo I: Datos Generales de la Organización

1.1 Descripción de la Organización

En sus inicios conocida como Casa de la Cultura de Lambayeque, paso a convertirse en Instituto Nacional de Cultura por el D.L. N° 18799, el 9 de Marzo de 1971 y finalmente fue absorbido por el Ministerio de Cultura creado el 21 de Julio del 2010 por Ley N° 29565 y decreto supremo N° 001–2010–MC, actualmente se denomina Dirección Desconcentrada de Cultura de Lambayeque y depende directamente de las decisiones del ministerio. (Coloma, 2010)

Las Direcciones Desconcentradas de Cultura son las encargadas de actuar en representación y por delegación del Ministerio de Cultura en cada región. Ejecutan lineamientos y directivas en concordancia con las políticas del Estado y con los planes sectoriales y regionales (Ministerio de Cultura del Perú, 2017).

1.2 Misión, Visión y Objetivos de la Organización

A continuación se detalla la misión, visión y objetivos del Ministerio de Cultura del Perú, considerando que la Dirección Desconcentrada de Cultura de Lambayeque no cuenta con lo antes mencionado.

1.2.1 Misión

> El Ministerio de Cultura establece, ejecuta y supervisa las políticas nacionales y sectoriales del Estado en materia de cultura, a través de sus áreas programáticas relacionadas con el patrimonio cultural de la nación, la gestión de las industrias culturales y la pluralidad creativa en todo el territorio peruano. También tiene la labor de concertar, articular y coordinar la política estatal de la implementación del derecho a la consulta, correspondiendo a los gobiernos regionales y locales la decisión final sobre la medida. (Ministerio de Cultura del Perú, 2017)

1.2.2 Visión

El Ministerio de Cultura es una institución reconocida como eje fundamental del desarrollo sostenible del país, que promueve la ciudadanía intercultural, la integración social y la protección del patrimonio cultural de la nación, facilitando un mayor acceso a la población, a los productos culturales y artísticos y afianzando la identidad peruana. (Ministerio de Cultura del Perú, 2017)

1.2.3 Objetivos

Sus objetivos según las funciones del Ministerio (Ministerio de Cultura del Perú, 2017) son los siguientes:

- Generar estrategias de promoción cultural de manera inclusiva y accesible.
- Conservar y proteger el patrimonio cultural.
- Fomentar toda forma de expresiones artísticas
- Convocar y reconocer el mérito a quienes aportan al desarrollo cultural del país.
- Planificar y gestionar con todos los niveles de gobierno actividades que permitan el desarrollo de los pueblos amazónicos, andinos y afroperuanos,
- Fortalecer la identidad cultural, abriendo espacios de participación de todas las culturas.

1.3 Estructura Orgánica

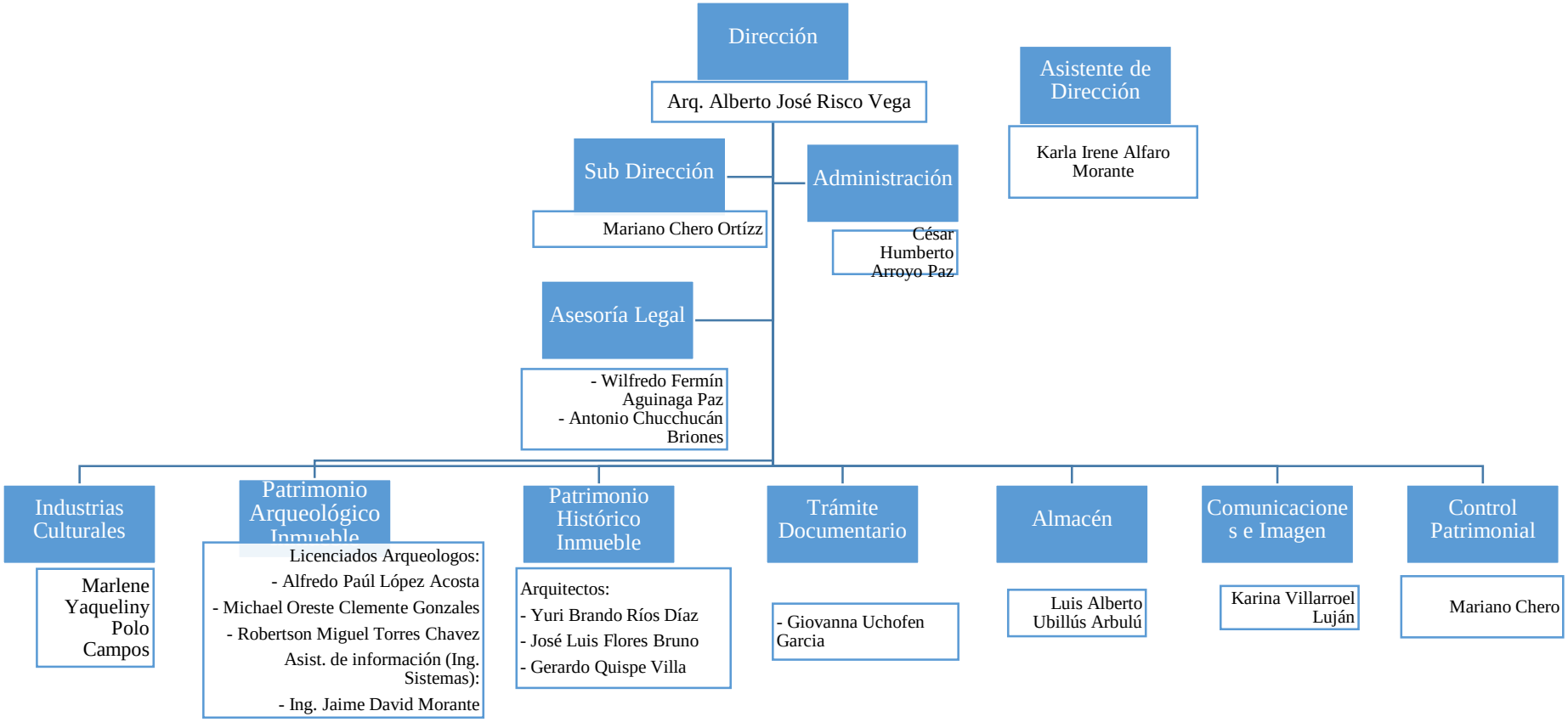


Figura 1: **Organigrama Dirección Desconcentrada de Cultura de Lambayeque**

Fuente: (Morante, 2016)

1.4 Funciones de la Organización

La Dirección desconcentrada de cultura de Lambayeque ejecuta su Plan operativo a través de las siguientes oficinas (Ministerio de Cultura del Perú, 2017):

- **Dirección Regional**

  Su función es de gestionar en la región la ejecución de las políticas y lineamientos establecidos por el Ministerio de Cultura en concordancia con la política del estado y con los planes sectoriales y regionales en materia de Cultura.

- **Oficina de Asesoría Legal**

  Se encargan del seguimiento de procedimientos legales y/o administrativos de la documentación ingresada a la Dirección. Es responsable del seguimiento de los procesos judiciales y policiales en las que se ve involucrada la DDC, de elaborar informes legales de los procesos y de la absolución de consultas legales.

- **Oficina de Administración**

  Esta Oficina se encarga de la elaboración y seguimiento de reportes financieros y administrativos en aplicación al presupuesto asignado, así mismo, de efectuar el control previo y concurrente de operaciones administrativas, financieras y rendición de cuentas, en aplicación de directivas y coordinación con las diferentes oficinas administrativas de la sede central del Ministerio de Cultura. Se desarrolla funciones de administración, tesorería, contabilidad y logística.

- **Oficina de Control Patrimonial**

  Se encarga del control y ubicación de los bienes muebles ubicados en la DDC, así mismo, de la asignación de dichos bienes al personal y de los trámites en coordinación con la sede central de los bienes dados de baja.

- **Oficina de Almacén**

  Se encarga del control de ingreso y salida de los bienes adquiridos mediante compras y la distribución de los mismos, según requerimiento del personal y buen funcionamiento de las oficinas.

- **Oficina de Arquitectura/Patrimonio Histórico**

  Se encarga del control, supervisión e inspección de los bienes inmuebles aplicando directivas técnicas y reglamentos relacionados en la conservación y preservación del patrimonio histórico y colonial en los diferentes distritos y provincias de la región Lambayeque. Es responsable de proponer, coordinar, fundamentar y asesorar a los usuarios en los trámites dentro del centro histórico de la ciudad.

- **Oficina de Arqueología**

  Se encarga en la atención de expedientes ingresados para la supervisión y elaboración del Certificado de Inexistencia de Restos Arqueológicos (CIRA), así mismo, de la inmediata atención en las afectaciones de sitios arqueológicos dentro de la región Lambayeque. Se encarga del asesoramiento en los proyectos arqueológicos a elaborar y ser ejecutados, así como la coordinación con entidades públicas y privadas de la región.

- **Oficina de Actividades Culturales**

  Se encarga en la promoción, difusión y desarrollo de los eventos culturales organizados por la DDC de Lambayeque, de la coordinación de ambientes en alquiler y de los talleres culturales.

- **Oficina de Trámite Documentario**

  Atención en el ingreso de documentos internos y externos a la Dirección para el despacho de dirección y ser distribuidos a las diferentes oficinas para el trámite documentario respectivo.

- **Oficina de Comunicaciones e Imagen Institucional**

  La Oficina de Comunicaciones e Imagen tiene por objetivo fortalecer las comunicaciones mediante estrategias de promoción y difusión del Patrimonio Cultural de la DDC. Esta Área es responsable de la producción de material gráfico de promoción y difusión cultural actividades artísticas, académicas.

Capítulo II: Problemática de la Investigación

2.1 Realidad Problemática

2.1.1 Planteamiento del Problema

La Dirección Desconcentrada de Cultura (DDC) de Lambayeque ubicada en la avenida Luis Gonzáles N° 345 en la ciudad de Chiclayo es una institución que vela por los aspectos culturales del departamento de Lambayeque. Esta institución se encarga de la promoción, difusión y desarrollo de eventos culturales así como de la evaluación y seguimiento del patrimonio histórico para su conservación y preservación.

En la Dirección Desconcentrada de Cultura de Lambayeque, en adelante DDC Lambayeque, existen áreas que gestionan los procesos y actividades de la organización estos son: Dirección regional, asesoría legal, administración, patrimonio histórico (arquitectura), arqueología, actividades culturales, trámite documentario, comunicación e imagen institucional y control patrimonial (almacén).

Dichas áreas cumplen un papel importante en la gestión de la información de temas culturales del departamento de Lambayeque sin embargo según lo observado en la organización, las áreas presentan los siguientes puntos críticos:

La institución realiza el registro de información en el sistema integrado de trámite documentario pero el flujo de documentos es manual, es decir los documentos se derivan físicamente a las áreas correspondientes, considerando que a través de mesa de partes se reciben documentos importantes que se destinan al resto de áreas como por ejemplo: los certificados de Inexistencia de Restos Arqueológicos (CIRA) o PLAN DE MONITOREO ARQUEOLOGICO (PMA) que luego son enviado a la oficina de Arqueología.

El control de los documentos recibidos es deficiente, hasta el año 2016 la información ha sido digitada en un archivo de Excel, a partir del año 2017 se puso en funcionamiento el sistema de trámite documentario pero solo es de registro de ingreso o salida, no se puede validar el estado de un documento en el área correspondiente.

Los documentos son archivados en folders en la oficina compartida de asistente del director y trámite documentario, estos documentos son de fácil acceso, por lo tanto son vulnerables.

En la organización es inexistente una oficina de informática, las atenciones de soporte técnico e incidencias informáticas son dirigidas desde Lima, coordinadas por el área de administración para la atención por parte de un colaborador de mantenimiento o finalmente por terceros, no se controla el motivo de los incidentes y sus prioridades.

Las redes informáticas están instaladas incorrectamente, entre las áreas se trasmite internet a través de switches instalados por un colaborador de mantenimiento.

También se encontró la siguiente situación problemática como resultado de las encuestas realizadas con la herramienta de Google Forms según el Anexo 03: Encuesta Seguridad de la información.

El 86% de los colaboradores indicaron no tener conocimientos de seguridad informática.

El 93% cuenta con usuario y contraseña personal siendo el 7% de los colaboradores, los que presentan vulnerabilidad en el acceso a su información en la computadora, cabe resaltar que este resultado se presentó en Mesa de Partes, el área con mayor tránsito de información en la organización.

El 100% de los usuarios respondió que tienen antivirus ESET Security sin embargo el antivirus tiene licencia caducada.

El 46% indica que los documentos físicos se extravían en sus oficinas entre 11 a 20 veces.

El 64% indica que demora en buscar documentos entre 40 minutos hasta una hora al día.

El 43% indica que otros usuarios pueden acceder a la información de su computadora.

El 21% indica que los trámites pueden durar más de 1 mes.

Los usuarios respondieron que uno de los principales problemas de la institución es la falta de confidencialidad, siendo un 29% quienes opinan que los documentos son de fácil acceso.

Después de ingresar los documentos por mesa de partes y ser derivados a las áreas respectivas no existe un seguimiento del estado de los documentos, siendo el 79% de los usuarios los que opinan que esta es una debilidad de la institución.

Con respecto a la disponibilidad de los documentos, el 71% del personal coincide en que otro de los problemas de la institución, es la demora en la accesibilidad de la información.

El 86% indica que la falta de integridad de los documentos se debe a la cantidad de tiempo en proceso de evaluación en las áreas.

El 57% indicó que su computadora se encuentra en calificación 3, es decir su computadora tiene un desempeño medio.

Las computadoras reciben soporte técnico una vez al año según el 79% de los encuestados siendo el 21% los que indican en su respuesta Otros, que rara vez se hace mantenimiento de los equipos informáticos.

Ante los incidentes de red o acceso en los equipos informáticos el 47% indicó que le pide ayuda a un compañero de trabajo, 40% indicó que coordina la llegada de un externo (servicio técnico) y el 13% restante indicó que busca en internet la solución.

Finalmente el 100% de los colaboradores indicó que si sería necesario para proteger la información contar con un sistema de gestión de seguridad de la información en la Dirección Desconcentrada de Cultura de Lambayeque.

Según los resultados, la Dirección Desconcentrada de Cultura de Lambayeque presenta riesgos delicados en la información que maneja, por ese motivo se considera la evaluación de estos riesgos y el diseño de un sistema de gestión de seguridad de la información basado en los estándares ISO 27001, 27002 y

27005, para esta organización y su aplicación tendrá el soporte de herramientas Open Source ya existentes para validar el funcionamiento del sistema de seguridad, de manera que pueda evaluarse su nivel de vulnerabilidad y se mejore la gestión de la seguridad en todas las áreas.

2.2 Formulación del Problema

¿De qué manera un sistema de gestión de seguridad de la información y su automatización a través de herramientas Open Source, mejorará el control de la seguridad en la Dirección Desconcentrada de Cultura de Lambayeque?

2.3 Justificación e Importancia de la Investigación

La propuesta permite conocer la realidad actual en la que se encuentra la organización y le da la oportunidad a los colaboradores de conocer las herramientas necesarias para proteger su información, mejorar la integridad de los documentos y evitar pérdidas de la información.

2.3.1 Justificación teórica

Se realiza está investigación para obtener conocimiento de las últimas tendencias de los sistemas de gestión de seguridad de la información, de los estándares ISO 27001, ISO 27002, ISO 27005 y de metodologías para evaluar riesgos, en esta investigación se eligió MEHARI, con el soporte de herramientas open source para determinar los controles que se deben aplicar.

2.3.2 Justificación Práctica

El desarrollo de un sistema de gestión de la seguridad de la información en la Dirección Desconcentrada de Cultura de Lambayeque, nace de la necesidad de disminuir los riesgos de pérdida de información en la organización aprovechando las ventajas que brinda el estándar ISO 27001, que aporta en la mejorar de la seguridad de la información en la institución y además en el diseño de políticas y procedimientos alineadas al marco obligatorio de implementación de SGSI en entidades del estado peruano (RM-129-2012-PCM).

Teniendo en cuenta el tiempo que implica buscar información con el proceso actual, se plantea la oportunidad de generar una nueva estructura del acceso a la información para que los colaboradores adquieran conocimiento de las buenas prácticas e interactúen con la implementación del proyecto, teniendo al alcance controles que le aseguren la disponibilidad e integridad de su información.

2.3.3 Justificación tecnológica

El desarrollo del proyecto le permite a la organización aumentar y optimizar los niveles de seguridad de la información, primero determinando los riesgos a los que se encuentra expuesta y luego definiendo que controles son necesarios aplicar y el seguimiento de los procesos, utilizando herramientas open source para automatizar la gestión de seguridad.

2.3.4 Justificación académica

La investigación otorga un enfoque novedoso proponiendo herramientas open source para la identificación, análisis de riesgos y soporte a los controles elegidos para la implementación del sistema de gestión de seguridad de la información de la institución, siendo un referente para futuras investigaciones.

Además el proyecto presenta una lista de políticas y procedimientos basadas en los documentos de la ISO 27001 para la estructuración del SGSI en cualquier entidad.

2.3.5 Justificación económica

Considerando que la información es el recurso más importante de las organizaciones actuales, su pérdida implica un gasto tanto por el tiempo que se invierte en buscar documentos como en la recuperación de los mismos, por ese motivo, este proyecto permitirá tener controles para mejorar la seguridad de la información y realizar seguimiento a los

procesos necesarios para disminuir estas incidencias, lo que generará una mejor gestión de tiempos de trabajo y por ende una disminución en los gastos operativos, teniendo en cuenta también que la automatización a través de herramientas open source permitirá mejorar la seguridad de la información en la organización sin generar costos elevados que afecten su presupuesto.

2.4 Objetivos de la Investigación

2.4.1 Objetivo General

Diseñar un sistema de gestión de seguridad de la información y su automatización a través de herramientas Open Source para mejorar el control de la seguridad en la Dirección Desconcentrada de Cultura de Lambayeque.

2.4.2 Objetivos Específicos

- Realizar un diagnóstico de la situación actual de la seguridad de información en la dirección desconcentrada de Lambayeque.
- Realizar el modelado de los procesos correspondientes al alcance del Sistema de Gestión de Seguridad de la Información.
- Evaluar los procesos mediante el análisis de riesgos de la metodología MEHARI para optimizar la seguridad de los sistemas de información.
- Identificar los controles asociados a los riesgos identificados, empleando la norma ISO 27002.
- Aplicar herramientas Open source para dar soporte al sistema de gestión de seguridad de la información para la Dirección Desconcentrada de Cultura de Lambayeque.
- Determinar la evaluación económica de la propuesta.

2.5 Limitaciones de la Investigación

Como limitaciones de la investigación se pueden considerar:

- La institución no cuenta con una oficina de informática local, es decir no existe personal que realice actividades informáticas específicas, por lo tanto el área de administración se responsabilizará del cumplimiento y seguimiento del sistema de gestión de seguridad de la información y se capacitará al administrador como dueño de este proceso.
- La ausencia de documentación de los procesos de la institución para agilizar la implementación del sistema de gestión de seguridad de la información, por lo que se realizará el levantamiento de información y la evaluación respectiva para presentar en la propuesta.
- La aprobación para el desarrollo de la propuesta, siendo la Dirección desconcentrada de cultura de Lambayeque una institución que depende del Ministerio de Cultura.
- La ausencia de un procedimiento que respalde el seguimiento y utilización del sistema de gestión de seguridad de la información por parte de los colaboradores después de implementado.

Capítulo III: Marco Metodológico

3.1 Tipo de Investigación

Investigación tecnológica Formal

3.2 Hipótesis

Mediante el diseño de un sistema de gestión de seguridad de la información y su automatización con herramientas open source, se mejorará el control de la seguridad en la Desconcentrada de Cultura de Lambayeque.

3.3 Variables

3.3.1 Variable Independiente

Variable Independiente: Sistema de Gestión de la Seguridad de Información (SGSI):

Definición conceptual: Es un sistema que busca gestionar la seguridad de la información de una organización bajo un modelo basado en la mejora continua, donde la organización que decide implementarlo adopta un enfoque por procesos para la creación, implementación, operación, supervisión y mantenimiento de la seguridad de la información. (Merino & Cañizares, Auditoría de Sistemas de Gestión de la Información, 2014)

Dimensión: Es un sistema que permite modelar los procesos en la Dirección Desconcentrada de Cultura de Lambayeque para controlar los riesgos detectados y evitar la pérdida de información valiosa para la organización y a su vez implementar medidas correctivas que puedan generar un cambio en la gestión administrativa.

3.3.2 Variable Dependiente

Variable Dependiente: Control de la seguridad

Definición conceptual: Es la gestión, operación y controles técnicos recomendados por un sistema de información para proteger la confidencialidad, integridad y disponibilidad de los sistemas y de su información. (Broad, 2013)

Dimensión: Es la gestión en la que se emplearán los controles necesarios para proteger la información, con la finalidad de mejorar la confidencialidad, integridad y disponibilidad de la información en la Dirección Desconcentrada de Cultura de Lambayeque y de esta forma, evaluar las vulnerabilidades y mitigar los riesgos.

Capítulo IV: Marco Teórico

4.1. Antecedentes

4.1.1. Antecedentes en el contexto internacional

(Betin & Madera, 2015) En su investigación: Software de apoyo para el proceso de implantación del sistema de gestión de seguridad de la información en organizaciones basado en la norma ISO 27001. Universidad de Cartagena, Cartagena de Indias, Colombia.

En su resumen detalla que durante el proceso de implantación de un SGSI se pueden generar falencias como falta de conocimiento en el tema de seguridad de la información, tiempo implementado no acorde a los subprocesos en el establecimiento del sistema, documentación mal administrada y ausencia de compromiso por parte de la alta gerencia. Por lo tanto, se requiere un sistema de apoyo para un proceso que enmarcada complejidad, revisiones cíclicas y cuidado en el manejo de todos los informes generados en dicho proceso. Con el propósito de hacer menos tediosa, atenuar las complicaciones abordadas en la implantación y estándares relacionados, de tal forma que se contemple la seguridad en la información.

Los investigadores concluyen que el compromiso total en el momento de implantar un SGSI debe tener sus raíces enfocadas en la alta gerencia, al mantener esta parte de la organización conectada con el desarrollo del proyecto, se pretende minimizar la dependencia y la manera de ver este proceso como responsabilidad del departamento de las TIC.

(Yagual & Chilán, 2014) Análisis para la integración de un Sistema de Gestión de Seguridad de Información (SGSI) ISO-27001 Utilizando OSSIM para empresa Industrial. Universidad Politécnica Salesiana Sede Guayaquil. Guayaquil, Ecuador.

Menciona que la información, junto a los procesos y sistemas que hacen uso de ella, son activos muy importantes de una organización. La confidencialidad, integridad y disponibilidad de información sensible

pueden llegar a ser esenciales para mantener los niveles de competitividad, rentabilidad, conformidad legal e imagen empresarial necesarios para lograr los objetivos de la organización y asegurar beneficios económicos. El nivel de seguridad alcanzado por medios técnicos es limitado e insuficiente por sí mismo.

Con respecto a su justificación indica que el Sistema de Gestión de la Seguridad de la Información (SGSI) ayudará a establecer estas políticas y procedimientos en relación a los objetivos de negocio de la organización, con objeto de mantener un nivel de exposición siempre menor al nivel de riesgo que la propia organización ha decidido asumir. Con un SGSI, la organización conoce los riesgos a los que está sometida su información y los asume, minimiza, transfiere o controla mediante una sistemática definida, documentada y conocida por todos, que se revisa y mejora constantemente.

La competitividad es otro de los factores en el cual se encuentra muy interesada la empresa, en un mercado cada vez más competitivo, a veces es muy difícil encontrar algo que lo diferencie ante la percepción de sus clientes. La norma ISO 27001 puede ser un verdadero punto a favor, especialmente si se administra información sensible de los clientes.

4.1.2. Antecedentes en el contexto nacional

(Talavera, 2015) En su tesis: Diseño de un sistema de gestión de seguridad de la información para una entidad estatal de salud de acuerdo a la ISO/IEC 27001:2013.

Indica como objetivo realizar el modelado de los procesos correspondientes al alcance del Sistema de Gestión de Seguridad de la Información e incluye la metodología Business Process Management (BPM 2.0) que incluye diferentes herramientas – tanto de documentación, como tecnológicas – especializadas en el análisis de procesos de negocio con la finalidad de detectar oportunidades de mejora que permitan optimizarlos.

Con respecto a su investigación, detalla que en un caso ideal la institución sobre la que se realiza el proyecto debería contar con todos sus procesos documentados, sin embargo al no encontrarse esta información el equipo encargado de llevar a cabo las actividades se encuentra en la necesidad de realizar el levantamiento de información correspondiente para poder realizar el modelado de procesos con la finalidad de poder realizar un análisis de los riesgos de acuerdo a la situación real de la institución.

(Justino, 2015) Diseño de un sistema de gestión de seguridad de información para una empresa inmobiliaria alineado a la norma ISO/IEC 27001:2013. Pontificia Universidad Católica del Perú, Lima Perú.

Menciona en sus conclusiones que es necesario establecer una Política de Seguridad de Información que contenga los lineamientos para una eficiente administración de la información con el fin de garantizar la seguridad de los sistemas que satisfaga el requerimiento del negocio y de mantener la integridad de la información, de la infraestructura de procesamiento y minimizar el impacto de vulnerabilidades e incidentes de seguridad.

Asimismo indica que la Alta Dirección debe difundir esta política, conocer y dar a conocer a todo el personal que labora en la empresa, de igual manera, el personal es responsable de conocer y cumplir con lo que se especifica.

Además, recomienda crear el rol de Oficial de Seguridad de información, conocido como CISO por sus siglas en inglés (Chief Information Security Officer), quien será el encargado de planificar, presupuestar y verificar el rendimiento de los componentes de la seguridad de la información; así como de realizar una correcta gestión de riesgos para la toma de decisiones.

4.1.3. Antecedentes en el contexto local

(Alcántara, 2015) En su tesis Guía de implementación de la seguridad basado en la norma ISO/IEC 27001, para apoyar la seguridad en los sistemas informáticos de la comisaria del norte P.N.P en la ciudad de Chiclayo (tesis de pregrado). Universidad Santo Toribio de Mogrovejo, Chiclayo Perú.

Menciona que se evaluaron varias herramientas una de las mejores opciones de código abierto ha sido "Securia" SGSI, esta es una herramienta integral que cubre el proceso automático de implantación, puesta en funcionamiento, mantenimiento y mejora continua de un Sistema de Gestión de Seguridad de la Información (SGSI) según la norma internacional ISO 27001.

La herramienta seleccionada es actualizada periódicamente y cuenta con manuales de implementación y uso en español, adicional al uso de Securia, se usará hojas de cálculo lo cual permitirá llevar un control del avance de la implementación del SGSI.

La investigación concluye mencionando que se generó una guía de implementación, un plan de tratamiento de riesgos y un plan de capacitación, lo que le permitió lograr sus objetivos para minimizar los niveles de riesgo y comprometiendo al personal con la seguridad en favor de la institución.

(Leiva, 2016) En su tesis, "Diseño de un Sistema de Gestión de Seguridad de la Información basado en las Normas ISO/IEC 27001 e ISO/IEC 27002 para proteger los activos de información en el proceso de suministros de medicamentos de la Red de Salud de Lambayeque 2015" (tesis pregrado), Universidad Nacional Pedro Ruiz Gallo, Chiclayo – Perú.

Indica la estructura de su Sistema de Gestión de seguridad de la información, empezando por la definición de los procesos de negocio, identificando los activos de información para luego realizar la

valorización, luego realizó una identificación de los riesgos más resaltantes para luego desarrollar una metodología de evaluación de riesgos y un plan de evaluación en base a una serie de actividades para hacer cumplir el SGSI. Después de la identificación y administración de riesgos, propone las políticas que la institución adoptará y los controles para la mitigación de los riesgos que no pueden ser aceptados ya que causarían un daño en la continuidad del negocio. Se concluye con el mapeo a los controles usando el marco de referencia COBIT 5.0 y definiendo la declaración de aplicabilidad donde se muestra el detalle del producto del SGSI.

4.2. Base Teórica

4.2.1. SGSI

SGSI es la abreviatura utilizada para referirse a un Sistema de Gestión de la Seguridad de la Información, 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, oral, impresa en papel, almacenada electrónicamente, proyectada, enviada por correo, fax o e-mail, transmitida en conversaciones, etc.), de su origen (de la propia organización o de fuentes externas) o de la fecha de elaboración. (El portal de ISO 27001 en Español, 2012)

4.2.1.1 ¿Para qué sirve un SGSI?

La información, junto a los procesos y sistemas que hacen uso de ella, son activos muy importantes de una organización. La confidencialidad, integridad y disponibilidad de información sensible pueden llegar a ser esenciales para mantener los niveles de competitividad, rentabilidad, conformidad legal e imagen empresarial necesarios para lograr los objetivos de la organización y asegurar beneficios económicos.

Como se visualiza en la **Figura 2**, un sistema de gestión de la Seguridad de la Información (SGSI) ayuda a establecer estas políticas y

procedimientos en relación a los objetivos de negocio de la organización, con objeto de mantener un nivel de exposición siempre menor al nivel de riesgo que la propia organización ha decidido asumir. Con un SGSI, la organización conoce los riesgos a los que está sometida su información y los asume, minimiza, transfiere o controla mediante una sistemática definida, documentada y conocida por todos, que se revisa y mejora constantemente. (El portal de ISO 27001 en Español, 2012)

Figura 2: ¿Para qué sirve un SGSI?

Fuente: (El portal de ISO 27001 en Español, 2012)

4.2.1.2 ¿Qué incluye un SGSI?

En el ámbito de la gestión de la calidad según ISO 90001, siempre se ha mostrado gráficamente la documentación del sistema como una pirámide de cuatro niveles, es posible trasladar ese modelo a un Sistema de Gestión de la Seguridad de la Información basado en ISO 27001 de la siguiente forma como se visualiza en la **Figura 3**:

***Figura 3:* ¿Qué incluye un SGSI?**

Fuente: (El portal de ISO 27001 en Español, 2012)

Documentos de Nivel 1

Manual de seguridad: por analogía con el manual de calidad, aunque el término se usa también en otros ámbitos. Sería el documento que inspira y dirige todo el sistema, el que expone y determina las intenciones, alcance, objetivos, responsabilidades, políticas y directrices principales, etc., del SGSI.

Documentos de Nivel 2

Procedimientos: documentos en el nivel operativo, que aseguran que se realicen de forma eficaz la planificación, operación y control de los procesos de seguridad de la información.

Documentos de Nivel 3

Instrucciones, checklists y formularios: documentos que describen cómo se realizan las tareas y las actividades específicas relacionadas con la seguridad de la información.

Documentos de Nivel 4

Registros: documentos que proporcionan una evidencia objetiva del cumplimiento de los requisitos del SGSI; están asociados a documentos de los otros tres niveles como output que demuestra

que se ha cumplido lo indicado en los mismos. (www.ISO27000.es, 2012)

4.1.1.3 Aspectos Fundamentales del SGSI

La seguridad de la información según (Merino & Cañizares, 2011) consta de las siguientes dimensiones de la seguridad:

Confidencialidad: Es la garantía de la información que no es conocida por personas, organizaciones o procesos que no disponen de la autorización necesaria.

Integridad: Es la garantía de que la información no se ha transformado ni modificado de forma no autorizada durante su procesamiento, transporte o almacenamiento, y que además permite detectar fácilmente las posibles modificaciones que pudieron haberse producido.

Disponibilidad: Es la garantía de que la información es accesible en el momento en el que los usuarios autorizados (personas, organizaciones o procesos) tienen necesidad de acceder a ella.

Autenticidad: Es la garantía de la identidad del usuario que origina una información. Permite conocer con certeza quién envía o genera una información específica.

Trazabilidad: Es la garantía de que en todo momento se podrá determinar quién hizo qué y en qué momento lo hizo.

4.2.1 Norma ISO 27001

Norma publicada en 2005, la "27001" específica los requisitos para la implantación del Sistema de Gestión de Seguridad de la información (SGSI).

Es la norma certificable y fundamental de la serie, contiene los requisitos del sistema de gestión de seguridad de la información adoptando un enfoque basado en procesos para establecer, implementar, operar, revisar, mantener y

mejorar un Sistema de Seguridad de la información (Merino & Cañizares, 2011).

4.2.2.1 Aporte de la ISO 27001 a la seguridad de la Información

Aplica una arquitectura de gestión de la seguridad que identifica y evalúa los riesgos que afectan al negocio, con el objetivo de implantar contramedidas, procesos y procedimientos para su apropiado control y mejora continua.

Ayuda a la entidad a gestionar, de una forma eficaz, la seguridad de la información, evitando las inversiones innecesarias, ineficientes o mal dirigidas que se producen por contrarrestar amenazas sin una evaluación previa, por desestimar riesgos, por la falta de contramedidas, por implantar controles desproporcionados y de un coste más elevado del necesario, por el retraso en las medidas de seguridad en relación a la dinámica de cambio interno de la propia organización y del entorno, por la falta de claridad en la asignación de funciones y responsabilidades sobre los activos de información, por la ausencia de procedimientos que garanticen la respuesta puntual y adecuada ante incidencias o la propia continuidad del negocio, etc. (Formación SGSI, 2010)

4.2.2.2 ISO/ IEC 27001: Garantía de confidencialidad, integridad y disponibilidad

La norma/estándar ISO/IEC 27001 del "Sistema de Gestión de la Seguridad de la Información" es la solución de mejora continua más adecuada para evaluar los riesgos físicos (incendios, inundaciones, sabotajes, vandalismos, accesos indebidos e indeseados) y lógicos (virus informáticos, ataques de intrusión o denegación de servicios) y establecer las estrategias y controles adecuados que aseguren una permanente protección y salvaguarda de la información. (AENOR, 2012)

4.2.2.3 Estructura ISO 27001:2013

ISO/IEC 27001:2013 especifica los requerimientos para establecer, implementar, mantener y mejorar continuamente un sistema de gestión de seguridad de la información (SGSI) para cualquier organización sin importar su tipo o tamaño. (Collazos, 2014)

Los estándares para un sistema de gestión de seguridad de la información se han ido actualizando con el tiempo como se visualiza en la **Figura 4**:

Figura 4: **Evolución normas para SGSI**

Fuente: (Collazos, 2014)

El estándar internacional ISO/IEC 27001:2013 proporciona los requisitos que debe cumplir una organización para establecer, implementar, mantener y mejorar de manera continua su Sistema de Gestión de Seguridad de la Información. (Rendón, 2015)

El establecimiento e implementación del SGSI depende de los siguientes factores:

- Necesidades y objetivos de la Organización.
- Requisitos de Seguridad.
- Procesos Organizacionales.
- Tamaño y Estructura de la Organización

El propósito del SGSI es conservar la confidencialidad, integridad y disponibilidad de la información utilizando un proceso para la gestión de riesgos que permita garantizar a las partes interesadas que estos son atendidos de manera adecuada. Este estándar tiene una estructura de alto nivel, donde los títulos de subcapítulos, textos, términos y definiciones básicas se basan en lo establecido en el Anexo SL del ISO/IEC Directivas,

Parte1, por lo que se mantiene compatibilidad con otras normas del sistema de gestión que utilizan la estructura del Anexo SL. (Rendón, 2015)

4.2.2.4 Cláusulas de la norma ISO 27001:2013

El informe de "Migración de un SGSI basado En ISO/IEC 27001:2005 a la Versión ISO/IEC 27001:2013" de (Rendón, 2015), detalla las cláusulas de la norma ISO 27001:2013, las que se mencionan a continuación:

Cláusula 1 – Alcance: En esta sección del estándar se recalca que los requisitos definidos son genéricos y pueden ser aplicados a cualquier organización que requiera establecer, implementar, mantener y mejorar un SGSI alineados a su contexto. Vale la pena destacar que si la organización quiere certificar su sistema basado en ISO/IEC 27001:2013 no se acepta la exclusión de requisitos especificados en las cláusulas del 4 al 10.

Cláusula 2 – Referencias normativas: Esta norma en ciertos puntos hace referencia a otros estándares, por tal motivo en esta sección se indican los lineamientos para el adecuado uso de la documentación que menciona, en caso de no contar con fecha aplica la última versión vigente mientras que si es explicita la versión entonces ese es el documento que aplica.

Cláusula 3 – Términos y definiciones: Esta sección hace referencia a los términos y definiciones que se encuentran en ISO/IEC 27000 en su última versión los cuales se aplican en este estándar.

Cláusula 4 – Contexto de la Organización: Es importante conocer que la organización identifique los asuntos internos y externos que puedan influir en el los resultados esperados de su sistema de gestión, además las partes interesadas y sus requisitos relacionados a seguridad de la información.

Esta cláusula está formada por cuatro partes:

- **Clausula 4.1:** Conocimiento de la organización y su contexto.
- **Clausula 4.2:** Conocimiento de las necesidades y expectativas de las partes interesadas.

- **Clausula 4.3:** Determinación del Alcance.
- **Clausula 4.4:** Sistema de Gestión de la seguridad de la información.

Cláusula 5 – Liderazgo: El liderazgo y compromiso de la dirección con respecto al SGSI es un pilar fundamental para que el sistema se integre a los procesos y esté alineada con los objetivos estratégicos de la organización. Esta cláusula consta de tres partes:

- **Clausula 5.1:** Liderazgo y compromiso
- **Clausula 5.2:** Política
- **Clausula 5.3:** Funciones, responsabilidades y autoridad de la organización.

El establecimiento de la política de seguridad de la información es responsabilidad de la Alta Dirección de la organización y debe incluir los objetivos de seguridad de la información y el compromiso de la mejora continua. La política es información documentada del SGSI y debe estar disponible para las partes interesadas y ser comunicada internamente.

La Alta Gerencia debe velar que las responsabilidades y autoridad para los roles en la seguridad de la información sean asignados y comunicados, dentro de las responsabilidades se encuentra:

- Garantizar que el SGSI se adapta a los requisitos de ISO 27001:2013.
- Informar el desempeño del SGSI.

Cláusula 6 – Planificación: La planificación del Sistema de Gestión de Seguridad de la información consta de dos partes:

- **Clausula 6.1:** Acciones para enfrentar los riesgos y las oportunidades, contiene las siguientes sub partes:
- General.
- Evaluación de los riesgos de seguridad de la información.
- Tratamiento de los riesgos de la seguridad de la información.
- **Clausula 6.2:** Objetivos de seguridad de la información y planificación para alcanzarlos.

Cabe recalcar que se debe conservar información documentada asociada al proceso de evaluación de riesgos de la seguridad de la información y su plan de tratamiento.

Es mandatorio elaborar una Declaración de Aplicabilidad en la cual constan todos los objetivos de control y controles del Anexo A, en este documento se debe especificar si estos fueron seleccionados o no y justificar el motivo de su inclusión o exclusión según sea el caso.

En la cláusula 6.2 se especifica que la Organización debe establecer los objetivos de seguridad de la información los cuales deben estar relacionados y ser consistentes con la política de seguridad, ser medibles en caso de que aplique y difundir o comunicarlos. Los objetivos de seguridad de la información deben quedar registrados como información documentada. La organización debe planificar como alcanzar los objetivos planteados respecto a la seguridad de la información, para lo cual debe determinar:

- ¿Qué hacer?
- Recursos necesarios.
- ¿Quién es el responsable?
- ¿Cuándo se alcanzará el objetivo?
- ¿Cómo medir los resultados?

Cláusula 7 – Apoyo/Soporte: Esta sección del estándar cuenta con cinco partes:

- **Clausula 7.1:** Recursos
- **Clausula 7.2:** Competencia
- **Clausula 7.3:** Concientización
- **Clausula 7.4:** Comunicación
- **Clausula 7.5:** Documentación de la información

Dentro de un SGSI la asignación de recursos (Cláusula 7.1) para establecer, implementar, mantener y mejorar el sistema es una acción de apoyo al sistema. Respecto a la competencia de las

personas se debe garantizar que sea en base a: Educación, Entrenamiento y experiencia.

La cláusula 7.3 respecto a concientización es muy clara con la información con la cual el personal debe estar consciente dentro de la organización las cuales son:

- Política de Seguridad.
- Su contribución al SGSI.
- Consecuencias de la no conformidad con los requisitos del SGSI.

Otro tema relevante dentro del SGSI es la comunicación interna y externa respecto al SGSI, para lo cual la organización debe definir lo siguiente:

- ¿Qué se debe comunicar?
- ¿Cuándo?
- ¿A quién?
- ¿Quién es el responsable de comunicar?

Proceso mediante el cual se hace efectiva la comunicación.

Para demostrar conformidad con los requisitos del sistema a lo largo de esta revisión en algunos puntos se ha recalcado la importancia de mantener información documentada, para lo cual en la cláusula 7.5 se presentan los requisitos asociados a la creación, actualización y control de documentación de origen interno y externo necesaria para el SGSI.

Cláusula 8 – Operación: En esta sección se ejecuta lo planificado en la cláusula 6, manteniendo evidencia.

- **Clausula 8.1:** Planificación y control operacional
- **Clausula 8.2:** Evaluación de los riesgos de seguridad de la información.

- **Clausula 8.3:** Tratamiento de los riesgos de la seguridad de la información.

Cláusula 9 – Evaluación del desempeño: Mediante esta cláusula la organización puede medir y evaluar el desempeño de su SGSI, como se muestra en la figura 2.13 consta de tres partes.

- **Clausula 9.1:** Monitoreo, medición, análisis y evaluación.
- **Clausula 9.2:** Auditorías internas
- **Clausula 9.3:** Revisión por la Dirección

Se debe mantener la información documentada de los resultados del monitoreo y medición ya que sirven como evidencia del SGSI. Las auditorías internas son un mecanismo mediante el cual se puede evaluar si el SGSI se ha implementado y se mantiene de manera efectiva. Es importante conservar información de los programas y resultados de auditoría como evidencia.

Debido al compromiso y liderazgo que tiene la Alta Dirección con el SGSI, es importante que realice la revisión del SGSI, para ejecutar esa tarea la revisión debe incluir lo siguiente:

- Estado de acciones de revisiones previas por parte de la Dirección.
- Cambios en asuntos internos y externos que afecten al SGSI.
- Retroalimentación del desempeño basado en: o No conformidades y acciones correctivas. o Resultados de Monitoreo y medición. o Resultados de auditoría.
- Cumplimiento de objetivos de seguridad de la información
- Resultados de evaluación de riesgos.
- Estado del Plan de tratamiento de los riesgos.

- Oportunidades de mejora. Los resultados de la revisión por parte de la Alta dirección deben incluir las decisiones relacionadas con las oportunidades de mejora y cambios en el SGSI. Se debe conservar evidencia de los resultados de la revisión.

Cláusula 10 – Mejora: La cláusula, cuenta con dos partes, la primera asociada a las no conformidades y acciones correctivas y la última respecto a la mejora continua:

- **Clausula 10.1:** No conformidad y acción correctiva
- **Clausula 10.2:** Mejora continua

Al identificar no conformidades en el SGSI de la organización se debe:

- Tomar acciones para controlar y corregir.
- Lidiar con las consecuencias.
- Evaluar las acciones para eliminar las causas de la NC, con el propósito de evitar la recurrencia.

Las acciones correctivas deben ser coherentes a los efectos de las NC identificadas en el SGSI.

Anexo A – Objetivos de control y controles de referencia.

La norma cuenta con el Anexo A, cuya introducción es simplificada y establece que los objetivos de control y controles se derivan de ISO/IEC 27002:2013 y que se utiliza en el contexto de la cláusula 6.1.3 Tratamiento de los riesgos de seguridad de la información.

El anexo tiene un total de 114 controles y 14 dominios los cuales se muestran en la **Tabla 1**:

Dominios de Seguridad	
A.5	Políticas de seguridad de la información
A.6	Organización de la seguridad de la información
A.7	Seguridad de los recursos humanos
A.8	Gestión de los activos
A.9	Control de acceso
A.10	Criptografía
A.11	Seguridad física y medioambiental
A.12	Seguridad de las operaciones
A.13	Seguridad de las comunicaciones
A.14	Adquisición, desarrollo y mantenimiento del sistema
A.15	Relación con proveedores
A.16	Gestión de los incidentes de seguridad de la información
A.17	Gestión de los aspectos de la seguridad de la información para la continuidad del negocio
A.18	Cumplimiento

Tabla 1: **Dominios de Seguridad - ISO 27001**

Fuente: (Rendón, 2015)

4.2.2.5 Norma 27001 enfoque de proceso

El libro Gobierno de las Tecnologías y los sistemas de la información de (Piattini & Hervada, 2007) detalla que la norma 27001 adopta un enfoque de proceso para establecer, implantar, poner en funcionamiento, controlar, revisar, mantener y mejorar un Sistema de Gestión de la información de una organización.

El enfoque de proceso se refiere a la aplicación de un sistema de procesos dentro de una organización, junto con la identificación y la interacción de estos procesos, así como su gestión, adoptando el modelo PDCA, este proceso requiere:

- Entender de los requisitos de seguridad de la organización y de la necesidad de establecer una política y unos objetivos para la seguridad de la información.

- Implantar y poner en marcha los controles para gestionar los riesgos de seguridad de la información de la organización en el contexto de los riesgos globales del negocio de la organización.
- Controlar y revisar el comportamiento y la eficacia de un SGSI.
- Una mejora continua basada en mediciones objetivas.

4.2.3 Norma Técnica Peruana NTP ISO/IEC 27001:2014

El 8 de enero del 2016 se aprobó con RESOLUCIÓN MINISTERIAL N° 004-2016-PCM el uso obligatorio de la Norma Técnica Peruana "ISO NTP/IEC 27001:2014 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos 2a. Edición", en todas las entidades integrantes del Sistema Nacional de Informática (El Peruano, 2016)

La norma indica en el Artículo 3, que las entidades integrantes del Sistema Nacional de Informática, tendrán un plazo máximo de dos (2) años para la implementación y/o adecuación de la presente norma. (PCM, 2016)

Dichas entidades públicas tendrán un plazo de 60 días contados a partir de la fecha de publicación de la presente norma, para la presentación del cronograma de implementación y/o adecuación del sistema de gestión de la Seguridad de la Información, que deberá ser presentado a la Oficina Nacional de Gobierno Electrónico e Informática (ONGEI) de la Presidencia del Consejo de Ministros. (PCM, 2016).

La norma ISO/IEC 27001:2014 está basada en la ISO 27001:2013. (GTDI, 2014)

4.2.4 Norma ISO/IEC 27002:2013

La norma denominada: Técnicas de seguridad. Código de buenas prácticas para la gestión de la seguridad de la información, es una guía de buenas prácticas en la que se describen los objetivos de control y controles recomendables en cuanto a seguridad de la información. (Merino &

Cañizares, Implantación de un sistema de Gestión de Seguridad de la información según ISO 27001, 2011)

Las medidas de seguridad o controles que minimizan el riesgo se recogen en el "Anexo A": Objetivos de control y controles de referencia" de la norma ISO/IEC 27001:2013. (Nuñez, 2014)

Los objetivos de control y los controles se detallan en la norma ISO/IEC 27002:2013 y este anexo se va a utilizar en el contexto de la cláusula "6.1.3. Tratamiento de riesgos de la seguridad de la información". (Nuñez, 2014)

Contiene 35 objetivos de control y 114 controles, divididos en 14 dominios de seguridad. (Nuñez, 2014)

Esta norma no se centra solamente en las tecnologías de la información; también incluye aspectos sobre asuntos organizacionales, gestión de recursos humanos, seguridad, física, normativa legal, etc. (Merino & Cañizares, 2011)

4.2.5 Norma ISO/IEC 27005:2011

La norma denominada: Gestión de riesgos de la Seguridad de la información.

Publicada en 2011, se apoya en los conceptos generales y especificaciones en la ISO/IEC 27001 del ciclo PDCA, está diseñada para proporcionar las directrices en la ardua tare del enfoque basado en riesgos, describe detalladamente la evaluación y tratamiento de riesgos. Esta norma no es una metodología de riesgos, sino que describe las fases recomendadas de análisis incluyendo el establecimiento, evaluación, tratamiento, aceptación, comunicación, monitorización y revisión del riesgo. No es una norma certificable y se engloba dentro de las normas que ayudan la puesta en marcha del SGSI. (Merino & Cañizares, 2011)

4.2.6 El Modelo PDCA

Las siglas PDCA son el acrónimo de Plan, Do, Check, Act (Planificar, Hacer, Verificar, Actuar) (Merino & Cañizares, 2011).

Los sistemas de gestión de la seguridad de la información desarrollados según la norma ISO 27001, igual que muchos otros sistemas de gestión, se basan en el concepto de mejora continua.

Según (Merino & Cañizares, 2011), se describen las fases de la mejora continua del ciclo PDCA, en el caso de un Sistema de Gestión de Seguridad de la información, descritos en la **Figura 5**.

Fases de un Sistema de Gestión de Seguridad de la Información

4.2.6.1 Plan

- Estudio de la situación de la organización (desde el punto de vista de la seguridad), para estimar las medidas que se van a implantar en función de las necesidades detectadas.
- Realización de un análisis de riesgos que ofrezca una valoración de activos de información y las vulnerabilidades a las que están expuestos.
- Elaboración del plan de gestión de riesgos.

4.2.6.2 Do

- Ejecución del plan de acción e implantación de los controles.
- Revisión de la documentación (políticas, procedimientos, instrucciones y registros).
- Concientización y formación.

4.2.6.3 Check

- Evaluación de la eficacia y eficiencia de los controles implantados.
- Verificación de registros e indicadores.
- Verificación del correcto funcionamiento del SGSI.

4.2.6.4 Act

- Mantenimiento del sistema.
- Realización de tareas de mejora y de corrección.

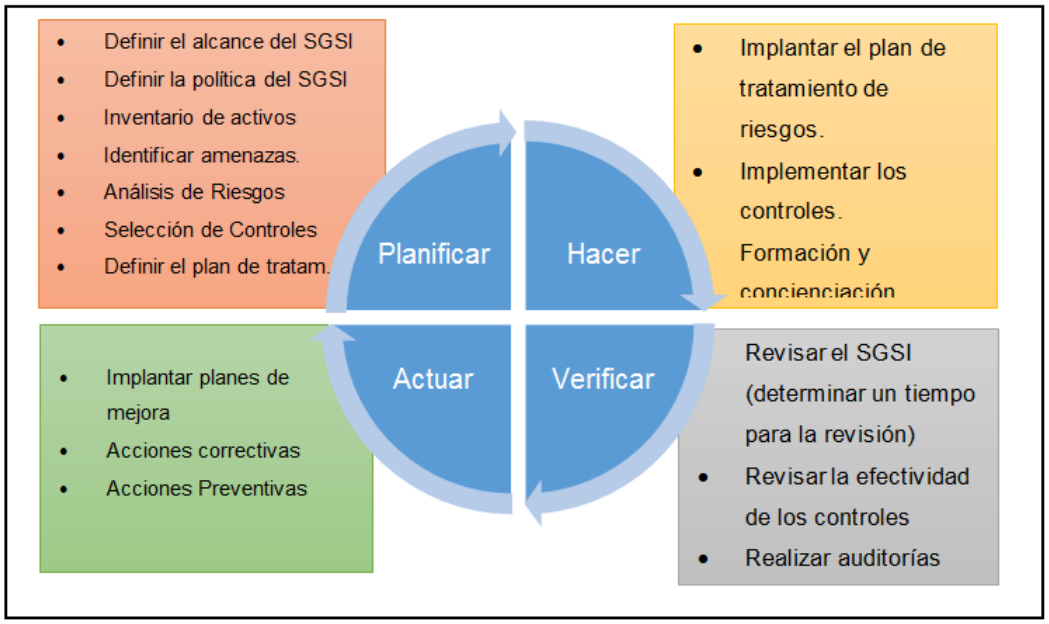


Figura 5: **SGSI según Modelo PDCA**

Fuente: (Merino & Cañizares, 2011)

4.2.7 Business Process Management (BPM)

Es un enfoque sistemático para identificar, levantar, documentar, diseñar, ejecutar, medir y controlar tanto los procesos manuales como automatizados, con la finalidad de lograr a través de sus resultados en forma consistente los objetivos de negocio que se encuentran alineados con la estrategia de la organización. BPM abarca el apoyo creciente de TI con el objetivo de mejorar, innovar y gestionar los procesos de principio a fin, que determinan los resultados de negocios, crean valor para el cliente y posibilitan el logro de los objetivos de negocio con mayor agilidad. (Freund, Rucker, & Hitpass, 2014)

Con respecto a la Gestión de Procesos, la Guía de Procesamiento de MEHARI (CLUSIF, 2011) indica que: Una identificación rigurosa y exhaustiva de las actividades puede hacerse mediante un análisis del proceso. Esto implica

identificar todos los procesos de la organización, incluso subdividirlos en tantos subprocesos como sean necesarios para sacar a la luz las diversas dependencias y resultados intermedios. La experiencia demuestra que un enfoque global e intuitivo, si tiene un nivel de gestión de procesos suficientemente alto, puede identificar rápidamente las principales funciones y sus objetivos.

4.2.7.1 BPMN 2.0 (Business Process Modeling Notation)

Es una especificación que se encuentra documentada en un manual, la versión 2.0 cuenta con más de 500 páginas, presenta los siguientes beneficios:

Para las organizaciones aumenta el grado de independencia de las herramientas de BPM, porque si cambian de herramientas no tienen que volver a capacitar en otras notaciones. . (Freund, Rucker, & Hitpass, 2014)

4.2.7.2 BIZAGI Modeler

Bizagi Modeler (BIZAGI, 2017) es un poderoso modelador de procesos de negocio compatible con el estándar BPMN 2.0 (Business Process Modeling Notation), diseñado para mapear, modelar y diagramar, permite a los expertos en negocios diseñar, documentar y evolucionar su modelo de proceso con total confianza. Tiene un sistema intuitivo llamado “drag and drop”, sus actualizaciones son libres de código y otorga herramientas de generación automática de documentos.

¿Cómo Funciona?

- Diseña mapas de procesos.
- Construye aplicaciones de procesos.
- Se implementa en la organización

4.2.8 Open Source

Open Source (Código abierto) es el término con el que se conoce al software distribuido y desarrollado libremente. El código abierto tiene un punto de vista más orientado a los beneficios prácticos de compartir el código que a las cuestiones éticas y morales las cuales destacan en el llamado software libre. (GPS Open Source, s.f.)

4.2.8.1 Características de Software Open Source

En la página Open Source Initiative (Open Source Initiative, 2007), los términos de distribución de software de código abierto deben cumplir con los siguientes criterios:

- **Libre redistribución:** La licencia no debe restringir a nadie vender o entregar el programa como parte de una distribución mayor que contiene programas de diferentes fuentes. La licencia no debe requerir una regalía u otras comisiones para esta venta.
- **Código Fuente:** El programa debe incluir el código fuente, y debe permitir su distribución en código fuente como en forma compilada. Si alguna forma de un producto no se distribuye con el código fuente, tiene que haber un medio muy publicitados de obtener el código fuente por no más de un costo razonable de reproducción preferentemente, la descarga a través de Internet sin cargo. El código fuente debe ser la forma preferida en la cual un programador podría modificar el programa.
- **Trabajos derivados:** La licencia debe permitir modificaciones y trabajos derivados y debe permitir que estos se distribuyan bajo los mismos términos que la licencia del software original.

- **Integridad del código fuente del autor:** La licencia puede restringir el código fuente de ser distribuido en forma modificada solamente si la licencia permite la distribución de "archivos parche" con el código fuente con el fin de modificar el programa en tiempo de construcción. La licencia debe

permitir explícitamente la distribución de software a partir de código fuente modificada. La licencia puede requerir que los trabajos derivados lleven un nombre o un número de versión diferente del software original.

- **No discriminación contra personas o grupos:** La licencia no debe discriminar a ninguna persona o grupo de personas.
- **No discriminación en función de la finalidad perseguida:** La licencia no debe restringir el uso del programa en un campo específico de actividad. Por ejemplo, no puede impedir que el programa sea utilizado en una empresa, o de ser utilizados para la investigación genética.
- **Distribución de la licencia:** Los derechos asociados al programa deben aplicarse a todos a los que se redistribuya el programa, sin necesidad de pedir una licencia adicional para estas terceras partes.
- **La licencia no debe ser específica para un producto:** Los derechos asociados al programa no deben depender de qué parte del programa de una distribución de software en particular. Si el programa se extrae de esa distribución y usado o distribuido dentro de los términos de la licencia del programa, todas las partes a las que se redistribuya el programa, deben tener los mismos derechos que los que se conceden con la distribución de software original.
- **La licencia no debe restringir el otro software:** La licencia no debe poner restricciones sobre otros programas que se distribuyan junto con el software con licencia. Por ejemplo, la licencia no puede insistir que todos los demás programas distribuidos en el mismo medio deben ser software de código abierto.
- **licencia debe ser tecnológicamente neutro:** Ninguna disposición de la licencia puede basarse en la tecnología o un estilo de interfaz.

4.2.8.2 Herramientas open source para el análisis de riesgos

Se evaluaron las siguientes herramientas Open Source para dar soporte al Sistema de gestión de seguridad:

4.2.8.2.1 Mehari knowledge base (base de conocimiento de Mehari)

La base de conocimiento de Mehari (herramienta de la metodología francesa del mismo nombre Mehari, dirigida por Clusif) proporciona un alto nivel de interfaz de usuario basado en Excel. Se puede utilizar para cualquier tamaño y tipo de organización, ya sea totalmente o en bien seleccionada subconjuntos de sus actividades y permite "puntuación" el cumplimiento de la organización con respecto a la norma ISO 27001.

Esta herramienta se ha descargado en más de 175 países, la revisión actual integra los controles de las normas ISO 27001/27002: 2013 e introduce algunas mejoras que permiten a las organizaciones hacerse cargo del uso de la metodología, dentro de un proceso continuo y controlado de gestión de la seguridad.

Es de distribución libre y se encuentra bajo la licencia Creative Commons. (CLUSIF, 2010)

Especificaciones: La hoja de cálculo del método contiene varias fórmulas que permiten mostrar paso a paso los resultados de las actividades de análisis y gestión de riesgos y propone controles adicionales para la reducción de riesgo.

Funcionalidad:

- Identificación del riesgo: En base a los activos, amenazas y vulnerabilidades

- Análisis de riesgos: A través de los escenarios.
- Evaluación de Riesgos: Cuantificación de los elementos de riesgo: Nivel de amenazas y la probabilidad de amenazas.
- Inventario de activos y evaluación: La lista de activos propuesto incluye servicios, información y normativa.
- Tratamiento del riesgo: El método propone medidas de seguridad para reducir el nivel de riesgo.
- Aceptación del riesgo: Opciones para aceptar o transferir el riesgo.
- La comunicación de riesgos: La hoja de trabajo se puede completar con elementos de comunicación.

4.2.8.2.2 SimpleRisk

SimpleRisk es una herramienta que permite realizar el seguimiento de los riesgos y genera planes de mitigación con su herramienta de gestión.

Se puede ejecutar desde su versión de código abierto en su propio servidor y también cuenta con una versión prueba de 30 días de forma gratuita. (SimpleRisk, 2016)

4.2.8.2.3 Eramba

Eramba es una aplicación web que ayuda en el análisis, la gestión y la presentación de informes de los desafíos de Seguridad, Gobernabilidad, Riesgo y Cumplimiento.

Fundada en 2011 y seguida por una gran comunidad, se está construyendo la aplicación líder de código abierto para GRC (Governance, Risk management and Compliance, en español "Gobierno, Gestión de Riesgo y Cumplimiento"). (Eramba, 2017)

4.2.8.3 Herramientas open source para los controles del SGSI

4.2.8.3.1 OCS Inventory (Open Computers and Software Inventory)

Es una herramienta open source que permite la administración e implementación de activos, utilizando agentes que inician el inventario en los equipos de los clientes y un servidor de administración que recupera los resultados del inventario. Se pueden obtener los datos inventariados, dispositivos de red detectados y, finalmente, crear paquetes de implementación desde una interfaz web.

El servidor de gestión está compuesto por: Servidor de base de datos Servidor de Comunicaciones Servidor de implementación Interfaz de administración

Está basado en el open source GLPI tool (herramienta GLPI), distribuido bajo la licencia GPL, OCS Inventory utilizado con esta herramienta, se obtiene un inventario completo y una herramienta de gestión que le permiten actualizar las configuraciones de sus clientes, gestionar las licencias, utilizar un helpdesk, etc. (OCS Inventory NG, 2017)

4.2.8.3.2 Practical Threat Analysis (PTA – Análisis Práctico de Amenazas)

El PTA (Análisis Práctico de Amenazas) es un análisis de amenazas y una metodología de modelado de amenazas que permite una evaluación eficaz del riesgo operacional y de seguridad en sistemas complejos. Proporciona una manera fácil de mantener modelos dinámicos de amenazas capaces de reaccionar ante cambios en los activos y vulnerabilidades del sistema. Con un análisis de PTA, se puede mantener una gran base de datos de amenazas, crear documentación para revisiones de seguridad y producir informes que muestren la importancia

de varias amenazas y las prioridades de las contramedidas correspondientes.

PTA recalcula automáticamente el riesgo de las amenazas y contramedidas las prioridades de implementación y proporciona a los encargados de la toma de decisiones un plan de mitigación actualizado que refleja los cambios en las realidades de la amenaza.

Las prioridades de la contramedida son una función de los valores de los activos del sistema, el nivel de daño potencial, las probabilidades de amenazas y los grados de mitigación proporcionados por las contramedidas.

El plan de mitigación recomendado está compuesto por las contramedidas que son las más rentables frente a las amenazas identificadas. (PTA Technologies, 2013)

4.2.8.3.3 OpenVas

OpenVAS (Open Vulnerability Assessment System), es un marco de varios servicios y herramientas que ofrecen una solución completa y potente de análisis de vulnerabilidades y vulnerabilidades. El marco forma parte de la solución comercial de gestión de vulnerabilidades de Greenbone Networks, desde la cual los desarrollos han contribuido a la comunidad Open Source desde 2009.

El escáner de seguridad real se acompaña con una actualización periódica de pruebas de vulnerabilidad de red (NVT), más de 50.000 en total. (Greenbone, 2016)

4.2.8.3.4 OpenKM

OpenKM permite a las empresas controlar la creación, almacenamiento, revisión y distribución de los documentos, incrementando la eficiencia en la capacidad de reutilizar la información; así como el control del flujo de los documentos.

OpenKM integra todo lo esencial para la gestión de los documentos, la colaboración entre usuarios y las funcionalidades de búsqueda avanzada, en una única solución fácil de usar. La aplicación incluye herramientas administrativas para definir los roles de los distintos usuarios, cuotas para cada usuario, seguridad a nivel de documento, un completo log de actividad y la configuración de tareas automáticas.

OpenKM permite construir un repositorio con la información de la empresa, para facilitar la creación de conocimiento y mejorar la toma de decisiones en el negocio. Unificando los grupos de trabajo e incrementando la productividad en la empresa a través de prácticas compartidas, mejorar las relaciones con los clientes, obtener ciclos de ventas más rápidos, mejorar el tiempo de comercialización de sus productos y disponer de una mejor información para la toma de decisiones. (Open Document Management System S.L, 2016)

4.2.8.3.5 Nagios

Nagios es una potente solución de monitorización de la infraestructura de TI y solución de alerta de software de monitoreo para los exigentes requisitos organizacionales de hoy.

Nagios XI proporciona a las organizaciones una visión más amplia de su infraestructura de TI antes de que los problemas afecten los procesos críticos del negocio. (Nagios Enterprises, LLC, 2017)

4.2.8.3.6 OSTicket

OsTicket, es un sistema automatizado de soporte al cliente, fácil de usar y de administrar, que integra discretamente todos los tickets creados vía email o por formulario web dentro de una interface web simple, administra, organiza y archiva fácilmente todas las solicitudes de soporte, en ambos casos, los clientes, al abrir una consulta recibirán un e-mail de auto-respuesta. Los clientes podrán ver el estado de los tickets que han abierto y su historial en línea, utilizando para ello su número de consulta.

OsTicket es una aplicación de código abierto simple escrita principalmente usando el lenguaje de programación PHP. (Avantys, 2017)

OSTICKET es de código abierto pues tiene licencia GNU. Se puede cambiar el aspecto de la aplicación mediante varios archivos CSS. Es una herramienta de Tickets de Soporte sencilla y simple escrita principalmente usando el lenguaje de programación PHP y MySQL, desarrollado en una interfaz basada en web. Maneja estos tickets vía email o por formulario web. (Barrios, 2010).

4.2.9 COBIT 5

En el libro "COBIT 5: An ISACA Framework", menciona que proporciona un marco integral que ayuda a las empresas a alcanzar sus objetivos de gobernanza y gestión de TI empresarial. En pocas palabras, ayuda a las empresas a crear un valor óptimo de TI manteniendo un equilibrio entre la realización de beneficios y la optimización de los niveles de riesgo y el uso de los recursos. COBIT 5 permite que la TI sea gobernada y administrada de una manera holística para toda la empresa, teniendo en cuenta las áreas de responsabilidad completas de negocios y TI de la TI, teniendo en cuenta los intereses de las partes interesadas internas y externas. COBIT 5 es genérico y útil para

empresas de todos los tamaños, ya sean comerciales, sin fines de lucro o en el sector público. (ISACA, 2012)

COBIT 5 se basa en cinco principios clave para la gobernanza y la gestión de TI empresarial:

Principio 1: Satisfacer las necesidades de las partes interesadas

Las empresas existen para crear valor para sus partes interesadas manteniendo un equilibrio entre la realización de los beneficios y la optimización del riesgo y el uso de los recursos. COBIT 5 proporciona todos los procesos necesarios y otros facilitadores para apoyar la creación de valor empresarial a través del uso de TI. Debido a que cada empresa tiene objetivos diferentes, una empresa puede personalizar COBIT 5 para adaptarse a su propio contexto a través de las metas en cascada, traduciendo las metas empresariales de alto nivel en objetivos manejables, específicos y relacionados con la TI y asignándolos a procesos y prácticas específicos.

Principio 2: Cobertura de la Empresa

COBIT 5 integra el gobierno de la TI empresarial en el gobierno empresarial:

Cubre todas las funciones y procesos dentro de la empresa; COBIT 5 no se centra sólo en la "función de TI", sino que trata la información y las tecnologías relacionadas como activos que necesitan ser tratados como cualquier otro activo por todos en la empresa.

Considera que todos los mecanismos de gestión y de TI deben ser integrales y de extremo a extremo, es decir, integrar todo y todo el mundo -interno y externo- son relevantes para el gobierno, la gestión de la información empresarial y las TI relacionadas.

Principio 3: Aplicación de un marco único e integrado:

Hay muchas normas y mejores prácticas relacionadas con las TI, cada una de las cuales proporciona orientación sobre un subconjunto de actividades de TI. COBIT 5 se alinea con otros estándares y marcos relevantes a un nivel alto y,

por lo tanto, puede servir como el marco general para la gobernanza y la gestión de TI empresarial.

Principio 4: Habilitación de un enfoque holístico

Una gestión eficaz y eficaz de la TI empresarial requiere un enfoque holístico, teniendo en cuenta varios componentes que interactúan. COBIT 5 define un conjunto de habilitadores para apoyar la implementación de un sistema integral de gobierno y administración para las TI empresariales. Los capacitadores se definen ampliamente como cualquier cosa que pueda ayudar a alcanzar los objetivos de la empresa. El marco COBIT 5 define siete categorías de activadores:

- Principios, políticas y marcos
- Procesos
- Estructuras Organizativas
- Cultura, Ética y Comportamiento
- Información
- Servicios, Infraestructura y Aplicaciones
- Personas, Habilidades y Competencias

Principio 5: Separar la gobernabilidad de la gestión

El marco COBIT 5 establece una clara distinción entre gobierno y gestión. Estas dos disciplinas abarcan diferentes tipos de actividades, requieren diferentes estructuras organizativas y sirven para propósitos diferentes. La visión de COBIT 5 sobre esta distinción clave entre gobernanza y gestión es:

- Gobierno: En la mayoría de las empresas, el gobierno general es responsabilidad de la junta directiva bajo el liderazgo del presidente. Las responsabilidades específicas de gobierno pueden delegarse en estructuras organizativas especiales a un nivel adecuado, en particular en las empresas más grandes y complejas.

- Administración: En la mayoría de las empresas, la dirección es responsabilidad de la dirección ejecutiva bajo el liderazgo del director ejecutivo.

En conjunto, estos cinco principios permiten a la empresa construir un marco de gestión y gestión eficaz que optimice la inversión y el uso de la información y la tecnología en beneficio de las partes interesadas.

Comparación de COBIT con la serie ISO / IEC 27000

Las siguientes áreas y dominios de COBIT 5 están cubiertos por ISO / IEC 27000:

- Seguridad y procesos relacionados con el riesgo en los dominios: "Evaluar, dirigir y supervisar", "Alinear, planificar y organizar" y "Entrega, Servicio y Soporte".
- Varias actividades relacionadas con la seguridad dentro de procesos en otros dominios.
- Monitorear y evaluar las actividades del dominio: "Monitorear y Evaluar".

4.2.10 Metodologías

Existen diferentes metodologías para dar soporte a la implementación de un sistema de gestión de la seguridad, a continuación se evaluarán las características de cada una y se realizará una comparativa de conceptos y especificaciones.

4.2.10.1 Austrian IT

La metodología Austrian IT desarrollado por la Cancillería federal austríaca, utiliza el Manual de Seguridad austríaco de TI (en inglés Austrian IT Security Handbook) que consiste en 2 partes:

La Parte 1 es una descripción detallada del proceso de gestión de la seguridad de TI, incluyendo el desarrollo de las políticas de seguridad,

análisis de riesgos, diseño de conceptos de seguridad, la aplicación del plan de seguridad y las actividades de seguimiento.

La Parte 2 es una colección de 230 medidas de seguridad de línea de base, una herramienta de apoyo a la aplicación está disponible como un prototipo.

El Manual de seguridad de TI fue desarrollado originalmente para organizaciones gubernamentales, y ahora está disponible para todos los tipos de negocios y es compatible con la norma ISO / IEC IS 13335, la norma alemana "IT-Grundschutz" y en parte con la norma ISO / IEC IS 17799. (ENISA, 2005 - 2017)

Contiene una descripción genérica de Análisis de Riesgo, pero no especifica un método especial. (Rodeia, 2009)

4.2.10.2 Cramm

CRAMM es una metodología de análisis de riesgo desarrollado por la organización gubernamental británica CCTA (Agencia Central de Comunicaciones y Telecomunicaciones), en la actualidad CRAMM es el método de análisis de riesgo preferido por el gobierno británico, pero también se utiliza en muchos países fuera del Reino Unido. (Rodeia, 2009)

Las primeras versiones tanto de la metodología como de la herramienta del mismo nombre: CRAMM, se basaron en las mejores prácticas de las organizaciones gubernamentales británicas.

Es apropiado para organizaciones grandes, gubernamentales e industriales. (Alvarez, 2013)

4.2.10.3 Ebios

La metodología EBIOS pertenece a la institución francesa DCSSI - Direction Centrale de la Sécurité des Systémes d'Information, (en español: Dirección Central de la Seguridad de los Sistemas de Información).

Es un conjunto complete de guías (Más una herramienta de software libre) dedicada a la gestión de riesgos en los sistemas de información. Es usada en el sector público y privado de Francia y el extranjero. Es compatible con los principales estándares de seguridad de TI.

Es una herramienta flexible que produce una amplia gama de productos (objetivos de seguridad, perfiles de protección, planes de acción, etc.).

Consiste en un ciclo de 5 fases, donde las 3 primeras son de análisis del riesgo y las dos últimas de gestión de riesgos. (Alvarez, 2013)

4.2.10.4 Magerit

MAGERIT es la metodología de análisis y gestión de riesgos elaborada por el Consejo Superior de Administración Electrónica que estima que la gestión de los riesgos es una piedra angular en las guías de buen gobierno. Actualizada en 2012 en su versión 3, MAGERIT se encuentra en idioma español y está dividido en 3 libros: Métodos, Catálogo de elementos y Guía de técnicas. (Gobierno de España, 2012)

La razón de ser de MAGERIT está directamente relacionada con la generalización del uso de las tecnologías de la información, que supone unos beneficios evidentes para los ciudadanos; pero también da lugar a ciertos riesgos que deben minimizarse con medidas de seguridad que generen confianza.

MAGERIT interesa a todos aquellos que trabajan con información digital y sistemas informáticos para tratarla. Si dicha información, o los servicios que se prestan gracias a ella, son valiosos, MAGERIT les permitirá saber cuánto valor está en juego y les ayudará a protegerlo. Conocer el riesgo al que están sometidos los elementos de trabajo es, simplemente, imprescindible para poder gestionarlos. Con MAGERIT se persigue una aproximación metódica que no deje lugar a la improvisación, ni dependa de la arbitrariedad del analista. . (Gobierno de España, 2012)

Además contiene una herramienta llamada PILAR que implementa la metodología MAGERIT de análisis y gestión de riesgos, desarrollada por

el Centro Criptológico Nacional (CCN) y de amplia utilización en la administración pública española. . (Gobierno de España, 2012)

4.2.10.5 Migra

En la página web de ENISA (ENISA, 2005 - 2017), menciona que la metodología MIGRA (La Metodología Integrata per la Gestione del Rischio Aziendale), es una metodología de evaluación de riesgos y de gestión adecuada para hacer frente a los riesgos tanto de la información y bienes tangibles cualitativa.

La metodología proporciona un marco de análisis basado en la visión clásica del riesgo como una entidad multidimensional dependiendo de las respuestas a tres preguntas:

- ¿qué podría salir mal?
- ¿Cuán probable es que salga mal?
- dado que sucede, ¿cuáles son las consecuencias?

De esta manera, la metodología permite entender con claridad las consecuencias (en términos de riesgos y costos) de la decisión de aplicar o no aplicar todas las medidas de seguridad.

Es una metodología apropiada para: instituciones gubernamentales y grandes compañías.

4.2.10.6 Octave / Octave Allegro/ Octave –S

El método OCTAVE, dirigido por el Instituto de Ingeniería de Software (SIE) de la Universidad Carnegie Mellon de Estados Unidos, es un método utilizado para evaluar las necesidades de seguridad de la información de una organización.

Los métodos OCTAVE son autodirigidos, flexibles y evolucionan, existen 3 tipos: Octave, Octave – S y el derivado de los dos anteriores Octave Allegro.

El método se puede adaptar al entorno de riesgo único de la organización, a los objetivos de seguridad y resistencia y al nivel de habilidad. OCTAVE mueve a una organización hacia una visión de seguridad operativa basada en el riesgo y aborda la tecnología en un contexto empresarial. (Carnegie Mellon University, 2017)

En el caso de OCTAVE Allegro, se centra en los activos de información. Los activos importantes de una organización son identificados y evaluados en base a los activos de información a los que están conectados. Este proceso elimina la confusión potencial sobre el alcance y reduce la posibilidad de que la recopilación y el análisis extensos de datos se realicen para los activos que están mal definidos, fuera del alcance de la evaluación o que necesitan una mayor descomposición. (Carnegie Mellon University, 2017)

En el caso de OCTAVE-S está dirigida para pequeños equipos (de 3 a 5 personas) que se encargarán de recopilar y analizar la información, produciendo planes de estrategias para mitigar riesgo, es una metodología para empresas pequeñas. (<100 empleados).

La metodología no es compatible con el estándar 27001. (Alvarez, 2013)

4.2.10.7 Mehari

Es una metodología desarrollada por el Club Francés de la Seguridad de la Información (CLUSIF), se diseñó inicialmente y se actualiza continuamente, para ayudar a la CISO (Chief Information Security Officers) en la gestión de las actividades de la seguridad de la información.

El primer objetivo de MEHARI es proporcionar un método para la evaluación y gestión de riesgos, concretamente en el dominio de la seguridad de la información, conforme a los requerimientos de la ISO/IEC 27005:2008, proporcionando el conjunto de herramientas y elementos necesarios para su implementación. (CLUSIF, 2010)

Es apropiado para organizaciones gubernamentales, pequeña y mediana empresa. (Alvarez, 2013)

La metodología incluye una herramienta open source llamada: “base de conocimiento” para la evaluación y reducción de riesgos. La base de conocimiento es un archivo disponible como un libro en Excel, es capaz de llevar a cabo la cualificación y cuantificación de todos los elementos de la gestión de riesgos.

Incluye la clasificación de activos, la probabilidad de las amenazas, medidas de vulnerabilidad, a través de la autoría.

Tiene ejemplos de múltiples escenarios con los que permite evaluar las diferentes situaciones de amenaza y proponer planes de acción para mitigar riesgos.

La metodología MEHARI es adaptable, permite tomar decisiones según las necesidades de seguridad de la organización o empresa.

4.2.11 Comparación de metodologías para SGSI

Se ha realizado una comparación de las metodologías según sus conceptos como se indica en el **Cuadro 1** y otra comparación según sus especificaciones como se indica en el **Cuadro 2**.

METODOLOGÍAS	AUSTRIAN IT	CRAMM	EBIOS	MAGERIT	MIGRA	OCTAVE / OCTAVE S	MEHARI
Nombre completo	Austrian IT Security Handbook	CCTA Risk Analysis and Management Method	Expression des Besoins et Identification des Objectifs de Sécurité	Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información	Metodologia Integrata per la Gestione del Rischio Aziendale	Operationally Critical Threat, Asset and Vulnerability Evaluation	Method for Harmonized Analysis of RIsk
País	Austria	Reino Unido	Francia	España	Italia	Estados Unidos	Francia
Organización	Bundeskanzleramt (Cancillería Federal de Austria)	British CCTA (Central Communication and Telecommunication	Club EBIOS	Ministerio Español de Administraciones Publicas	AMTEC/Elsag Datamat S.p.A	Carnegie Mellon University, SEI (Software Engineering	CLUSIF (Club para la seguridad de la información en Francia)
Fecha inicio	1998	1985	1995	1997	1999	1999	1998
Fecha ultima versión	2004	2003	2004	2013	2006	2005	2010*
Estandar (es)	ISO/IEC 13335, ISO/IEC17799	BS 7799	ISO 13335, ISO 15408, ISO 17799	ISO/IEC 27001: 2005 ISO/IEC 17799: 2005 ISO/IEC 13335: 2004	ISO27000	ISO/IEC 27005	ISO / IEC 13335, ISO / IEC 27001: 2013; ISO / IEC 27002: 2013; ISO / IEC 27005
Sitio Web	http://www.cio.gv.at/securenetworks/sihb/	http://www.rac.cz/rac/homepage.nsf/EN/CCTA	https://www.club-ebios.org https://www.ssi.gouv.fr	https://administracionelectronica.gob.es/ctt/magerit	-	http://www.cert.org/resilience/products-services/octave/	https://clusif.fr/mehari http://meharipedia.org
Idiomas	Alemán	Inglés, holandés, checo	Francés, Inglés, Alemán, Español	Español, Inglés, Italiano	Italiano, Inglés	Inglés	Inglés y Francés, español, italiano,etc.
Herramienta Comercial	-	CRAMM expert / CRAMM express	-	EAR/Pilar	MIGRA Tool	-	Risicare
Herramienta No Comercial	-	-	Ebios Application	Pilar / Pilar Basic	-	The Risk IT Framework	Mehari Knowledge Base Pro/Expert

Cuadro 1: Comparación de metodologías (Conceptos básicos)

Fuente: Elaboración propia

METODOLOGÍAS / ESPECIFICACIONES		AUSTRIAN IT	CRAMM	EBIOS	MAGERIT	MIGRA	OCTAVE / OCTAVE S	MEHARI
ALCANCE	INST. GUBERNAMENTALES	SI	SI	SI	SI	SI	SI	SI
	PEQUEÑA Y MEDIANA EMPRESA	NO	NO	NO	NO	NO	SI	SI
	GRANDES COMPAÑIAS	SI	SI	SI	SI	SI	SI	SI
COMPATIBILIDAD	ISO 27001	NO	SI	NO	SI	NO	NO	SI
HERRAMIENTAS	COMERCIAL	NO	SI	NO	SI	SI	NO	SI
	NO COMERCIAL	NO	NO	SI	SI	NO	SI	SI
SOPORTE	COMUNIDAD	NO	NO	NO	NO	NO	NO	SI

Cuadro 2: Comparación de metodologías (Especificaciones)

Fuente: Elaboración propia basada en (ENISA, 2005 - 2017)

Según la evaluación de los **Cuadro 1 y 2**, se eligió la metodología MEHARI porque cumple con los requisitos para un sistema de gestión de seguridad en la Dirección Desconcentrada de Cultura de Lambayeque, por ser una metodología que se puede aplicar a una organización gubernamental de menos de 100 empleados y además porque es compatible con el estándar 27001, necesario para aplicar un sistema de gestión de seguridad de la información.

4.2.12 Metodología por aplicar: MEHARI

La metodología MEHARI acrónimo de Método para el Análisis Armonizado del Riesgo (MEthod for Harmonized Analysis of RIsk) tiene 3 fases para la administración de riesgos como parte de la implementación del SGSI.

- Fase 1: Análisis de Riesgos.
- Fase 2: Tratamiento de Riesgos.
- Fase 3: Gestión del Riesgos.

El libro de MEHARI, "Principales Especificaciones y Conceptos" (CLUSIF, 2010), presenta en la **Figura 6,** un diagrama detallando las tres fases principales de la metodología de riesgos. Las dos primeras fases son la evaluación de los riesgos y las opciones para tratarlos, y corresponden a la fase del Plan de la norma ISO / IEC 27001. La fase de gestión integra las fases de despliegue (Do), supervisión (Check) y mejora (Act).

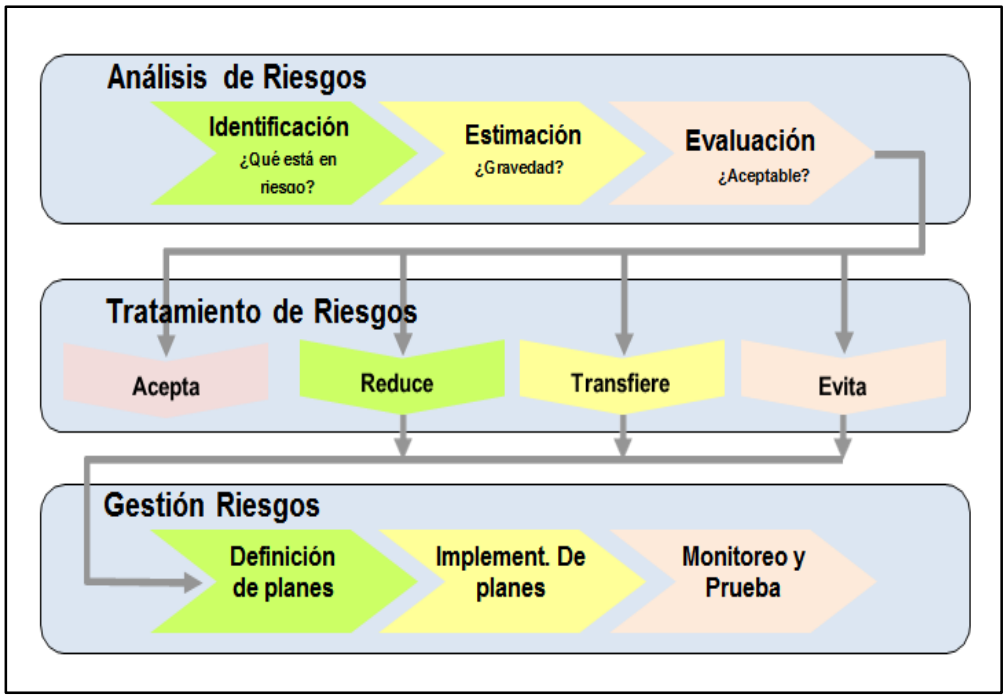


Figura 6: **Fases para la Evaluación de Riesgos de MEHARI**

Fuente*:* (CLUSIF, 2010, pág. 8)

4.2.12.1 Fase 1: Análisis de riesgos

La evaluación de los riesgos consiste en identificar, de la manera más exhaustiva posible, todos los riesgos a los que está expuesta una empresa u organización, estimar la gravedad de cada riesgo y juzgar si cada riesgo se evalúa como aceptable o no. (CLUSIF, 2010)

a. Identificación de riesgos

Este paso apunta no sólo a buscar y reconocer situaciones de riesgo, sino también a caracterizar cada uno de estos riesgos con suficiente precisión para lograr estimar su gravedad. . (CLUSIF, 2010)

Primero es necesario conocer los elementos que deben incluirse en los riesgos:

a.1 Elementos del riesgo:

Los principales elementos según la metodología son los siguientes:

- ***Activos principales:*** Son los activos cuyas características claves deben referirse a las necesidades de las organizaciones, que pueden dividirse en tres categorías principales: Servicios (Servicios de TI y general), datos o información y procesos de gestión.

- ***Activos secundarios:*** Los activos tienen vulnerabilidades, y es la explotación de estas vulnerabilidades lo que causa el riesgo. Para encontrar estas vulnerabilidades, es crucial distinguir lo siguiente para cada activo principal: Las diferentes formas que el activo puede tomar. Y diferentes contingencias de las que depende este activo.

  Estas formas y contingencias pueden agruparse bajo la etiqueta de activos "secundarios" o "de apoyo".

  Debido a que los activos primarios corresponden a las necesidades de las organizaciones, este es el nivel en el que se debe evaluar la importancia de estas necesidades, dependiendo de su importancia se determina el nivel del riesgo. (CLUSIF, 2010)

- ***Vulnerabilidad:***

  Los riesgos surgen del hecho de que un activo determinado tiene una o más vulnerabilidades. . (CLUSIF, 2010)

- ***Vulnerabilidad Intrínseca:***

  Se define a la vulnerabilidad como una característica intrínseca de un sistema, objeto o activo que puede ser susceptible a amenazas (por ejemplo, el hecho de que el material en el que se escribe un documento es degradable).Cada riesgo identificado incluirá una descripción de la vulnerabilidad intrínseca implicada. (CLUSIF, 2010)

- ***Amenaza:***

  No puede haber riesgo sin una causa que conduzca a la vulnerabilidad intrínseca. Lo que produce una amenaza son:

  - **Eventos:** Los eventos se pueden describir por categorías y luego por tipo dentro de cada categoría. Se deben considerar al menos tres categorías: Accidentes, Errores y Actos voluntarios (maliciosos o no).
  - **Actores:** En el caso de las amenazas que son originadas por las personas, es importante distinguir categorías de personas de acuerdo a sus derechos y privilegios. .
  - **Circunstancias:** Las circunstancias pueden incluir factores tales como: Proceso o pasos del proceso, ubicación, tiempo, etc.

- ***Escenarios***

  Los diferentes elementos necesarios para describir un riesgo pueden utilizarse para crear un escenario de riesgo, que reitera los diversos aspectos antes mencionados. . (CLUSIF, 2010)

a.2 Proceso de identificación de riesgos:

Se deben seguir tres pasos para asegurar que la lista de riesgos sea lo más exhaustiva posible, como detalla la **Figura 7**:

- Enumerar los elementos característicos de los riesgos,
- Enumerar los riesgos teóricamente posibles.
- Seleccionar todos los riesgos de esta lista que sean posibles dentro del contexto específico de la gestión de riesgos ya existente. (CLUSIF, 2011)

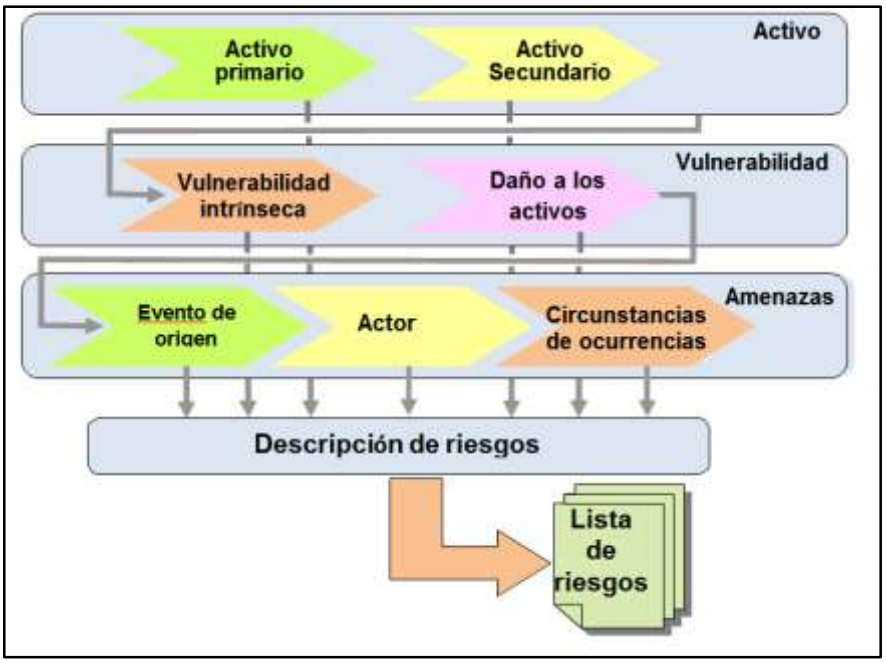


Figura 7: **Identificación de Riesgos**

Fuente: (CLUSIF, 2010)

b. Estimación de riesgos:

Este paso tiene por objeto estimar la gravedad de cada riesgo previamente identificado, teniendo en cuenta las diferentes medidas de seguridad implementadas. (CLUSIF, 2010)

b.1. Métricas del riesgo

El riesgo se mide por dos parámetros: El nivel de gravedad de las consecuencias, o "impacto" y la probabilidad de la ocurrencia, o "probabilidad".

En esta metodología se introducen los conceptos de impacto intrínseco y probabilidad intrínseca, ambos conceptos se detallan a continuación:

- ***Impacto intrínseco:***

  El impacto intrínseco de un riesgo se define por el nivel máximo de consecuencias en que puede incurrir la organización, en ausencia de cualquier medida de seguridad diseñada específicamente para reducir estas consecuencias.

- ***Probabilidad intrínseca:***

  La probabilidad intrínseca se define como la probabilidad máxima de que ocurra el riesgo, en ausencia de cualquier medida de seguridad diseñada específicamente para reducir esta probabilidad. La probabilidad intrínseca también puede denominarse "exposición natural" al riesgo en cuestión.

b.2 Factores de reducción de riesgos

Las medidas de seguridad implementadas pueden actuar como factores de reducción del riesgo. Para manejar los riesgos, es necesario entender cómo, en qué nivel estas medidas reducen el riesgo.

- ***Factores de reducción de la probabilidad:***

  Medidas adecuadas pueden reducir la probabilidad de riesgo a través de diversos mecanismos que pueden actuar de forma independiente o acumulativa.

  - **Medidas disuasorias**, dirigidas a las acciones humanas y destinadas a hacer menos probable que un actor realice la acción.
  - **Medidas preventivas**, cuyo objetivo es hacer menos probable que cualquier acción, ya sea humana o no, conduzca a la aparición del riesgo.

- ***Factores de reducción del impacto:***

  Medidas adecuadas pueden reducir el impacto del riesgo (el nivel de sus consecuencias) a través de diversos mecanismos que pueden actuar de forma independiente o acumulativa y no se aplican a los mismos tipos de consecuencias.

  - **Las medidas de protección**, que tienen por objeto limitar la magnitud de las consecuencias directas.
  - **Las medidas de mitigación**, cuyo objetivo es

minimizar las consecuencias indirectas de un riesgo, anticipando la gestión de crisis.

b.3 Proceso de estimación de riesgos:

En este proceso, se definen las escalas de probabilidad e impacto por el encargado del SGSI de la institución, la propuesta considerará 4 niveles tanto para ambas tablas, cabe resaltar que en esta etapa también se definirán las escalas de las medidas para reducir el impacto y las medidas para reducir la probabilidad, estas tablas también tienen 4 niveles cada una, la propuesta se indica en la parte de desarrollo del proyecto.

En la Figura 8, se muestras un resumen del proceso de estimación de riesgos:

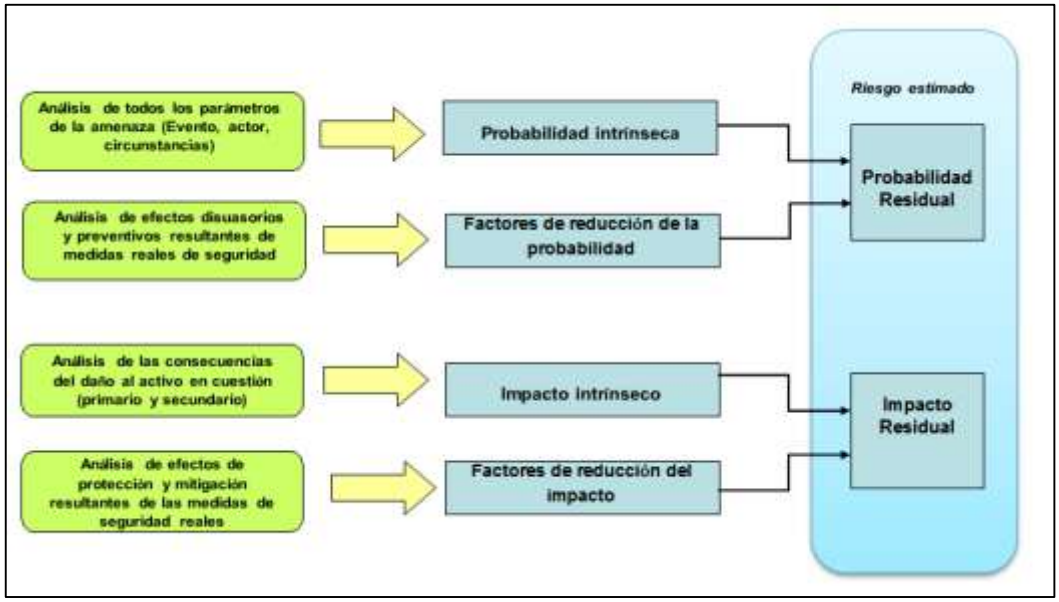


Figura 8: **Proceso de la Estimación de Riesgos**

Fuente: (CLUSIF, 2010)

c. Evaluación de riesgos:

La gravedad de cada escenario o situación de riesgo es una función de su probabilidad e impacto residual. (CLUSIF, 2010)

Para ello es necesario desarrollar una tabla de aceptabilidad del riesgo

considerando 4 tipos de riesgo:

- Riesgos intolerables, que requieren medidas de emergencia fuera de los ciclos presupuestarios normales,
- Riesgos inadmisibles, que deben reducirse o eliminarse en algún momento. Esto debería integrarse en un ciclo de planificación (plan de seguridad),
- Riesgos tolerables.
- Riesgos aceptables.

La tabla de aceptabilidad se definirá en la etapa inicial del desarrollo del proyecto como parte de la fase preparatoria.

4.2.12.2 Fase 2: Tratamiento de Riesgos

Hay diferentes opciones disponibles para tratar los riesgos una vez que se han identificado, enumerado y evaluado, es decir, una vez que cada riesgo se ha considerado aceptable o no (CLUSIF, 2010).

En esta fase se examinarán las cuatro principales opciones disponibles para el tratamiento de riesgos, las cuales se describen en la norma ISO/IEC 27005 y se representan en el siguiente diagrama. Estas opciones se detallan el a **Figura 9**:

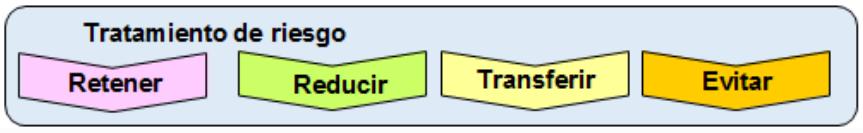


***Figura 9*: Tratamiento del riesgo según ISO/IEC 27005 - Mehari**

Fuente: (CLUSIF, 2010)

a. Retención del riesgo

Retener un riesgo significa aceptar la situación de riesgo descrita en el escenario de riesgo, esto significa que la empresa u organización acepta no hacer nada para cambiar la situación.

b. Reducción del riesgo

Reducir un riesgo significa reducir uno de los dos parámetros característicos de ese riesgo, probabilidad o impacto, o ambos simultáneamente usando acciones específicas. Tales acciones se determinan para cada riesgo identificado como inaceptable.

- ***Elegir qué servicios de seguridad implementar para incrementar ciertos factores de reducción del riesgo***

  El primer paso en el proceso de toma de decisiones utilizado en relación con la reducción de riesgos es elegir los servicios de seguridad adecuados tanto para el escenario de riesgo en cuestión como para el factor de reducción del riesgo que se va a mejorar.

- ***Elección del nivel de calidad objetivo para el servicio de seguridad a implementar***

  La mejor manera de hacerlo es definir una escala de calidad, similar a las escalas establecidas para los diferentes parámetros de riesgo.

- ***Proceso de toma de decisiones para la reducción de riesgos***

  El proceso de toma de decisiones para la reducción de riesgos implica:

  - Selección de servicios de seguridad adecuados.
  - Selección de un nivel objetivo para estos servicios.
  - Deducir nuevos valores para los factores de reducción del riesgo,
  - Comprobar que estos nuevos valores reducen el riesgo a un nivel de gravedad aceptable.

  Cabe resaltar que también existe una opción de reducir riesgos mediante “medidas estructurales”, esto significa reducir riesgos cambiando el contexto de la empresa u organización y su relación con el entorno.

c. Transferencia del riesgo

Transferir un riesgo significa, en términos prácticos, analizar el riesgo desde el punto de vista financiero y transferir, en caso de que el riesgo se materialice, a un tercero.

En la mayoría de los casos, esto significa obtener un seguro, pero también puede significar transferir la responsabilidad a un tercero (el responsable) a través de procedimientos legales.- (CLUSIF, 2010)

d. Evitar el riesgo

Evitar un riesgo es similar a reducir un riesgo mediante medidas estructurales, (cambiar el contexto del riesgo), la diferencia está en el hecho de que, en lugar de cambiar la relación entre una empresa u organización y su entorno, los procesos internos se cambian para que el riesgo ya no exista en absoluto. (CLUSIF, 2010)

4.2.12.3 Fase 3: Gestión de Riesgos

Implica todos los procesos que facilitan la implementación de las decisiones tomadas anteriormente en relación con el tratamiento de los riesgos, el seguimiento del efecto de estas decisiones y su mejora si es necesario. (CLUSIF, 2010)

a. Elaboración de planes de acción

Como tal, los planes de acción deben desarrollarse de acuerdo con los siguientes pasos:

- Elija objetivos prioritarios en términos de servicios de seguridad para implementar y optimizar esta elección,
- Transformar la (s) elección (es) de servicios de seguridad en planes de acción concretos (contar previamente con un manual de referencia de los servicios de seguridad).
- Elija posibles medidas estructurales y medidas de prevención del riesgo.

- Validar las decisiones anteriores.

b. Implementación de planes de acción

La implementación de los planes de acción puede plantear problemas de aplicación en contextos específicos.

En este caso, es importante poder referirse a los riesgos que cada plan de acción debía reducir para determinar la mejor respuesta.

c. Seguimiento y gestión directa de los riesgos

Se deben llevar a cabo numerosas verificaciones para orientar la gestión directa de los riesgos, como se ilustra en la **Figura 10**:

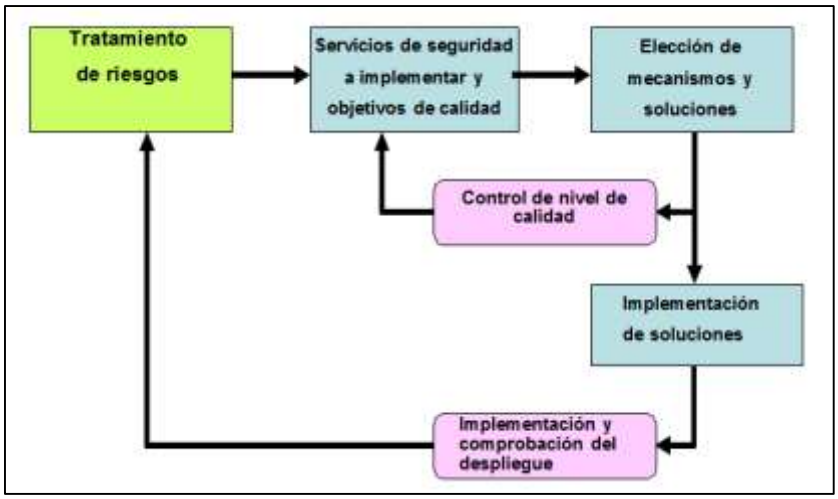


Figura 10: **Proceso de Gestión de Riesgos**

Fuente: (CLUSIF, 2010)

El primer nivel de monitoreo consiste en verificar que las soluciones y mecanismos de seguridad planificados y seleccionados corresponden efectivamente a los niveles de calidad de servicio escogidos durante la fase de tratamiento de riesgos.

La segunda verificación está relacionada con el cumplimiento de la implementación.

La dirección general de la gestión directa de riesgos es similar a toda la dirección del proyecto e incluye:

- Indicadores y un cuadro de indicadores,
- Un sistema de presentación de informes,
- Un sistema para revisiones periódicas y toma de decisiones sobre las acciones correctivas necesarias.

4.2.13 MEHARI y su compatibilidad con la norma ISO/IEC 27001

MEHARI se puede integrar de forma sencilla en el proceso PDCA (Plan – Do – Check – Act) tal y como se encuentra formulado por la ISO/IEC 27001, principalmente en la fase 'PLAN': MEHARI cubre completamente la descripción de las tareas que permiten la creación de las bases del SGSI.

Para la fase 'DO', cuyo objetivo es implementar y administrar el SGSI, MEHARI proporciona elementos útiles de partida, como la construcción de planes para la gestión del riesgo, con priorización directamente relacionada a la clasificación de los riesgos y las medidas de progreso durante su uso.

Para la fase 'CHECK', MEHARI proporciona elementos que permiten la evaluación del riesgo residual, y las mejoras efectuadas sobre las medidas de seguridad. Además, cualquier cambio en el entorno (los riesgos, amenazas, soluciones y organización) pueden ser fácilmente reevaluados por auditorias concretas que utilicen los resultados de la auditoría inicial sobre MEHARI. De esta forma, los panes de seguridad se pueden revisar y evolucionar a lo largo del tiempo.

Para la fase 'ACT', implícitamente MEHARI emplea controles y una mejora continua de la seguridad, asegurando de esta forma que se alcanzan los objetivos de reducción del riesgo. En estas tres fases, si bien MEHARI no se encuentra en el corazón de los procesos, contribuye en gran medida a su puesta en marcha y a asegurar su eficiencia. (CLUSIF, 2010)

4.2.14 MEHARI y su compatibilidad con el estándar ISO/IEC 27005

El marco de trabajo del estándar ISO 27005:2008 es totalmente aplicable en la forma en la que MEHARI permite la gestión de riesgos:

- Los procesos del análisis, evaluación y tratamiento de riesgos
- La identificación de los activos principales y los de soporte, así como la clasificación en niveles aparejada a los mismos, tras el análisis de amenazas.
- La identificación de amenazas incluyendo su nivel (exposición natural), considerando que MEHARI es muy preciso en la descripción de los escenarios de riesgo,
- La identificación y cuantificación de la eficiencia de las medidas de seguridad (o controles) en la reducción de vulnerabilidades,
- La combinación de estos elementos para la evaluación del nivel de severidad de los escenarios de riesgos,
- La habilidad de seleccionar directamente las medidas de seguridad requeridas para los planes de reducción de riesgos.

Por lo tanto, MEHARI no sólo se integra fácilmente en un SGSI, tal y como se solicita por la ISO 27001, sino que cumple con los requerimientos de la ISO 27005 para un método de gestión de riesgos. (CLUSIF, 2010)

4.3 Conceptos y definiciones

Activo: Un activo es un componente o parte de un sistema global al que la organización asigna un valor. (Areitio, 2008)

Amenaza: Cualquier circunstancia o evento que pueda explorar, intencionadamente o no, una vulnerabilidad específica de un sistema de información y comunicaciones, resultando en una pérdida de confidencialidad, integridad, disponibilidad, autenticidad o trazabilidad de la información manejada o de la integridad o disponibilidad del propio sistema. (Merino & Cañizares, 2011)

Análisis de riesgos: Es un proceso que permite comprender la naturaleza del riesgo, determinando su nivel, que proporciona las bases para la evaluación del riesgo y para tomar las decisiones relativas a su tratamiento. (Merino & Cañizares, 2011)

Auditoría: Proceso sistemático, independiente y documentado para obtener evidencias y evaluarlas de manera objetiva con el fin de determinar el grado en que se cumplen los criterios asociados (norma ISO 19011), dicho de otro modo, es verificar que el sistema de gestión de seguridad de la información trabaja con eficacia y eficiencia según los criterios definidos en el sistema. (Merino & Cañizares, 2011)

Autenticación: Es la situación en la cual se puede verificar que un documento ha sido elaborado o pertenece a quien el documento lo dice. (Costas, 2011)

Automatización: Que implica la operación, actuación o autorregulación independiente, sin intervención humana. La automatización involucra herramientas, máquinas, dispositivos, instalaciones y sistemas para realizar determinadas actividades sin que se produzca intervención humana en el transcurso de las mismas. (Montesino Perurena, Baluja García, & Porvén Rubier, 2013)

CISO: Son las siglas de Chief Information Security Officer, cuya función es construir una comprensión conjunta, tangible y concreta de los riesgos de la información desde la dinámica del negocio. (Cano, 2013)

Confidencialidad: Se trata de la cualidad que debe poseer un documento o archivo para que este sólo se entienda de manera comprensible o sea leído por la persona o sistema que esté autorizado. (Costas, 2011)

Disponibilidad: Se trata de la capacidad de un servicio, de unos datos o de un sistema de ser accesible y utilizable por los usuarios (o procesos) autorizados cuando estos lo requieran. (Costas, 2011)

Dominio: Un ambiente o contexto que incluye un paquete de recursos y entidades del sistema y que tiene el correcto acceso a los recursos definidos como políticas de seguridad, modelo de seguridad o arquitectura de seguridad. (Broad, 2013)

Escenario del riesgo: Una descripción de todas las características de un riesgo, incluyendo el activo afectado, la vulnerabilidad intrínseca del activo afectado y la amenaza que conduce a la ocurrencia del riesgo. (CLUSIF, 2010)

Exposición Natural: También llamada "probabilidad intrínseca". (CLUSIF, 2010)

Gestión de riesgos: Definición conceptual: Es el proceso por el cual se evalúan los riesgos y se seleccionan y aplican los controles necesarios para mantener el nivel de riesgos a los niveles aceptados por la Dirección. (Merino & Cañizares, Implantación de un sistema de Gestión de Seguridad de la información según ISO 27001, 2011)

GLP: Es la licencia Pública General de GNU, que pretende garantizar la libertad de compartir y cambiar todas las versiones de un programa para asegurarse de que sigue siendo libre para todos sus usuarios. (Free Software Foundation, 2007)

Impacto: Es la consecuencia que tiene la materialización de una amenaza sobre un activo, sobre un sistema de información y comunicaciones o sobre una organización. (Merino & Cañizares, Implantación de un sistema de Gestión de Seguridad de la información según ISO 27001, 2011)

Impacto intrínseco: La consecuencia, para la organización en cuestión, de que el riesgo en cuestión se produce en ausencia de todas las medidas de seguridad. (CLUSIF, 2010)

Integridad: Es la cualidad que posee un documento o archivo que no ha sido alterado y que además permite comprobar que no se ha producido manipulación alguna en el documento original, Aplicado a las bases de datos sería la correspondencia entre los datos y los hechos que refleja. (Costas, 2011)

ISO: Son las siglas de "International Standarization Organization" (Organización Internacional para la Normalización), cuya sede se encuentra en Suiza. (Castellanos, 2014)

ISO/IEC 27001: Norma que específica los requisitos para la implantación del SGSI, es la norma más importante de la familia 27000. Adopta un enfoque de gestión de riesgos y promueve la mejora continua de los procesos. (Castellanos, 2014)

Norma / Estándar: Una práctica de negocio o producto tecnológico que es una práctica aceptada, avalada por la empresa o por el equipo gerencial de TI. (Merino & Cañizares, 2011)

Política: Por lo general, un documento que ofrece un principio de alto nivel o una estrategia a seguir. (Merino & Cañizares, 2011)

Probabilidad: La probabilidad de que el riesgo en cuestión ocurra, en el contexto de la organización en cuestión. . (CLUSIF, 2010)

Probabilidad intrínseca: La probabilidad de que el riesgo en cuestión ocurra, en el contexto de la organización en cuestión, en ausencia de cualquier medida de seguridad, también llamada "Exposición Natural". . (CLUSIF, 2010)

Procedimiento: Una descripción de una manera particular de lograr algo, una forma establecida de hacer las cosas; una serie de pasos que siguen un orden regular definido, garantizando un enfoque consistente y repetitivo hacia las actividades. (Merino & Cañizares, 2011)

Riesgo: Es la estimación del grado de exposición a que una amenaza se materialice sobre uno o más activos causando daños o perjuicios a la organización. (Merino & Cañizares, 2011)

Seguridad de la información: La protección de los sistemas de información y de la información, contra el acceso, uso, divulgación, interrupción, modificación o destrucción, no autorizados a fin de proporcionar confidencialidad, integridad y disponibilidad. (Broad, 2013)

SGSI: Las siglas son el acrónimo de Sistema de Gestión de la Seguridad de la información. (Merino & Cañizares, 2014)

Vulnerabilidad: Cualquier debilidad o falta de control que aumente la probabilidad de que se materialice una de las amenazas a las que están expuestos los activos o los elementos del sistema de información y comunicaciones. (Merino & Cañizares, 2011)

Vulnerabilidad intrínseca: La característica intrínseca de un sistema, objeto o activo que puede ser susceptible de amenazas. (CLUSIF, 2010)

Capítulo V: Desarrollo de la Propuesta

ETAPA I: PREPARACIÓN PARA EL SGSI: FASE INICIAL

5.1.1 Coordinación para realizar el SGSI

Se solicitó permiso a través de mesa de partes para el desarrollo del presente proyecto al Director de la Dirección Desconcentrada de Lambayeque, Arquitecto Alberto José Risco Vega, quien dio su visto bueno de conformidad y otorgó las facilidades para el inicio del proyecto, con respecto al acceso a la información e instalaciones para el análisis del contexto, de esta manera realizar una propuesta a la medida de la institución, visualizar el Anexo 01: Solicitud de permiso para desarrollo de proyecto.

Contando con el compromiso de la institución se puede dar inicio al desarrollo del proyecto.

5.1.2 Levantamiento de información

Después de obtener los permisos necesarios para realizar la investigación y desarrollo de la propuesta con respecto a seguridad informática en la institución, se realizó el levantamiento de información a través de preguntas a los usuarios: Anexo 02: Cuestionario para entrevista a usuarios de la Dirección Desconcentrada de Cultura de Lambayeque.

También se utilizó la observación y el seguimiento de las actividades de las áreas de la Dirección Desconcentrada de Cultura de Lambayeque como herramientas de recopilación de información, estos resultados han sido estructurados en fichas de información de procesos, señalados en el apartado "Modelado de Procesos".

5.1.3. Análisis Del Contexto

5.1.3.1 Contexto Actual

La Dirección Desconcentrada de Cultura de Lambayeque es una institución que pertenece al Ministerio de Cultura del Perú y que tiene como principales funciones la gestión del patrimonio histórico, gestión de proyectos arqueológicos, gestión de actividades culturales y difusión cultural de la región de Lambayeque, funciones que

determinan el nivel de importancia de dicha institución en el ámbito regional y nacional.

Debido a estas funciones, la institución a pesar de solo ser una pequeña locación en la ciudad de Chiclayo, mantiene un amplio flujo de documentos y expedientes técnicos necesarios para trámites tanto personales como institucionales, que son vitales para la toma de decisiones en la gestión cultural de la región.

Es necesario mencionar que los colaboradores prestan servicios de asesoría y monitoreo en proyectos arqueológicos y arquitectónicos con respecto al patrimonio histórico, actividades que solo están permitidas y validadas en esta institución, además se debe considerar que la mayoría de eventos culturales e incidencias relacionadas a la cultura de la región son aprobadas y validadas por la dirección y que la correcta difusión juega un papel importante si es respaldada por una entidad gubernamental como la DDC Lambayeque.

Por tal motivo y demostrando que toda la información, servicios y gestión resultantes de las actividades de esta organización son relevante tanto para sus procesos internos como para la administración pública, se realizará un análisis de su entorno para detectar riesgos que puedan ser controlados, manteniendo su confidencialidad, integridad y disponibilidad, en la medida en la que se puedan controlar y brindando de esta forma, los primeros pasos en el cumplimiento de la normativa del gobierno peruano.

5.1.3.2 Contexto estratégico

Posicionamiento estratégico:

- **Estructura:** La institución pertenece a la gestión pública y depende directamente del Ministerio de Cultura del Perú.
- **Naturaleza de la actividad:** Servicios relacionados al patrimonio histórico, arqueológico, gestión y difusión de eventos culturales.

Política de seguridad de la información existente:

- **Objetivos de seguridad:** La institución no cuenta con objetivos de seguridad definidos.

5.1.3.3 Contexto técnico

La Dirección desconcentrada de cultura de Lambayeque cuenta con la siguiente infraestructura tecnológica:

a. **Hardware**

Equipos de cómputo: La institución cuenta con los siguientes equipos de cómputo, descritos en el **Cuadro 3:**

Oficinas	PC
Dirección	2*
Asistente Dirección	1
Sub-dirección	2
Administración	2
Asesoría legal	2
Arqueología	5
Patrimonio histórico	3
Actividades Culturales	1
Control Patrimonial	1
Trámite Documentario	1
Almacén	1
Comunicaciones	2
Total	**23**

Cuadro 3: Equipos de Cómputo

Fuente: Elaboración propia.

*Cabe resaltar que todos los equipos de cómputo son equipos de Escritorio, solo el director tiene 1 PC de Escritorio y 1 laptop.

Impresoras: La institución cuenta con los siguientes dispositivos descritos en el **Cuadro 4**.

Tipo	Marca	Modelo	Cantidad
Matricial	EPSON	LQ-2090	1
Laser	HP	LaserJet P3005	1
Multifuncional	Xerox	WorkCentre 5330	1
	Brother	DCP-8060	1
Total			**4**

Cuadro 4: Lista de Impresoras

Fuente: Elaboración propia.

Equipos de Red: La institución cuenta con una red local (LAN), se detallan los dispositivos encontrados en el **Cuadro 5**:

Equipo de Red	Marca	Modelo	Cantidad
Router	Cisco	1900 Series	1
	Adtran	NetVanta 832T	1
	Zyxel	Prestiga 650 HW-31	1
Switch	D-Link	DES-1024D	1
	Trendnet	TEG-S80G	2
Telefonía IP	Yeastar	MyPBX SOHO	1
Firewall	Fortinet	FG-60C	1
TOTAL			**8**

Cuadro 5: Equipos de Red

Fuente: Elaboración propia.

b. Software

Sistema Operativo: Los equipos de trabajo utilizan. Windows 7 Professional, cuenta con licencia en todas las computadoras. Los equipos de trabajo utilizan. Microsoft Office 2013, cuenta con licencia en todas las computadoras.

Programas instalados: Los equipos de trabajo tienen los siguientes programas instalados según el **Cuadro 6**:

Programa	Versión
Adobe Reader XI	11.0.06
Google Chrome	49.0.2623.87
Google Earth	7.1.5.1557
OpenOffice	4.00.9702
TeamViewer 8	8.0.44109
Microsoft Office Professional Plus 2013	15.0.4420.1017
Autodesk - Autocad	2.0.90
Adobe Photoshop CS5	12.0
CorelDRAW Graphics Suite X5	15.0
Eset Nod 32	

***Cuadro 6:* Programas instalados**

Fuente: Elaboración propia.

Finalmente, en el **Cuadro 7** se visualiza un resumen de la infraestructura tecnológica:

Infraestructura	Tipo	Cantidad
Equipos de Computo	PC	22
	Laptop	1
	Impresoras	4
Equipos de Red	Routers	3
	Switches	3
	Teléfono IP	1
	Firewall	1
Aplicaciones	Oficina	5
	Diseño	3
	Otros	3
Total		**46**

Cuadro 7: Resumen de Infraestructura Tecnológica

Fuente: Elaboración propia

c. Proveedores internos y proveedores externos

Proveedores de servicios estructurales:

- Servicio de internet: Movistar Perú
- Instalaciones: Ministerio de Cultura del Perú

Proveedores ocasionales de servicios

- Mantenimiento: Contrato CAS
- Soporte técnico: Contrato a terceros
- Vigilancia: Empresa externa

5.1.3.4 Contexto Organizacional

La distribución de las responsabilidades de seguridad de la información estará a cargo del director de la Dirección desconcentrada de cultura de Lambayeque, quien determinará los roles y responsabilidad en el comité de seguridad, decidido en la etapa de implementación.

5.1.4 Modelamiento de Procesos

El modelado de procesos es una tarea crítica y obligatoria para cualquier proyecto que pretenda establecer un Sistema de Gestión de Seguridad de la Información en alguna organización, puesto que es necesario conocer cómo se desarrollan los distintos procesos de negocio, así como el flujo de información a través de los mismos. (Talavera, 2015)

La Dirección desconcentrada de cultura de Lambayeque tiene procesos que se desarrollan sin estar documentados por lo tanto se realizará mapeo de los procesos más relevantes con respecto a seguridad de la información siguiendo los siguientes pasos:

5.1.4.1 Matriz de Procesos de la Dirección Desconcentrada de Lambayeque

La dirección desconcentrada de cultura de Lambayeque, parte de Ministerio de Cultura, el core de la institución es la protección del

patrimonio histórico de la región, el seguimiento de incidentes arqueológicos, la gestión y difusión de eventos culturales.

- **Mapa del Macro proceso:** Se ha definido como macro proceso a la Gestión Institucional, identificando los siguientes procesos:
- **Procesos Misionales:** Gestión Patrimonio histórico, Gestión de Proyectos Arqueológicos y Gestión de Actividades Culturales.
- **Procesos Estratégicos:** Gestión directiva, Gestión administrativa, Gestión de las comunicaciones
- **Procesos de Soporte:** Gestión Control Patrimonial y Gestión de Trámite Documentario.

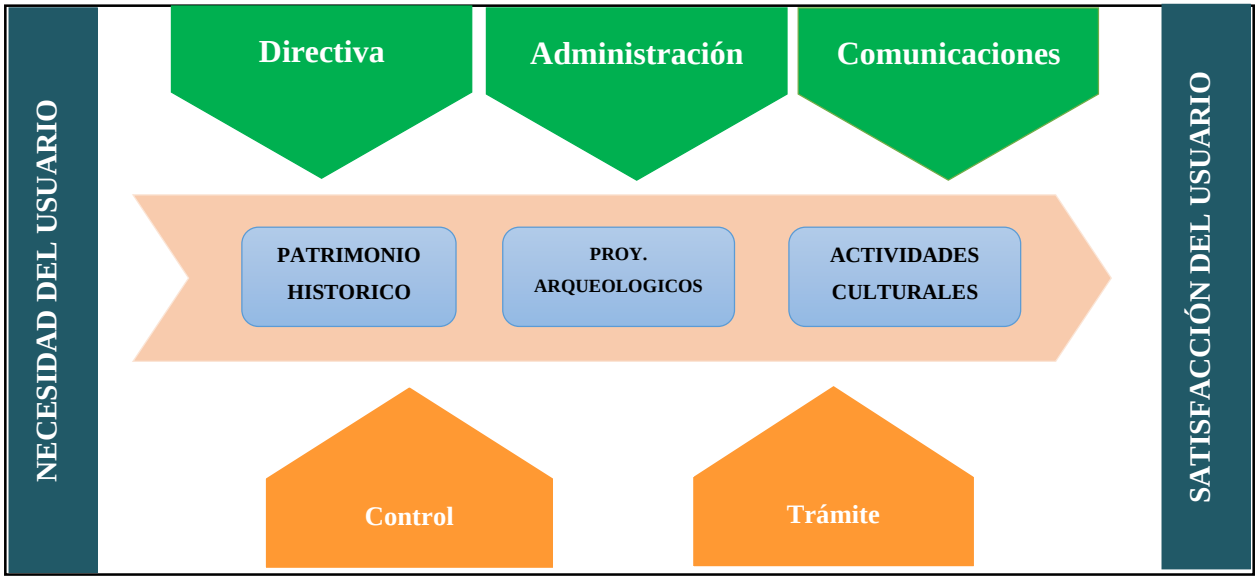


Figura 11: Mapa del Macro Proceso: Gestión institucional

Fuente: Elaboración propia

Como se visualiza en el **Cuadro 8** se ha definido la matriz de identificación de procesos, iniciando por el macro proceso: "Gestión institucional", se puede visualizar los diferentes procesos de la institución, donde se ha definido los siguientes procesos:

MATRIZ DE IDENTIFICACION DE PROCESOS

MACROPROCESO: **GESTIÓN INSTITUCIONAL - DIRECCIÓN DESCONCENTRADA DE CULTURA LAMBAYEQUE**

ENTRADAS Y PROVEEDORES (Insumos de Proveedores)	**PROCESOS** (Macroprocesos, Procesos y/o Subprocesos)	**SALIDAS Y CLIENTES** (Productos y/o Servicios para Clientes)	**RESPONSABLE** (Puesto a cargo del Proceso)
	GESTIÓN INSTITUCIONAL		
	1.- Gestión Directiva		
Políticas y Normas del Ministerio de Cultura	1.1 Supervisar las actividades de la institución	Check list de supervisión	Director DDC
Proyectos Culturales	1.2 Dar conformidad de los proyectos culturales en la región.	Resolución	Director DDC / Asistente Gerencia
Documentación DDC	1.3 Solicitar documentación dirigida a DDC Lambayeque	Documentación firmada y respuesta	Director DDC / Asistente Gerencia
Informe de Supervisión, Conformidad de Proyectos	1.4 Reportar al ministerio las incidencias DDC Lambayeque	Correo con incidencias DDC	Director DDC
	2.- Gestión Administrativa		
Presupuesto DDC	2.1 Administración del presupuesto	Reporte financiero / administrativo	Administrador DDC

Reporte financiero / administrativo	2.2 Elaboración de informe Rendición de cuentas	Rendición de cuentas	Administrador DDC
Reunión Áreas	2.3 Coordinación con Sede Central	Lista de actividades	Administrador DDC
Funciones/tareas DDC	2.4 Gestionar tareas	Informes DDC	Administrador DDC
Notificaciones legales	2.5 Seguimiento procesos legales (judiciales y policiales)	Informes legales	Asesor Legal
Documentación consolidada	2.6 Reportar documentación a Director DDC	Informe Administración	Administrador DDC
	3.- Gestión documentaria		
Documento / Expediente	3.1 Recepción de Expedientes	Documento / Expediente (validado)	Mesa de Partes
Documento / Expediente	3.2 Registro de Expedientes	Documento / Expediente (registrado)	Mesa de Partes
Documento / Expediente	3.3 Aprobación de Recepción	Documento / Expediente (aprobado)	Mesa de Partes
	4.- Gestión de Proyectos Arqueológicos		
Documento/Expediente	4.1 Gestionar de Expedientes Arqueológico	Expediente (atendido)	Arqueólogo
Expediente (tipo PMA)	4.2 Gestionar PMA	Informe de Aprobación de PMA	Arqueólogo
Expediente(tipo CIRA)	4.3 Gestionar CIRA	Informe de CIRA	Arqueólogo
Solicitud de Asesoría	4.4 Asesoría de Proyectos Arqueológicos	Informe de Asesoría	Arqueólogo

	5.- Gestión de Control Patrimonial		
Bienes Muebles DDC	5.1 Ubicación de Bienes Muebles	Lay out de distribución	Coordinador patrimonial
Bienes Muebles DDC	5.2 Control de Bienes Muebles	Reporte Inventario de bienes muebles	Coordinador patrimonial
Bienes Muebles DDC	5.3 Asignación de bienes Muebles	Cuadros de asignación	Coordinador patrimonial
	6.- Gestión del Patrimonio Histórico		
Bienes inmuebles	6.1 Control Bienes inmuebles	Informe de seguimiento	Arquitecto
Bienes inmuebles	6.2 Inspección de Bienes inmuebles	Informe de estados de los bienes	Arquitecto
Solicitud de asesoría	6.3 Asesoría a usuarios	Informe aprobado	Arquitecto
	7.- Gestión Actividades Culturales		
Lista de actividades	7.1 Coordinación de actividades	Cronograma de Eventos / Talleres	Gestor de Actividades
Eventos	7.2 Gestionar eventos	Correos/Invitaciones físicas	Gestor de Actividades
Talleres	7.3 Gestionar talleres	Informe liquidación de talleres	Gestor de Actividades
Ambientes DDC Lambayeque	7.4 Gestionar alquiler de ambientes	Informe liquidación de alquileres	Gestor de Actividades
	8.- Gestión de Comunicaciones		

Lista de actividades	8.1 Gestionar Material	Impresiones	Gestor de comunicaciones
Diseño físico / digital	8.2 Difusión de Eventos Culturales	Publicaciones en local y redes sociales	Gestor de comunicaciones

Cuadro 8: Matriz Identificación de Procesos

Fuente: Elaboración Propia

La matriz de identificación de procesos permite definir los procesos y actividades de la institución y tener una estructura más clara de sus flujos de entrada y salida, así como de quienes proveen o son clientes de cada proceso, esta matriz se define como el macro proceso: “Gestión Institucional”.

El propósito de esta identificación es lograr un nivel de detalle que nos muestre la realidad de la institución y así entender como es su desempeño diario.

A continuación el diagrama de flujo del macro-proceso: gestión institucional:

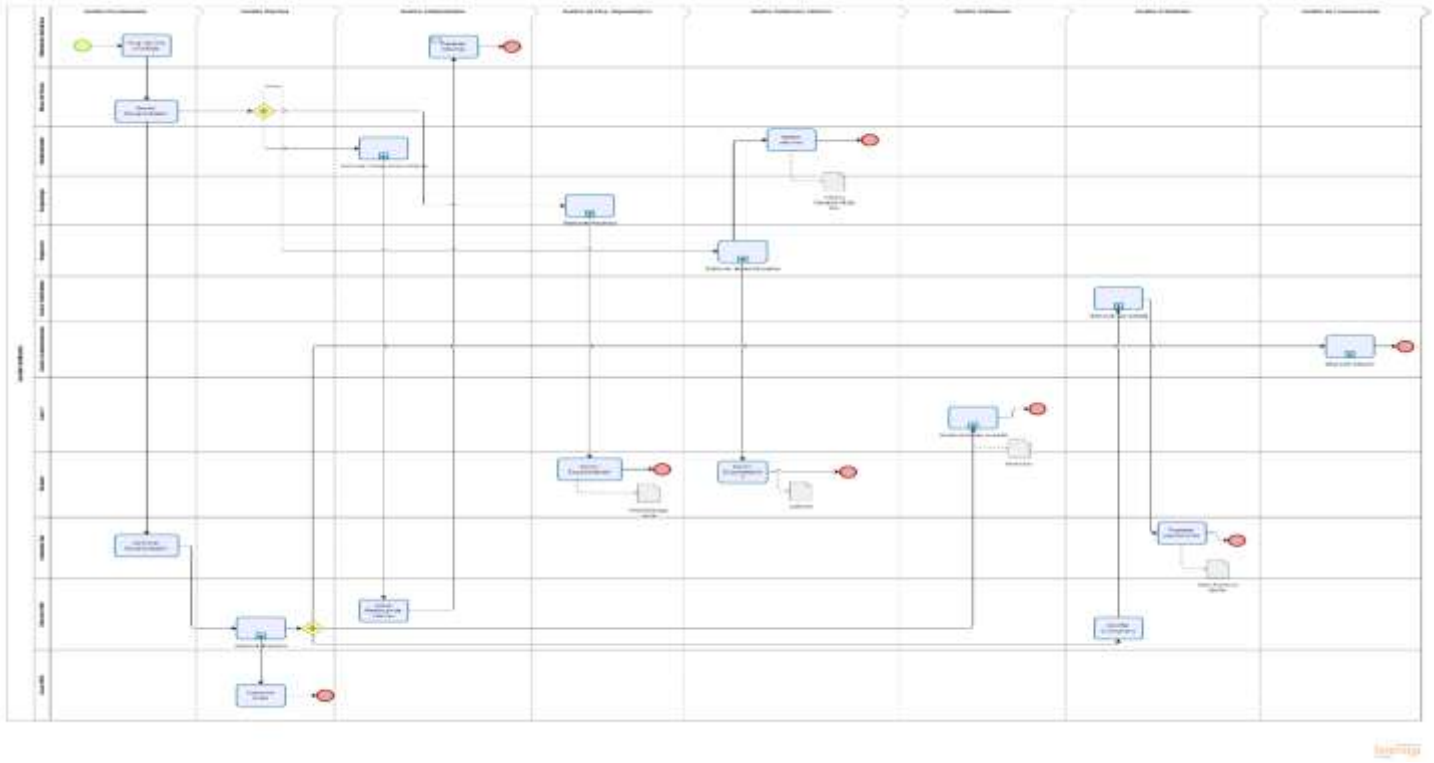


Figura 12: Diagrama de Flujo del Macro Proceso "Gestión institucional"

Fuente: Elaboración propia

Se ha definido también, el análisis de los procesos derivados del macro-proceso, identificando los siguientes:

1. Gestión directiva:

Define todos los sub procesos y las actividades de la Dirección, incluyendo las actividades de la asistenta de dirección.

Los sub procesos y las actividades de la gestión directiva son:

1.1 Supervisar las actividades de la institución

1.1.1 Cumplir los lineamientos del Ministerio

1.1.2 Realizar una revisión de las actividades de las áreas

1.2 Dar conformidad de los proyectos culturales

1.2.1 Revisar proyectos culturales

1.2.2 Firmar resolución de aprobación

1.3 Solicitar documentación dirigida a DDC Lambayeque

1.3.1 Seleccionar documentación

1.3.2 Evaluación documentación

1.4 Reportar al ministerio las incidencias

1.4.1 Enviar correo de incidencias

Se ha definido mayor detalle de la gestión directiva en el Anexo 04: Ficha de gestión directiva.

2. Gestión administrativa:

Define las actividades del administrador, sub administrador, asesores legales y encargado de almacén, considerándolos como apoyo administrativo.

Los sub procesos y las actividades de la gestión administrativa son las siguientes:

2.1. Administración del presupuesto

- 2.1.1 Evaluar Presupuesto
- 2.1.2 Establecer planes
- 2.1.3 Solicitar Caja Chica
- 2.1.4 Enviar Guía de remisión y Caja Chica
- 2.1.5 Control y seguimiento de presupuesto

2.2. Elaboración de informe Rendición de cuentas

- 2.2.1 Elaboración de redición de cuentas
- 2.2.2 Dar conformidad
- 2.2.3 Enviar rendición de cuentas

2.3. Coordinación con Sede Central

- 2.3.1 Solicitar lista de tareas
- 2.3.2 Consolidar lista de tareas
- 2.3.3 Enviar lista de tareas

2.4. Gestionar tareas

- 2.4.1 Gestionar boletas de pago
- 2.4.2 Gestionar operaciones logísticas
- 2.4.3 Gestionar soporte técnico
- 2.4.4 Presentar informes

2.5. Seguimiento procesos legales (judiciales y policiales)

- 2.5.1 Evaluar procesos legales
- 2.5.2 Enviar informes legales

2.6. Reportar documentación a Director DDC

- 2.6.1 Consolidar documentación
- 2.6.2 Validar documentación

Se ha definido mayor detalle de la gestión administrativa en el Anexo 05: Ficha de gestión administrativa.

3. Gestión documentaria:

Define las actividades de la mesa de partes, considerando las funciones del encargado de mesa de partes y todo el flujo de documentos en esta área.

Los sub procesos y las actividades de la gestión administrativa son:

3.1. Recepción de Expedientes

3.1.1 Presentar documento
3.1.2 Validar documento
3.1.3 Sellar Cargo

3.2. Registro de Expedientes

3.2.1 Registrar documento en sistema
3.2.2 Generar código de documento

3.3. Aprobación de Recepción

3.3.1 Derivar a las áreas
3.3.2 Archivador documento
3.3.2 Levantar observaciones
3.3.3 Aprobar documento

Se ha definido mayor detalle de la gestión documentaria en la ficha del Anexo 06: Ficha de gestión documentaria.

4. Gestión de proyectos arqueológicos:

Define las actividades de la oficina de Arqueología, considerando las funciones de los arqueólogos.

4.1 Gestionar de Expedientes Arqueológico

4.1.1 Recibir Expediente Arqueológico
4.1.2 Definir tipo de expediente
4.1.3 Gestionar Expediente

4.2 Gestionar PMA

4.2.1 Recibir Expediente Tipo PMA

4.2.2 Autorizar ejecución de PMA

4.2.3 Levantamiento de observaciones

4.2.4 Supervisión de ejecución PMA

4.2.5 Aprobación de PMA

4.3 Gestionar CIRA

4.3.1 Recibir solicitud tipo CIRA

4.3.2 Elaborar CIRA

4.3.3 Levantar observaciones

4.4 Asesoría de Proyectos Arqueológicos

4.4.1 Realizar asesoría

4.4.2 Presentar informe

Se ha definido mayor detalle de la gestión de proyectos arqueológicos en la ficha del Anexo 07: Ficha de proyectos arqueológicos.

5. Gestión de Control Patrimonial:

Define las actividades del encargado con respecto a los bienes muebles de la institución.

5.1 Ubicación de Bienes Muebles

5.1.1 Revisar ubicación

5.1.2 Realizar lay out de distribución

5.2 Control de Bienes Muebles

5.2.1 Realizar inventario

5.2.2 Consolidar inventario

5.3 Asignación de bienes Muebles

5.3.1 Asignar bienes a usuario

5.3.2 Aprobación de usuario

Se ha definido mayor detalle de la gestión de control patrimonial en la ficha del Anexo 08: Ficha de control patrimonial.

6. Gestión de patrimonio histórico:

Define las actividades de la oficina de patrimonio histórico, considerando las funciones de los arquitectos y practicante.

6.1. Control Bienes inmuebles

6.1.1 Registrar Bienes inmuebles

6.1.2 Mapeo de bienes inmuebles

6.1.3 Seguimiento de bienes inmuebles

6.2. Inspección de Bienes inmuebles

6.2.1Realizar inspección de bienes inmuebles

6.2.2 Validar estados

6.3. Asesoría a usuarios

6.3.1 Solicitar asesoría

6.3.2 Aprobación de asesoría

Se ha definido mayor detalle de la gestión de patrimonio histórico en la ficha del Anexo 09: Ficha de patrimonio histórico.

7. Gestión de Actividades culturales:

Define las actividades de la oficina de Actividades Culturales, considerando los eventos y talleres que se coordinan y desarrollan por la encargada.

7.1 Coordinación de actividades

7.1.1 Generar cronograma de actividades

7.1.2 Aprobación de actividades

7.1.3 Consolidar actividades

7.2 Gestionar eventos

7.2.1 Coordinar eventos

7.2.2 Solicitar participación

7.2.3 Enviar invitaciones

7.3 Gestionar talleres

7.3.1 Publicar horarios / costos

7.3.2 Inscribir a público

7.3.3 Realizar liquidación de talleres

7.4 Gestionar alquiler de ambientes

7.4.1 Ofrecer alquiler

7.4.2 Alquilar espacio

7.4.3 Realizar liquidación de espacio

Se ha definido mayor detalle de la gestión de actividades culturales en la ficha del Anexo 10: Ficha actividades culturales.

8. Gestión de comunicaciones:

Define las actividades de la oficina de Comunicación e imagen institucional con respecto a la difusión de eventos y talleres.

8.1 Gestionar Material

8.1.1 Coordinar difusión

8.1.2 Coordinar diseño

8.1.3 Enviar a imprenta

8.2 Difusión de Eventos Culturales

8.2.1 Validar material físico/virtual

8.2.2 Gestionar publicaciones

Se ha definido mayor detalle de la gestión de actividades culturales en la ficha del Anexo 11: Ficha gestión de comunicaciones.

5.1.4.2 Diagramas de flujo de Procesos:

Los diagramas de flujo de los procesos de la gestión institucional de la Dirección desconcentrada de cultura de Lambayeque, se realizaron con la herramienta Bizagi Modeler. Anexo 12: Diagramas de los procesos de la Dirección desconcentrada de cultura de Lambayeque.

La finalidad de realizar los diagramas de flujos es entender la estructura de las actividades de la institución y detectar de esta manera los activos que participan en sus actividades.

El nivel de especificación permite definir con claridad lo que necesita tomarse en cuenta, con respecto a la seguridad de la información y demás sistemas de gestión.

5.2 ETAPA II DISEÑO DEL SGSI: FASE PLAN

El diseño del sistema de gestión de seguridad de la información está basado en el modelo PDCA (Plan - Do – Check - Act) bajo el enfoque de la metodología MEHARI.

La herramienta Open Source por aplicar es la base de conocimiento de Mehari, tanto Mehari Pro y Mehari Experto, que partiendo de la identificación de activos y procesos, define los niveles globales de impacto y probabilidad, para llevar a un análisis de escenarios y los posibles tratamientos a aplicar, sugiriendo una lista de planes de acción enlazados a la ISO 27002.

5.2.1 Definición Organizacional

5.2.1.1 Alcance del SGSI

El Sistema de Gestión de Seguridad de Información abarcará todas las áreas de la institución, enfocándose principalmente en los procesos críticos y está dirigido a los encargados de dichas áreas y sus colaboradores, detallado en el anexo 13: Alcance del SGSI para la Dirección desconcentrada de cultura de Lambayeque.

Las plantillas utilizadas para los formatos, han sido descargadas de la página "Perú Gobierno Digital" (Portal de la Oficina Nacional de Gobierno Electrónico e Informática (ONGEI) de la Presidencia del Consejo de Ministros (PCM), 2017).

5.2.1.2 Política del SGSI

La política de seguridad de la información recogerá las directrices y los principios de alto nivel que rigen las actividades de seguridad de la organización; al igual que, los objetivos y responsabilidades que se demandarán a los diferentes participantes en la gestión de la seguridad de la información.

Una política de seguridad, como declaración de principios de la organización, debe plasmar las directrices generales y principios de actuación que seguirá la organización en materia de seguridad, así como la estrategia a seguir para la definición de objetivos. La política de seguridad debe ser un documento robusto y a la ve1a lo suficientemente preciso para que se pueda aplicar de forma horizontal en toda la organización, de tal forma que desde el primero hasta el último pueda cumplirla. A partir de ella, se desarrollará todo el cuerpo normativo y se establecerán los procedimientos acordes a la misma.

Con la promulgación de esta política de seguridad, por parte de la dirección, se establece un nuevo modelo de cultura de seguridad de la información en la organización. (Merino & Cañizares, Implantación de un sistema de Gestión de Seguridad de la información según ISO 27001, 2011)

En el anexo 14: Política del SGSI para la Dirección desconcentrada de cultura de Lambayeque, se puede visualizar la política del sistema de gestión de la seguridad de la información de la dirección desconcentrada de cultura de Lambayeque.

5.2.1.3 Definición de parámetros

5.2.1.3.1 Tabla de aceptabilidad del riesgo

La **tabla 2** muestra la aceptabilidad del riesgo, según el apartado de Evaluación de Riesgo, la tabla de aceptabilidad se basa en el nivel de gravedad de un riesgo y eso depende del nivel de probabilidad de que ocurra y el nivel de impacto con el que ocurre:

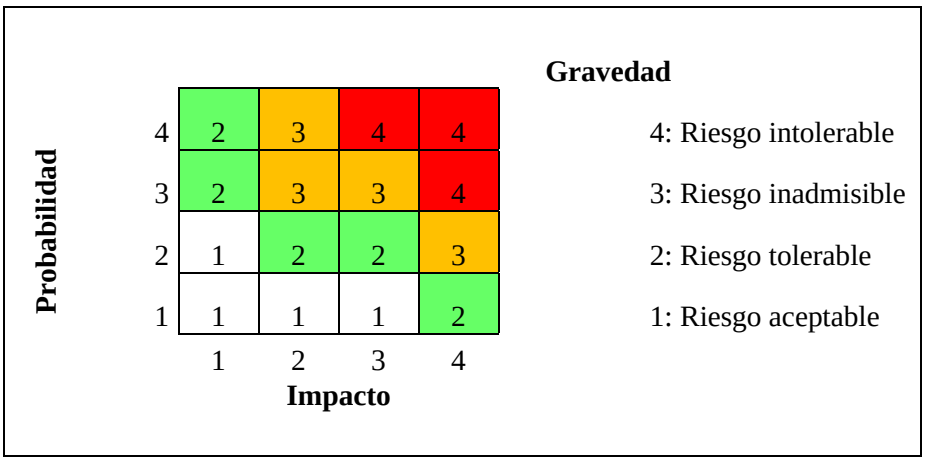


Tabla 2: Aceptabilidad de Riesgos

Fuente: (CLUSIF, 2010)

5.2.1.3.2 Tabla de exposición natural

La tabla 3 de Exposición Natural es un listado predeterminado con niveles de probabilidades para incidentes comunes y que permite elegir la probabilidad para la institución llamada exposición natural decida, a continuación la elección de niveles de exposición natural para la Dirección Desconcentrada de Cultura de Lambayeque:

Tipo	Tipo del Código	Evento	Código
Ausencia del personal	AB.P	Ausencia de personal necesario (interna o externa)	AB.P.Per
Ausencia o servicio no disponible	AB.S	Ausencia de servicio: Energía	AB.S.Ene
		Ausencia de servicio: el acceso a la imposibilidad locales	AB.S.Loc
Accidente ambiental	AC.E	Accidente debido al ambiente (incendios, inundaciones, etc.)	AC.E.Env
Accidente hardware	AC.M	falla en hardware	AC.M.Equ
		Falla en partes del hardware (fuente de alimentación, suministro de fluido, etc.)	AC.M.Ser
Error de equipos	ER.P	Pérdida de documentos	ER.P.Peo
		Error de manipulación	ER.P.Pro
Incidente lógico o funcional	IF.L	incidente operativo	IF.L.Exp
		Error en sistema operativo	IF.L.Lsp
		Error en un programa de usuario	IF.L.Lfu
		Virus	IF.L.Vir
Acción negativa intencional: lógica o a través de puerto funcional	MA.L	Bloqueo de Cuentas (hackeo)	MA.L.Blo
		Eliminación intencional de medios lógicos o físicos	MA.L.Del
		Falsificación (de datos o roles)	MA.L.Fal
		Saturación intencional de equipos informáticos o redes	MA.L.Sam
		Manipulación de archivos o datos (descarga o copia)	MA.L.Vol
Acción negativa intencional: física	MA.P	Manipulación o alteración hardware	MA.P.Fal
		Vandalismo	MA.P.Van
		Robo físico	MA.P.Vol

Tabla 3: Exposición Natural

Fuente: (CLUSIF, 2010)

5.2.1.3.3 Tablas de evaluación de riesgos

En esta propuesta se está considerando niveles tanto para medir el Impacto y la Probabilidad, según la tabla 4:

Nivel	Impacto	Probabilidad
4	Muy grave	Muy probable
3	Grave	Probable
2	Serio	Poco Probable
1	No significativo	Improbable

Tabla 4: Escala de Impacto y Probabilidad

Fuente: Elaboración Propia

5.2.2. Análisis y gestión de riesgos

5.2.2.1 Análisis de las amenazas y clasificación de los activos

5.2.2.1.1 Escala de valores de fallos

Una vez identificadas las actividades, se pone en manifiesto las posibles sospechas de mal funcionamiento asociadas con ellas, en el **cuadro 9**.

A nivel funcional, el objetivo es identificar posibles fallas que tengan un impacto significativo en las actividades de la institución. Estos serán típicamente fallas en los procesos.

Proceso	Posibles Fallos
Gestión directiva	Actividades no supervisadas
	incumplimiento de lineamientos
	Corrupción en los informes mensuales
	Divulgación de la información de la institución
	Divulgación de datos de proyectos culturales
	Pérdida de la documentación
	Falta de disponibilidad de informe de incidencias
Gestión administrativa	Pérdidas financieras (Incumplimiento del presupuesto)
	Fraude o malversación de caja chica
	Falta de disponibilidad de herramientas para la planificación
	Corrupción de los datos de los informes y de los informes mensuales
	Divulgación de información relativa a reportes de operaciones internas
	Divulgación de las condiciones financieras
	Falta de disponibilidad de las rendiciones
	Perdida de comunicación con sede central
	Falta de disponibilidad de lista de actividades
	Divulgación de lista de actividades
	Perdida de elementos históricos que justifiquen una operación legal o judicial
	Divulgación de partes de un expediente penal relativo a la institución
	Falta de disponibilidad del correo electrónico
	Divulgación de la información administrativa
	Pérdida o desaparición de originales de documentos
Gestión documentaria	Falta de disponibilidad de expedientes
	Pérdida o desaparición de expedientes originales
	Pérdida de todos los archivos que ingresan
	Falta de disponibilidad de sistema de registro
	Corrupción de los datos registrados
	Código de documento no disponible
	Demora en la aprobación de documentos
	Perdida de documentos al derivar a las áreas
	Falta de confiabilidad en el levantamiento de observaciones

	Pérdida de documento aprobado
Gestión Proyectos Arqueológicos	Falta de disponibilidad de expedientes arqueológico
	Pérdida de expediente arqueológico
	Falta de disponibilidad de atención de expediente.
	Demora en la aprobación de expediente.
	Corrupción de los datos en informe CIRA.
	Falta de disponibilidad en la elaboración de informe CIRA.
	Falta de supervisión in situ de informe CIRA.
	Divulgación de la información del usuario.
	Divulgación de información técnica.
	Falta de disponibilidad del análisis de resultados de la asesoría.
	Corrupción de los datos de los informes de asesoría.
	Alteración de los acuerdos de confidencialidad del usuario.
	Falta de disponibilidad de herramientas de gestión para proyectos arqueológicos.
Gestión Control Patrimonial	incapacidad para asegurar la ubicación de los bienes muebles
	Divulgación del equipamiento de la institución
	Incapacidad para realizar un lay out de distribución
	Falta de control de bienes muebles
	Herramienta de gestión de inventario no disponible
	Alteración de resultado de inventario
	Pérdida de bienes muebles
	Falta de gestión en la adquisición de bienes muebles
	Falsificación de asignaciones de bienes

	Aprobación no disponible
Gestión Patrimonio Histórico	Falta de herramientas para el control de bienes muebles
	Fraude o malversación de bienes inmuebles
	Falta de supervisión en el mapeo de bienes muebles
	Indisponibilidad de los resultados de seguimiento de bienes muebles
	Alteración de datos resultados del informe de inspección
	Divulgación de resultados de inspección de bienes muebles
	Indisponibilidad de documentos de informe de estado de bienes muebles
	Alteración de datos resultados del informe de asesoría
	Pérdida de los archivos de documentos del usuario
	Demora en la aprobación de asesoría solicitada
Gestión de Eventos Culturales	Falta de coordinación en eventos
	Cronograma de actividades no disponible
	Divulgación de eventos antes de la publicidad
	Falta de disponibilidad en la gestión de eventos
	Eventos mal organizados
	Participantes no disponibles
	Invitaciones inexistentes
Gestión de Comunicaciones	Perdidas de material de publicidad
	Falta de disponibilidad del sistema de correo electrónico
	Falta de disponibilidad de redes sociales
	Divulgación de los diseños previa difusión
	Diseño de material no ejecutado
	Falta de disponibilidad de recursos de difusión
	Material de difusión no validado
	Falta de experiencia en la gestión de publicaciones

Cuadro 9: Posibles fallos en la institución

Fuente: Elaboración propia

5.2.2.2 Análisis de amenazas de seguridad: evaluación de la gravedad:

Se establece la tabla para la evaluación de la gravedad, con escala del 1 al 4 detallando el nivel de gravedad de cada fallo:

Nivel	Gravedad
1	Insignificante
2	Serio
3	Muy Serio
4	Vital

Tabla 5: Evaluación de la gravedad

Fuente: (CLUSIF, 2010)

5.2.2.3 Criterios de las amenazas y Umbrales de criticidad:

Como resultado de las entrevistas realizadas, se definen los umbrales de criticidad, que mueven al fallo de un nivel de gravedad a otro y junto a los criterios permitirán evaluar la gravedad desde los fallos que tienen un impacto insignificante hasta los que tengan un impacto vital.

A continuación, el cuadro 10 de fallos y su escala de valor respectiva (nivel de criticidad):

Niveles de Criticidad	Nivel 1: Insignificante	Nivel 2: Serio	Nivel 3: Muy Serio	Nivel 4: Vital
Disponibilidad	No requiere estar disponible o al menos disponible lo mínimo (0 a 5%).	Requiere estar disponible (al menos un 20%).	Requiere estar disponible para funcionar correctamente (al menos un 70%).	Requiere estar totalmente disponible (100%).
Integridad	Requiere la mínima integridad (0 a 5%).	Requiere que este integro (completo y en buen estado al menos en un 20%).	Requiere estar completo y en buen estado (al menos un 70%).	Requiere su total funcionamiento, correcto y en buen estado (100%).
Confidencialidad	No es necesario o al menos un mínimo confidencial. (0 a 5%).	Requiere que sea confidencial (al menos un 50%).	Requiere que sea muy confidencial (al menos un 90%).	Requiere que sea totalmente confidencial (100%).

Cuadro 10: Niveles de Criticidad

Fuente: Elaboración propia

5.2.2.4 Clasificación de activos:

Según la metodología MEHARI se clasifican los activos en 3 rubros: Datos e información, Servicios y Procesos, en esta propuesta solo usaremos los activos de la tabla 6 y 7:

ACTIVOS DE TIPO DATOS E INFORMACIÓN	
DATOS E INFORMACIÓN	
D01	Archivos de datos y bases de datos a las que acceden las aplicaciones
D02	Archivos y datos de la oficina compartida
D03	Archivos personales de oficina (en estaciones de trabajo y equipos)
D04	Información y datos escritos o impresos guardados por usuarios y archivos personales
D05	Listados o documentos impresos
D06	Mensajes intercambiados, vistas de pantalla, datos individualmente sensibles
D07	Correo electrónico
D08	Correo postal y faxes
D09	Archivos patrimoniales o documentos utilizados como prueba
D10	Archivos Relacionados con TI
D11	Datos e información publicados en sitios públicos o internos

Tabla 6: Activos tipo Datos

Fuente: (CLUSIF, 2010)

ACTIVOS DE TIPO SERVICIOS	
SERVICIOS GENERALES	
G01	Espacio de trabajo y entorno de usuario
G02	Servicios de telecomunicaciones (voz, fax, audio y videoconferencia, etc.)
SERVICIOS TI	
R01	Servicio de red ampliado
R02	Servicio de red de área local
S01	Servicios prestados por las aplicaciones
S02	Servicios compartidos de Office (servidores, gestión de documentos, impresoras compartidas, etc.)
S03	Disposición de Equipos (estaciones de trabajo, impresoras locales, periféricos, interfaces específicas, etc.)
S04	Servicios comunes, entorno de trabajo: mensajería, archivado, impresión, edición, etc.
S05	Servicio de edición web (interno o público)

Tabla 7: Activos tipo Servicios

Fuente: (CLUSIF, 2010)

5.2.2.5 Identificación de los activos a clasificar:

Como resultado del análisis de procesos, se han detectado los principales activos de la institución y se han clasificado según su tipo, además se le ha asignado un código con el que se evaluaran lo más relevantes para realizar un plan de tratamiento.

A continuación los activos identificados se describen en el cuadro 11:

Código Activo	Activo	Tipo de Activo	Código de Tipo
A001	Actividad de la institución	DATO	D02
A002	Antivirus	SERVICIO	S01
A003	Archivadores de documentos	SERVICIO	S04
A004	Auditorio	SERVICIO	G01
A005	Base de datos de bienes inmuebles	DATO	D01
A006	Base de datos de bienes muebles	DATO	D01
A007	Bien inmueble	SERVICIO	G01
A008	Bien mueble	SERVICIO	G01
A009	Bitácora de rendición de cuenta de usuario interno	DATO	D03
A010	Boletas de pago	DATO	D04
A011	Brochure informativo	SERVICIO	S05
A012	Carta de envío Caja Chica (envío del ministerio de cultura)	DATO	D08
A013	Caja chica (ingreso de Oficina Actividades)	DATO	D03
A014	Cámara de vigilancia	SERVICIO	G02
A015	Carpetas compartidas	SERVICIO	S01
A016	Carta con factura de servicios	DATO	D08
A017	Carta de autorización de actividades	DATO	D02
A018	Carta de autorización de evento	DATO	D02
A019	Carta de autorización de taller	DATO	D02
A020	Carta de instituciones dirigidas a la DDC Lambayeque	DATO	D09
A021	Carta de persona natural dirigida a la DDC Lambayeque	DATO	D09
A022	carta oficializando levantamiento de observaciones CIRA	DATO	D03
A023	carta oficializando levantamiento de observaciones PMA	DATO	D03
A024	Carta respuesta a solicitud	DATO	D03
A025	CD	SERVICIO	S03
A026	Cédula de notificación del Ministerio Publico	DATO	D09
A027	Check list de supervisión	DATO	D05
A028	Código de referencia (correlativo)	DATO	D06

A029	Computadora de escritorio	SERVICIO	S03
A030	Correo Electrónico	DATO	D07
A031	Cotización (imprenta)	DATO	D03
A032	Cronograma mensual de actividades	DATO	D02
A033	Cronograma mensual de eventos	DATO	D02
A034	Cronograma mensual de talleres	DATO	D02
A035	Cuadro de asignación de bien mueble	DATO	D04
A036	Diseño gráfico	SERVICIO	S05
A037	Formato inventario / asignación	DATO	D02
A038	Equipo de telefonía IP	SERVICIO	G02
A039	Evento cultural	DATO	D02
A040	Expediente de usuario externo	DATO	D09
A041	Expediente de usuario externo (tipo: Arqueología)	DATO	D09
A042	Factura por servicios	DATO	D03
A043	Fanpage de Facebook	DATO	D11
A044	Formato de asesoría	DATO	D02
A045	formatos técnicos (otros)	DATO	D02
A046	Formulario CIRA	DATO	D03
A047	Formulario PMA	DATO	D03
A048	Fotocopiadora	SERVICIO	S02
A049	Guía de remisión para caja chica	DATO	D03
A050	Impresora	SERVICIO	S02
A051	Incidencia de la institución	DATO	D02
A052	Información digital: Expedientes de arqueología	DATO	D10
A053	Información digital: Otras áreas	DATO	D10
A054	Informe administración	DATO	D02
A055	Informe conformidad/aprobación	DATO	D03
A056	informe de aprobación de PMA	DATO	D03
A057	Informe de Asesoría	DATO	D03
A058	informe de autorización PMA	DATO	D03
A059	informe de estado de bienes inmuebles	DATO	D02
A060	informe de inspección ocular	DATO	D03
A061	informe de levantamiento de observaciones CIRA	DATO	D03
A062	informe de levantamiento de observaciones PMA	DATO	D03
A063	informe de liquidación	DATO	D03
A064	Informe de planes (para ejecución de presupuesto)	DATO	D02
A065	informe de remisión de CIRA	DATO	D03
A066	Informe de rendición de cuentas	DATO	D03
A067	informe de requerimientos	DATO	D02
A068	informe de seguimiento de bienes inmuebles	DATO	D03
A069	informe de supervisión PMA	DATO	D03
A070	informe legal	DATO	D03
A071	informe mensual de supervisión	DATO	D03
A072	Informe técnico (patrimonio histórico)	DATO	D03
A073	Inscripción a talleres	DATO	D01

A074	Invitación a público a participar de evento DDC Lambayeque	DATO	D08
A075	Invitación digital a público a participar de evento DDC Lambayeque	DATO	D11
A076	Laptop	SERVICIO	S03
A077	Lay out de distribución	DATO	D02
A078	Licencia de Microsoft Office 2013	SERVICIO	S01
A079	Licencia de Microsoft Windows 7 Profesional	SERVICIO	S01
A080	Lineamiento (norma)	DATO	D02
A081	lista de actividades	DATO	D05
A082	lista de eventos	DATO	D05
A083	lista de talleres	DATO	D05
A084	material publicitario	DATO	D10
A085	Memo circular del Ministerio de cultura	DATO	D09
A086	Memo individual del Ministerio de cultura	DATO	D09
A087	Nota de remisión de valores del ministerio de cultura	DATO	D08
A088	Oficina	SERVICIO	G01
A089	Oficio usuario externo (entidad publico/privado)	DATO	D09
A090	Página de Facebook DDC Lambayeque	DATO	D11
A091	Página web del Ministerio de Cultura del Perú	DATO	D11
A092	Carta con Presupuesto	DATO	D08
A093	Publicación en redes sociales, tv, radio	DATO	D11
A094	Recurso de difusión	SERVICIO	S04
A095	Red local	SERVICIO	R02
A096	Registro designación de arqueólogo	SERVICIO	S01
A097	Reporte administrativo	DATO	D03
A098	Reporte financiero	DATO	D03
A099	Informe de ubicación de bienes inmuebles	DATO	D02
A100	Reporte Inventario de bienes muebles	DATO	D02
A101	Router	SERVICIO	S02
A102	Sala de taller	SERVICIO	G01
A103	Scanner	SERVICIO	S02
A104	Sistema de registro	SERVICIO	S01
A105	Solicitud de usuario externo	DATO	D09
A106	Solicitud de usuario interno	DATO	D09
A107	Switch	SERVICIO	S02
A108	Taller	DATO	D02
A109	Teléfono	SERVICIO	G02
A110	USB	SERVICIO	S03
A111	Proyecto cultural	DATO	D02
A112	Documentos / Expediente	DATO	D03
A113	Aplicación	SERVICIO	S01
A114	Aprobación de Proyecto	DATO	D03
A115	Resolución	DATO	D09
A116	Tarea de la institución	DATO	D02
A117	Carta de autorización de tarea	DATO	D02

A118	Cronograma de tareas	DATO	D02
A119	Lista de tareas	DATO	D05
A120	Informe de mantenimiento	DATO	D03
A121	Informe de soporte	DATO	D03

Cuadro11: Clasificación de Activos según tipo

Fuente: Elaboración propia

5.2.2.6 Valorización de Activos según su nivel de Criticidad:

La valorización toma los datos de las escalas de disponibilidad, integridad y confidencialidad para definir el nivel de criticidad que puede ser: Vital, (valor más alto), Muy serio (valor alto), Serio (valor medio), Insignificantes (valor bajo).

La descripción de los niveles de criticidad se detallan en el anexo 30: Definición del nivel de criticidad.

En el Cuadro 12 se visualiza la valorización inicial de activos según su nivel de criticidad:

Código Activo	Activo	Tipo de Activo	Código de Tipo	Disponibilidad	Integridad	Confidencialidad	Valor total	Criticidad
A001	Actividad de la institución	DATO	D02	2	2	2	6	Serio
A002	Antivirus	SERVICIO	S01	4	4	4	12	Vital
A003	Archivadores de documentos	SERVICIO	S04	2	2	-	4	Serio
A004	Auditorio	SERVICIO	G01	3	-	-	3	Muy Serio
A005	Base de datos de bienes inmuebles	DATO	D01	2	2	2	6	Serio
A006	Base de datos de bienes muebles	DATO	D01	2	2	2	6	Serio
A007	Bien inmueble	SERVICIO	G01	3	-	-	3	Muy Serio
A008	Bien mueble	SERVICIO	G01	3	-	-	3	Muy Serio
A009	Bitácora de rendición de cuenta de usuario interno	DATO	D03	4	3	2	9	Muy Serio
A010	Boletas de pago	DATO	D04	2	-	4	6	Muy Serio
A011	Brochure informativo	SERVICIO	S05	1	1	-	2	Insignificante
A012	Carta de envío Caja Chica (envío del ministerio de cultura)	DATO	D08	4	4	4	12	Vital
A013	Caja chica (ingreso de Oficina Actividades)	DATO	D03	4	4	4	12	Vital
A014	Cámara de vigilancia	SERVICIO	G02	4	4	-	8	Vital

A015	Carpetas compartidas	SERVICIO	S01	3	3	4	10	Vital
A016	Carta con factura de servicios	DATO	D08	2	3	4	9	Muy Serio
A017	Carta de autorización de actividades	DATO	D02	2	2	2	6	Serio
A018	Carta de autorización de evento	DATO	D02	2	2	2	6	Serio
A019	Carta de autorización de taller	DATO	D02	2	2	2	6	Serio
A020	Carta de instituciones dirigidas a la DDC Lambayeque	DATO	D09	3	-	3	6	Muy Serio
A021	Carta de persona natural dirigida a la DDC Lambayeque	DATO	D09	2	-	2	4	Serio
A022	carta oficializando levantamiento de observaciones CIRA	DATO	D03	2	2	2	6	Serio
A023	carta oficializando levantamiento de observaciones PMA	DATO	D03	2	2	2	6	Serio
A024	Carta respuesta a solicitud	DATO	D03	2	2	2	6	Serio
A025	CD	SERVICIO	S03	3	-	-	3	Muy Serio
A026	Cédula de notificación del Ministerio Publico	DATO	D09	2	-	4	6	Muy Serio
A027	Check list de supervisión	DATO	D05	-	-	3	3	Muy Serio
A028	Código de referencia (correlativo)	DATO	D06	4	4	3	11	Vital
A029	Computadora de escritorio	SERVICIO	S03	4	-	-	4	Vital
A030	Correo Electrónico	DATO	D07	4	4	4	12	Vital
A031	Cotización (imprenta)	DATO	D03	2	2	3	7	Muy Serio
A032	Cronograma mensual de actividades	DATO	D02	2	2	2	6	Serio
A033	Cronograma mensual de eventos	DATO	D02	2	2	2	6	Serio
A034	Cronograma mensual de talleres	DATO	D02	2	2	2	6	Serio
A035	Cuadro de asignación de bien mueble	DATO	D04	1	-	2	3	Serio
A036	Diseño gráfico	SERVICIO	S05	2	4	-	6	Muy Serio
A037	Formato inventario / asignación	DATO	D02	2	2	2	6	Serio
A038	Equipo de telefonía IP	SERVICIO	G02	3	3	-	6	Muy Serio
A039	Evento cultural	DATO	D02	3	2	2	7	Muy Serio

A040	Expediente de usuario externo	DATO	D09	4	-	4	8	Vital
A041	Expediente de usuario externo (tipo: Arqueología)	DATO	D09	4	-	4	8	Vital
A042	Factura por servicios	DATO	D03	2	3	4	9	Muy Serio
A043	Fanpage de Facebook	DATO	D11	4	3	2	9	Muy Serio
A044	Formato de asesoría	DATO	D02	2	3	4	9	Muy Serio
A045	formatos técnicos (otros)	DATO	D02	2	3	4	9	Muy Serio
A046	Formulario CIRA	DATO	D03	4	4	4	12	Vital
A047	Formulario PMA	DATO	D03	4	4	4	12	Vital
A048	Fotocopiadora	SERVICIO	S02	3	3	-	6	Muy Serio
A049	Guía de remisión para caja chica	DATO	D03	3	3	3	9	Muy Serio
A050	Impresora	SERVICIO	S02	3	3	-	6	Muy Serio
A051	Incidencia de la institución	DATO	D02	2	3	4	9	Muy Serio
A052	Información digital: Expedientes de arqueología	DATO	D10	4	4	4	12	Vital
A053	Información digital: Otras áreas	DATO	D10	4	4	4	12	Vital
A054	Informe administración	DATO	D02	3	3	4	10	Vital
A055	Informe conformidad/aprobación	DATO	D03	3	3	3	9	Muy Serio
A056	informe de aprobación de PMA	DATO	D03	3	3	3	9	Muy Serio
A057	Informe de Asesoría	DATO	D03	3	3	4	10	Vital
A058	informe de autorización PMA	DATO	D03	3	3	3	9	Muy Serio
A059	informe de estado de bienes inmuebles	DATO	D02	3	3	2	8	Muy Serio
A060	informe de inspección ocular	DATO	D03	3	3	3	9	Muy Serio
A061	informe de levantamiento de observaciones CIRA	DATO	D03	3	3	3	9	Muy Serio
A062	informe de levantamiento de observaciones PMA	DATO	D03	3	3	3	9	Muy Serio
A063	informe de liquidación	DATO	D03	3	3	3	9	Muy Serio
A064	Informe de planes (para ejecución de presupuesto)	DATO	D02	4	3	3	10	Vital

A065	informe de remisión de CIRA	DATO	D03	4	4	4	12	Vital
A066	Informe de rendición de cuentas	DATO	D03	4	4	4	12	Vital
A067	informe de requerimientos	DATO	D02	2	2	3	7	Muy Serio
A068	informe de seguimiento de bienes inmuebles	DATO	D03	2	2	2	6	Serio
A069	informe de supervisión PMA	DATO	D03	4	4	4	12	Vital
A070	informe legal	DATO	D03	3	2	4	9	Muy Serio
A071	informe mensual de supervisión	DATO	D03	3	2	4	9	Muy Serio
A072	Informe técnico (patrimonio histórico)	DATO	D03	3	3	4	10	Vital
A073	Inscripción a talleres	DATO	D01	2	1	1	4	Serio
A074	Invitación a público a participar de evento DDC Lambayeque	DATO	D08	3	2	1	6	Serio
A075	Invitación digital a público a participar de evento DDC Lambayeque	DATO	D11	3	2	1	6	Serio
A076	Laptop	SERVICIO	S03	4	-	-	4	Vital
A077	Lay out de distribución	DATO	D02	2	2	2	6	Serio
A078	Licencia de Microsoft Office 2013	SERVICIO	S01	4	4	4	12	Vital
A079	Licencia de Microsoft Windows 7 Profesional	SERVICIO	S01	4	4	4	12	Vital
A080	Lineamiento (norma)	DATO	D02	4	4	3	11	Vital
A081	lista de actividades	DATO	D05	-	-	2	2	Serio
A082	lista de eventos	DATO	D05	-	-	2	2	Serio
A083	lista de talleres	DATO	D05	-	-	2	2	Serio
A084	material publicitario	DATO	D10	3	4	2	9	Muy Serio
A085	Memo circular del Ministerio de cultura	DATO	D09	2	-	3	5	Muy Serio
A086	Memo individual del Ministerio de cultura	DATO	D09	2	-	3	5	Muy Serio
A087	Nota de remisión de valores del ministerio de cultura	DATO	D08	4	4	4	12	Vital

A088	Oficina	SERVICIO	G01	3	-	-	3	Muy Serio
A089	Oficio usuario externo (entidad publico/privado)	DATO	D09	2	-	3	5	Muy Serio
A090	Página de Facebook DDC Lambayeque	DATO	D11	4	3	2	9	Muy Serio
A091	Página web del Ministerio de Cultura del Perú	DATO	D11	3	4	2	9	Muy Serio
A092	Carta con Presupuesto	DATO	D08	4	4	4	12	Vital
A093	Publicación en redes sociales, tv, radio	DATO	D11	3	3	3	9	Muy Serio
A094	Recurso de difusión	SERVICIO	S04	3	3	-	6	Muy Serio
A095	Red local	SERVICIO	R02	4	4	-	8	Vital
A096	Registro designación de arqueólogo	SERVICIO	S01	3	3	3	9	Muy Serio
A097	Reporte administrativo	DATO	D03	3	3	3	9	Muy Serio
A098	Reporte financiero	DATO	D03	3	3	3	9	Muy Serio
A099	Informe de ubicación de bienes inmuebles	DATO	D02	2	4	3	9	Muy Serio
A100	Reporte Inventario de bienes muebles	DATO	D02	2	4	3	9	Muy Serio
A101	Router	SERVICIO	S02	4	3	-	7	Vital
A102	Sala de taller	SERVICIO	G01	3	-	-	3	Muy Serio
A103	Scanner	SERVICIO	S02	3	3	-	6	Muy Serio
A104	Sistema de registro	SERVICIO	S01	4	4	4	12	Vital
A105	Solicitud de usuario externo	DATO	D09	3	-	3	6	Muy Serio
A106	Solicitud de usuario interno	DATO	D09	3	-	3	6	Muy Serio
A107	Switch	SERVICIO	S02	4	3	-	7	Vital
A108	Taller	DATO	D02	3	3	1	7	Muy Serio
A109	Teléfono	SERVICIO	G02	3	3	-	6	Muy Serio
A110	USB	SERVICIO	S03	3	-	-	3	Muy Serio
A111	Proyecto cultural	DATO	D02	2	3	3	8	Muy Serio
A112	Documentos / Expediente	DATO	D03	3	3	3	9	Muy Serio

A113	Aplicación	SERVICIO	S01	4	3	3	10	Vital
A114	Aprobación de Proyecto	DATO	D03	3	3	3	9	Muy Serio
A115	Resolución	DATO	D09	4	-	4	8	Vital
A116	Tarea de la institución	DATO	D02	4	3	2	9	Muy Serio
A117	Carta de autorización de tarea	DATO	D02	2	2	2	6	Serio
A118	Cronograma de tareas	DATO	D02	2	2	2	6	Serio
A119	Lista de tareas	DATO	D05	-	-	3	3	Muy Serio
A120	Informe de mantenimiento	DATO	D03	3	3	2	8	Muy Serio
A121	Informe de soporte	DATO	D03	3	3	2	8	Muy Serio

Cuadro 12: Valorización inicial de activos de la institución

Fuente: Elaboración propia

5.2.2.7 Identificación de activos vinculados a procesos de negocio:

También se realizó la clasificación por procesos y subprocesos, vinculando la disponibilidad, integridad y confidencialidad de cada activo por cada sub proceso en el Cuadro 13:

N°	Proceso	N° SP	Sub Procesos	Cod. Activo	Tipo	Código Tipo	Disponibilidad	Integridad	Confidencialidad
1	Gestión directiva	1	Supervisar las actividades de la institución	A080	DATO	D02	4	4	3
1	Gestión directiva	1	Supervisar las actividades de la institución	A027	DATO	D05	-	-	3
1	Gestión directiva	1	Supervisar las actividades de la institución	A071	DATO	D03	3	2	4
1	Gestión directiva	1	Supervisar las actividades de la institución	A030	DATO	D07	4	4	4
1	Gestión directiva	1	Supervisar las actividades de la institución	A029	SERVICIO	S03	4	-	-
1	Gestión directiva	1	Supervisar las actividades de la institución	A076	SERVICIO	S03	4	-	-
1	Gestión directiva	1	Supervisar las actividades de la institución	A050	SERVICIO	S02	3	3	-
1	Gestión directiva	1	Supervisar las actividades de la institución	A088	SERVICIO	G01	3	-	-
1	Gestión directiva	2	Dar conformidad de los proyectos culturales en la región.	A105	DATO	D09	3	-	3
1	Gestión directiva	2	Dar conformidad de los proyectos culturales en la región.	A111	DATO	D02	2	3	3
1	Gestión directiva	2	Dar conformidad de los proyectos culturales en la región.	A114	DATO	D03	3	3	3
1	Gestión directiva	2	Dar conformidad de los proyectos culturales en la región.	A115	DATO	D09	4	-	4
1	Gestión directiva	3	Solicitar documentación dirigida a DDC Lambayeque	A112	DATO	D03	3	3	3
1	Gestión directiva	3	Solicitar documentación dirigida a DDC Lambayeque	A105	DATO	D09	3	-	3
1	Gestión directiva	3	Solicitar documentación dirigida a DDC Lambayeque	A024	DATO	D03	2	2	2

1	Gestión directiva	4	Reportar al ministerio las incidencias DDC Lambayeque	A051	DATO	D02	2	3	4
1	Gestión directiva	4	Reportar al ministerio las incidencias DDC Lambayeque	A030	DATO	D07	4	4	4
1	Gestión directiva	4	Reportar al ministerio las incidencias DDC Lambayeque	A029	SERVICIO	S03	4	-	-
1	Gestión directiva	4	Reportar al ministerio las incidencias DDC Lambayeque	A050	SERVICIO	S02	3	3	-
2	Gestión administrativa	5	Administración del presupuesto	A080	DATO	D02	4	4	3
2	Gestión administrativa	5	Administración del presupuesto	A064	DATO	D02	4	3	3
2	Gestión administrativa	5	Administración del presupuesto	A092	DATO	D08	4	4	4
2	Gestión administrativa	5	Administración del presupuesto	A012	DATO	D08	4	4	4
2	Gestión administrativa	5	Administración del presupuesto	A049	DATO	D03	3	3	3
2	Gestión administrativa	5	Administración del presupuesto	A097	DATO	D03	3	3	3
2	Gestión administrativa	5	Administración del presupuesto	A030	DATO	D07	4	4	4
2	Gestión administrativa	5	Administración del presupuesto	A098	DATO	D03	3	3	3
2	Gestión administrativa	5	Administración del presupuesto	A067	DATO	D02	2	2	3
2	Gestión administrativa	5	Administración del presupuesto	A016	DATO	D08	2	3	4
2	Gestión administrativa	5	Administración del presupuesto	A042	DATO	D03	2	3	4
2	Gestión administrativa	6	Elaboración de informe Rendición de cuentas	A098	DATO	D03	3	3	3
2	Gestión administrativa	6	Elaboración de informe Rendición de cuentas	A097	DATO	D03	3	3	3
2	Gestión administrativa	6	Elaboración de informe Rendición de cuentas	A009	DATO	D03	4	3	2
2	Gestión administrativa	6	Elaboración de informe Rendición de cuentas	A066	DATO	D03	4	4	4
2	Gestión administrativa	6	Elaboración de informe Rendición de cuentas	A055	DATO	D03	3	3	3
2	Gestión administrativa	6	Elaboración de informe Rendición de cuentas	A029	SERVICIO	S03	4	-	-

2	Gestión administrativa	6	Elaboración de informe Rendición de cuentas	A050	SERVICIO	S02	3	3	-
2	Gestión administrativa	7	Coordinación con Sede Central	A116	DATO	D02	4	3	2
2	Gestión administrativa	7	Coordinación con Sede Central	A117	DATO	D02	2	2	2
2	Gestión administrativa	7	Coordinación con Sede Central	A118	DATO	D02	2	2	2
2	Gestión administrativa	7	Coordinación con Sede Central	A119	DATO	D05	-	-	3
2	Gestión administrativa	7	Coordinación con Sede Central	A030	DATO	D07	4	4	4
2	Gestión administrativa	8	Gestionar tareas	A087	DATO	D08	4	4	4
2	Gestión administrativa	8	Gestionar tareas	A010	DATO	D04	2	-	4
2	Gestión administrativa	8	Gestionar tareas	A002	SERVICIO	S01	4	4	4
2	Gestión administrativa	8	Gestionar tareas	A014	SERVICIO	G02	4	4	-
2	Gestión administrativa	8	Gestionar tareas	A029	SERVICIO	S03	4	-	-
2	Gestión administrativa	8	Gestionar tareas	A038	SERVICIO	G02	3	3	-
2	Gestión administrativa	8	Gestionar tareas	A048	SERVICIO	S02	3	3	-
2	Gestión administrativa	8	Gestionar tareas	A050	SERVICIO	S02	3	3	-
2	Gestión administrativa	8	Gestionar tareas	A053	DATO	D10	4	4	4
2	Gestión administrativa	8	Gestionar tareas	A078	SERVICIO	S01	4	4	4
2	Gestión administrativa	8	Gestionar tareas	A079	SERVICIO	S01	4	4	4
2	Gestión administrativa	8	Gestionar tareas	A076	SERVICIO	S03	4	-	-
2	Gestión administrativa	8	Gestionar tareas	A095	SERVICIO	R02	4	4	-
2	Gestión administrativa	8	Gestionar tareas	A101	SERVICIO	S02	4	3	-
2	Gestión administrativa	8	Gestionar tareas	A107	SERVICIO	S02	4	3	-
2	Gestión administrativa	8	Gestionar tareas	A109	SERVICIO	G02	3	3	-
2	Gestión administrativa	8	Gestionar tareas	A110	SERVICIO	S03	3	-	-
2	Gestión administrativa	8	Gestionar tareas	A113	SERVICIO	S01	4	3	3
2	Gestión administrativa	8	Gestionar tareas	A119	DATO	D05	-	-	3
2	Gestión administrativa	8	Gestionar tareas	A120	DATO	D03	3	3	2
2	Gestión administrativa	8	Gestionar tareas	A121	DATO	D03	3	3	2

2	Gestión administrativa	8	Gestionar tareas	A088	SERVICIO	G01	3	-	-
2	Gestión administrativa	9	Seguimiento procesos legales (judiciales y policiales)	A070	DATO	D03	3	2	4
2	Gestión administrativa	9	Seguimiento procesos legales (judiciales y policiales)	A030	DATO	D07	4	4	4
2	Gestión administrativa	10	Reportar documentación a Director DDC	A112	DATO	D03	3	3	3
2	Gestión administrativa	10	Reportar documentación a Director DDC	A054	DATO	D02	3	3	4
3	Gestión trámite documentario	11	Recepción de Expedientes	A080	DATO	D02	4	4	3
3	Gestión trámite documentario	11	Recepción de Expedientes	A040	DATO	D09	4	-	4
3	Gestión trámite documentario	11	Recepción de Expedientes	A041	DATO	D09	4	-	4
3	Gestión trámite documentario	11	Recepción de Expedientes	A112	DATO	D03	3	3	3
3	Gestión trámite documentario	11	Recepción de Expedientes	A106	DATO	D09	3	-	3
3	Gestión trámite documentario	11	Recepción de Expedientes	A105	DATO	D09	3	-	3
3	Gestión trámite documentario	11	Recepción de Expedientes	A020	DATO	D09	3	-	3
3	Gestión trámite documentario	11	Recepción de Expedientes	A021	DATO	D09	2	-	2
3	Gestión trámite documentario	11	Recepción de Expedientes	A026	DATO	D09	2	-	4
3	Gestión trámite documentario	11	Recepción de Expedientes	A085	DATO	D09	2	-	3
3	Gestión trámite documentario	11	Recepción de Expedientes	A086	DATO	D09	2	-	3
3	Gestión trámite documentario	11	Recepción de Expedientes	A089	DATO	D09	2	-	3
3	Gestión trámite documentario	12	Registro de Expedientes	A104	SERVICIO	S01	4	4	4
3	Gestión trámite documentario	12	Registro de Expedientes	A028	DATO	D06	4	4	3
3	Gestión trámite documentario	12	Registro de Expedientes	A112	DATO	D03	3	3	3
3	Gestión trámite documentario	12	Registro de Expedientes	A029	SERVICIO	S03	4	-	-
3	Gestión trámite documentario	12	Registro de Expedientes	A050	SERVICIO	S02	3	3	-
3	Gestión trámite documentario	12	Registro de Expedientes	A103	SERVICIO	S02	3	3	-
3	Gestión trámite documentario	13	Aprobación de Recepción	A003	SERVICIO	S04	2	2	-
3	Gestión trámite documentario	13	Aprobación de Recepción	A055	DATO	D03	3	3	3

3	Gestión trámite documentario	13	Aprobación de Recepción	A112	DATO	D03	3	3	3
3	Gestión trámite documentario	13	Aprobación de Recepción	A112	DATO	D03	3	3	3
3	Gestión trámite documentario	13	Aprobación de Recepción	A055	DATO	D03	3	3	3
4	Gestión de Proyectos arqueológicos	14	Gestión de Expedientes Arqueológico	A080	DATO	D02	4	4	3
4	Gestión de Proyectos arqueológicos	14	Gestión de Expedientes Arqueológico	A041	DATO	D09	4	-	4
4	Gestión de Proyectos arqueológicos	14	Gestión de Expedientes Arqueológico	A052	DATO	D10	4	4	4
4	Gestión de Proyectos arqueológicos	14	Gestión de Expedientes Arqueológico	A096	SERVICIO	S01	3	3	3
4	Gestión de Proyectos arqueológicos	14	Gestión de Expedientes Arqueológico	A029	SERVICIO	S03	4	-	-
4	Gestión de Proyectos arqueológicos	14	Gestión de Expedientes Arqueológico	A050	SERVICIO	S02	3	3	-
4	Gestión de Proyectos arqueológicos	14	Gestión de Expedientes Arqueológico	A015	SERVICIO	S01	3	3	4
4	Gestión de Proyectos arqueológicos	14	Gestión de Expedientes Arqueológico	A025	SERVICIO	S03	3	-	-
4	Gestión de Proyectos arqueológicos	15	Gestionar PMA	A023	DATO	D03	2	2	2
4	Gestión de Proyectos arqueológicos	15	Gestionar PMA	A047	DATO	D03	4	4	4
4	Gestión de Proyectos arqueológicos	15	Gestionar PMA	A056	DATO	D03	3	3	3
4	Gestión de Proyectos arqueológicos	15	Gestionar PMA	A058	DATO	D03	3	3	3
4	Gestión de Proyectos arqueológicos	15	Gestionar PMA	A062	DATO	D03	3	3	3
4	Gestión de Proyectos arqueológicos	15	Gestionar PMA	A069	DATO	D03	4	4	4
4	Gestión de Proyectos arqueológicos	15	Gestionar PMA	A029	SERVICIO	S03	4	-	-
4	Gestión de Proyectos arqueológicos	15	Gestionar PMA	A050	SERVICIO	S02	3	3	-
4	Gestión de Proyectos arqueológicos	16	Gestionar CIRA	A022	DATO	D03	2	2	2
4	Gestión de Proyectos arqueológicos	16	Gestionar CIRA	A046	DATO	D03	4	4	4
4	Gestión de Proyectos arqueológicos	16	Gestionar CIRA	A061	DATO	D03	3	3	3
4	Gestión de Proyectos arqueológicos	16	Gestionar CIRA	A065	DATO	D03	4	4	4

4	Gestión de Proyectos arqueológicos	16	Gestionar CIRA	A029	SERVICIO	S03	4	-	-
4	Gestión de Proyectos arqueológicos	16	Gestionar CIRA	A050	SERVICIO	S02	3	3	-
4	Gestión de Proyectos arqueológicos	17	Asesoría de Proyectos Arqueológicos	A044	DATO	D02	2	3	4
4	Gestión de Proyectos arqueológicos	17	Asesoría de Proyectos Arqueológicos	A057	DATO	D03	3	3	4
4	Gestión de Proyectos arqueológicos	17	Asesoría de Proyectos Arqueológicos	A029	SERVICIO	S03	4	-	-
4	Gestión de Proyectos arqueológicos	17	Asesoría de Proyectos Arqueológicos	A050	SERVICIO	S02	3	3	-
5	Gestión de control patrimonial	18	Ubicación de Bienes Muebles	A080	DATO	D02	4	4	3
5	Gestión de control patrimonial	18	Ubicación de Bienes Muebles	A077	DATO	D02	2	2	2
5	Gestión de control patrimonial	18	Ubicación de Bienes Muebles	A030	DATO	D07	4	4	4
5	Gestión de control patrimonial	18	Ubicación de Bienes Muebles	A008	SERVICIO	G01	3	-	-
5	Gestión de control patrimonial	19	Control de Bienes Muebles	A006	DATO	D01	2	2	2
5	Gestión de control patrimonial	19	Control de Bienes Muebles	A037	DATO	D02	2	2	2
5	Gestión de control patrimonial	19	Control de Bienes Muebles	A100	DATO	D02	2	4	3
5	Gestión de control patrimonial	19	Control de Bienes Muebles	A008	SERVICIO	G01	3	-	-
5	Gestión de control patrimonial	20	Asignación de bienes Muebles	A037	DATO	D02	2	2	2
5	Gestión de control patrimonial	20	Asignación de bienes Muebles	A035	DATO	D04	1	-	2
5	Gestión de control patrimonial	20	Asignación de bienes Muebles	A055	DATO	D03	3	3	3
5	Gestión de control patrimonial	20	Asignación de bienes Muebles	A029	SERVICIO	S03	4	-	-
5	Gestión de control patrimonial	20	Asignación de bienes Muebles	A050	SERVICIO	S02	3	3	-
6	Gestión de patrimonio histórico	21	Control Bienes inmuebles	A080	DATO	D02	4	4	3
6	Gestión de patrimonio histórico	21	Control Bienes inmuebles	A005	DATO	D01	2	2	2
6	Gestión de patrimonio histórico	21	Control Bienes inmuebles	A007	SERVICIO	G01	3	-	-
6	Gestión de patrimonio histórico	21	Control Bienes inmuebles	A099	DATO	D02	2	4	3
6	Gestión de patrimonio histórico	21	Control Bienes inmuebles	A068	DATO	D03	2	2	2
6	Gestión de patrimonio histórico	22	Inspección de Bienes inmuebles	A060	DATO	D03	3	3	3

6	Gestión de patrimonio histórico	22	Inspección de Bienes inmuebles	A059	DATO	D02	3	3	2
6	Gestión de patrimonio histórico	22	Inspección de Bienes inmuebles	A029	SERVICIO	S03	4	-	-
6	Gestión de patrimonio histórico	22	Inspección de Bienes inmuebles	A050	SERVICIO	S02	3	3	-
6	Gestión de patrimonio histórico	22	Inspección de Bienes inmuebles	A015	SERVICIO	S01	3	3	4
6	Gestión de patrimonio histórico	23	Asesoría a usuarios	A044	DATO	D02	2	3	4
6	Gestión de patrimonio histórico	23	Asesoría a usuarios	A072	DATO	D03	3	3	4
6	Gestión de patrimonio histórico	23	Asesoría a usuarios	A045	DATO	D02	2	3	4
6	Gestión de patrimonio histórico	23	Asesoría a usuarios	A057	DATO	D03	3	3	4
6	Gestión de patrimonio histórico	23	Asesoría a usuarios	A029	SERVICIO	S03	4	-	-
6	Gestión de patrimonio histórico	23	Asesoría a usuarios	A050	SERVICIO	S02	3	3	-
7	Gestión de actividades culturales	24	Coordinación de Actividades	A080	DATO	D02	4	4	3
7	Gestión de actividades culturales	24	Coordinación de Actividades	A081	DATO	D05	-	-	2
7	Gestión de actividades culturales	24	Coordinación de Actividades	A033	DATO	D02	2	2	2
7	Gestión de actividades culturales	24	Coordinación de Actividades	A034	DATO	D02	2	2	2
7	Gestión de actividades culturales	24	Coordinación de Actividades	A032	DATO	D02	2	2	2
7	Gestión de actividades culturales	24	Coordinación de Actividades	A001	DATO	D02	2	2	2
7	Gestión de actividades culturales	24	Coordinación de Actividades	A017	DATO	D02	2	2	2
7	Gestión de actividades culturales	24	Coordinación de Actividades	A015	SERVICIO	S01	3	3	4
7	Gestión de actividades culturales	25	Gestionar eventos	A082	DATO	D05	-	-	2
7	Gestión de actividades culturales	25	Gestionar eventos	A039	DATO	D02	3	2	2
7	Gestión de actividades culturales	25	Gestionar eventos	A074	DATO	D08	3	2	1
7	Gestión de actividades culturales	25	Gestionar eventos	A075	DATO	D11	3	2	1
7	Gestión de actividades culturales	25	Gestionar eventos	A004	SERVICIO	G01	3	-	-
7	Gestión de actividades culturales	25	Gestionar eventos	A018	DATO	D02	2	2	2
7	Gestión de actividades culturales	25	Gestionar eventos	A029	SERVICIO	S03	4	-	-
7	Gestión de actividades culturales	25	Gestionar eventos	A050	SERVICIO	S02	3	3	-
7	Gestión de actividades culturales	26	Gestionar talleres	A108	DATO	D02	3	3	1

7	Gestión de actividades culturales	26	Gestionar talleres	A019	DATO	D02	2	2	2
7	Gestión de actividades culturales	26	Gestionar talleres	A083	DATO	D05	-	-	2
7	Gestión de actividades culturales	26	Gestionar talleres	A102	SERVICIO	G01	3	-	-
7	Gestión de actividades culturales	26	Gestionar talleres	A073	DATO	D01	2	1	1
7	Gestión de actividades culturales	26	Gestionar talleres	A011	SERVICIO	S05	1	1	-
7	Gestión de actividades culturales	26	Gestionar talleres	A013	DATO	D03	4	4	4
7	Gestión de actividades culturales	26	Gestionar talleres	A063	DATO	D03	3	3	3
7	Gestión de actividades culturales	26	Gestionar talleres	A029	SERVICIO	S03	4	-	-
7	Gestión de actividades culturales	26	Gestionar talleres	A050	SERVICIO	S02	3	3	-
8	Gestión de comunicaciones	27	Gestionar Material	A080	DATO	D02	4	4	3
8	Gestión de comunicaciones	27	Gestionar Material	A084	DATO	D10	3	4	2
8	Gestión de comunicaciones	27	Gestionar Material	A094	SERVICIO	S04	3	3	-
8	Gestión de comunicaciones	27	Gestionar Material	A036	SERVICIO	S05	2	4	-
8	Gestión de comunicaciones	27	Gestionar Material	A031	DATO	D03	2	2	3
8	Gestión de comunicaciones	27	Gestionar Material	A015	SERVICIO	S01	3	3	4
8	Gestión de comunicaciones	28	Difusión de Eventos Culturales	A094	SERVICIO	S04	3	3	-
8	Gestión de comunicaciones	28	Difusión de Eventos Culturales	A084	DATO	D10	3	4	2
8	Gestión de comunicaciones	28	Difusión de Eventos Culturales	A093	DATO	D11	3	3	3
8	Gestión de comunicaciones	28	Difusión de Eventos Culturales	A036	SERVICIO	S05	2	4	-
8	Gestión de comunicaciones	28	Difusión de Eventos Culturales	A043	DATO	D11	4	3	2
8	Gestión de comunicaciones	28	Difusión de Eventos Culturales	A090	DATO	D11	4	3	2
8	Gestión de comunicaciones	28	Difusión de Eventos Culturales	A091	DATO	D11	3	4	2
8	Gestión de comunicaciones	28	Difusión de Eventos Culturales	A011	SERVICIO	S05	1	1	-
8	Gestión de comunicaciones	28	Difusión de Eventos Culturales	A029	SERVICIO	S03	4	-	-
8	Gestión de comunicaciones	28	Difusión de Eventos Culturales	A050	SERVICIO	S02	3	3	-
8	Gestión de comunicaciones	28	Difusión de Eventos Culturales	A113	SERVICIO	S01	4	3	3

Cuadro13: Activos vinculados a los procesos de la institución

Fuente: Elaboración propia

5.2.2.8 Valorización de activos por sub Procesos:

Después de realizar una tabla dinámica con la información del valorizado de activos por procesos y sub procesos, se obtienen un consolidado de valorizaciones por tipo de activo.

Los contadores de Disponibilidad, integridad y confidencialidad están configurados para tomar el máximo de sus valores por cada sub proceso, como lo determina la metodología MEHARI.

Cabe resaltar que según la metodología no todos los activos son evaluados en sus niveles de disponibilidad, integridad y confidencialidad.

5.2.2.8.1 Evaluación de criticidad de activos tipo datos

La tabla 8 es el resultado de la herramienta Mehari Experto, para la clasificación y evaluación de activos tipo datos e información tomando la información de los sub procesos:

Tabla T1		CLASIFICACIÓN ACTIVOS TIPO DATOS E INFORMACIÓN																												
Procesos del Negocio		Datos de aplicación (bases de datos)			Datos de aplicación individualmente sensibles (transitorios, mensajes)			Datos de oficinas compartidas			Datos personales de oficina			Documentos personales		Listas o impresiones	Correo Electrónico			Correo postal			Documentos archivados		Archivos digitalizados			Datos web en línea (externos o internos)		
		D	I	C	D	I	C	D	I	C	D	I	C	D	C	C	D	I	C	D	I	C	D	C	D	I	C	D	I	C
		D01	D01	D01	D06	D06	D06	D02	D02	D02	D03	D03	D03	D04	D04	D05	D07	D07	D07	D08	D08	D08	D09	D09	D10	D10	D10	D11	D11	D11
N°	Sub Procesos																													
1	Supervisar las actividades de la institución							4	4	3	3	2	4			3	4	4	4											
2	Dar conformidad de los proyectos culturales en la región.							2	3	3	3	3	3										4	4						
3	Solicitar documentación dirigida a DDC Lambayeque										3	3	3										3	3						
4	Reportar al ministerio las incidencias DDC Lambayeque							2	3	4							4	4	4											
5	Administración del presupuesto							4	4	3	3	3	4				4	4	4	4	4	4								
6	Elaboración de informe Rendición de cuentas										4	4	4																	
7	Coordinación con Sede Central							4	3	2						3	4	4	4											
8	Gestionar tareas										3	3	2	2	4	3				4	4	4			4	4	4			
9	Seguimiento procesos legales (judiciales y policiales)										3	2	4				4	4	4											
10	Reportar documentación a Director DDC							3	3	4	3	3	3																	
11	Recepción de Expedientes							4	4	3	3	3	3										4	4						
12	Registro de Expedientes				4	4	3				3	3	3																	
13	Aprobación de Recepción										3	3	3																	
14	Gestión de Expedientes Arqueológico							4	4	3													4	4	4	4	4			
15	Gestionar PMA										4	4	4																	
16	Gestionar CIRA										4	4	4																	
17	Asesoría de Proyectos Arqueológicos							2	3	4	3	3	4																	
18	Ubicación de Bienes Muebles							4	4	3							4	4	4											
19	Control de Bienes Muebles	2	2	2				2	4	3																				

20	Asignación de bienes Muebles							2	2	2	3	3	3	1	2																
21	Control Bienes inmuebles	2	2	2				4	4	3	2	2	2																		
22	Inspección de Bienes inmuebles							3	3	2	3	3	3																		
23	Asesoría a usuarios							2	3	4	3	3	4																		
24	Coordinación de Actividades							4	4	3						2															
25	Gestionar eventos							3	2	2						2				3	2	1						3	2	1
26	Gestionar talleres	2	1	1				3	3	2	4	4	4			2															
27	Gestionar Material							4	4	3	2	2	3													3	4	2			
28	Difusión de Eventos Culturales																									3	4	2	4	4	3
Clasificación total		2	2	2	4	4	3	4	4	4	4	4	4	2	4	3	4	4	4	4	4	4	4	4	4	4	4	4	4	4	3
Clasificación seleccionando Sub Procesos		2	2	2	4	4	3	4	4	4	4	4	4	2	4	3	4	4	4	4	4	4	4	4	4	4	4	4	4	4	3

Tabla 8: Matriz de criticidad de activos tipo Datos:

Fuente: (CLUSIF, 2010)

5.2.2.8.2 Matriz de criticidad de riesgos tipo Servicios:

La siguiente tabla 9 es el resultado de la herramienta Mehari Experto, para la clasificación y evaluación de activos tipo servicios:

Procesos del Negocio		Servicio de Red Extendida		Servicios de red de área local		Servicios de aplicación			Servicios de oficina compartida		Disposición de los equipos por los usuarios	Servicios de TI (sistemas, periféricos, etc.)		Servicios de edición web		Servicios comunes, ambiente de trabajo	Servicios de telecomunicaciones	
		D	I	D	I	D	I	C	D	I	D	D	I	D	I	D	D	I
		R01	R01	R02	R02	S01	S01	S01	S02	S02	S03	S04	S04	S05	S05	G01	G02	G02
N°	Sub Procesos																	
1	Supervisar las actividades de la institución								3	3	4					3		
4	Reportar al ministerio las incidencias DDC Lambayeque								3	3	4							
6	Elaboración de informe Rendición de cuentas								3	3	4							
8	Gestionar tareas			4	4	4	4	4	4	3	4					3	4	4
12	Registro de Expedientes					4	4	4	3	3	4							
13	Aprobación de Recepción											2	2					
14	Gestión de Expedientes Arqueológico					3	3	4	3	3	4							
15	Gestionar PMA								3	3	4							
16	Gestionar CIRA								3	3	4							
17	Asesoría de Proyectos Arqueológicos								3	3	4							
18	Ubicación de Bienes Muebles															3		
19	Control de Bienes Muebles															3		
20	Asignación de bienes Muebles								3	3	4							
21	Control Bienes inmuebles															3		
22	Inspección de Bienes inmuebles					3	3	4	3	3	4							

23	Asesoría a usuarios								3	3	4								
24	Coordinación de Actividades					3	3	4											
25	Gestionar eventos								3	3	4					3			
26	Gestionar talleres								3	3	4			1	1	3			
27	Gestionar Material					3	3	4				3	3	2	4				
28	Difusión de Eventos Culturales					4	3	3	3	3	4	3	3	2	4				
Clasificación Total				4	4	4	4	4	4	3	4	3	3	2	4	3	4	4	
Clasificación por Actividades				4	4	4	4	4	4	3	4	3	3	2	4	3	4	4	

Tabla 9: Matriz de evaluación de criticidad de activos tipo Servicios

Fuente: (CLUSIF, 2010)

Por ser la institución de menos de 100 empleados, se ha realizado una agrupación de los activos en 10 familias, como propuesta de la herramienta MEHARI PRO (herramienta para instituciones de pequeña envergadura), en el Cuadro 14, estos son los activos:

Código Activo	Descripción Activo	Reemplaza a:
D01	Documentos informáticos (datos de las aplicaciones)	D01
D02	Datos de aplicaciones (sensibles o transferibles)	D06
D03	Archivos de Oficina	D02, D03, D10
D04	E-mail	D07
D05	Documentos no informáticos, impresos o escritos a mano	D04, D05, D08,D09
D06	Información publicada o servicios disponibles en un servidor de Internet	D11
G01	Entorno de trabajo del usuario	G01
S01	TI y servicios de telecomunicaciones	G02, R01, R02, S01
S02	Disposición de Equipos (PC, impresoras locales, periféricos, interfaces específicas, etc.)	S02, S03, S04
S03	Los servicios ofrecidos en los sitios web	S05

Cuadro 14: Familia de Activos según herramienta Mehari PRO

Fuente: Elaboración propia

Después de reagrupar los activos en 10 familias, se ha realizado nuevamente la tabla dinámica para reemplazar los datos en la herramienta MEHARI PRO, a continuación en el Tabla 10 un resumen de las valorizaciones por procesos, un enfoque global después del análisis detallado realizado anteriormente:

Tabla T1	Activos de Tipo datos															Activos de tipo servicio				
Procesos del negocio, Área de aplicación, Campo de actividad	**Archivos informáticos**			**Datos informáticos en tránsito**			**Archivos de oficina**			**Correo electrónico**			**Documentos no informáticos, impresos o escritos a mano**		**Información Web**	**Servicios TI**		**Instalaciones para usuarios**	**Servicios Web**	**Servicios Ambiente de Trabajo**
Servicios Comunes	**D**	**I**	**C**	**D**	**I**	**C**	**D**	**I**	**C**	**D**	**I**	**C**	**D**	**C**	**I**	**D**	**I**	**D**	**D**	**D**
Tipo de Activo	**D01**	**D01**	**D01**	**D02**	**D02**	**D02**	**D03**	**D03**	**D03**	**D04**	**D04**	**D04**	**D05**	**D05**	**D06**	**S01**	**S01**	**S02**	**S03**	**G01**
Áreas Organizacionales																				
Gestión directiva							4	4	4	4	4	4	4	4				4		3
Gestión administrativa							4	4	4	4	4	4	4	4		4	4	4		3
Gestión trámite documentario				4	4	3	4	4	3				4	4		4	4	4		
Gestión de Proyectos arqueológicos							4	4	4				4	4		4	4	4		
Gestión de control patrimonial	2	2	2				4	4	3	4	4	4	1	2				4		3
Gestión de patrimonio histórico	2	2	2				4	4	4							4	4	4		3
Gestión de eventos culturales	2	1	1				4	4	4				3	1	2	4	4	4	1	3
Gestión de comunicaciones							4	4	3						3	4	4	4	3	
Clasificación final	2	2	2	4	4	3	4	4	4	4	4	4	4	4	3	4	4	4	3	3

Tabla 10: Matriz final de evaluación de criticidad – Herramienta Mehari PRO

Fuente: (CLUSIF, 2010)

5.2.2.9 Tabla de Impacto intrínseco:

La tabla de impacto intrínseco es el resumen de la evaluación de la criticidad de los activos:

Tabla de Impacto Intrínseco				
Activos Tipo Datos e Información		**D**	**I**	**C**
Datos e Información				
D01	Documentos informáticos (datos de las aplicaciones)	2	2	2
D02	Datos de aplicaciones (sensibles o transferibles)	4	4	3
D03	Archivos de Oficina	4	4	4
D04	E-mail	4	4	4
D05	Documentos no informáticos, impresos o escritos a mano	4		4
D06	Información publicada o servicios disponibles en un servidor de Internet		3	
Activos Tipo Servicios		**D**	**I**	**C**
Servicios generales comunes				
G01	Entorno de trabajo del usuario	3		
Servicios TI y de Red				
S01	TI y servicios de telecomunicaciones	4	4	
S02	Disposición de Equipos (PC, impresoras locales, periféricos, interfaces específicas, etc.)	4		
S03	Los servicios ofrecidos en los sitios web	3		

Tabla 11: Impacto intrínseco de la institución – Herramienta Mehari PRO

Fuente: (CLUSIF, 2010)

5.2.2.10 Tabla de Probabilidad Intrínseca:

La tabla 12 muestra la exposición natural a la que están expuestos los activos según eventos, este proceso también llamado probabilidad.

Tipo	Tipo del Código	Evento	Código	Expo Natural Resultante
Ausencia del personal	AB.P	Ausencia de personal necesario (interna o externa)	AB.P.Per	4
Ausencia o servicio no disponible	AB.S	Ausencia de servicio: Energía	AB.S.Ene	4
		Ausencia de servicio: el acceso a la imposibilidad locales	AB.S.Loc	3
Accidente ambiental	AC.E	Accidente debido al ambiente (incendios, inundaciones, etc.)	AC.E.Env	2
Accidente hardware	AC.M	falla en hardware	AC.M.Equ	3
		Falla en partes del hardware (fuente de alimentación, suministro de fluido, etc.)	AC.M.Ser	2
Error de equipos	ER.P	Pérdida de documentos	ER.P.Peo	4
		Error de manipulación	ER.P.Pro	2
Incidente lógico o funcional	IF.L	incidente operativo	IF.L.Exp	3
		Error en sistema operativo	IF.L.Lsp	2
		Error en un programa de usuario	IF.L.Lfu	3
		Virus	IF.L.Vir	4
Acción negativa intencional: lógica o a través de puerto funcional	MA.L	Bloqueo de Cuentas (hackeo)	MA.L.Blo	2
		Eliminación intencional de medios lógicos o físicos	MA.L.Del	2
		Falsificación (de datos o roles)	MA.L.Fal	3
		Saturación intencional de equipos informáticos o redes	MA.L.Sam	2
		Manipulación de archivos o datos (descarga o copia)	MA.L.Vol	3
Acción negativa intencional: física	MA.P	Manipulación o alteración hardware	MA.P.Fal	2
		Vandalismo	MA.P.Van	1
		Robo físico	MA.P.Vol	3

Tabla 12: Probabilidad Intrínseca de la institución

Fuente: **(CLUSIF, 2010)**

5.2.3 Evaluación del riesgo

5.2.3.1 Selección de escenarios de riesgo:

Se realiza la agrupación en familias de escenarios para evaluar los riesgos resultantes en la tabla 13:

Código Familia	Familia de Escenario
D01-D	Pérdida de Archivos informáticos
D02-D	Pérdida de datos (almacenado temporalmente o en tránsito)
D03-D	Pérdida de datos de oficina
D04-D	Pérdida de mensajes de correo electrónico (enviando o recibiendo)
D05-D	Pérdida de documentos no informáticos
D01-I	Alteración (no detectada) de archivos informáticos
D02-I	Alteración de datos sensibles o de datos en tránsito
D03-I	Alteración (no detectada) de archivos de oficina
D04-I	Alteración de correos electrónicos enviados o recibidos
D06-I	Alteración de contenido de sitio web o del servicio de internet
D01-C	Divulgación de archivos informáticos
D02-C	Divulgación de datos después de su consulta o captura
D03-C	Divulgación de archivos de oficina
D04-C	Divulgación de correos electrónicos enviados o recibidos
D05-C	Divulgación de documentos
G01-D	Ambiente de trabajo indisponible
S01-D	Servicios informáticos y telecomunicaciones indisponibles
S02-D	Equipos de trabajo o terminales de usuario indisponibles (PC, impresoras, etc.).
S03-D	Servicio de publicación o servicio de sitio web indisponible
S01-I	Alteración en los servicios informáticos o telecomunicaciones

Tabla13 : Familia de escenarios – Herramienta Mehari PRO

Fuente: **(CLUSIF, 2010)**

5.2.3.2 Contexto de Gravedad de escenarios

En la siguiente tabla 14 se describe el contexto de gravedad de escenarios, se puede visualizar el resumen de 74 riesgos detectados, de los cuales 31 son riesgos intolerables.

Contexto de Gravedad de Escenarios Evaluación de gavedad intrínseca ➔ Evaluación de la gravedad restante ➔ Consideración de las medidas actuales y las medidas previstas ➔	Disponibilidad					Integridad					Confidencialidad				
Activos de tipo Datos e Información	Gr. 1	Gr. 2	Gr. 3	Gr. 4		Gr. 1	Gr. 2	Gr. 3	Gr. 4		Gr. 1	Gr. 2	Gr. 3	Gr. 4	
Datos e Información															
D01 Archivos informáticos (aplicaciones)	0	7	1	0	>	0	5	0	0	>	0	6	0	0	>
D02 Datos informáticos aislados (almacenamiento temporal o en tránsito)	0	0	2	1	>	0	0	0	2	>	0	0	3	0	>
D03 Archivos de oficina	0	0	4	3	>	0	0	1	3	>	0	0	1	6	>
D04 Email	0	0	0	1	>	0	0	0	1	>	0	0	1	1	>
D05 documentos no informáticos, impresos o escritos a mano	0	0	1	3	>						0	0	0	3	>
D06 La información publicada o servicios disponibles en un servidor de Internet						0	0	1	0	>					
Activos de tipo Servicios	Gr. 1	Gr. 2	Gr. 3	Gr. 4		Gr. 1	Gr. 2	Gr. 3	Gr. 4		Gr. 1	Gr. 2	Gr. 3	Gr. 4	
Servicios generales comunes															
G01 Entorno de trabajo de usuario	0	0	2	0	>										
Servicios información y telecomunicaciones															
S01 Servicios informáticos	0	1	5	3	>	0	0	1	1	>					
S02 Instalaciones a disposición de los usuarios	0	0	0	3	>										
S03 Servicios ofrecidos en sitios web	0	0	1	0	>										
Nombre de escenarios	0	8	16	14		0	5	3	7		0	6	5	10	

Tabla 14 : Contexto de gravedad de escenarios – Herramienta Mehari Pro

Fuente: **(CLUSIF, 2010)**

5.2.3.3 Matriz de Evaluación de Riesgos

Después de identificar los escenarios se evalúan las amenazas que pueden afectar a los escenarios, en el cuadro 15 se puede visualizar el nivel de gravedad de cada riesgo detectado:

Riesgo	Código Familia	Familia Escenario	Tipo de Activo	Activo	Soporte	Vulnerabilidad	Amenaza	Tipo AEM	Impacto Intrins.	Exposición	Gravedad Intrínseca	Gravedad
R01	D01-D	Pérdida de Archivos informáticos	D01	Documentos informáticos (datos de las aplicaciones)	Archivo	Eliminación	Pérdida accidental de archivos de computadora, a raíz de un virus.	Accidente	2	4	**3**	Riesgo inadmisible
R02	D01-D	Pérdida de Archivos informáticos	D01	Documentos informáticos (datos de las aplicaciones)	Archivo	Eliminación	Pérdida de archivos por error en computadora, por usuario autorizado.	Error	2	2	**2**	Riesgo tolerable
R03	D01-D	Pérdida de Archivos informáticos	D01	Documentos informáticos (datos de las aplicaciones)	Archivo	Eliminación	Pérdida maliciosa de archivos de computadora, por usuario autorizado.	Malicioso	2	2	**2**	Riesgo tolerable
R04	D01-D	Pérdida de Archivos informáticos	D01	Documentos informáticos (datos de las aplicaciones)	Archivo	Eliminación	Pérdida maliciosa de archivos de computadora por un usuario no autorizado.	Malicioso	2	2	**2**	Riesgo tolerable
R05	D01-D	Pérdida de Archivos informáticos	D01	Documentos informáticos (datos de las aplicaciones)	Archivo	Daño	Daño accidental de archivos de computadora, debido a incidentes de funcionamiento.	Accidente	2	3	**2**	Riesgo tolerable
R06	D01-D	Pérdida de Archivos informáticos	D01	Documentos informáticos (datos de las aplicaciones)	Media	Desaparición	Robo de archivos digitales por un miembro del personal no autorizado.	Malicioso	2	3	**2**	Riesgo tolerable
R07	D01-D	Pérdida de Archivos informáticos	D01	Documentos informáticos (datos de las aplicaciones)	Media	Pérdida	Pérdida debido a un accidente o debido al ambiente (incendio, inundación, etc.).	Accidente	2	2	**2**	Riesgo tolerable
R08	D01-D	Pérdida de Archivos informáticos	D01	Documentos informáticos (datos de las aplicaciones)	Acceso	Desaparición	Robo o destrucción maliciosa para el acceso a archivos de computadora.	Malicioso	2	3	**2**	Riesgo tolerable

R09	D02-D	Pérdida de datos aislados (almacenado temporalmente o en tránsito)	D02	Datos de aplicaciones (sensibles o transferibles)	mensaje	Pérdida	Pérdida accidental de datos en tránsito: mensajes o transacciones pendientes después de un incidente operacional.	Accidente	4	3	**4**	Riesgo intolerable
R10	D02-D	Pérdida de datos aislados (almacenado temporalmente o en tránsito)	D02	Datos de aplicaciones (sensibles o transferibles)	datos	Eliminación	Pérdida accidental de datos por el usuario autorizado.	Malicioso	4	2	**3**	Riesgo inadmisible
R11	D02-D	Pérdida de datos aislados (almacenado temporalmente o en tránsito)	D02	Datos de aplicaciones (sensibles o transferibles)	datos	Eliminación	Datos eliminados por un usuario no autorizado.	Malicioso	4	2	**3**	Riesgo inadmisible
R12	D03-D	Pérdida de datos de oficina	D03	Archivos de Oficina	Archivo	Eliminación	Pérdida de archivos de oficina, a raíz de un virus.	Accidente	4	4	**4**	Riesgo intolerable
R13	D03-D	Pérdida de datos de oficina	D03	Archivos de Oficina	Archivo	Eliminación	Pérdida de archivos de oficina por error, por un usuario autorizado.	Error	4	2	**3**	Riesgo inadmisible
R14	D03-D	Pérdida de datos de oficina	D03	Archivos de Oficina	Archivo	Eliminación	Borrado de archivos compartidos por un usuario no autorizado.	Malicioso	4	2	**3**	Riesgo inadmisible
R15	D03-D	Pérdida de datos de oficina	D03	Archivos de Oficina	Media	Eliminación	Pérdida de archivos compartidos después de un accidente debido al ambiente (incendios, inundaciones, etc.).	Accidente	4	2	**3**	Riesgo inadmisible
R16	D03-D	Pérdida de datos de oficina	D03	Archivos de Oficina	Media	Desaparición	Pérdida accidental, archivos personales en oficinas.	Malicioso	4	4	**4**	Riesgo intolerable
R17	D03-D	Pérdida de datos de oficina	D03	Archivos de Oficina	Laptop	Desaparición	Robo de laptops o medios que soportan los archivos personales de oficina.	Malicioso	4	3	**4**	Riesgo intolerable

R18	D03-D	Pérdida de datos de oficina	D03	Archivos de Oficina	Acceso	Desaparición	Eliminación accidental de los recursos necesarios para archivos de oficina	Accidente	4	2	**3**	Riesgo inadmisible
R19	D04-D	Pérdida de mensajes de correo electrónico (enviando o recibiendo)	D04	E-mail	Mensaje E-mail	Pérdida	Pérdida accidental de datos de: correo electrónico enviados o recibidos, después de un incidente operacional	Accidente	4	3	**4**	Riesgo intolerable
R20	D05-D	Pérdida de documentos no informáticos	D05	Documentos no informáticos, impresos o escritos a mano	Documento	Destrucción	Pérdida accidental de documentos escritos o impresos después de un accidente debido al ambiente (incendios, inundaciones, etc.)	Accidente	4	2	**3**	Riesgo inadmisible
R21	D05-D	Pérdida de documentos no informáticos	D05	Documentos no informáticos, impresos o escritos a mano	Documento	Desaparición	Desaparición por robo de documentos escritos o impresos por una persona autorizada a entrar en las instalaciones.	Malicioso	4	3	**4**	Riesgo intolerable
R22	D05-D	Pérdida de documentos no informáticos	D05	Documentos no informáticos, impresos o escritos a mano	Documento	Desaparición	Desaparición por el robo, divulgación o eliminación de documentos.	Malicioso	4	3	**4**	Riesgo intolerable
R23	D05-D	Pérdida de documentos no informáticos	D05	Documentos no informáticos, impresos o escritos a mano	Documento	Desaparición	Desaparición por robo de documentos, escritos o impresos en poder de los usuarios de fuera de la institución	Malicioso	4	3	**4**	Riesgo intolerable
R24	D01-I	Modificación (no detectada) de archivos informáticos	D01	Documentos informáticos (datos de las aplicaciones)	Archivo	Modificación	Modificación accidental (no detectado) de archivos debido incidentes operacionales.	Accidente	2	3	**2**	Riesgo tolerable
R25	D01-I	Modificación (no detectada) de archivos informáticos	D01	Documentos informáticos (datos de las aplicaciones)	Archivo	Modificación	Modificación accidental (no detectado) de archivos de computadora debido a un error de un programa de usuario.	Error	2	3	**2**	Riesgo tolerable

R26	D01-I	Modificación (no detectada) de archivos informáticos	D01	Documentos informáticos (datos de las aplicaciones)	Archivo	Modificación	Modificación maliciosa (no detectado) de archivos por un usuario no autorizado.	Malicioso	2	3	**2**	Riesgo tolerable
R27	D01-I	Modificación (no detectada) de archivos informáticos	D01	Documentos informáticos (datos de las aplicaciones)	Archivo	Modificación	Modificación maliciosa (no detectado) de archivos por un usuario no autorizado, conecta desde fuera de red LAN.	Malicioso	2	3	**2**	Riesgo tolerable
R28	D01-I	Modificación (no detectada) de archivos informáticos	D01	Documentos informáticos (datos de las aplicaciones)	Media	Intercambio	Cambio malicioso del funcionamiento en los archivos informáticos.	Malicioso	2	2	**2**	Riesgo tolerable
R29	D02-I	Modificación de datos sensibles o de datos en tránsito	D02	Datos de aplicaciones (sensibles o transferibles)	datos	Modificación	Datos sensibles manipulados maliciosamente, por un miembro del personal no autorizado.	Malicioso	4	3	**4**	Riesgo intolerable
R30	D02-I	Modificación de datos sensibles o de datos en tránsito	D02	Datos de aplicaciones (sensibles o transferibles)	datos	Modificación	Manipulación maliciosa de mensajes, en la red local por un miembro del personal no autorizado.	Malicioso	4	3	**4**	Riesgo intolerable
R31	D03-I	Modificación (no detectada) de archivos de oficina	D03	Archivos de Oficina	Archivo	Modificación	Modificación accidental (no detectado) de archivos de oficina, debido a un error de procedimiento.	Error	4	2	**3**	Riesgo inadmisible
R32	D03-I	Modificación (no detectada) de archivos de oficina	D03	Archivos de Oficina	Archivo	Modificación	Modificación accidental (no detectado) de archivos de oficina, debido a un error en función de un programa de usuario.	Error	4	3	**4**	Riesgo intolerable
R33	D03-I	Modificación (no detectada) de archivos de oficina	D03	Archivos de Oficina	Archivo	Modificación	Modificación maliciosa (no detectado) de archivos de oficina compartida, por un usuario no autorizado.	Malicioso	4	3	**4**	Riesgo intolerable

R34	D03-I	Modificación (no detectada) de archivos de oficina	D03	Archivos de Oficina	Archivo	Modificación	Modificación maliciosa (no detectado) archivos de oficina personales por un usuario no autorizado.	Malicioso	4	3	**4**	Riesgo intolerable
R35	D04-I	Modificación de correos electrónicos enviados o recibidos	D04	E-mail	Correo	Modificación	Manipulación maliciosa de correo electrónico que se envía o se recibe por una parte no autorizada.	Malicioso	4	3	**4**	Riesgo intolerable
R36	D06-I	Modificación de contenido de sitio web o del servicio de internet	D06	Información publicada o servicios disponibles en un servidor de Internet	Sitio internet	Modificación	Manipulación maliciosa de información o servicios ofrecidos en los sitios web por un usuario no autorizado.	Malicioso	3	3	**3**	Riesgo inadmisible
R37	D01-C	Divulgación de archivos informáticos	D01	Documentos informáticos (datos de las aplicaciones)	datos	Divulgación	Divulgación de archivos debido a un error de procedimiento en una operación de mantenimiento.	Error	2	2	**2**	Riesgo tolerable
R38	D01-C	Divulgación de archivos informáticos	D01	Documentos informáticos (datos de las aplicaciones)	Archivo de datos	Divulgación	El mal uso de los archivos informáticos por parte de usuario autorizado.	Malicioso	2	3	**2**	Riesgo tolerable
R39	D01-C	Divulgación de archivos informáticos	D01	Documentos informáticos (datos de las aplicaciones)	Archivo de datos	Divulgación	El mal uso de los archivos informáticos por parte de usuario no autorizado.	Malicioso	2	3	**2**	Riesgo tolerable
R40	D01-C	Divulgación de archivos informáticos	D01	Documentos informáticos (datos de las aplicaciones)	Archivo de datos	Divulgación	El mal uso de los archivos informáticos por parte de usuario no autorizado desde fuera de la red interna.	Malicioso	2	3	**2**	Riesgo tolerable
R41	D01-C	Divulgación de archivos informáticos	D01	Documentos informáticos (datos de las aplicaciones)	Media	Desaparición	El mal uso de los archivos informáticos por parte de usuario autorizado.	Malicioso	2	3	**2**	Riesgo tolerable
R42	D01-C	Divulgación de archivos informáticos	D01	Documentos informáticos (datos de las aplicaciones)	Media	Desaparición	Divulgación de la información, por un miembro del personal no autorizado.	Malicioso	2	3	**2**	Riesgo tolerable
R43	D02-C	Divulgación de datos después de su	D02	Datos de aplicaciones	Pantalla	Divulgación	Divulgación de datos en la conexión de la red interna.	Malicioso	3	3	**3**	Riesgo inadmisible

		consulta o captura		(sensibles o transferibles)								
R44	D02-C	Divulgación de datos después de su consulta o captura	D02	Datos de aplicaciones (sensibles o transferibles)	Pantalla	Divulgación	Divulgación de datos fuera de la red interna.	Malicioso	3	3	**3**	Riesgo inadmisible
R45	D02-C	Divulgación de datos después de su consulta o captura	D02	Datos de aplicaciones (sensibles o transferibles)	datos en Transito	Captura	Divulgación de correos por parte de persona autorizada de entrar en los locales.	Malicioso	3	3	**3**	Riesgo inadmisible
R46	D03-C	Divulgación de archivos de oficina	D03	Archivos de Oficina	Archivo	Divulgación	Divulgación de archivos de oficina debido a un error de procedimiento, durante un mantenimiento de hardware.	Error	4	2	**3**	Riesgo inadmisible
R47	D03-C	Divulgación de archivos de oficina	D03	Archivos de Oficina	Archivo	Divulgación	El uso indebido de archivos de oficina, por usuario autorizado.	Malicioso	4	3	**4**	Riesgo intolerable
R48	D03-C	Divulgación de archivos de oficina	D03	Archivos de Oficina	Archivo	Divulgación	El uso indebido de archivos de oficina, por usuario no autorizado.	Malicioso	4	3	**4**	Riesgo intolerable
R49	D03-C	Divulgación de archivos de oficina	D03	Archivos de Oficina	Archivo	Divulgación	El uso indebido de la oficina archivos compartidos por usuario autorizado.	Malicioso	4	3	**4**	Riesgo intolerable
R50	D03-C	Divulgación de archivos de oficina	D03	Archivos de Oficina	Media	Divulgación	El uso indebido de la oficina archivos compartidos por usuario no autorizado	Malicioso	4	3	**4**	Riesgo intolerable
R51	D03-C	Divulgación de archivos de oficina	D03	Archivos de Oficina	Media	Desaparición	Robo de ordenadores portátiles o de oficina por persona autorizada a entrar en las instalaciones de la institución.	Malicioso	4	3	**4**	Riesgo intolerable
R52	D03-C	Divulgación de archivos de oficina	D03	Archivos de Oficina	PC portable	Desaparición	Robo de ordenadores portátiles o de oficina por persona no autorizada a entrar en	Malicioso	4	3	**4**	Riesgo intolerable

							las instalaciones de la institución.					
R53	D04-C	Divulgación de correos electrónicos enviados o recibidos	D04	E-mail	Mensaje E-mail	Divulgación	Divulgación accidental de correo electrónico, error de direccionamiento.	Error	4	2	**3**	Riesgo inadmisible
R54	D04-C	Divulgación de correos electrónicos enviados o recibidos	D04	E-mail	Mensaje E-mail	Divulgación	La divulgación voluntaria de correo electrónico que se envía o se recibe por un miembro del personal no autorizado.	Malicioso	4	3	**4**	Riesgo intolerable
R55	D05-C	Divulgación de documentos	D05	Documentos no informáticos, impresos o escritos a mano	Documento	Desaparición	Publicación de documentos escritos o impresos, por una persona autorizada a entrar en las instalaciones.	Malicioso	4	3	**4**	Riesgo intolerable
R56	D05-C	Divulgación de documentos	D05	Documentos no informáticos, impresos o escritos a mano	Documento	Desaparición	Publicación de documentos escritos o impresos por los usuarios de fuera de la institución	Malicioso	4	3	**4**	Riesgo intolerable
R57	D05-C	Divulgación de documentos	D05	Documentos no informáticos, impresos o escritos a mano	Documento	Desaparición	Divulgación o eliminación de documentos no informáticos.	Malicioso	4	3	**4**	Riesgo intolerable
R58	G01-D	Ambiente de trabajo no disponible	G01	Entorno de trabajo del usuario	Local	Indisponible	Oficina de trabajo no disponible, debido a un accidente o debido al ambiente (incendios, inundaciones, etc.)	Accidente	3	2	**3**	Riesgo inadmisible
R59	G01-D	Ambiente de trabajo no disponible	G01	Entorno de trabajo del usuario	Local	Indisponible	Oficina de trabajo no disponible, debido a la falta de acceso a los locales (causa externa).	Accidente	3	3	**3**	Riesgo inadmisible
R60	S01-D	Servicios informáticos y telecomunicaciones no disponibles	S01	TI y servicios de telecomunicaciones	Archivo de programa	Eliminación	Pérdida de configuración de software (programas de sistemas y aplicaciones, ajustes de configuración, etc.)	Accidente	4	3	**4**	Riesgo intolerable

							después de incidente operacional.					
R61	S01-D	Servicios informáticos y telecomunicaciones no disponibles	S01	TI y servicios de telecomunicaciones	Servidor de aplicaciones	Indisponible	Pérdida accidental de servicios informáticos o de telecomunicaciones (sin disponibilidad prolongada), debido a un accidente o debido al ambiente (incendios, inundaciones, etc.)	Accidente	4	2	**3**	Riesgo inadmisible
R62	S01-D	Servicios informáticos y telecomunicaciones no disponibles	S01	TI y servicios de telecomunicaciones	Servidor de aplicaciones	Indisponible	Pérdida accidental de servicios informáticos o de telecomunicaciones a la fallas de los equipos (sin disponibilidad temporal).	Accidente	4	3	**4**	Riesgo intolerable
R63	S01-D	Servicios informáticos y telecomunicaciones no disponibles	S01	TI y servicios de telecomunicaciones	Servicios	Indisponible	Pérdida de servicios TI, debido a la falta de suministro de energía (Sin disponibilidad temporal).	Accidente	4	2	**3**	Riesgo inadmisible
R64	S01-D	Servicios informáticos y telecomunicaciones no disponibles	S01	TI y servicios de telecomunicaciones	Servicios	Indisponible	Fallo en los servicios (sin disponibilidad temporal).	Accidente	4	2	**3**	Riesgo inadmisible
R65	S01-D	Servicios informáticos y telecomunicaciones no disponibles	S01	TI y servicios de telecomunicaciones	Servidor de aplicaciones	Daño	Daño malicioso de servicios debido al vandalismo en las instalaciones por una persona autorizada a entrar en las instalaciones.	Malicioso	4	1	**2**	Riesgo tolerable
R66	S01-D	Servicios informáticos y telecomunicaciones no disponibles	S01	TI y servicios de telecomunicaciones	Servidor de aplicaciones	Indisponible	Servicios informáticos o de telecomunicaciones sin funcionamiento debido a la falta del personal necesario.	Accidente	4	4	**4**	Riesgo intolerable

R67	S01-D	Servicios informáticos y telecomunicaciones no disponibles	S01	TI y servicios de telecomunicaciones	Aplicación	Bloqueo	Bloqueo de los servicios informáticos o de telecomunicaciones, debido a un fallo.	Error	4	2	**3**	Riesgo inadmisible
R68	S01-D	Servicios informáticos y telecomunicaciones no disponibles	S01	TI y servicios de telecomunicaciones	Cuenta de aplicación	Bloqueo	Bloqueo de cuentas necesarias, debido a un acto malicioso en las cuentas.	Malicioso	4	2	**3**	Riesgo inadmisible
R69	S02-D	Equipos de trabajo o terminales de usuario no disponibles (PC, impresoras, etc.).	S02	Disposición de Equipos (PC, impresoras locales, periféricos, interfaces específicas, etc.)	Config. Software	Eliminación	Pérdida de configuración en equipos disponibles para los usuarios.	Accidente	4	3	**4**	Riesgo intolerable
R70	S02-D	Equipos de trabajo o terminales de usuario no disponibles (PC, impresoras, etc.).	S02	Disposición de Equipos (PC, impresoras locales, periféricos, interfaces específicas, etc.)	Estaciones de trabajo	Indisponible	Falta de disponibilidad de equipos a disposición de los usuarios, debido a un virus.	Accidente	4	4	**4**	Riesgo intolerable
R71	S02-D	Equipos de trabajo o terminales de usuario no disponibles (PC, impresoras, etc.).	S02	Disposición de Equipos (PC, impresoras locales, periféricos, interfaces específicas, etc.)	Estaciones de trabajo	Indisponible	Equipos no disponibles para usuario debido a una falta de suministro de energía (fallo externo).	Accidente	4	4	**4**	Riesgo intolerable
R72	S03-D	Servicio de publicación o servicio de sitio web no disponible	S03	Los servicios ofrecidos en los sitios web	Sitio Server	Saturación	Saturación y error de redes.	Accidente	3	2	**3**	Riesgo inadmisible

R73	S01-I	Modificación en los servicios informáticos o telecomunicaciones	S01	TI y servicios de telecomunicaciones	Archivo de programa	Modificación	Modificación accidental (no detectado) de los servicios informáticos o de telecomunicaciones.	Error	4	2	**3**	Riesgo inadmisible
R74	S01-I	Modificación en los servicios informáticos o telecomunicaciones	S01	TI y servicios de telecomunicaciones	Archivo de programa	Modificación	Modificación maliciosa (no detectado) de los servicios informáticos o de telecomunicaciones.	Malicioso	4	3	**4**	Riesgo intolerable

Cuadro 15: Matriz de Evaluación de riesgos

Fuente: Elaboración propia

Finalmente se definen los niveles de riesgos por familia de escenarios en el cuadro 16, siendo 19 riesgos tolerables, 24 riesgos inadmisibles y 31 riesgos intolerables:

ESCENARIOS		RIESGOS		
Código Familia	**Familia Escenario**	**2**	**3**	**4**
D01-C	Divulgación de archivos informáticos	6		
D01-D	Pérdida de Archivos informáticos	7	1	
D01-I	Modificación (no detectada) de archivos informáticos	5		
D02-C	Divulgación de datos después de su consulta o captura		3	
D02-D	Pérdida de datos aislados (almacenado temporalmente o en tránsito)		2	1
D02-I	Modificación de datos sensibles o de datos en tránsito			2
D03-C	Divulgación de archivos de oficina		1	6
D03-D	Pérdida de datos de oficina		4	3
D03-I	Modificación (no detectada) de archivos de oficina		1	3
D04-C	Divulgación de correos electrónicos enviados o recibidos		1	1
D04-D	Pérdida de mensajes de correo electrónico (enviando o recibiendo)			1
D04-I	Modificación de correos electrónicos enviados o recibidos			1
D05-C	Divulgación de documentos			3
D05-D	Pérdida de documentos no informáticos		1	3
D06-I	Modificación de contenido de sitio web o del servicio de internet		1	
G01-D	Ambiente de trabajo no disponible		2	
S01-D	Servicios informáticos y telecomunicaciones no disponibles	1	5	3
S01-I	Modificación en los servicios informáticos o telecomunicaciones		1	1
S02-D	Equipos de trabajo o terminales de usuario no disponibles (PC, impresoras, etc.).			3
S03-D	Servicio de publicación o servicio de sitio web no disponible		1	
Total general		**19**	**24**	**31**

Cuadro16: Niveles de riesgo familia de escenarios

Fuente: Elaboración propia

5.2.4 Tratamiento de Riesgos

5.2.4.1 Elección de riesgos para tratamiento

Se han elegido los riesgos intolerables es decir con gravedad nivel 4 para su tratamiento, siendo 31 riesgos intolerables, en el cuadro 17 se indica el escenario, vulnerabilidad y la amenaza en la institución:

Riesgo	Código Familia	Familia Escenario	Soporte	Vulnerabilidad	Amenaza	Tipo AEM	Gravedad	Amenaza en institución
R09	D02-D	Pérdida de datos aislados (almacenado temporalmente o en tránsito)	mensaje	Pérdida	Pérdida accidental de datos en tránsito: mensajes o transacciones pendientes después de un incidente operacional.	Accidente	Riesgo intolerable	Pérdida accidental de documentos enviados del Ministerio de Cultura a la institución, con respecto a mensajes o transacciones pendientes.
R12	D03-D	Pérdida de datos de oficina	Archivo	Eliminación	Pérdida de archivos de oficina, a raíz de un virus.	Accidente	Riesgo intolerable	Pérdida de archivos de la DDC Lambayeque por virus.
R16	D03-D	Pérdida de datos de oficina	Media	Desaparición	Pérdida accidental, archivos personales en oficinas.	Malicioso	Riesgo intolerable	Pérdida accidental de archivos confidenciales en las oficinas de la DDC Lambayeque.
R17	D03-D	Pérdida de datos de oficina	Laptop	Desaparición	Robo de laptops o medios que soportan los archivos personales de oficina.	Malicioso	Riesgo intolerable	Robo de laptops o medios digitales de la DDC Lambayeque.
R19	D04-D	Pérdida de mensajes de correo electrónico (enviando o recibiendo)	Mensaje E-mail	Pérdida	Pérdida accidental de datos de: correo electrónico enviados o recibidos, después de un incidente operacional	Accidente	Riesgo intolerable	Pérdida de datos enviados o recibidos por correo.

R21	D05-D	Pérdida de documentos no informáticos	Documento	Desaparición	Desaparición por robo de documentos escritos o impresos por una persona autorizada a entrar en las instalaciones.	Malicioso	Riesgo intolerable	Pérdida por robo de documentos escritos o impresos por personal interno.
R22	D05-D	Pérdida de documentos no informáticos	Documento	Desaparición	Desaparición por el robo, divulgación o eliminación de documentos.	Malicioso	Riesgo intolerable	Divulgación de información importante de la institución.
R23	D05-D	Pérdida de documentos no informáticos	Documento	Desaparición	Desaparición por robo de documentos, escritos o impresos en poder de los usuarios de fuera de la institución	Malicioso	Riesgo intolerable	Robo de documentos escritos o impresos por personal no autorizado.
R29	D02-I	Modificación de datos sensibles o de datos en tránsito	datos	Modificación	Datos sensibles manipulados maliciosamente, por un miembro del personal no autorizado.	Malicioso	Riesgo intolerable	Modificación de informes o expedientes por personal no autorizado.
R30	D02-I	Modificación de datos sensibles o de datos en tránsito	datos	Modificación	Manipulación maliciosa de mensajes, en la red local por un miembro del personal no autorizado.	Malicioso	Riesgo intolerable	Manipulación de correos en la red local, por personal no autorizado.

R32	D03-I	Modificación (no detectada) de archivos de oficina	Archivo	Modificación	Modificación accidental (no detectado) de archivos de oficina, debido a un error en función de un programa de usuario.	Error	Riesgo intolerable	Error en el funcionamiento de un software instalado en la DDC Lambayeque.
R33	D03-I	Modificación (no detectada) de archivos de oficina	Archivo	Modificación	Modificación maliciosa (no detectado) de archivos de oficina compartida, por un usuario no autorizado.	Malicioso	Riesgo intolerable	Datos modificados de archivos de oficina compartida por usuario no autorizado.
R34	D03-I	Modificación (no detectada) de archivos de oficina	Archivo	Modificación	Modificación maliciosa (no detectado) archivos de oficina personales por un usuario no autorizado.	Malicioso	Riesgo intolerable	Modificación de archivos de oficina personal por un usuario no autorizado.
R35	D04-I	Modificación de correos electrónicos enviados o recibidos	Correo	Modificación	Manipulación maliciosa de correo electrónico que se envía o se recibe por una parte no autorizada.	Malicioso	Riesgo intolerable	Manipulación de correo electrónico por personal no autorizado.
R47	D03-C	Divulgación de archivos de oficina	Archivo	Divulgación	El uso indebido de archivos de oficina, por usuario autorizado.	Malicioso	Riesgo intolerable	Divulgación de información sensible de oficina, por usuario interno de la DDC Lambayeque.

R48	D03-C	Divulgación de archivos de oficina	Archivo	Divulgación	El uso indebido de archivos de oficina, por usuario no autorizado.	Malicioso	Riesgo intolerable	Divulgación de información sensible de oficina, por usuario externo de la DDC Lambayeque.
R49	D03-C	Divulgación de archivos de oficina	Archivo	Divulgación	El uso indebido de la oficina archivos compartidos por usuario autorizado.	Malicioso	Riesgo intolerable	Divulgación de información sensible de oficina compartida, por usuario interno de la DDC Lambayeque.
R50	D03-C	Divulgación de archivos de oficina	Media	Divulgación	El uso indebido de la oficina archivos compartidos por usuario no autorizado	Malicioso	Riesgo intolerable	Divulgación de información sensible de oficina compartida, por usuario externo de la DDC Lambayeque.
R51	D03-C	Divulgación de archivos de oficina	Media	Desaparición	Robo de ordenadores portátiles o de oficina por persona autorizada a entrar en las instalaciones de la institución.	Malicioso	Riesgo intolerable	Robo de ordenadores por personal autorizado.
R52	D03-C	Divulgación de archivos de oficina	PC portable	Desaparición	Robo de ordenadores portátiles o de oficina por persona no autorizada a entrar en las instalaciones de la institución.	Malicioso	Riesgo intolerable	Robo de ordenadores por personal no autorizado.

R54	D04-C	Divulgación de correos electrónicos enviados o recibidos	Mensaje E-mail	Divulgación	La divulgación voluntaria de correo electrónico que se envía o se recibe por un miembro del personal no autorizado.	Malicioso	Riesgo intolerable	Divulgación de un correo electrónico.
R55	D05-C	Divulgación de documentos	Documento	Desaparición	Publicación de documentos escritos o impresos, por una persona autorizada a entrar en las instalaciones.	Malicioso	Riesgo intolerable	Documentos extraviados por personal autorizado.
R56	D05-C	Divulgación de documentos	Documento	Desaparición	Publicación de documentos escritos o impresos por los usuarios de fuera de la institución	Malicioso	Riesgo intolerable	Documentos extraviados por personal no autorizado.
R57	D05-C	Divulgación de documentos	Documento	Desaparición	Divulgación o eliminación de documentos no informáticos.	Malicioso	Riesgo intolerable	Destrucción de documentos.
R60	S01-D	Servicios informáticos y telecomunicaciones indisponibles	Archivo de programa	Eliminación	Pérdida de configuración de software (programas de sistemas y aplicaciones, ajustes de configuración, etc.) después de incidente operacional.	Accidente	Riesgo intolerable	Eliminación accidental de software.

R62	S01-D	Servicios informáticos y telecomunicaciones indisponibles	Servidor de aplicaciones	Indisponible	Pérdida accidental de servicios informáticos o de telecomunicaciones a la fallas de los equipos (sin disponibilidad temporal).	Accidente	Riesgo intolerable	Equipos informáticos y servicio de red., sin disponibilidad temporal.
R66	S01-D	Servicios informáticos y telecomunicaciones indisponibles	Servidor de aplicaciones	Indisponible	Servicios informáticos o de telecomunicaciones sin funcionamiento debido a la falta del personal necesario.	Accidente	Riesgo intolerable	Servicios informáticos no disponibles por ausencia de personal.
R69	S02-D	Equipos de trabajo o terminales de usuario indisponibles (PC, impresoras, etc.).	Config. Software	Eliminación	Pérdida de configuración en equipos disponibles para los usuarios.	Accidente	Riesgo intolerable	Pérdida de configuración en equipos disponibles en la DDC Lambayeque.
R70	S02-D	Equipos de trabajo o terminales de usuario indisponibles (PC, impresoras, etc.).	Estaciones de trabajo	Indisponible	Falta de disponibilidad de equipos a disposición de los usuarios, debido a un virus.	Accidente	Riesgo intolerable	Falta de disponibilidad de equipos por Virus (antivirus caducado) en la DDC Lambayeque.
R71	S02-D	Equipos de trabajo o terminales de usuario indisponibles (PC, impresoras, etc.).	Estaciones de trabajo	Indisponible	Equipos no disponibles para usuario debido a una falta de suministro de energía (fallo externo).	Accidente	Riesgo intolerable	Equipos no disponibles por falta de suministro de energía en la DDC Lambayeque.

R74	S01-I	Modificación en los servicios informáticos o telecomunicaciones	Archivo de programa	Modificación	Modificación maliciosa (no detectado) de los servicios informáticos o de telecomunicaciones.	Malicioso	Riesgo intolerable	Manipulación en los equipos y servicios informáticos en la DDC Lambayeque.

Cuadro 17: Riesgos intolerables elegidos para tratamiento.

Fuente: Elaboración propia.

5.2.4.2 Identificación de controles según la ISO/IEC 27002:2013

La norma ISO 27002 proporciona un listado de controles que pueden ser utilizados en el plan de tratamiento para generar medidas que ayuden a la prevención, protección y mitigación de riesgos, en la tabla 15 se describen sus objetivos:

Cláusulas de los controles ISO/IEC 27002:2013	Descripción de objetivo
5. POLÍTICAS DE SEGURIDAD	Proporcionar a la institución, la gestión y apoyo en temas relacionados a la seguridad de la información, de acuerdo a los requerimientos de la organización, sus normas y lineamientos.
6. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	Realizar una estructura para implementar y controlar un sistema de seguridad de información dentro de la institución. Garantizar la seguridad de teletrabajo y el uso de dispositivos móviles.
7. SEGURIDAD EN LOS RECURSOS HUMANOS	Comunicar y establecer las responsabilidades de seguridad de la información a los colaboradores internos y terceros según sus roles, considerando los objetivos de la institución.
8. GESTIÓN DE ACTIVOS.	Identificar los activos de la institución y definir las responsabilidades de protección. Garantizar los niveles de confiabilidad, disponibilidad e integridad, evitando la divulgación, modificación, alteración de la información almacenada.
9. CONTROL DE ACCESOS.	Garantizar el acceso de usuarios autorizados y evitar/prevenir el acceso no autorizado a servicios de TI. Cada usuario debe ser responsable de proteger su información.
10. CRIPTOGRAFÍA.	Garantizar el uso adecuado y eficaz del cifrado para proteger autenticidad de la información.
11. SEGURIDAD FÍSICA Y DEL ENTORNO	Prevenir el acceso físico no autorizado, daños y modificación a la información de la institución, así como evitar la pérdida, daño, robo o alteración de los activos.
12. SEGURIDAD EN LAS OPERACIONES	Asegurar que la información este protegida contra el código malicioso. Evitar la pérdida de datos. Registrar eventos y generar evidencia. Evitar

	vulnerabilidades en los sistemas operativos.
13. SEGURIDAD EN LAS COMUNICACIONES	Garantizar la protección de la información en las redes. Mantener la seguridad de la información transferida desde la organización con cualquier usuario externo.
14. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS.	Garantizar que la seguridad de la información sea parte importante de los sistemas de información en todo su ciclo de vida. Garantizar la protección de datos en las pruebas.
15. RELACIONES CON PROVEEDORES.	Garantizar la protección de los activos de la institución que sea accesible por los proveedores. Mantener las mismas políticas de seguridad de la información con los servicios prestados por los proveedores.
16. GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN.	Garantizar una estructura eficaz para la gestión de incidentes de la seguridad de información.
17. ASPECTOS DE SEGURIDAD DE LA INFORMACION PARA LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	Garantizar la disponibilidad y continuidad de los sistemas de información dentro de la institución.
18. CUMPLIMIENTO.	Cumplir con las obligaciones legales, reglamentarias o contractuales relacionadas a la seguridad de la información. Garantizar que la seguridad de la información se implementa y funciona de acuerdo a las políticas y lineamientos de la institución.

Tabla15 : Objetivos de los Controles de la Norma ISO 27002.

Fuente: (Justino, 2015)

5.2.4.3 Tabla de tratamiento de riesgos con controles de la ISO 27002:2013:

En esta etapa se analizan que controles pueden tratar a los riesgos intolerables elegidos, se realiza el siguiente cuadro 18 cruzando la información de riesgos y controles ISO 27002:

DOMINIOS	OBJETIVOS DE CONTROL	CONTROLES		RIESGOS
7 Seguridad de los recursos humanos	7.2 Durante el empleo	7.2.2	Concientización, educación y capacitación en materia de seguridad de la información	R16,R21,R22,R23 ,R48
		7.2.3	Proceso disciplinario	R17,R22,R23,R51 ,R52
8 Gestión de activos	8.1 Responsabilidad patrimonial	8.1.1	Inventario de activos	R17,R51,R52
		8.1.2	Propiedad de los activos	R17,R51,R52
		8.1.3	Uso aceptable de los activos	R12,R16,R29,R48
	8.3 Manejo de medios	8.3.1	Gestión de medios extraíbles	R12,R70,R17
		8.3.3	Transferencia de medios físicos	R09
9 Control de acceso	9.1 Requerimientos empresariales del control de acceso	9.1.1	Política de control de acceso	R16,R29,R48,R62 ,R66,R70
		9.1.2	Acceso a redes y servicios de red	R19,R48,R62,R62 ,R66
	9.2 Gestión de acceso de usuario	9.2.1	Gestión de altas/bajas en el registro de usuarios	R22,R34,R62,R66
		9.2.2	Gestión de los derechos de acceso asignados a usuarios	R30,R33,R34,R35 ,R48,R49,R50,R5 4
		9.2.3	Gestión de derechos de acceso privilegiados	R34,R62,R66,R62
		9.2.4	Gestión de la información de autenticación secreta de los usuarios	R48,R60
		9.2.5	Revisión de derechos de acceso de usuario	R48
		9.2.6	Eliminación o ajuste de los derechos de acceso	R48
	9.3 Responsabilidad es del usuario	9.3.1	Uso de la información confidencial para la autenticación	R30,R35,R54
	9.4 Acceso a sistemas y aplicaciones	9.4.1	Restricción de acceso a la información	R60,R62,R66,R70
		9.4.3	Sistema de gestión de contraseñas	R30,R35,R54
		9.4.4	Uso de programas de utilidad privilegiada	R32,R60,R70

		9.4.5	Control de acceso al código fuente del programa	R32,R60
10 Criptografía	10.1 Controles criptográficos	10.1.1	Política sobre el uso de controles criptográficos	R29
		10.1.2	Gestión de claves	R29
11 Seguridad física y ambiental	11.1 Zonas seguras	11.1.1	Perímetro de seguridad física	R17,R21,R23,R34,R50,R51,R52,R55,R57
		11.1.2	Controles físicos de entrada	R16,R17,R21,R23,R34,R51,R52,R56,R55,R57
		11.1.3	Asegurar oficinas, habitaciones e instalaciones	R16,R21,R23,R34,R50,R51,R52,R55,R56,R57
		11.1.4	Protección contra las amenazas externas y ambientales	R71
		11.1.5	Trabajo en áreas seguras	R17,R21,R23,R51,R52
		11.1.6	Zonas de entrega y carga	R09
	11.2 Equipo	11.2.1	Ubicación y protección del equipo	R17,R49,R69
		11.2.2	Instalaciones de suministro	R71
		11.2.4	Mantenimiento de equipo	R69,R70
		11.2.6	Seguridad de equipos y activos fuera de las instalaciones	R17
		11.2.8	Equipo de usuario desatendido	R69, R70
12 Seguridad de las operaciones	12.2 Protección contra el código malicioso	12.2.1	Controles contra el código malicioso	R12,R70
	12.3 Copia de seguridad	12.3.1	Copia de seguridad de la información	R09, R33, R16
	12.4 Registro y monitoreo	12.4.1	Registro de eventos	R21,R23, R34
	12.5 Control del software operativo	12.5.1	Instalación de software en sistemas operativos	R12,R16
	12.6 Gestión de vulnerabilidades técnicas	12.6.2	Restricciones en la instalación del software	R12,R70
13 Seguridad de las comunicaciones	13.1 Gestión de la seguridad de la red	13.1.1	Controles de red	R29,R30,R33,R74
		13.1.2	Seguridad de los servicios de red	R19,R29,R30,R33,R49,R62,R74,
		13.1.3	Segregación en redes	R29,R30,R33,
	13.2 Transferencia de información	13.2.1	Políticas y procedimientos de transferencia de información	R09,R35,R48,R54,R55,R56
		13.2.2	Acuerdos sobre transferencia de información	R19,R47,R48,R54,R55,R56
		13.2.3	Mensajería electrónica	R19,R35,R54,

		13.2.4	Acuerdos de confidencialidad o no divulgación	R22,R47,R48,R49 ,R50,R54,R55,R5 6
14 Adquisición, desarrollo y mantenimiento del sistema	14.2 Seguridad en los procesos de desarrollo y soporte	14.2.3	Revisión técnica de aplicaciones tras cambios en la plataforma operativa	R60,
		14.2.4	Restricciones a los cambios en los paquetes de software	R60,
15 Relaciones con los proveedores	15.2 Gestión de la entrega de servicios de proveedores	15.2.1	Seguimiento y revisión de los servicios de proveedores	R71
16 Gestión de incidentes de seguridad de la información	16.1 Gestión de incidentes y mejoras en la seguridad de la información	16.1.5	Respuesta a incidentes de seguridad de la información	R62,R71
17 Aspectos de la seguridad de la información en la continuidad del negocio	17.1 Continuidad de la seguridad de la información	17.1.1	Planificación de la continuidad de la seguridad de la información	R62,R66,R69,R70 ,R71
18 Cumplimiento	18.1 Cumplimiento de los requisitos legales y contractuales	18.1.2	Derechos de propiedad intelectual	R29
		18.1.4	Privacidad y protección de la información de identificación personal	R29, R34

Cuadro 18 : Tratamiento de Riesgos con controles ISO 27002

Fuente: Elaboración propia.

5.2.4.4 Mapeo de los Controles con COBIT 5.

Para complementar los controles del sistema de seguridad de la información, se están considerando la guía de mejores prácticas de COBIT con la finalidad de alinear las necesidades del negocio y los servicios de TI.

Basado en las tablas de Objetivos del negocio y objetivos de TI de COBIT (Anexo 31: Objetivos COBIT), se ha realizado el mapeo de controles para la Dirección desconcentrada de Cultura de Lambayeque en el cuadro 19:

Objetivos del Negocio		Objetivos TI	
2	Cartera de productos y servicios competitivos	1	Alineación de TI y estrategia institucional
		5	Beneficios obtenidos de la cartera de inversiones y servicios de TI
		9	Agilidad de TI
		17	Conocimiento, experiencia e iniciativas para la innovación institucional
3	Gestión de riesgos del negocio (salvaguarda de activos)	4	Gestión de riesgos de negocio relacionados con TI
		10	Seguridad de la información, infraestructura de procesamiento y aplicaciones
4	Cumplimiento con leyes y reglamentos externos	2	Cumplimiento de las TI y soporte para el cumplimiento de las leyes y reglamentos externos
		10	Seguridad de la información, infraestructura de procesamiento y aplicaciones
5	Transparencia financiera	6	Transparencia de los costos, beneficios y riesgos de TI
6	Cultura de servicio orientada al cliente	1	Alineación de TI y estrategia institucional
		7	Entrega de servicios de TI en línea con los requisitos del negocio
7	Continuidad y disponibilidad de servicios	1	Alineación de TI y estrategia institucional
		4	Gestión de riesgos de negocio relacionados con TI
		10	Seguridad de la información, infraestructura de procesamiento y aplicaciones
		14	Disponibilidad de información confiable y útil para la toma de decisiones
8	Respuestas ágiles a un entorno cambiante	7	Entrega de servicios de TI en línea con los requisitos del negocio
		9	Agilidad de TI
		17	Conocimiento, experiencia e iniciativas para la innovación institucional

9	Toma de decisiones estratégicas basadas en información	1	Alineación de TI y estrategia institucional
		3	Compromiso de la dirección para tomar decisiones relacionadas con TI
		14	Disponibilidad de información confiable y útil para la toma de decisiones
10	Optimización de los costes de la prestación de servicios	6	Transparencia de los costos, beneficios y riesgos de TI
		11	Optimización de los recursos, recursos y capacidades de TI
11	Optimización de la funcionalidad de los procesos institucionales	1	Alineación de TI y estrategia institucional
		8	Uso adecuado de aplicaciones, soluciones de información y tecnología
		9	Agilidad de TI
		12	Capacitación y soporte de procesos de negocio integrando aplicaciones y tecnología en procesos de negocio
12	Optimización de los costes de los procesos institucionales	5	Beneficios obtenidos de la cartera de inversiones y servicios de TI
		6	Transparencia de los costos, beneficios y riesgos de TI
		11	Optimización de los recursos, recursos y capacidades de TI
14	Productividad operativa y de personal	8	Uso adecuado de aplicaciones, soluciones de información y tecnología
			Personal de la institución y de TI: competente y motivado
15	Cumplimiento de las políticas internas	2	Cumplimiento de las TI y soporte para el cumplimiento de las leyes y reglamentos externos
		10	Seguridad de la información, infraestructura de procesamiento y aplicaciones
		15	Cumplimiento de las políticas internas con las TI
16	Personas cualificadas y motivadas	16	Personal de la institución y de TI: competente y motivado

17	Cultura de innovación de productos y negocios	9	Agilidad de TI
		17	Conocimiento, experiencia e iniciativas para la innovación institucional

Cuadro 19: Uso de los controles COBIT

Fuente: Elaboración propia

5.2.4.5 Declaración de Aplicabilidad

Gracias al análisis de riesgos se identificaron los activos de información propensos a vulnerabilidades y además los riesgos a los que pueden encontrarse expuestos luego se realizó el tratamiento de riesgos, proceso en el que se seleccionaron los riesgos que serían tratados y las medidas que se deberían aplicar, como propuesta.

Después de todo lo mencionado y según la documentación solicitada por el sistema de gestión de seguridad de la información, basado en la ISO 27001:2013, se propone también el siguiente listado de controles detallados en el Anexo A de la norma, eligiendo que controles pueden ser implementados o deben implementarse según el requerimiento de seguridad de la institución, este importante documento es la "Declaración de aplicabilidad".

En este documento se presenta el listado de los 114 controles, eligiendo que controles si son aplicables en la institución, su justificación y un breve comentario de lo que sería su implementación.

En el cuadro 20 se visualizan 74 controles que aplican en la institución y 40 no aplicables.

Clausula	Sección	Objetivo de Control / Control	Es Aplicable a la organización	Justificación	Comentarios
5. Políticas de Seguridad	**5.1**	**Dirección de la Alta Gerencia para la Seguridad de la Información**			
	5.1.1	Políticas de Seguridad de la Información	Aplica	Actualmente la institución no cuenta con políticas de Seguridad de la información.	Para iniciar un Sistema de gestión de seguridad de la información es necesario establecer una Política de Seguridad de la información, se ha realizado una propuesta.
	5.1.2	Revisión de las Políticas de Seguridad de la Información	Aplica	Actualmente la institución no cuenta con políticas de Seguridad de la información, como parte del diseño del SGSI se ha realizado dentro de esta propuesta.	Es necesario que la política de seguridad de la información sea revisada y aprobada.
6. Organización de la seguridad de la información	**6.1**	**Organización Interna**			
	6.1.1	Roles y Responsabilidad de Seguridad de la Información	Aplica	Actualmente no existen roles de seguridad de la información, esta responsabilidad estará a cargo por el administrador.	Es necesario que la institución apruebe los roles indicados en la política de seguridad de la información.
	6.1.2	Segregación de deberes	Aplica	Actualmente no existen roles de seguridad de la información, esta responsabilidad estará a cargo por el administrador.	Es necesario que se revise y apruebe lo indicado en las políticas de seguridad de la información establecida en esta propuesta.
	6.1.3	Contacto con autoridades	Aplica	Anteriormente no se ha realizado el contacto para este proceso.	Es importante realizar reuniones para la aprobación del SGSI.
	6.1.4	Contacto con grupos de interés especial	Aplica	Anteriormente no se ha realizado el contacto para este proceso.	Es importante realizar reuniones para la aprobación del SGSI.
	6.1.5	Seguridad de la Información en la gestión de proyectos	Aplica	Una de las principales funciones de la institución es gestionar proyectos.	Es necesario implementar un sistema de seguridad de la información.
	6.2	**Dispositivos móviles y teletrabajo**			
	6.2.1	Política de dispositivos móviles	No Aplica	-	Los principales riesgos de la institución no están vinculados a dispositivos móviles.
	6.2.2	Teletrabajo	No Aplica	-	Los principales riesgos de la institución no están vinculados al teletrabajo.
7. Seguridad en los recursos humanos	**7.1**	**Previo al Empleo**			
	7.1.1	Verificación de antecedentes	No Aplica	-	Los lineamientos de la institución indican que este proceso es función de recursos humanos.

	7.1.2	Términos y condiciones del empleo	Aplica	Actualmente no están incluidas estas condiciones en el contrato de empleo.	Es necesario contar con cláusulas en el contrato con respecto a la confidencialidad de la empresa y protección de datos, se está considerando una declaración de confidencialidad.
	7.2	**Durante el Empleo**			
	7.2.1	Responsabilidades de la Alta Gerencia	Aplica	Actualmente no están incluidas estas responsabilidades en los lineamientos de la institución.	Es necesario determinar el cumplimiento de las políticas y procedimientos con respecto a seguridad de la información en la institución y darle a conocer a todos los colaboradores.
	7.2.2	Conciencia, educación y entrenamiento de Seguridad de la Información	Aplica	Actualmente no hay un programa de concientización y/o capacitaciones sobre seguridad de la información.	Es establecer un cronograma de inducción, concientización y capacitación sobre SGSI y dar a conocer a todos los colaboradores, se establecerán declaraciones y compromisos.
	7.2.3	Proceso disciplinario	Aplica	Actualmente no hay proceso disciplinario para faltas contra la seguridad de la información.	Es necesario que existan sanciones para aquellos colaboradores que comentan una falta grave a la seguridad, se establecen reglas en la Política del SGSI.
	7.3	**Terminación y Cambio de Empleo**			
	7.3.1	Termino de responsabilidades o cambio de empleo	No Aplica	-	Los lineamientos de la institución indican que este proceso es función de recursos humanos.
8. Gestión de activos	**8.1**	**Responsabilidad de los Activos**			
	8.1.1	Inventario de activos	Aplica	Anteriormente la institución no tenía un inventario de activos, se ha realizado un inventario de activos de información en esta propuesta.	Es necesario realizar un listado de activos, que se encuentre constantemente actualizado según el periodo que determine la institución, este proceso será apoyado por una herramienta software.
	8.1.2	Propiedad de activos	Aplica	Anteriormente la institución no tenía un inventario de activos, se ha realizado un inventario de activos de información en esta propuesta.	Es necesario se conozcan las propiedades de los activos con el fin de hacerles seguimiento y monitoreo, se establece en la política de activos.
	8.1.3	Uso aceptable de los activos	Aplica	Anteriormente la institución no tenía un inventario de activos, se ha realizado un inventario de activos de información en esta propuesta.	Es necesario considerar el uso aceptable de los activos en las políticas de la seguridad de la información, se establece en la política de activos.
	8.1.4	Devolución de activos	No Aplica	-	No se considera dentro del diseño ya que este proceso sería decisión directa de la institución

	8.2	**Clasificación de la Información**			
	8.2.1	Clasificación de la información	Aplica	Actualmente la institución no cuenta con clasificación de la información.	Es importante tener clara la clasificación de la información, según su valor y nivel de criticidad para la institución.
	8.2.2	Etiquetado de la información	Aplica	Actualmente la institución no cuenta con clasificación de la información.	Es importante tener clara la clasificación de la información, según su valor y nivel de criticidad para la institución.
	8.2.3	Manejo de activos	Aplica	Anteriormente la institución no tenía un inventario de activos, se ha realizado un inventario de activos de información en esta propuesta.	Es necesario determinar el tratamiento y manejo para cada tipo de activo.
	8.3	**Manejo de Medios**			
	8.3.1	Gestión de medios removibles	Aplica	La institución cuenta con medios removibles pero no hay una gestión de ellos.	Es importante el uso de medio removibles por lo tanto es necesario contar con estrategias para evitar riesgos, se establece en política de activos.
	8.3.2	Eliminación de medios	No Aplica	La institución cuenta con medios removibles pero no hay una gestión de ellos.	No se considera dentro del diseño ya que este proceso sería decisión directa de la institución
	8.3.3	Transporte de medios físicos	Aplica	Mediante correo postal (envío físico de documentos) se envían muchos documentos importantes y no existe un seguimiento de los transportes.	Es necesario contar con estrategias para evitar riesgos, se establece en política de activos.
9. Control de Accesos	**9.1**	**Requerimientos de Negocio para el Control de Acceso**			
	9.1.1	Política de control de acceso	Aplica	No hay políticas actualizadas con respecto al control de acceso.	El control de acceso es vital para evitar la vulnerabilidad de documentación importante para la institución, se establece en política de gestión de accesos.
	9.1.2	Política en el uso de servicios de red	Aplica	El servicio tiene calidad media y no hay una correcta instalación de redes.	Es importante contar con un buen servicio de red y un correcto cableado estructurado, se establece en el procedimiento operativo para TI.
	9.2	**Gestión de Accesos de Usuario**			

	9.2.1	Registro y baja del usuario	Aplica	Actualmente la institución cuenta con usuarios pero no se gestionan efectivamente.	Es necesario contar con una gestión de usuarios personales para cada colaborador, se establece en política de control de accesos.
	9.2.2	Abastecimiento de usuarios de acceso	Aplica	No hay un procedimiento en el que se abastezcan de usuarios de acceso.	Es necesario contar con una gestión de usuarios personales para cada colaborador, se establece en política de control de accesos.
	9.2.3	Gestión de accesos privilegiados	Aplica	Actualmente la institución cuenta con usuarios pero no se gestionan efectivamente.	Es necesario realizar un procedimiento documentado, en el que se indique que cada jefe de área debe solicitar los permisos adecuados para cada colaborador, se establece en política de control de accesos.
	9.2.4	Gestión de información de autenticación secreta de usuarios	Aplica	Actualmente la institución cuenta con usuarios pero no se gestionan efectivamente.	Es necesario es establecer lineamientos para la adecuada gestión de autenticación de usuarios, se establece en política de control de accesos.
	9.2.5	Revisión de derechos de acceso de usuarios	Aplica	Actualmente la institución cuenta con usuarios pero no se gestionan efectivamente.	Es necesario contar con una matriz de perfiles de acceso autorizada y firmada como compromiso de la seguridad de la información, se establece en política de control de accesos.
	9.2.6	Eliminación o ajuste de derechos de acceso	Aplica	Actualmente la institución cuenta con usuarios pero no se gestionan efectivamente.	Es necesario contar con una matriz de perfiles de acceso autorizada y firmada como compromiso de la seguridad de la información, se establece en política de control de accesos.
	9.3	**Responsabilidades del Usuario**			
	9.3.1	Uso de información de autenticación secreta	Aplica	No existe cultura de seguridad en los colaboradores de la institución.	La información es el activo más valioso por lo tanto es necesario proteger, priorizando la información secreta y que cada usuario sea responsable de su usuario y contraseña, se establece la declaración de confiabilidad que deberá ser firmada por los colaboradores.
	9.4	**Control de Acceso de Sistemas y Aplicaciones**			
	9.4.1	Restricción de acceso a la información	Aplica	Actualmente la institución cuenta con usuarios pero no se gestionan efectivamente.	Es necesario tener establecida un listado de tipos de usuarios y permisos y restricciones de los mismos, se establece en la política de control de accesos.
	9.4.2	Procedimientos de conexión segura	Aplica	Actualmente no hay restricciones en el sistema local.	Es necesario establecer lineamientos para establecer una conexión segura al acceder a los sistemas y aplicaciones.

	9.4.3	Sistema de gestión de contraseñas	Aplica	Actualmente los usuario tienen contraseña pero no hay una gestión efectiva de su uso.	Es necesario establecer tiempos de caducidad de contraseñas para mejorar el control de la gestión de contraseñas, se establece en la política de control de accesos.
	9.4.4	Uso de programas y utilidades privilegiadas	Aplica	Actualmente la institución cuenta con usuarios pero no se gestionan efectivamente.	Los usuarios deben ser gestionados por sus perfiles y privilegios para el acceso de programas, se establece en la política de control de accesos.
	9.4.5	Control de acceso al código fuente del programa	No Aplica	-	La institución no presenta riesgos de este tipo.
10. Criptografía	**10.1**	**Controles Criptográficos**			
	10.1.1	Política en el uso de controles criptográficos	No Aplica	-	La institución no cuenta con información criptográfica, su implementación es decisión del Ministerio de Cultura.
	10.1.2	Gestión de claves	Aplica	Actualmente los usuario tienen contraseña pero no hay una gestión efectiva de su uso.	Es necesario establecer tiempos de caducidad de contraseñas para mejorar el control de la gestión de contraseñas.
11. Seguridad física y del entorno	**11.1**	**Áreas Seguras**			
	11.1.1	Perímetro de seguridad físico	Aplica	No existen restricciones de acceso físico a la documentación de la institución.	El perímetro de seguridad es necesario para la protección de las áreas que contienen información, con el objetivo de establecer un límite de accesos a lugares que almacenen información sensible.
	11.1.2	Controles físicos de entrada	Aplica	No existen restricciones de acceso físico a la documentación de la institución.	Utilizar controles de acceso al personal interno y externo a los ambientes con información sensible. Los colaboradores deberían estar identificados.
	11.1.3	Seguridad de oficinas, habitaciones y facilidades	Aplica	No existen restricciones de acceso físico a la documentación de la institución.	Evitar el acceso de personal externo o no autorizado que haga uso de servicios en los ambientes con información sensible dentro de la institución.
	11.1.4	Protección contra amenazas externas y del ambiente	Aplica	Actualmente la institución es vulnerable a amenazas externas y del ambiente.	Generar estrategias para implementar medidas que puedan proteger la información sensible de desastres naturales o provocados (incendio), teniendo espacios y armarios con mejores distribuciones.
	11.1.5	Trabajo en áreas seguras	Aplica	Las áreas de la institución son seguras pero pueden presentarse vulnerabilidades.	Es importante tener clara la información con respecto a seguridad en las zonas de trabajo, se establece dentro de la política de Zonas Seguras.
	11.1.6	Áreas de entrega y carga	Aplica	Es probable que se presenten riesgos en los envíos de documentación o encomiendas a través de terceros.	Se deben considerar mecanismos de seguimientos, se establece dentro de la política de zonas seguras.
	11.2	**Equipo**			

	11.2.1	Instalación y protección de equipo	Aplica	Es necesario que exista una infraestructura segura para los equipos.	Los equipos utilizados en la institución deben instalarse de manera que se evite el acceso no autorizado por parte de personas ajenas o no autorizadas, se establece en la política de activos.
	11.2.2	Instalaciones de suministro	Aplica	El servicio de suministro eléctrico y no se ha considerado acciones en el caso de fallas.	Establecer la ruta correcta para la solución ante fallas técnicas del servicio de suministro eléctrico, se establece en la política de gestión de incidentes.
	11.2.3	Seguridad en el cableado	Aplica	Es necesario determinar si el cableado es seguro para evitar incidentes de pérdida de información.	Se considera la revisión de las instalaciones de red con la propuesta de implementar una red de cableado estructurado para la institución.
	11.2.4	Mantenimiento de equipos	Aplica	Existe el servicio de soporte y mantenimiento de equipos pero los colaboradores no lo utilizan porque no tienen claro su funcionamiento por lo tanto no es eficiente.	Establecer la ruta correcta para el soporte y mantenimiento necesario para los equipos, se establece en la gestión de incidentes.
	11.2.5	Retiro de activos	No Aplica	-	La decisión es del Ministerio de Cultura, canalizada por la Dirección desconcentrada de cultura de Lambayeque.
	11.2.6	Seguridad del equipo	Aplica	El trabajo de los colaboradores es muchas veces de campo, es decir si es probable que los equipos se expongan a vulnerabilidades fuera de la institución.	Establecer pautas de salida de equipos, con firmas y compromisos, el detalle en la política de activos.
	11.2.7	Eliminación segura o re uso del equipo	No Aplica	-	La decisión es del Ministerio de Cultura, canalizada por la Dirección desconcentrada de cultura de Lambayeque.
	11.2.8	Equipo de usuario desatendido	Aplica	En oportunidades los usuarios están fuera de oficina y los equipos no están bloqueados los que permiten su fácil acceso.	Establecer políticas que especifiquen el requisito de mantener el equipo bloqueado en caso se requiera ausentarse del mismo o cambios de contraseña, se establece en la política
	11.2.9	Política de escritorio limpio y pantalla limpia	Aplica	En los escritorios se puede encontrar la información sensible expuesta.	Se incluye en la política de zonas seguras el lineamiento con respecto a mantener el escritorio ordenado.
12. Seguridad en las operaciones	**12.1**	**Procedimientos Operacionales y Responsabilidades**			
	12.1.1	Documentación de procedimientos operacionales	No Aplica	-	Los procedimientos operaciones son decididos por el Ministerio de Cultura.

	12.1.2	Gestión de cambios	No Aplica	-	El alcance del SGSI no considera estas actividades.
	12.1.3	Gestión de la capacidad	No Aplica	-	El alcance del SGSI no considera estas actividades.
	12.1.4	Separación de los ambientes de desarrollo, pruebas y operación	No Aplica	-	El alcance del SGSI no considera estas actividades.
	12,2	**Protección de Software Malicioso**			
	12.2.1	Controles contra software malicioso	Aplica	La institución cuenta con el antivirus pero la licencia es obsoleta por ese motivo los equipos no están protegidos.	Es necesario adquirir la licencia del software para los 23 equipos de la institución.
	12.3	**Respaldo**			
	12.3.1	Respaldo de información	Aplica	No se realiza ningún tipo de backup de la información.	Se propone utilizar una herramienta open source para el backup y mapeo de la información.
	12.4	**Registro y Monitoreo**			
	12.4.1	Registro de eventos	No Aplica	-	Esta función es realizada en la sede central.
	12.4.2	Protección de registros de información	Aplica	No se realiza ningún tipo de protección de información.	Es necesario establecer protección con una herramienta que permita verificar el acceso de los usuario y las tareas que estos realizan.
	12.4.3	Registros de Administrador y Operador	No Aplica	-	Esta función es realizada en la sede central.
	12.4.4	Sincronización de relojes	No Aplica	-	Esta función es realizada en la sede central.
	12.5	**Control de Software Operacional**			
	12.5.1	Instalación de software en sistemas operacionales	No Aplica	-	El alcance del SGSI no considera estas actividades.
	12,6	**Gestión de Vulnerabilidades Técnicas**			
	12.6.1	Gestión de vulnerabilidades técnicas	No Aplica	-	El alcance del SGSI no considera estas actividades.
	12.6.2	Restricciones en la instalación de software	No Aplica	-	El alcance del SGSI no considera estas actividades.
	12.7	**Consideraciones de Auditoria de Sistemas de información**			
	12.7.1	Controles de Auditoría de Sistemas de Información	No Aplica	-	El alcance del SGSI no considera estas actividades.
	13.1	**Gestión de Seguridad en Red**			

13. Seguridad en las comunicaciones	13.1.1	Controles de red	Aplica	No existen controles de red establecidos en la institución.	Se propone utilizar una herramienta open source para el monitoreo y control de red, la política también establece limitaciones de modo que solo los equipos de la institución puedan conectarse a la red y compartir los recursos de la misma.
	13.1.2	Seguridad de los servicios en red	Aplica	No existen controles de red establecidos en la institución.	Se propone utilizar una herramienta open source para el monitoreo y control de red.
	13.1.3	Segregación en redes	No Aplica	-	La decisión es del Ministerio de Cultura, canalizada por la Dirección desconcentrada de cultura de Lambayeque.
	13.2	**Transferencia de Información**			
	13.2.1	Políticas y procedimientos para la transferencia de información	Aplica	La institución no cuenta con políticas de transferencia de información.	Se debe establecer la documentación para definir la transferencia de información tanto externa como interna, debidamente autorizada, se establece en la política de transferencia de información.
	13.2.2	Acuerdos en la transferencia de información	Aplica	La institución no cuenta con acuerdos de transferencia de información.	Se debe establecer la categoría de la información (confidencial. Sensible o publica), esto se define y establece en la política de transferencia de información.
	13.2.3	Mensajería electrónica	Aplica	La mensajería electrónica es la principal fuente de información para la institución y puede ser vulnerada.	Se establece el uso correcto del correo electrónico en la política de transferencia de información.
	13.2.4	Acuerdos de confidencialidad o no-revelación	Aplica	No existen acuerdos de confidencialidad o no revelación.	La institución establece acuerdo de confidencialidad que debe ser firmado por todos los colaboradores.
14. Adquisición, desarrollo y mantenimiento de sistemas	**14.1**	**Requerimientos de Seguridad de Sistemas de Información**			
	14.1.1	Análisis y especificación de requerimientos de seguridad	Aplica	No se han determinado pautas con respecto a seguridad de sistemas de información	Las políticas deben contener pautas sobre las especificaciones técnicas de los software instalados o aplicaciones en uso.
	14.1.2	Aseguramiento de servicios de aplicación en redes públicas	Aplica	No se han determinado pautas con respecto a seguridad de sistemas de información	Las políticas deben considerar el control de acceso de redes públicas para los equipos de la institución.
	14.1.3	Protección de transacciones de servicios de aplicación	No Aplica	-	El alcance del SGSI no considera estas actividades.
	14.2	**Seguridad en el Proceso de Desarrollo y Soporte**			
	14.2.1	Política de desarrollo seguro	No Aplica	-	El alcance del SGSI no considera estas actividades.

	14.2.2	Procedimientos de control de cambios	No Aplica	-	El alcance del SGSI no considera estas actividades.
	14.2.3	Revisión técnica de aplicaciones después de cambios a la plataforma operativa	No Aplica	-	El alcance del SGSI no considera estas actividades.
	14.2.4	Restricción de cambios a paquetes de software	No Aplica	-	El alcance del SGSI no considera estas actividades.
	14.2.5	Procedimientos de desarrollo de sistemas	No Aplica	-	El alcance del SGSI no considera estas actividades.
	14.2.6	Entorno de desarrollo seguro	No Aplica	-	El alcance del SGSI no considera estas actividades.
	14.2.7	Desarrollo tercerizado	No Aplica	-	El alcance del SGSI no considera estas actividades.
	14.2.8	Pruebas de seguridad del sistema	No Aplica	-	El alcance del SGSI no considera estas actividades.
	14.2.9	Pruebas de aceptación del sistema	No Aplica	-	El alcance del SGSI no considera estas actividades.
	14.3	**Datos de Prueba**			
	14.3.1	Protección de datos de prueba	No Aplica	-	El alcance del SGSI no considera estas actividades.
15. Relaciones con los proveedores	**15.1**	**Seguridad en Relaciones con el Proveedor**			
	15.1.1	Política de Seguridad de la Información para relaciones con proveedores	No Aplica	-	El alcance del SGSI no considera estas actividades.
	15.1.2	Atención de tópicos de seguridad dentro de los acuerdos con proveedores	No Aplica	-	El alcance del SGSI no considera estas actividades.
	15.1.3	Cadena de suministros de TIC	No Aplica	-	La decisión es del Ministerio de Cultura, canalizada por la Dirección desconcentrada de cultura de Lambayeque.
	15.2	**Gestión de Entrega de Servicios de Proveedor**			
	15.2.1	Monitoreo y revisión de servicios de proveedor	No Aplica	-	El alcance del SGSI no considera estas actividades.
	15.2.2	Gestión de cambios a servicios de proveedor	No Aplica	-	La decisión es del Ministerio de Cultura, canalizada por la Dirección desconcentrada de cultura de Lambayeque.
16. Gestión de incidencias de seguridad de la información	**16.1**	**Gestión de Incidentes de Seguridad de la Información y Mejoras**			
	16.1.1	Responsabilidades y Procedimientos	Aplica	Existe el proceso de gestión de incidentes pero la información no es clara para los usuario por lo tanto no usan el servicio.	Se determina el proceso de gestión de incidentes mediante la política de gestión de incidentes.

	16.1.2	Reporte de eventos de Seguridad de la Información	Aplica	Existe el proceso de gestión de incidentes pero la información no es clara para los usuario por lo tanto no usan el servicio.	Se determina el proceso de gestión de incidentes mediante la política de gestión de incidentes.
	16.1.3	Reporte de debilidades de Seguridad de la Información	Aplica	Existe el proceso de gestión de incidentes pero la información no es clara para los usuario por lo tanto no usan el servicio.	Se determina el proceso de gestión de incidentes mediante la política de gestión de incidentes.
	16.1.4	Valoración y decisión de eventos de Seguridad de la Información	Aplica	Existe el proceso de gestión de incidentes pero la información no es clara para los usuario por lo tanto no usan el servicio.	Se determina el proceso de gestión de incidentes mediante la política de gestión de incidentes.
	16.1.5	Respuesta a incidentes de Seguridad de la Información	Aplica	Existe el proceso de gestión de incidentes pero la información no es clara para los usuario por lo tanto no usan el servicio.	Se plantea además el uso de unas herramientas open source para apoyar la gestión de incidentes desde la institución y luego los incidentes reportarlos a la sede central para su solución.
	16.1.6	Aprendizaje de incidentes de Seguridad de la Información	Aplica	Existe el proceso de gestión de incidentes pero la información no es clara para los usuario por lo tanto no usan el servicio.	Se determina el aprendizaje en la propuesta de política de gestión de incidentes.
	16.1.7	Colección de evidencia	Aplica	Existe el proceso de gestión de incidentes pero la información no es clara para los usuario por lo tanto no usan el servicio.	Se propone realizar un historial con las soluciones decididas para cada incidente de modo que se pueden decidir acciones ya tomadas o mejorarlas.
17. Aspectos de Seguridad de la información para la gestión de continuidad del negocio	**17.1**	**Seguridad de la Información en la Continuidad**			
	17.1.1	Planeación de Seguridad de la Información en la continuidad	Aplica	No existe un plan de continuidad en la institución.	La gestión de la continuidad es necesaria para mantener los sistemas de información operativos lo más antes posible, se establece en la política de continuidad.
	17.1.2	Implementación de Seguridad de la Información en la continuidad	Aplica	No existe un plan de continuidad en la institución.	La gestión de la continuidad es necesaria para mantener los sistemas de información operativos lo más antes posible, se establece en la política de continuidad.
	17.1.3	Verificación, revisión y evaluación de Seguridad de la Información en la continuidad	Aplica	No existe un plan de continuidad en la institución.	La gestión de la continuidad es necesaria para mantener los sistemas de información operativos lo más antes posible, se establece en la política de continuidad.
	17.2	**Redundancias**			

	17.2.1	Disponibilidad de instalaciones de procesamiento de información	No Aplica	-	La decisión es del Ministerio de Cultura, canalizada por la Dirección desconcentrada de cultura de Lambayeque.
18. Cumplimiento	**18.1**	**Revisiones de Seguridad de la Información**			
	18.1.1	Revisión independiente de Seguridad de la Información	Aplica	No existe un plan de seguridad de la información	Se establece un plan de mejora continua del SGSI.
	18.1.2	Cumplimiento con políticas y estándares de seguridad	Aplica	No existe un plan de seguridad de la información	Se establece un plan de mejora continua del SGSI.
	18.1.3	Inspección de cumplimiento técnico	Aplica	No existe un plan de seguridad de la información	Se establece un plan de mejora continua del SGSI.
	18.1.4	Privacidad y protección de información personal identificable	Aplica	La institución cumple con los requerimientos legales y contractuales	Se determina en las políticas el cumplimiento de los requerimientos necesarios.
	18.1.5	Regulación de controles criptográficos	No Aplica	-	El alcance del SGSI no considera estas actividades.
	18.2	**Cumplimiento con Requerimientos Legales y Contractuales**			
	18.2.1	Identificación de legislación aplicable y requerimientos contractuales	Aplica	La institución cumple con los requerimientos legales y contractuales	Se determina en las políticas el cumplimiento de los requerimientos necesarios.
	18.2.2	Derechos de propiedad intelectual (IPR)	Aplica	La institución cumple con los requerimientos legales y contractuales	Se determina en las políticas el cumplimiento de los requerimientos necesarios.
	18.2.3	Protección de información documentada	Aplica	La institución cumple con los requerimientos legales y contractuales	Se determina en las políticas el cumplimiento de los requerimientos necesarios.

Cuadro 20: Declaración de aplicabilidad

Fuente: Elaboración propia

5.2.4.6 Plan de Tratamiento de Riesgos

Como resultado de los controles seleccionados, se ha elaborado el siguiente cuadro 21 “Plan de tratamiento de riesgos”, en el que se definen las medidas que se implementaran y las acciones inmediatas para su funcionamiento, en el plan se han elegido 43 controles aplicables para su ejecución:

CONTROLES	DESCRIPCIÓN DE CONTROLES	RIESGOS	TIPO DE MEDIDA	MEDIDAS POR IMPLEMENTAR	PLANES DE ACCIÓN	CÓDIGO	DOCUMENTO / APLICACIÓN
7.2.2	Concientización, educación y capacitación en materia de seguridad de la información.	R16,R21,R22 ,R23,R48	Disuasoria	Sensibilización y capacitación	Presentación en auditorio de la institución, sensibilización con afiches y folletos, Publicidad en computadoras, capacitaciones	SGSI_002	Política del SGSI
						SGSI_013	Plan de sensibilización y capacitación
7.2.3	Proceso disciplinario	R17,R22,R23 ,R51,R52	Disuasoria	Elaboración de política del SGSI, declaraciones y compromisos.	Firmas de declaraciones y compromisos, inducción de políticas del SGSI.	SGSI_002	Política del SGSI
						SGSI_A01	Acta de reunión
						SGSI_A02	Declaración de aceptación de documentos del SGSI
						SGSI_A03	Declaración de confidencialidad
						SGSI_A04	Formato de inducción
8.1.1	Inventario de activos	R17,R51,R52	Preventiva	Adquisición de Software open source	Instalación de Software open source	AP01	OCS Inventory
8.1.2	Propiedad de los activos	R17,R51,R52	Preventiva	Elaboración de política de	Firmar documentación e implementar política.	SGSI_006	Política de gestión de activos de la información

				gestión de activos del SGSI.			
8.1.3	Uso aceptable de los activos	R12,R16,R29,R48	Preventiva	Elaboración de política de gestión de activos del SGSI.	Firmar documentación e implementar política.	SGSI_006	Política de gestión de activos de la información
8.3.1	Gestión de medios extraíbles	R12,R70,R17	Preventiva	Elaboración de política de gestión de activos del SGSI.	Firmar documentación e implementar política.	SGSI_006	Política de gestión de activos de la información
8.3.3	Transferencia de medios físicos	R09	Preventiva	Elaboración de política de gestión de activos del SGSI.	Firmar documentación e implementar política.	SGSI_006	Política de gestión de activos de la información
9.1.1	Política de control de acceso	R16,R29,R48,R62,R66,R70	Mitigación	Elaboración de política de control de acceso del SGSI.	Firma de documentación e implementación de política.	SGSI_007	Política de control de acceso del SGSI
9.1.2	Acceso a redes y servicios de red	R19,R48,R62,R62,R66	Protección	Elaboración de política, propuesta de cableado estructurado	Implementación de cableado estructurado.	SGSI_009	Procedimientos operativos para TI
9.2.1	Gestión de altas/bajas en el registro de usuarios	R22,R34,R62,R66	Mitigación	Elaboración de política de control de acceso del SGSI.	Firma de documentación e implementación de política.	SGSI_007	Política de control de acceso del SGSI
9.2.2	Gestión de los derechos de acceso asignados a usuarios	R30,R33,R34,R35,R48,R49,R50,R54	Mitigación	Elaboración de política de control de acceso del SGSI.	Firma de documentación e implementación de política.	SGSI_007	Política de control de acceso del SGSI
9.2.3	Gestión de derechos de acceso privilegiados	R34,R62,R66,R62	Mitigación	Elaboración de política de control de acceso del SGSI.	Firma de documentación e implementación de política.	SGSI_007	Política de control de acceso del SGSI

9.2.4	Gestión de la información de autenticación secreta de los usuarios	R48,R60	Mitigación	Elaboración de política de control de acceso del SGSI.	Firma de documentación e implementación de política.	SGSI_007	Política de control de acceso del SGSI
9.2.5	Revisión de derechos de acceso de usuario	R48	Mitigación	Elaboración de política de control de acceso del SGSI.	Firma de documentación e implementación de política.	SGSI_007	Política de control de acceso del SGSI
9.2.6	Eliminación o ajuste de los derechos de acceso	R48	Mitigación	Elaboración de política de control de acceso del SGSI.	Firma de documentación e implementación de política.	SGSI_007	Política de control de acceso del SGSI
9.3.1	Uso de la información confidencial para la autenticación	R30,R35,R54	Disuasoria	Elaboración de declaración de confidencialidad	Firma de declaración	SGSI_A03	Declaración de confidencialidad
9.4.1	Restricción de acceso a la información	R60,R62,R66,R70	Mitigación	Elaboración de política de control de acceso del SGSI.	Firma de documentación e implementación de política.	SGSI_007	Política de control de acceso del SGSI
9.4.3	Sistema de gestión de contraseñas	R30,R35,R54	Mitigación	Elaboración de política de control de acceso del SGSI.	Firma de documentación e implementación de política.	SGSI_007	Política de control de acceso del SGSI
9.4.4	Uso de programas de utilidad privilegiada	R32,R60,R70	Mitigación	Elaboración de política de control de acceso del SGSI.	Firma de documentación e implementación de política.	SGSI_007	Política de control de acceso del SGSI
10.1.2	Gestión de claves	R29	Mitigación	Elaboración de política de control de acceso del SGSI.	Firma de documentación e implementación de política.	SGSI_007	Política de control de acceso del SGSI
11.1.1	Perímetro de seguridad física	R17,R21,R23,R34,R50,R51,R52,R55,R57	Preventiva	Elaboración de procedimiento zonas seguras	Firma e implementación de procedimiento.	SGSI_008	Procedimiento para trabajo en zonas seguras

11.1.2	Controles físicos de entrada	R16,R17,R21,R23,R34,R51,R52,R56,R55,R57	Preventiva	Elaboración de procedimiento zonas seguras	Firma e implementación de procedimiento.	SGSI_008	Procedimiento para trabajo en zonas seguras
11.1.3	Asegurar oficinas, habitaciones e instalaciones	R16,R21,R23,R34,R50,R51,R52,R55,R56,R57	Preventiva	Elaboración de procedimiento zonas seguras, validación del sistema de vigilancia y monitoreo	Firma e implementación de procedimiento, contrato de un personal externo para validación y mantenimiento del sistema de vigilancia.	SGSI_008	Procedimiento para trabajo en zonas seguras
11.1.4	Protección contra las amenazas externas y ambientales	R71	Preventiva	Elaboración de procedimiento zonas seguras	Firma e implementación de procedimiento.	SGSI_008	Procedimiento para trabajo en zonas seguras
11.1.5	Trabajo en áreas seguras	R17,R21,R23,R51,R52	Preventiva	Elaboración de procedimiento zonas seguras, validación del sistema de vigilancia y monitoreo	Firma e implementación de procedimiento, contrato de un personal externo para validación y mantenimiento del sistema de vigilancia.	SGSI_008	Procedimiento para trabajo en zonas seguras
11.1.6	Zonas de entrega y carga	R09	Preventiva	Elaboración de procedimiento zonas seguras	Firma e implementación de procedimiento.	SGSI_008	Procedimiento para trabajo en zonas seguras
11.2.1	Ubicación y protección del equipo	R17,R49,R69	Preventiva	Elaboración de procedimiento zonas seguras	Firma e implementación de procedimiento.	SGSI_008	Procedimiento para trabajo en zonas seguras
11.2.2	Instalaciones de suministro	R71	Preventiva	Elaboración de procedimiento zonas seguras	Firma e implementación de procedimiento.	SGSI_008	Procedimiento para trabajo en zonas seguras
11.2.4	Mantenimiento de equipo	R69,R70	Preventiva	Elaboración de procedimiento TI	Firma e implementación de procedimiento.	SGSI_009	Procedimientos operativos para TI

11.2.6	Seguridad de equipos y activos fuera de las instalaciones	R17	Preventiva	Elaboración de procedimiento zonas seguras	Firma e implementación de procedimiento.	SGSI_008	Procedimiento para trabajo en zonas seguras
11.2.8	Equipo de usuario desatendido	R69, R70	Protección	Elaboración de procedimiento TI	Firma e implementación de procedimiento.	SGSI_009	Procedimientos operativos para TI
12.2.1	Controles contra el código malicioso	R12,R70	Protección	Adquisición de licencia software propietario	Instalación de software en todos los equipos	AP02	ESET NOD
12.3.1	Copia de seguridad de la información	R09, R33, R16	Protección	Adquisición de Software open source	Instalación y uso de Software open source por comité de seguridad	AP03	Open KM
			Protección	Elaboración de procedimiento TI	Firma e implementación de procedimiento.	SGSI_009	Procedimientos operativos para TI
13.1.1	Controles de red	R29,R30,R33,R74	Protección	Elaboración de política, propuesta de cableado estructurado	Implementación de cableado estructurado.	SGSI_009	Procedimientos operativos para TI
13.1.2	Seguridad de los servicios de red	R19,R29,R30,R33,R49,R62,R74,	Protección	Elaboración de política, propuesta de cableado estructurado	Implementación de cableado estructurado.	SGSI_009	Procedimientos operativos para TI
13.2.1	Políticas y procedimientos de transferencia de información	R09,R35,R48,R54,R55,R56	Mitigación	Elaboración de política de transferencia de información.	Firmar documentación e implementar política.	SGSI_010	Política de transferencia de la información
13.2.2	Acuerdos sobre transferencia de información	R19,R47,R48,R54,R55,R56	Mitigación	Elaboración de política de transferencia de información.	Firmar documentación e implementar política.	SGSI_010	Política de transferencia de la información

13.2.3	Mensajería electrónica	R19,R35,R54,	Mitigación	Elaboración de política de transferencia de información.	Firmar documentación e implementar política.	SGSI_010	Política de transferencia de la información
13.2.4	Acuerdos de confidencialidad o no divulgación	R22,R47,R48,R49,R50,R54,R55,R56	Disuasoria	Elaboración de declaración de confidencialidad	Firma de declaración	SGSI_A03	Declaración de confidencialidad
16.1.5	Respuesta a incidentes de seguridad de la información	R62,R71	Preventiva	Adquisición de Software open source	Instalación y uso de Software open source por comité de seguridad	AP04	OS Ticket
			Preventiva	Elaboración de procedimiento gestión de incidentes	Firma e implementación de procedimiento.	SGSI_011	Procedimiento para la gestión de incidentes
17.1.1	Planificación de la continuidad de la seguridad de la información	R62,R66,R69,R70,R71	Preventiva	Elaboración de política de continuidad.	Firmar documentación e implementar política.	SGSI_012	Política de la continuidad del negocio
18.1.2	Derechos de propiedad intelectual	R29	Disuasoria	Elaboración de política del SGSI, declaraciones y compromisos.	Firmar documentación e implementar política.	SGSI_002	Política del SGSI
18.1.4	Privacidad y protección de la información de identificación personal	R29, R34	Disuasoria	Elaboración de política del SGSI, declaraciones y compromisos.	Firmar documentación e implementar política.	SGSI_002	Política del SGSI

Cuadro 21: Plan de tratamiento de riesgos

Fuente: Elaboración propia

ETAPA III: IMPLEMENTACIÓN DEL SGSI: FASE DO

5.3.1 Acuerdos para la implementación del SGSI

5.3.1.1 Comité de Seguridad

Según lo determinado en las políticas del sistema de gestión de seguridad de la información de la Dirección desconcentrada de cultura de Lambayeque, se ha definido la estructura como el Cuadro 22:

COMITÉ DE SEGURIDAD DE LA INFORMACIÓN
Director de DDC Lambayeque
Administrador DDC Lambayeque
Encargado de Of. Patrimonio Arqueológico

Cuadro 22: Comité de Seguridad de la información.

Fuente: Elaboración propia

5.3.1.2 Roles y Responsabilidades

Para el cumplimiento de las funciones del SGSI de la institución, se han determinado las siguientes responsabilidades generales:

- Director del comité de seguridad: Aprobar la política de seguridad y sus futuras modificación con el visto bueno del Comité de Seguridad de la información de la Dirección desconcentrada de cultura de Lambayeque.

- Comité de Gestión de Seguridad de la información: Dirigir, coordinar y supervisar la implementación y funcionamiento de la seguridad de la información en la Dirección desconcentrada de Cultura.

- Oficial de Seguridad de la Información: Supervisar el cumplimiento de la presente política en coordinación con las oficinas de la institución.

- Propietario de Seguridad de la información: Determinar los accesos y autorizaciones a las peticiones sobre las distintas formas de utilizar la información.

- Usuario: Ser responsables del uso de los activos de información a los que tiene acceso autorizado.

5.3.1.3 Matriz de Roles y Responsabilidades

Se han definido los siguientes roles y responsabilidades del comité de Seguridad de la información, en el cuadro 23:

Directivo	Rol	Responsabilidades
Director de DDC Lambayeque	Director de Comité de Seguridad	Presidir el comité de seguridad de la información
Administrador DDC Lambayeque	Oficial de seguridad	Definir, revisar y actualizar las políticas y procedimientos definidos en el SGSI.
		Mantener actualizado el inventario de activos de la información.
		Promover en la institución una cultura que fomente la seguridad y el uso aceptable de todos los activos de la información.
		Realizar capacitaciones de concientización y educación en seguridad de la información.
		Detectar nuevas amenazas y vulnerabilidades.
Encargado de Of. Patrimonio Arqueológico	Propietario de la información	Tener una matriz identificada de los perfiles de usuario.
		Supervisar el correcto acceso de los usuarios.
		Canalizar y autorizar todos los permisos de autenticación de usuario

Cuadro 23: Matriz de responsabilidades del comité

Fuente: Elaboración propia

5.3.1.4 Procedimientos:

Cumpliendo con la norma ISO 27001 y los documentos obligatorios para implementar en un sistema de gestión de la seguridad, se propone implementar en la institución los siguientes procedimientos:

5.3.1.4.1 Metodología para la gestión de riesgos

El procedimiento "Metodología para la gestión de riesgos" se detalla en el Anexo 15: Metodología de gestión de riesgos para SGSI, considerando principalmente las fases de la gestión de riesgos:

- Fase 1: Análisis de Riesgos
- Fase 2: Tratamiento de Riesgos
- Fase 3: Gestión de Riesgos

5.3.1.4.2 Declaración de Aplicabilidad

En el documento se detalla la declaración de aplicabilidad para la institución, se presenta una muestra en el anexo 16: Declaración de aplicabilidad del SGSI.

5.3.1.4.3 Plan de Tratamiento de riesgos

En el documento se detalla el tratamiento de riesgos según la metodología MEHARI y el plan del tratamiento derivado de los controles de la ISO 27002, detallado en el anexo 17: Plan de tratamiento de riesgos del SGSI, considerando los siguientes puntos:

- Tratamiento de riesgos
  - Factores de reducción de la probabilidad
  - Factores de reducción del impacto
- Plan tratamiento de riesgos

5.3.1.4.4 Procedimiento de Gestión de Activos

Se detalla el anexo 18: Procedimiento de Gestión de activos considerando lo siguiente:

- Definiciones
- Políticas de uso aceptable
- Propiedad de los activos
- Políticas de gestión de medios extraíbles
- Políticas de transferencia de medios físicos

5.3.1.4.5 Política de Control de Acceso

Se detalla en el anexo 19: El procedimiento "Control de Acceso", considerando principalmente la gestión de accesos:

- Administración de usuarios
- Gestión de contraseñas
- Controles de acceso de red
- Controles de acceso a aplicaciones

5.3.1.4.6 Procedimiento Trabajo en Zonas Seguras

En el Anexo 20: procedimiento "Trabajo en Zonas Seguras" se detalla lo siguiente:

- Lista de zonas seguras
- Derechos de acceso
- Controles de ingreso
- Ubicación y protección del equipo

5.3.1.4.7 Procedimientos operativos para la gestión de TI

El anexo 21: "Procedimientos operativos para la gestión de TI", considera los siguientes procedimientos operativos:

- Documentación operativa
- Control de Cambios
- Uso de la Tecnología
- Servicios de red
- Servicios Web
- Software
- Equipos de cómputo móviles
- Control de código Malicioso
- Telefonía

5.3.1.4.8 Política de Transferencia de la Información

El anexo 22: Política "Transferencia de la información" se consideran las siguientes políticas:

- Canales de comunicación electrónica
- Políticas de uso del correo electrónico

5.3.1.4.9 Procedimiento de Gestión de incidentes

Se ha definido en el anexo 23: Procedimiento "Gestión de incidentes", considerando las fases para la gestión de incidentes:

- Registro de incidentes
- Clasificación de incidentes
- Escalamiento
- Respuesta inmediata

5.3.4.10 Procedimiento de Continuidad del Negocio

Se ha definido este documento en el Anexo 24: Procedimiento de continuidad del negocio, considerando las siguientes fases:

- Entendimiento de la organización y el contexto.
- Planificación.
- Soporte
- Información documentada
- Determinación y estrategia de continuidad
- Desarrollo e implementación de procedimientos de continuidad
- Pruebas y actualización
- Evaluación del desempeño

5.3.4.11 Plan de Sensibilización y Capacitación

Este plan determina la necesidad de trasmitir, concientizar y entrenar a los colaboradores de la institución con respecto al sistema de seguridad de la información por implementar en la institución considerando una etapa previa de sensibilización en la que se muestran los cambios necesarios en materia de seguridad de la información a aplicar en la organización para cumplir con las políticas establecidas, utilizando afiches, folletos y comunicación a través de las tecnologías.

Además se considera un plan de capacitación dividido en etapas y según las funciones de los colaboradores dentro del sistema de gestión de la seguridad para el correcto desarrollo y respaldo de la seguridad de la información en la Dirección desconcentrada de Lambayeque. Anexo 25: Plan de sensibilización y capacitación.

5.3.4.5 Documentos Adicionales

5.3.4.5.1 Acta de reunión

El acta de reunión define los puntos importantes a tratar con las personas involucradas en el sistema de gestión de seguridad de la información de la institución, en el anexo 26: Acta de reunión del comité, se muestra un ejemplo de lo que sería el acta de la primera reunión.

5.3.4.5.2 Declaración de aceptación

El objetivo de este documento es que los colaboradores tengan conocimiento del sistema de gestión de seguridad de la información y a través de este compromiso exigir el cumplimiento de los documentos del sistema de gestión de seguridad de la información en la institución. Anexo 27: Declaración de aceptación.

5.3.4.5.3 Declaración de confidencialidad

El objetivo de este documento es que los colaboradores acepten el compromiso de no divulgar la información obtenida o recibida a lo largo de su relación laboral con la institución y aún después de finalizar dicha relación, con la finalidad de mantener la confidencialidad de los datos. Anexo 28: Declaración de confidencialidad.

5.3.4.5.4 Formato de registro de inducción

El objetivo de este formato es hacer el seguimiento a la asistencia de las inducciones que se desarrollaran en la institución con la finalidad de dar a conocer el sistema de gestión de la seguridad de la información, así como todo lo relacionado a buenas prácticas y controles por aplicar para disminuir las vulnerabilidades de la información. Anexo 29: Registro de inducción.

5.3.2 Ejecución de los planes de Acción

5.3.2.1 Cronograma de actividades para la implementación del SGSI

Después de tener claros los planes de acción que se aplicarán para que el sistema de gestión de seguridad de la información de la Dirección desconcentrada de Cultura de Lambayeque, sea necesario realizar un consolidado de las acciones a tomar realizando un cronograma, se propone en el cuadro 24:

Actividades	Inicio	Fin
Creación de comité de seguridad	15.05.2017	15.05.2017
Definición de la situación actual	22.05.2017	24.05.2017
Mapeo de los procesos de la institución	25.05.2017	02.06.2017
Decisión de uso de metodología	05.06.2017	09.06.2017
Inventario de activos	12.06.2017	14.06.2017
Valorización de activos	15.06.2017	16.06.2017
Análisis e identificación de riesgos	19.06.2017	22.06.2017
Definición de controles	23.06.2017	27.06.2017
Tratamiento de riesgos	28.06.2017	30.06.2017
Generación de políticas y procedimientos	03.07.2017	07.07.2017
Implementación de herramientas de soporte	10.07.2017	21.07.2017
Inicio de plan de capacitación para comité	24.07.2017	02.08.2017
Presentación de SGSI	04.08.2017	04.08.2017
Inicio del plan de sensibilización	04.08.2017	15.09.2017
Inicio de plan de capacitación	08.08.2017	15.08.2017
1° Revisión del funcionamiento	18.09.2017	18.09.2017
2° etapa de plan de capacitación	09.10.2017	13.10.2017

Cuadro 24: Cronograma de actividades para la implementación del SGSI
Fuente: Elaboración propia

5.3.2.2 Automatización de los controles con herramientas Open source

Tomando en cuenta que el sistema de seguridad de la información ha sido implementado y puesto en funcionamiento, se considera en la propuesta controles de seguridad informática automatizables con herramientas open source.

Siguiendo el modelo para la Gestión automatizada e integrada de controles de Seguridad informática (Montesino Perurena, Baluja García, & Porvén Rubier, 2013), se toma en cuenta algunas de sus características:

- 10 macro-controles que pueden ser automatizados.
- La automatización es aplicada a acciones de operación, monitorización y revisión de los 10 macro-controles.

5.3.2.2.1 Definición de los Macro-Controles:

Los controles automatizables según (Montesino Perurena, Baluja García, & Porvén Rubier, 2013) son los siguientes:

1. Inventario de Activos: Mantener un inventario actualizado de todos los activos informáticos de la institución.
2. Gestión de usuarios: Garantizar la correcta activación, modificación y eliminación de cuentas de usuario.
3. Gestión de trazas (cifrado) : Almacenar y conservar por el tiempo establecido, en una localización centralizada, las trazas de las aplicaciones, sistemas operativos y diferentes dispositivos, donde se registre la actividad de los usuarios, errores, conexiones de red y otros eventos de seguridad en general.
4. Monitoreo de los sistemas: Realizar un monitoreo constante de los sistemas para detectar ataques informáticos, falta de disponibilidad de las aplicaciones y modificaciones a la información.

5. Protección contra programas malignos: Emplear mecanismos de protección contra programas malignos que se encuentren constantemente actualizados, para detectar y erradicar código malicioso.
6. Detección de vulnerabilidades: Detectar y mitigar las vulnerabilidades presentes en los sistemas.
7. Configuraciones de seguridad y cumplimiento de políticas: Garantizar que los sistemas operativos, aplicaciones y demás dispositivos posean configuraciones seguras, acorde a las políticas definidas por la institución.
8. Respaldo informático: Realizar frecuentemente copias de respaldo de la información y los sistemas, que posibiliten la recuperación ante la ocurrencia de algún incidente.
9. Seguridad física: Proteger adecuadamente los locales y las tecnologías mediante sistemas de control de acceso físico, respaldo eléctrico, protección y sistemas de alarmas.
10. Gestión de incidentes: Establecer un sistema de gestión de incidentes de seguridad de la información que incluya la detección, análisis, contención, solución y recuperación de los incidentes.

5.3.2.2.2 Análisis de los Macro-Controles y herramientas Open Source:

A continuación en el **Cuadro 25** se detallan las herramientas Open Source que pueden ser el soporte de un sistema de gestión de seguridad de la información, considerando los 10 macro controles y los controles de la ISO 27002 a los que agrupa:

Macro Control	Controles ISO 27002	Herramienta Open Source
Gestión de activos	8.1.1, 12.1.2	OCS Inventory
Gestión de usuarios	9.2.6, 9.2.3, 9.2.4, 10.1.2, 9.4.2, 9.4.3	ApacheDS
Gestión de trazas	12.4.1 12.4.2 12.4.3	Mantis Bug Tracker
Monitoreo de Sistemas	12.1.3, 13.1.1, 8.3.1, 13.2.3, 14.1.2, 12.4.1, 12.4.3	Nagios
Protección contra Programas Malignos	12.2.1, 13.2.3	ClamWin
Detección de vulnerabilidades	12.6.1	Open Vas
Configuración de seguridad	12.1.2, 13.1.1, 15.2.2	Open SCAP
Respaldo informático	12.3.1, 14.1.3	Open KM
Seguridad física	11.1.2, 11.2.2	Oshozi
Gestión de incidentes	16.1.2	OS Ticket

Cuadro 25 Herramientas Open Source para macro controles automatizables

Fuente: Elaboración propia

En el sistema de gestión de la información para la dirección desconcentrada de cultura de Lambayeque se están considerando 3 herramientas de las mencionadas anteriormente, en el Cuadro 26 se detalla porque son o no son aplicables en la institución:

Macro Control	Herramienta Open Source	Aplicable en la institución	Justificación
Gestión de activos	OCS Inventory	Si	La herramienta es necesaria para mantener actualizado el inventario de activos de la información.
Gestión de usuarios	ApacheDS	No	Los usuarios son manejados con Active Directory desde la oficina informática en Lima.
Gestión de trazas	Mantis Bug Tracker	No	La institución no tiene funciones de creación de software, por lo tanto este control es innecesario.
Monitoreo de Sistemas	Nagios	No	El monitoreo de sistemas se realiza desde la oficina informática en Lima.
Protección contra Programas Malignos	ClamWin	No	En la propuesta, se está adquiriendo software propietario ESET por políticas de la institución.
Detección de vulnerabilidades	Open Vas	No	La institución no cuenta con servidores por lo que no es necesario este control.
Configuración de seguridad	Open SCAP	No	La configuración de seguridad se realiza desde la oficina informática en Lima.
Respaldo informático	Open KM	Si	Es importante para el respaldo y seguimiento de los documentos en la institución.
Seguridad física	Oshozi	No	Siendo una institución de pequeña envergadura, la seguridad física se manejará con políticas y procedimientos.
Gestión de incidentes	OS Ticket	Si	La herramienta es necesaria para la atención de incidentes en la institución.

Cuadro 26: Herramientas Open Source aplicables para la institución

Fuente: Elaboración propia

5.3.2.2.3 Aplicación de herramientas Open Source

OCS Inventory:

La herramienta open source brinda un soporte para mantener actualizado el inventario de activos informáticos y aplicaciones instaladas, para instalarlo es flexible y compatible con plataformas Linux y Windows, cuenta con un servidor web XAMPP (Apache y MySQL), el que se puede configurar desde la misma aplicación de servidor o instalarlo manualmente y además con una aplicaci

ón agente que se instala en las computadoras que serán monitoreadas.

Es importante tener Apache y MySql correctamente configuradas en el equipo de cómputo que será el monitor del inventario para que la aplicación de los agentes funcione, en este caso el usuario a cargo de este proceso será el CISO de la Dirección Desconcentrada de Cultura de Lambayeque.

Cabe resaltar que OCS Inventory es considerada una aplicación top en la gestión de inventarios de activos.

La documentación con respecto a la instalación de servidor y agente de OCS Inventory se encuentra en el Anexo 32: Instalación y configuración OCS Inventory.

Open KM

La herramienta open source, sirve para la gestión documental para administrar contenido y el flujo de envío y recepción de documentación sea más eficiente.

En su versión Community edition es soportada por Java JDK, se configura desde símbolo del sistema para instalar el servidor web tomcat y descargar la aplicación Open KM.

Después se instala mysql con Workbench para la creación de la base de datos con los scripts de la herramienta.

El ingreso a través de localhost permite al administrador la configuración de otros usuarios según perfiles y la gestión de documentos: añadir, buscar,

derivar documento, enviar correos entre otros permite consolidar la información y realizar seguimiento continuo.

La documentación con respecto a la instalación de la herramienta se encuentra en el Anexo 33: Instalación y configuración OpenKM.

OS Ticket

La herramienta open source brinda soporte para la gestión de tickets, una solución integral que permite la configuración de un portal con un nombre propio para la institución, la selección de los agentes que brindaran el soporte a las incidencias, una creación de grupos de usuario, configuración de correos de envío con notificaciones automáticas, tipos de incidentes, soluciones específicas para cada tipo de incidente.

El agente en este caso el oficial de Seguridad creará los usuarios que podrán acceder considerando el correo corporativo al que llegarán las notificaciones vinculadas a su número de caso utilizando un correo de soporte de incidentes propio de la herramienta.

Del lado cliente, la creación de tickets es bastante sencilla de generar y hacer seguimiento, así como de cerrar el caso si fue atendido y solucionado, puede editar, comentar y hacer seguimiento.

La elección de la herramienta permite tener un consolidado de los incidentes que ocurren en la institución, contar con un listado de posibles soluciones ante incidentes futuros, la disponibilidad de un servicio que antes no era atendido, la solución inmediata a consultas y requerimientos y finalmente el constante seguimiento a los activos de información.

La documentación con respecto a la configuración de los agentes y usuarios de OS Ticket se encuentra en el Anexo 34: Instalación y configuración OS Ticket.

5.3.3 Sensibilización y formación

Esta importante etapa inicia con la sensibilización, con la finalidad que el personal esté involucrado con la implementación de la seguridad de la información, cambiando conductas habituales por buenas prácticas, es importante considerar que el control es necesario dentro de las instituciones para generar cambios y mejoras.

Se utilizaran las siguientes herramientas:

- Reuniones: Se convocará a reunión para la presentación del sistema de gestión de seguridad de la información de la institución en el auditorio principal.
- Folletos: Se entregarán en la presentación del sistema de gestión de la seguridad con todo el personal de institución presente.
- Afiches: Se exhibirán afiches de manera interna y áreas comunes de los colaboradores.
- Uso de tecnología: Se realizará una campaña interna a través de los fondos de pantalla.

Se realizaran campañas de sensibilización para toda la institución, las que abarcaran los siguientes temas:

- Contraseñas seguras: Publicidad con mensajes con mensajes alusivos a cuidar la información personal, contraseñas, equipos de cómputo y usuarios.
- Internet seguro: Publicidad con mensajes alusivos a cuidar los accesos de internet y correos electrónicos de usuarios no conocidos.
- Sesiones: Publicidad con respecto a inicio y cierre de sesión, buenas prácticas de accesos al sistema y equipos de cómputo.

En el caso de la formación, se han considerado dos tipos de niveles de instrucción, el nivel básico para el personal general indicado en el Cuadro 27 y en el Cuadro 28 se indica el nivel intermedio para el

comité de seguridad, quienes deben ser los principales gestores para que el sistema de seguridad de la información funcione.

Módulos	Temas	Grupo 1	Grupo 2
I	Políticas claves para la Seguridad de la información	08.08.2017	09.08.2017
	Riesgos de la información		
II	Gestión de Activos	10.08.2017	11.08.2017
	Trabajo en Áreas seguras		
	Transferencia de la información		
III	Gestión de incidentes	14.08.2017	15.08.2017

Cuadro 27: Capacitación SGSI Nivel Básico para la institución

Fuente: Elaboración propia

Módulos	Temas	Comité
I	Políticas claves para la Seguridad de la información	24.07.2017
II	Riesgos de la información	24.07.2017
III	Metodología de riesgos	25.07.2017
	Tratamiento de riesgos	25.07.2017
IV	Gestión de Activos	26.07.2017
V	Trabajo en Áreas seguras	31.07.2017
VI	Transferencia de la información	31.07.2017
VII	Gestión de incidentes	01.08.2017
	Gestión de la continuidad	01.08.2017
VIII	Auditoría de Seguridad de la información	02.08.2017

Cuadro28: Capacitación SGSI Nivel Básico para la institución

Fuente: Elaboración propia

ETAPA IV: REVISIÓN DEL SGSI: FASE CHECK

5.4.1 Evaluación de los controles e indicadores

La evaluación de los controles es la etapa de revisión del SGSI para determinar si los controles utilizados para los riesgos tuvieron efecto positivo mejorando el nivel de la seguridad en la institución.

Según el cuadro 29, podemos validar los controles con los siguientes indicadores:

MEDIDAS GENERALES	ACCIÓN	INDICADOR
Elaboración de políticas y procedimientos	Implementación de políticas y procedimientos	%Nivel de información adquirido
Elaboración de declaraciones y compromisos.	Firmas de declaraciones y compromisos	% Firmas del personal
Sensibilización y capacitación	Lista de asistencia a capacitaciones	%Asistencia a capacitaciones
	Capacitaciones según cronograma	%Avance Capacitaciones dictadas
Elaboración de política de control de acceso del SGSI.	Política de control de acceso	%Altas/bajas usuario
Adquisición de Software open source para inventario de activos	Inventario de activos	%Activos Periodo vs Periodo Anterior
Adquisición de Software open source para incidentes	Registro de incidentes en software open source	%incidentes atendidos
Adquisición de Software open source para backup información	Registro y seguimiento de documentos para mesa de partes.	%Documentos ingresados
Validación del sistema de vigilancia y monitoreo	Contrato de personal para la validación	%Funcionamiento de cámaras
Adquisición de licencia software propietario	Instalación de ESET	%Equipos con licencia
Propuesta de cableado estructurado	Implementación de cableado estructurado	% Fallas de red anuales

Cuadro 29 : Indicadores de desempeño de los controles SGSI

Fuente: Elaboración propia

ETAPA V: MEJORA CONTINUA DEL SGSI: FASE ACT

5.5.1 Mejora y corrección

Todo sistema de gestión de seguridad de la información debe ser mejorado cada cierto periodo de tiempo porque los riesgos van cambiando según el contexto, así como los activos pueden incrementarse o disminuir, es por eso que esta etapa es importante ya que permite mantener actualizado el sistema y da opción a la institución de estar preparada para cualquier incidente.

El comité de seguridad realizará una primera revisión de funcionamiento a un mes de la presentación del SGSI a la institución y del inicio del plan de sensibilización y capacitación, con ayuda del ingeniero de computación e informática responsable de la implementación podrán realizar una reunión de ajuste de puntos para la primera mejora del SGSI.

Después de esta primera validación se sugiere que el comité mantenga reuniones cada 2 meses para evaluar nuevas propuestas en las buenas prácticas en la institución hasta completar su establecimiento.

Cabe resaltar que el resultado de las revisiones de funcionamiento y los indicadores de validación permitirá tener un alcance de que tenemos que mejorar y corregir del sistema de gestión de seguridad de la información.

Se propone también después de las primeras validaciones en el año de la implementación, realizar auditorías anuales del cumplimiento de los procedimientos y políticas establecidas para revisar si forman parte de la cultura institucional.

Capítulo VI: Costos y beneficios

6.1 Análisis de Costos de implementación de SGSI

6.1.1 Software

Se considera la compra de licencias corporativas de antivirus Nod Eset para 23 equipos informáticos y además 3 licencias de las herramientas open source: OCS Inventory, OS Ticket y OpenKM, los costos se detallan en el Cuadro 30:

Tipo	Descripción	Costo
Antivirus	ESET ENDPOINT SECURITY - Empresarial	S/. 3,516.46
Inventario Activos	OCS Inventory	S/. -
Backup informático	Open KM	S/. -
Gestión incidentes	OS Ticket	S/. -
TOTAL		**S/. 3,516.46**

Cuadro30 : Costos de Software para SGSI

Fuente: Elaboración propia

6.1.2 Recursos Humanos

Se considera el contrato de una ingeniera en computación e informática para la implementación del sistema de gestión de seguridad de la información, cubriendo todo el proceso de análisis, diseño y gestión del proyecto, así como la implementación y seguimiento necesario para el correcto funcionamiento dentro de la organización, el costo en el Cuadro 31:

Cantidad	Personal	Duración (meses)	Pago Mensual	Pago
1	Ingeniero en Computación e Informática	12	1800	21600
TOTAL				**21600**

Cuadro 31 : Costos de Recursos Humanos para SGSI

Fuente: Elaboración propia

6.1.3 Materiales

Los materiales a utilizar para la implementación considerando la impresión de procedimientos, políticas, la propuesta de cableado estructurado para la institución y también como parte de la concientización del sistema de gestión de seguridad: elementos publicitarios y sus costos, detallados en el Cuadro 32:

Tipo	Materiales	Precio	Cantidad	Total
Procedimientos / Políticas	Papel Bond A4 (500 UN)	S/. 11.00	20	S/. 220.00
Cableado estructurado	Cable UTP Categoría 5E	S/. 2.00	200	S/. 400.00
	Canaleta 50 x 20 mm	S/. 80.00	4	S/. 320.00
	Conectores RJ45 Bolsa x 100 UN	S/. 2.00	45	S/. 90.00
	Fundas de Conectores RJ45 Bolsa x 100 UN	S/. 2.00	30	S/. 60.00
Sensibilización (publicidad)	Afiches	S/. 5.00	20	S/. 100.00
	Manuales	S/. 10.00	50	S/. 500.00
Total				**S/. 1,690.00**

Cuadro 32 : Costos de Materiales para SGSI

Fuente: Elaboración propia

6.1.4 Hardware

Se considera el siguiente hardware para uso de la ingeniera de computación e informática como soporte a la implementación, en el Cuadro 33:

Equipo	Descripción	Cantidad	Costo	Total
PC	Computadora Intel Corei5, 4 GB de RAM, 1 TB Disco Duro	1	S/. 2,500.00	S/. 2,500.00
Impresora	Epson L455	1	S/. 850.00	S/. 850.00
TOTAL				**S/. 3,350.00**

Cuadro 33 : Costos de Hardware para SGSI

Fuente: Elaboración propia

6.1.5 Resumen de Costo de inversión

A continuación, en el Cuadro 34 el resumen de costos de inversión:

Costo de Inversión	
Tipo	**Costo**
Recursos Humanos	S/. 21,600.00
Materiales	S/. 1,690.00
Hardware	S/. 3,350.00
Software	S/. 3,516.46
TOTAL	**S/. 30,156.46**

Cuadro 34: Costos de inversión

Fuente: Elaboración propia

6.2 Beneficios

Los beneficios que se obtendrán con un sistema de gestión de la seguridad se muestran en el Cuadro 35:

Beneficios	Ratios de Mejora	% Actual	% Mejora
Mejora en los procesos de la organización	Mejora en el desempeño de los colaboradores con respecto a seguridad informática	67%	90%
Aumento del nivel de desempeño de los colaboradores			
Mejora en la confidencialidad de la información	Mejora en la confidencialidad, integridad y disponibilidad de la información	62%	86%
Aumento del nivel de disponibilidad de documentos			
Mejora en la integridad de la información			
Mejora en la solución inmediata a incidencias	Mejora en la solución inmediata de incidentes	69%	90%
Disminución de incidencias por virus			
Rendimiento Total en Seguridad de la Información		**29%**	**70%**

Cuadro 35: Beneficios del SGSI

Fuente: Elaboración propia

6.3 Costos Operacionales

Después de realizar la inversión se evalúan que costos se mantienen fijos en el tiempo:

6.3.1 Software

Se mantiene la compra de licencias, Cuadro 36:

Tipo	Descripción	Costo
Antivirus	ESET ENDPOINT SECURITY – Empresarial	S/. 3,516.46
Inventario Activos	OCS Inventory	S/. -
Backup informático	Open KM	S/. -
Gestión incidentes	OS Ticket	S/. -
TOTAL		**S/. 3,516.46**

Cuadro36: Costo operacional Software

Fuente: Elaboración propia

6.2.2 Recursos Humanos

Se mantiene el contrato de personal externo: Ingeniero en Computación e informática para el seguimiento del SGSI, según el Cuadro 37:

Cantidad	Personal	Duración (meses)	Pago Mensual	Pago
1	Ingeniero en Computación e Informática	12	1800	21600
TOTAL				**21600**

Cuadro37: Costo operacional Recursos humanos

Fuente: Elaboración propia

6.2.3 Materiales

Los materiales por utilizar después de la implementación se detallan en el Cuadro 38:

Tipo	Materiales	Precio	Cantidad	Total
Procedimientos / Políticas	Papel Bond A4 (500 UN)	S/. 11.00	20	S/. 220.00
Total				**S/. 220.00**

Cuadro 38: Costo operacional Materiales

Fuente: Elaboración propia

6.2.4. Mantenimiento de Hardware

Se considera adicional el mantenimiento de los equipos hardware en el Cuadro 39:

Mantenimiento	Costo	Frecuencia	Total
PC	S/. 50.00	2	S/. 100.00
Impresora	S/. 50.00	2	S/. 100.00
Insumo (cartucho)	S/. 120.00	3	S/. 360.00
TOTAL			S/. 560.00

Cuadro39: Costos por Mantenimiento Hardware

Fuente: Elaboración propia

6.2.5. Depreciación

Se detalla la depreciación de equipos en el Cuadro 40:

Equipo	Costo	Depreciación	Total
PC	S/. 2,500.00	25%	S/. 625.00
Impresora	S/. 850.00	25%	S/. 212.50
TOTAL			S/. 837.50

Cuadro 40: Costos por depreciación

Fuente: Elaboración propia

6.2.6 Resumen de Costo Operacional:

El costo del sistema de gestión de seguridad de la información que será considerado los próximos años se denomina costo operacional y se muestra en el Cuadro 41:

Costo de Inversión	
Tipo	**Costo**
Recursos Humanos	S/. 21,600.00
Software	S/. 3,516.46
Materiales	S/. 220.00
Hardware	S/. 560.00
Depreciación	S/. 837.50
TOTAL	**S/. 26,733.96**

Cuadro 41: Resumen Costos operacionales

Fuente: Elaboración propia

6.3. Retorno de la inversión (ROI):

En el siguiente análisis se está considerando un promedio de coste de hora del colaborador para definir un aproximado de costo de un proceso y luego definir el valor total de los procesos de la organización en un año, el detalle en el Cuadro 42:

Análisis del ROI de Sistema de Gestión de la Seguridad DDC Lambayeque

Costes de operación en la organización

Coste medio de hora / colaborador	**S/.8.00**
Horas de trabajo semanales / colaborador	**40**
Coste semanal por proceso	**S/.320**
Semanas al año que la organización trabaja	**48**
Total costo directo de trabajo por proceso al año	**S/.15,360**
Número de procesos de la organización	**8**
Costo total aproximado de los procesos de la organización	**S/.122,880**

Retorno de la inversión (1 año)

Inversión en la implementación del SGSI	30156.46	
Inversión total	**S/.30,156**	
Ratio actual de Desempeño laboral	**67.0%**	
Ratio actual de Confidencialidad, Disponibilidad e integridad	**62.0%**	
Ratio actual Soporte a incidencias	**69.0%**	
Desempeño actual	**29%**	
		Aumento %
Ratio después de SGSI de Desempeño laboral	**90.0%**	23%
Ratio después de SGSI de Confidencialidad, Disponibilidad e integridad	**86.0%**	24%
Ratio después de SGSI de Soporte a incidencias	**90.0%**	21%
Desempeño después del SGSI	**70%**	
Capacidad de mejora de procesos	**143.0%**	
Ahorros anuales si se trabaja con los mismos procesos considerando SGSI	**S/.72,319**	
Ahorros totales en el periodo	**S/.72,319**	
ROI	**140%**	

Cuadro 42: Análisis del ROI – Dirección desconcentrada de cultura de Lambayeque

Fuente: Elaboración propia

Considerando que la inversión es de 30156.46 soles, se toma en cuenta que el desempeño actual se encuentra en un 29% y se estima que con el SGSI se podrá llegar a un rendimiento de 70%, con una capacidad de mejora de procesos en un 143.0%, considerando que esto generaría un ahorro de S/.72 319 soles y un retorno de inversión del 140% en un año.

6.3.1 Retorno de inversión por periodos

Considerando en el primer periodo el costo de inversión y en los periodos siguientes el costo operacional, el ROI durante los próximos 5 años se muestra en el Cuadro 43:

Cálculo del ROI (ROI-Por períodos)					
	AÑOS O PERÍODOS				
	1	2	3	4	5
Ingresos netos	**S/.72,319**	72,319.27	72,319.27	72,319.27	72,319.27
Gastos netos (-)	-30156.46	-26,733.96	-26,733.96	-26,733.96	-26,733.96
	Poner los gastos en negativo				
R.O.I. 1 año	**139.81%**				
R.O.I. 2 años	**154.24%**				
R.O.I. 3 años	**159.44%**				
R.O.I. 4 años	**162.13%**				
R.O.I. 5 años	**163.76%**				

Cuadro43: Análisis del ROI por periodos – Dirección desconcentrada de cultura de Lambayeque

Fuente: Elaboración propia

6.4 Análisis de la Rentabilidad:

En el siguiente análisis se considera una evaluación de rentabilidad de dos años considerando el primer año el costo de inversión.

6.4.1 Inversión:

Se considera la inversión determinada en los puntos anteriores, periodo de dos años mínimo en el Cuadro 44:

INVERSIÓN	1ER AÑO	2DO AÑO
Costo de Inversión / operacional	30,156	26,734
TOTAL	**30,156**	**26,734**

Cuadro 44: Inversión del SGSI

Fuente: Elaboración propia

6.4.2 Flujo de Caja libre:

El flujo de caja libre es la resta del valor del beneficio de implementar un SGSI con el costo de inversión (según el periodo), en la tabla se detallan los dos primeros años:

RESULTADOS	1ER AÑO	2DO AÑO
AHORRO POR MEJORA DE PROCESOS	72,319	72,319
TOTAL	**72,319**	**72,319**
TOTAL BENEFICIO A 2 AÑOS		***87,748***
FCF	**42,163**	**45,585**

Cuadro45: Flujo Caja Libre

Fuente: Elaboración propia

6.4.3 Valor Actual Neto:

El valor actual neto (VAN) es un criterio de inversión que consiste en actualizar los cobros y pagos de un proyecto o inversión para conocer cuánto se va a ganar o perder con esa inversión. El VAN expresa una medida de rentabilidad del proyecto en términos absolutos netos, es decir en número de unidades monetarias. (Economipedia, 2015)

Fórmula:

$$VAN = -I_0 + \frac{B-C}{(1+i)1} + \frac{B-C}{(1+i)2} + \frac{B-C}{(1+i)3}$$

I_0: Inversión en el año 0
B: Beneficios
C: Costos
i: Tasa de interés

Considerando los siguientes datos el VAN a dos años, se presenta en el Cuadro 46:

Datos VAN		
Inversión	S/.	30,156
Tasa		15%
Año 1	S/.	72,319
Año 2	S/.	72,319
VAN		**87414**

2 años

Cuadro46: Valor Actual Neto (VAN)

Fuente: Elaboración propia

6.4.4 Tasa interna de Retorno (TIR):

Según (Didier, Pymes Futuro, 2012), la tasa interna de retorno también es conocida como la tasa de rentabilidad producto de la reinversión de los flujos netos de efectivo dentro de la operación propia del negocio y se expresa en porcentaje. También es conocida como Tasa crítica de rentabilidad cuando se compara con la tasa mínima de rendimiento requerida (tasa de descuento) para un proyecto de inversión específico.

La evaluación de los proyectos de inversión cuando se hace con base en la Tasa Interna de Retorno, toman como referencia la tasa de descuento. Si la Tasa Interna de Retorno es mayor que la tasa de descuento, el proyecto se debe aceptar pues estima un rendimiento mayor al mínimo requerido.

A continuación en el Cuadro 47, la tasa interna de retorno (TIR) de la propuesta:

Datos TIR		
Inversión (2 años)	- S/.56890.42	
TASA	15%	
Año 1	S/. 72,319	
Año 2	S/. 72,319	
TIR	46%	2 años

Cuadro 47: Tasa interna de retorno (TIR)

Fuente: Elaboración propia

6.4.5 Periodo de Recuperación de Inversión:

El periodo de recuperación de la inversión, es un instrumento que permite medir el plazo de tiempo que se requiere para que los flujos netos de efectivo de una inversión recuperen su costo o inversión inicial. (Didier, 2010)

$$PRI = AÑO^{*} + A / B$$

Datos PRI		
Año	0	Año flujo acumulado negativo
A	S/. 30,156	Último flujo acumulado negativo
B	S/. 72,319	Flujo no acumulado del año siguiente
PRI	5	**Meses**

Cuadro 48: Periodo de Recuperación de Inversión (PRI)

Fuente: Elaboración propia

CONCLUSIONES

- Se realizó un diagnóstico de la situación actual de la seguridad de la información en la dirección desconcentrada de Lambayeque, identificando los procesos de la institución y las principales actividades del personal, obteniendo información que permita entender el desempeño de la organización y las áreas que necesitan cambios y mejoras.
- El modelamiento de procesos se realizó con la herramienta freeware Bizagi Modeler utilizando notación BPMN, obteniendo una descripción gráfica del flujo y funcionamiento de la institución.
- Se realizó una comparativa de metodologías, eligiendo a MEHARI, una metodología de gestión de riesgos soportada por el "Club de la seguridad de la información francesa", que permitió el análisis de riesgos a través de sus herramientas open source: Mehari Expert y Mehari Pro. Las plantillas sirven como soporte para generar planes de acción vinculados a una base de conocimientos de posibles escenarios de riesgo, MEHARI como metodología, está basada en las ISO 27001e ISO 27005.
- Se eligieron 43 controles basados en la ISO 27002 para aplicar en la institución y se clasificaron en medidas de disuasión, protección, mitigación y prevención para los riesgos seleccionados, estos planes de acción incluyen la implementación de políticas, procedimientos, planes de capacitación y sensibilización y el uso de herramientas automatizadas.
- Las herramientas open source elegidas como soporte a la automatización de los controles del sistema de gestión de seguridad de la información son: OCS Inventory, que permite gestionar en tiempo real el inventario de activos de la información, Open KM que da soporte a trámite documentario y finalmente OS Ticket para la gestión de incidentes en la institución. Estas herramientas serán monitoreadas por el oficial de seguridad de la información.

- Finalmente se realizó la evaluación económica obteniendo resultados favorables en la implementación del sistema de gestión de seguridad de la información, demostrando que es una propuesta rentable, que genera beneficios a la institución, mejorando la productividad de los colaboradores, el desempeño de los procesos y las buenas prácticas en materia de seguridad de la información.

RECOMENDACIONES

- La institución necesita crear el comité de seguridad para el seguimiento del sistema de gestión de seguridad de la información.
- El comité de seguridad debe reunirse periódicamente para realizar feedback del funcionamiento del SGSI, es importante documentar la información, utilizando las actas de reunión establecidas en el SGSI.
- Los procedimientos y políticas deben ser implementados según el cronograma propuesto y cumplirse para tener resultados favorables para la institución.
- El oficial de seguridad, líder de esta propuesta debe realizar un constante seguimiento al sistema de gestión de la seguridad de la información, evaluando las mejoras con indicadores de desempeño y gestionando si es necesario realizar cambios.
- Se recomienda la instalación de las herramientas open source, gracias a su accesibilidad brindan el soporte necesario para un sistema de gestión de seguridad de la información.
- Es recomendable que la institución considere el presupuesto indicado por los beneficios que se podrán obtener después de la implementación.

BIBLIOGRAFÍA

Nagios Enterprises, LLC. (2017). *Nagios*. Obtenido de https://www.nagios.org

El portal de ISO 27001 en Español. (2012). Recuperado el 03 de 04 de 2016, de http://www.iso27000.es/download/doc_sgsi_all.pdf

AENOR. (2012). *Asociación Española para la Calidad.* Obtenido de La norma ISO 27001 del Sistema de Gestión de la seguridad de la información: http://www.aec.es/c/document_library/get_file?uuid=a89e72de-d92b-47cf-ba5e-5ea421fcbeb4&groupId=10128

Alcántara, J. (2015). *Guía de implementación de la seguridad basado en la norma ISO/IEC 27001, para apoyar la seguridad en los sistemas informáticos de la comisaria del norte P.N.P en la ciudad de Chiclayo.*

Alvarez, Y. (2013). Diseño de una metodología para el análisis de riesgo en los sistemas de gestión de seguridad de información (MARISGSI) en las Universidades de Barquisimeto Estado Lara.

Areitio, J. (2008). *Seguridad de la Información.* Madrid,España: Paraninfo.

Avantys. (2017). *Avantys Web*.

Barrios, C. (2010). Help Desk - OsTicket.

Betin, A. D., & Madera, J. E. (2015). *Software de apoyo para el proceso de implantación del Sistema de Gestión de Seguridad de la Información basado en la norma ISO 27001*. Cartagena de Indias.

BIZAGI. (2017). *Bizagi Modeler*. Obtenido de http://www.bizagi.com/es/productos/bpm-suite/modeler

Broad, J. (2013). Risk Management Framework. Elsevier Inc.

Cano, J. (2013). Inseguridad de la información. Colombia: ALFAOMEGA .

Carnegie Mellon University. (2017). *Software Engineer Institute*. Obtenido de http://www.cert.org/resilience/products-services/octave/

Castellanos, L. (2014). Seguridad en Informática. España: Editorial Académica Española.

CLUSIF. (Abril de 2010). *Fundamentals Concepts and Functional Specifications.* Recuperado el 12 de Abril de 2017, de www.meharipedia.org

CLUSIF. (2010). *Guía del Analisis y Tratamiento del Riesgo.*

CLUSIF. (2010). Introducción a MEHARI. En CLUSIF, *MEHARI.*

CLUSIF. (AGOSTO de 2010). *MEHARIPEDIA.ORG.* Recuperado el 30 de 04 de 2017, de www.meharipedia.org/on-line-documents-documents-ligne/

CLUSIF. (2011). *Evaluación de Riesgos.* Obtenido de www.meharipedia.org

CLUSIF. (2011). *Processing guide for risk analysis and management.*

Cohen, D., & Asín, E. (2005). *Sistema de información para los negocios.* Mexico: Mc Graw Hill.

Collazos, M. (2014). *La nueva versión ISO 27001:2013.* Obtenido de http://www.cip.org.pe/index.php/eventos/conferencias-ceremonias-y-patrocinios/item/download/125_2f7be404f0dba27dabc8efd91bd14668.html.

Coloma, C. (2010). *El Perú y su Historia.* Recuperado el 28 de 04 de 2017, de https://sites.google.com/site/elperuysuhistoria/el-instituto-nacional-de-cultura-del-peru

Costas, J. (2011). Seguridad informática. Ra-ma.

Didier, J. (2010). *Pymes Futuro*. Obtenido de https://www.pymesfuturo.com/pri.htm

Didier, J. (2012). *Pymes Futuro*. Obtenido de https://www.pymesfuturo.com/tiretorno.htm

Economipedia. (2015). Obtenido de http://economipedia.com/definiciones/valor-actual-neto.html

El Peruano. (8 de Enero de 2016). Aprueban el uso obligatorio de la Norma Técnica Peruana “NTP ISO/IEC 27001:2014 Tecnología de la Información. Técnicas

de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos. 2a. Edición". *El Peruano*.

ENISA. (2005 - 2017). *Eurpean Union Agency for Network and Information Security*. Recuperado el 20 de 4 de 2017, de www.enisa.europa.eu

Eramba. (2017). *Eramba*. Obtenido de http://www.eramba.org

Formación SGSI. (2010). *Centro de Servicios para la estandarización de la Seguridad informactica*. Obtenido de http://www.ceeisec.com/nuevaweb/doc/FORMACION_SGSI_2010.pdf

Free Software Foundation. (29 de Junio de 2007). *GNU*. Recuperado el 05 de Mayo de 2017, de https://www.gnu.org/licenses/gpl-3.0.html

Freund, J., Rucker, B., & Hitpass, B. (2014). BPM. En J. Freund, B. Rucker, & B. Hitpass, *BPMN 2.0.*

Gobierno de España. (Octubre de 2012). *Portal de Administración Electrónica*. Obtenido de https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.WTiAm2g1-00

GPS Open Source. (s.f.). Obtenido de http://www.gpsos.es/soluciones-open-source/definicion-de-open-source/

Greenbone. (2016). *Open Vas*. Obtenido de http://www.openvas.org/

GTDI. (3 de Junio de 2014). *GTDI-Tecnologías de la información y auditoría*. Obtenido de http://www.gtdi.pe/Como-descargar-ISO-IEC-27000

ISACA. (2012). *COBIT 5: An ISACA Framework.* Illinois, USA: ISACA.

Justino, Z. (2015). *Diseño de un Sistema de Gestión de Seguridad de información para una empresa inmobiliaria alineado a la norma ISO/IEC 27001:2013.*

Leiva, R. (2016). *Diseño de un Sistema de Gestión de Seguridad de la Información basado en las normas ISO/IEC 27001 e ISO/IEC 27002 para proteger los activos de información en el proceso de suministros de medicamentos de la Red de Salud de Lambayeque 2015.* Chiclayo.

Merino, C., & Cañizares, R. (2011). En *Implantación de un sistema de Gestión de Seguridad de la información según ISO 27001*. Madrid: Fundación CONFEMETAL.

Merino, C., & Cañizares, R. (2014). En *Auditoría de Sistemas de Gestión de la Información.* España: Fundación Confemetal.

Ministerio de Cultura del Perú. (2017). *Página Oficial Ministerio de Cultura.* Obtenido de http://www.cultura.gob.pe/es/ddc

Ministerio de Cultura del Perú. (2017). *Página Oficial Ministerio de Cultura.* Obtenido de http://www.cultura.gob.pe/es/ddc

Montesino Perurena, R., Baluja García, W., & Porvén Rubier, J. (2013). *Ingeniería Electrónica, Automática y Comunicaciones.* Recuperado el 12 de 05 de 2017, de Gestión automatizada e integrada de controles de seguridad informática: http://scielo.sld.cu/

Morante, K. (2016). Organigrama DDC Lambayeque.

Nuñez, M. (09 de Mayo de 2014). *En Colaboración - Consultoría Colaborativa*. Recuperado el 28 de Mayo de 2017, de https://encolaboracion.wordpress.com/2014/05/09/la-norma-isoiec-270022013/

OCS Inventory NG. (2017). *OCS Inventory*. Obtenido de https://www.ocsinventory-ng.org/en/

Open Document Management System S.L. (2016). *Open KM - Knowledge Management*. Obtenido de Gestión Documental: https://www.openkm.com/es.html#GestionDocumental

Open Source Initiative. (2007). *Definición Open Source*. Obtenido de https://opensource.org/docs/osd

PCM. (Enero de 2016). *Presidencia de Consejo de Ministros del Perú.* Obtenido de http://www.pcm.gob.pe/wp-content/uploads/2016/01/RM_N_04-2016-PCM.pdf

Piattini, M., & Hervada, F. (2007). Gobierno de las Tecnologías y los Sistemas de información.

Portal de la Oficina Nacional de Gobierno Electrónico e Informática (ONGEI) de la Presidencia del Consejo de Ministros (PCM). (2017). *Perú Gobierno Digital*. Obtenido de http://www.ongei.gob.pe/entidad/ongei_tematicos.asp?cod_tema=4552

PTA Technologies. (2013). *Practical Threat Analysis*. Obtenido de http://www.ptatechnologies.com/

Rendón, M. (2015). *Migración de un SGSI basadod en ISO/IEC 27001:2005 a la versión ISO/IEC 27001:2013.*

Rodeia, F. (2009). *Models for Assessing Information Security Risk.* Lisboa.

SimpleRisk. (2016). *SimpleRisk*. Obtenido de https://www.simplerisk.com/

Talavera, V. (2015). *Diseño de un Sistema de Gestión de Seguridad de la Información para una entidad estatal de salud de acuerdo a la ISO/IEC 27001:2013. .*

WWW.ISO27000.ES. (s.f.). *Sistema de Gestión de la Seguridad de la Información*. Obtenido de http://www.iso27000.es/download/doc_sgsi_all.pdf

Yagual, C., & Chilán, L. (2014). *Análisis para la integración de un Sistema de Gestión de Seguridad de Información (SGSI) ISO-27001 Utilizando OSSIM para empresa Industrial.*

Anexo 01: Solicitud de permiso para desarrollo de proyecto

Ministerio de Cultura
Dirección Desconcentrada de Cultura Lambayeque
RECIBIDO
16 FEB. 2016
Exp. 802 Folios 01
Hora 5:43 Firma

Solicitud para realizar investigación para Tesis

Arq. Alberto José Risco Vega
Dirección Desconcentrada de Cultura de Lambayeque

Yo, Clara Patricia Cubas Penas con DNI: 43861453, bachiller de Ing. Computación e Informática de la Universidad Nacional Pedro Ruiz Gallo, ante usted me presento y expongo:

Que, deseando realizar mi tesis para obtener el titulo profesional solicito a usted su autorización para realizar la investigación en la Dirección Desconcentrada de Cultura de Lambayeque.

Por lo expuesto, quedo a espera de su permiso para acceder a mi solicitud.

Chiclayo, 18 de Febrero de 2016

Atentamente,

Clara Patricia Cubas Penas
DNI:43861453

Anexo 02: Cuestionario para entrevista a usuarios de la Dirección Desconcentrada de Cultura de Lambayeque.

1. ¿Cuáles son tus actividades diarias en tu área?
2. ¿Qué tipo de documentos e información empleas en tu actividad diaria?
3. ¿Con qué áreas interactúa los documentos e información que recibes o entregas? ¿Se puede hacer seguimiento a los documentos?
4. ¿Consideras que tu información sensible es accesible? ¿Alguna vez tus documentos han perdido su integridad, es decir se han extraviado o los has encontrado incompletos?
5. ¿Qué función de tus actividades consideras como la más importante?
6. ¿Consideras que tu ambiente de trabajo es seguro, con respecto a la confidencialidad de la información?
7. ¿Consideras que tu equipo de cómputo es seguro? ¿Tu computadora tiene usuario y contraseña?
8. ¿Cuentas con antivirus? ¿Utilizas correctamente tu antivirus?
9. ¿Tienes conocimiento con respecto a la seguridad de la información?
10. ¿La dirección cuenta con procedimientos y políticas sobre seguridad de la información? De ser sí la respuesta, ¿Haz recibido alguna inducción sobre estos documentos?
11. ¿Cuáles son los problemas más frecuentes con respecto a la información física en tu área?
12. ¿Cuáles son los problemas más frecuentes con respecto a la información digital en tu área?
13. ¿Existe algún control de activos? ¿El control es efectivo?
14. ¿Existe algún control con respecto a los programas (software) instalados?
15. ¿Considera que el soporte a incidencias informáticas sea adecuado?
16. ¿Consideras necesario crear un acuerdo de confidencialidad?
17. ¿Consideras importante la seguridad de tu información mejorará el desempeño de las actividades en tu área?

Anexo 03: Encuesta Seguridad de la información

“Encuesta para Investigación – Seguridad de la información”

Esta encuesta valida la seguridad y los riesgos que se pueden presentar en la organización con respecto a la información y documentos:

Nombres y Apellidos:

_____

Ocupación / Cargo:

_____

Oficina:

_____

1. ¿Cuenta usted con una computadora personal en el trabajo?

   ○ Sí ○ No

2. ¿Cuenta usted con otro dispositivo informático?

   ☐ Laptop
   ☐ Impresora
   ☐ Teléfono IP
   ☐ Otro:_____

3. ¿Qué programas de escritorio utiliza en su computadora?

   ☐ Excel
   ☐ Word
   ☐ Power Point
   ☐ Otro: _____

4. ¿Tiene acceso a internet?

   ○ Sí ○ No

5. ¿Considera importante tener acceso a internet?

   ○ Sí ○ No

6. ¿En internet a qué páginas accedes?

   ☐ Redes sociales (facebook, twitter, instagram)
   ☐ Correo electrónico (hotmail, gmail, etc.)
   ☐ Navegadores en búsqueda de información (google, bing, etc.)
   ☐ Otro:_____

7. ¿Su computadora tiene antivirus?

- ○ Sí
- ○ No

8. Si su respuesta es si, mencione el nombre de su antivirus:

_____

9. Con respecto al registro de información ¿Tiene conocimientos sobre seguridad informática?

- ○ Sí
- ○ No

10. ¿Tiene un usuario específico y contraseña para el acceso a su computadora?

- ○ Sí
- ○ No

11. Presenta alguno de estos problemas con respecto a la información de su área:

- ☐ Falta de confidencialidad.
- ☐ No hay control ni seguimiento de documentos.
- ☐ No se precisa el estado del proceso (trámite iniciado, pendiente, terminado).
- ☐ Demora en la búsqueda de la información.
- ☐ Los documentos no mantienen su integridad (documentos incompletos o vulnerados).
- ☐ Otro:_____

12. Con respecto a la pérdida de información ¿Con que frecuencia mensual se extravían los documentos de su área?

- ○ 1 vez al mes.
- ○ De 2 a 5 veces al mes.
- ○ De 6 a 10 veces al mes.
- ○ De 11 a 20 veces al mes.
- ○ Más de 20 veces al mes.
- ○ Otro: _____

13. Con respecto a la búsqueda de información ¿Cuánto tiempo al día toma buscar un documento en su área?

- ○ 10 minutos.
- ○ 20 a 30 minutos.
- ○ De 40 minutos a 1 hora.
- ○ Más de 1 hora.
- ○ Otro: _____

14. Con respecto a la confidencialidad de la información ¿Usted es el único que tiene acceso a su información?

- ○ Sí
- ○ No

15. Con respecto al seguimiento de la información ¿En cuánto tiempo se obtiene respuesta de un trámite con el proceso actual?

- ○ 2 días
- ○ 4 - 5 días
- ○ 1 semana ……. ….○ 1 mes
- ○ Más de 1 mes
- ○ Otro: _____

16. Con respecto a la integridad de los documentos ¿Qué factores afectan?

- ☐ Manipulación de documentos en varias áreas.
- ☐ Los documentos se registran físicamente.
- ☐ Cantidad de tiempo en proceso de evaluación.
- ☐ Otro:_____

17. Si pudiera calificar su equipo informático, ¿Cuánto le pondría?

Muy malo ○ 1 ○ 2 ○ 3 ○ 4 ○ 5 Muy Bueno

18. ¿Con qué frecuencia se realiza soporte técnico en su computadora?

- ○ 1 vez al mes
- ○ Cada 3 meses
- ○ Cada 6 meses
- ○ 1 vez al año
- ○ Otro: _____

19. Cuando el equipo informático presenta errores de red o de acceso, ¿A quién le pide ayuda?

- ○ Coordino la llegada de un técnico
- ○ Le pido ayuda a un amigo del trabajo
- ○ Busco soluciones en internet
- ○ Contamos con un área de soporte técnico
- ○ Otro: _____

20. ¿Considera necesaria la implementación de un sistema de seguridad de la información?

- ○ Sí es necesario
- ○ No es necesario

Anexo 04: Ficha Gestión directiva

PROCESO 01: GESTIÓN DIRECTIVA					
MACROPROCESO:	**GESTIÓN INSTITUCIONAL**				**CODIGO: P01**
PROCESO:	**Gestión Directiva**				**CODIGO: PE.1**
OBJETIVO:	Dirigir las actividades de la institución de acuerdo a las políticas del Ministerio de Cultura, fomentando eventos culturales y protegiendo el patrimonio histórico de la región Lambayeque.				**ESTRATEGICOS**
ALCANCE:	Desde la supervisión de funciones de la institución hasta el visto bueno de las actividades culturales a realizarse.				
RESPONSABLE:	**Director DDC Lambayeque**				**FECHA REV: 20/5/2017**
PROVEEDORES	**ENTRADAS**	**PROCESOS, SUBPROCESOS Y ACTIVIDADES**		**SALIDAS**	**CLIENTES**
		1.1	**Supervisar las actividades de la institución**		
Ministerio de Cultura	Lineamientos	1.1.1	Cumplir los lineamientos del Ministerio	Check list Supervisión	DDC Lambayeque
Director DDC	Check list de supervisión	1.1.2	Realizar una revisión de las actividades de las áreas	Informe de supervisión	DDC Lambayeque
		1.2	**Dar conformidad de los proyectos culturales en la región.**		
Director DDC	Solicitud de proyectos culturales	1.2.1	Revisar proyectos culturales	Aprobación de proyecto	Usuario externo
Director DDC / Asistente	Aprobación de proyecto	1.2.2	Firmar resolución de aprobación	Resolución	Usuario externo
		1.3	**Solicitar documentación dirigida a DDC Lambayeque**		
Asistente Gerencia	Documentos varios	1.3.1	Seleccionar documentación	Documentos por respuesta	Director DDC
Director DDC	Documentos por respuesta	1.3.2	Evaluación documentación	Respuesta a Documento	Usuario externo
		1.4	**Reportar al ministerio las incidencias DDC Lambayeque**		
Director DDC	Resoluciones/Informe supervisión	1.3.1	Enviar correo de incidencias	Correo con incidencias DDC	Ministerio de Cultura
NORMATIVIDAD				**Indicadores**	
Políticas y Normas internas - Ministerio de Cultura del Perú				%Incidencias solucionadas, %ProyectosAprobados	

Anexo 05: Fichas Gestión administrativa

Proceso 02: GESTIÓN ADMINISTRATIVA					
MACROPROCESO:	**GESTIÓN INSTITUCIONAL**			**CODIGO: P01**	
PROCESO:	**Gestión Administrativa**			**CODIGO: PE.02**	
OBJETIVO:	Controlar las operaciones administrativas, financieras y logísticas, así como la gestión de presupuesto de la institución.			**ESTRATEGICOS**	
ALCANCE:	Desde la administración de presupuesto hasta la consolidación de información administrativa y financiera de las áreas de la DDC Lambayeque				
RESPONSABLE:	**Administrador DDC Lambayeque**				**FECHA REV: 20/05/2017**
PROVEEDORES	**ENTRADAS**	**PROCESOS, SUBPROCESOS Y ACTIVIDADES**		**SALIDAS**	**CLIENTES**
		2.1	**Administración del presupuesto**		
Ministerio de Cultura	Presupuesto	2.1.1	Evaluar Presupuesto	Solicitud de planes por áreas	DDC Lambayeque
Áreas DDC	Solicitud de planes por áreas	2.1.2	Establecer planes	Informe de planes	DDC Lambayeque
Administrador	Informe de planes	2.1.3	Solicitar Caja Chica	Correo de solicitud de Caja Chica	DDC Lambayeque
Ministerio de Cultura (tesorería)	Solicitud de Caja Chica	2.1.4	Enviar Guía de remisión y Caja Chica	Importe de Caja Chica	DDC Lambayeque
Administrador	Solicitud cuentas por áreas	2.1.5	Control y seguimiento de presupuesto	Reporte financiero / administrativo	DDC Lambayeque
		2.2	**Elaboración de informe Rendición de cuentas**		
Administrador	Reporte financiero / administrativo	2.2.1	Elaboración de redición de cuentas	Rendición de cuentas	DDC Lambayeque
Director	Rendición de cuentas	2.2.2	Dar conformidad	Validación de RC	DDC Lambayeque
Administrador	Validación	2.2.3	Enviar rendición de cuentas	Correo de Rendición de Cuentas	Ministerio de Cultura
		2.3	**Coordinación con Sede Central**		
Administrador	Reunión Áreas	2.3.1	Solicitar lista de tareas	Lista de tareas	DDC Lambayeque
Administrador	Lista de tareas	2.3.2	Consolidar lista de tareas	Cronograma de tareas	DDC Lambayeque
Administrador	Cronograma de tareas	2.3.3	Enviar lista de tareas	Aprobación de lista	Ministerio de Cultura
		2.4	**Gestionar tareas**		
Administrador	Notas con remisión de valores	2.4.1	Gestionar boletas de pago	Boletas de Pago	DDC Lambayeque
Administrador	Operaciones logísticas (vigilancia)	2.4.2	Gestionar operaciones logísticas	Informe de mantenimiento	DDC Lambayeque
Administrador	Red/equipos varios	2.4.3	Gestionar soporte técnico	Informe soporte	DDC Lambayeque
Administrador	Informes	2.4.4	Presentar informes	Correo con informes	Ministerio de Cultura
		2.4	**Seguimiento procesos legales**		
Abogado	Notificaciones legales	2.4.1	Evaluar procesos legales	Procesos legales	DDC Lambayeque
Abogado	Procesos legales	2.4.1	Enviar informes legales	informes legales	Ministerio de Cultura
		2.5	**Reportar documentación a Director DDC**		
Administrador	Resoluciones / informe de actividades	2.5.1	Consolidar documentación	Documentos consolidados	DDC Lambayeque
Director	Documentos consolidados	2.5.2	Validar documentación	Informe administración	Ministerio de Cultura
NORMATIVIDAD				**INDICADORES**	

Políticas y Normas internas - Ministerio de Cultura del Perú	%Presupuesto Mensual vs. Gasto Mensual, %ProcesosLegales atendidos

Anexo 06: Ficha Gestión Documentaria

PROCESO 03: GESTIÓN DOCUMENTARIA					
MACROPROCESO:	**GESTIÓN INSTITUCIONAL**				**CODIGO: PS.1**
PROCESO:	**Gestión Documentaria**				**CODIGO: PS.1**
OBJETIVO:	Ingresar documentación interna y externa, registrarla y distribuirla a todas las áreas.				**SOPORTE**
ALCANCE:	Desde la recepción de documentación y expedientes, registro en el sistema, aprobación hasta la distribución hacia todas las áreas priorizando la dirección y oficina de Arqueología				
RESPONSABLE:	**Encargado de Mesa de Partes**				**FECHA REV: 20/05/2017**
PROVEEDORES	**ENTRADAS**	**PROCESOS, SUBPROCESOS Y ACTIVIDADES**		**SALIDAS**	**CLIENTES**
		3.1	**Recepción de Expedientes**		
Usuario	Documento / Expediente	3.1.1	Presentar documento	Documento y Cargo	DDC Lambayeque
Mesa de Partes	Documento / Expediente (recibido)	3.1.2	Validar documento	Documento / Expediente (validado)	DDC Lambayeque
Mesa de Partes	Documento / Expediente (validado)	3.1.3	Sellar Cargo	Cargo Sellado	Usuario
		3.2	**Registro de Expedientes**		
Mesa de Partes	Documento / Expediente	3.2.1	Registrar documento en sistema	Documento / Expediente (registrado)	DDC Lambayeque
Mesa de Partes	Documento / Expediente	3.2.2	Generar codigo de documento	Codigo referido	DDC Lambayeque
		3.3	**Aprobación de Recepción**		
Mesa de Partes	Documento / Expediente	3.3.1	Derivar a las areas	Documento / Expediente (derivado)	DDC Lambayeque
Mesa de Partes	Documento / Expediente (aceptado)	3.3.2	Archivador documento	Documento / Expediente (archivado)	DDC Lambayeque
Usuario	Documento / Expediente (observado)	3.3.2	Levantar observaciones	Documento / Expediente (corregido)	DDC Lambayeque
Mesa de Partes	Documento / Expediente	3.3.3	Aprobar documento	Documento / Expediente (aprobado)	Usuario
NORMATIVIDAD				**INDICADORES**	
Políticas y Normas internas - Ministerio de Cultura del Perú				Cantidad de Documentos recepcionados por tipo, Expedientes de Arqueología, Estado de Documentos	

Anexo 07: Ficha Gestión de proyectos arqueológicos

Proceso 04: GESTIÓN PROYECTOS ARQUEOLÓGICOS					
MACROPROCESO:	**GESTIÓN INSTITUCIONAL**				**CODIGO: PS.1**
PROCESO:	**Gestión de Proyectos Arqueológicos**				**CODIGO: PM.1**
OBJETIVO:	Atender los expedientes arqueológicos y elaborar el Certificado de Inexistencia de Restos Arqueológicos (CIRA), así como la atención en las afectaciones de sitios arqueológicos dentro de la región Lambayeque				**MISIONALES**
ALCANCE:	Desde la recepción de expedientes, designación de arqueólogos, gestión de PMA y CIRA, hasta asesorías de proyectos arqueológicos.				
RESPONSABLE:	**Arqueólogos DDC Lambayeque**				**20/05/2017**
PROVEEDORES	**ENTRADAS**	**PROCESOS, SUBPROCESOS Y ACTIVIDADES**		**SALIDAS**	**CLIENTES**
		4.1	**Gestionar de Expedientes Arqueológico**		
Mesa de Partes	Documento/Expediente	4.1.1	Recibir Expediente Arqueológico	Designación de Arqueólogo	Usuario externo
Arqueólogo	Designación	4.1.2	Definir tipo de expediente	Expediente (derivado)	Usuario externo
Arqueólogo	Documento/Expediente (común Arqueología)		Gestionar Expediente	Expediente (atendido)	Usuario externo
		4.2	**Gestionar PMA**		
Usuario	Expediente (tipo PMA)	4.2.1	Recibir Expediente Tipo PMA	Solicitud de autorización PMA y Formulario PMA	DDC Lambayeque
Arqueólogo	Solicitud de autorización PMA y Formulario PMA	4.2.2	Autorizar ejecución de PMA	Informe de Autorización de PMA/Observaciones	Usuario externo
Usuario	Solicitud de levantamiento de Observaciones PMA	4.2.3	Levantamiento de observaciones	Informe de observaciones levantadas PMA	Usuario externo
Arqueólogo	Informe de Autorización de PMA / Observaciones levantadas	4.2.4	Supervisión de ejecución PMA	Informe de Supervisión de PMA	Usuario externo
Arqueólogo	Informe de Supervisión de PMA	4.2.5	Aprobación de PMA	Informe de Aprobación de PMA	Usuario externo
		4.3	**Gestionar CIRA**		
Usuario	Expediente(tipo CIRA)	4.3.1	Recibir solicitud tipo CIRA	Solicitud de elaboración de CIRA y Formulario CIRA	DDC Lambayeque
Arqueólogo	Solicitud de elaboración de CIRA y Formulario CIRA	4.3.2	Elaborar CIRA	Informe de CIRA / Observaciones	Usuario externo
Usuario	Solicitud de levantamiento de Observaciones CIRA	4.3.3	Levantar observaciones	Informe de CIRA	Usuario externo
		4.4	**Asesoría de Proyectos Arqueológicos**		
Arqueólogo	Solicitud de Asesoría	4.4.1	Realizar asesoría	Formato Asesoría	Usuario externo
Arqueólogo	Formato	4.4.2	Presentar informe	Informe asesoría	Usuario externo
NORMATIVIDAD				**INDICADORES**	
Políticas y Normas internas - Ministerio de Cultura del Perú				%CIRA al mes, %Expedientes, %Asesorías	

Anexo 08: Gestión control patrimonial

Proceso 05: GESTIÓN DE CONTROL PATRIMONIAL					
MACROPROCESO:	**GESTIÓN INSTITUCIONAL**				**CODIGO: P01**
PROCESO:	**Gestión Control Patrimonial**				**CODIGO: PS.2**
OBJETIVO:	Controlar los bienes muebles y la asignación a las diferentes áreas de la institución.				**SOPORTE**
ALCANCE:	Desde la ubicación de bienes muebles de la institución, inventario y asignación de bienes muebles a los colaboradores.				
RESPONSABLE:	**Director DDC Lambayeque**				**20/05/2017**
PROVEEDORES	**ENTRADAS**	**PROCESOS, SUBPROCESOS Y ACTIVIDADES**		**SALIDAS**	**CLIENTES**
		5.1	**Ubicación de Bienes Muebles**		
Coordinador	Lineamientos	5.1.1	Revisar ubicación	Mapeo de institución	DDC Lambayeque
Coordinador	Mapeo	5.1.2	Realizar lay out de distribución	Lay out de distribución	DDC Lambayeque
		5.2	**Control de Bienes Muebles**		
Coordinador	Bienes	5.2.1	Realizar inventario	Formato de inventario	DDC Lambayeque
	Formato de inventario	5.2.2	Consolidar inventario	Reporte de inventario	DDC Lambayeque
		5.3	**Asignación de bienes Muebles**		
Coordinador	Bienes	5.3.1	Asignar bienes a usuario	Formato de asignación	Usuario
Coordinador	Formato de asignación	5.3.2	Aprobación de usuario	Cuadros de asignación firmados	Usuario
NORMATIVIDAD				**INDICADORES**	
Políticas y Normas internas - Ministerio de Cultura del Perú				Cuadros de asignación de bienes de la institución	

Anexo 09: Ficha de Patrimonio Histórico

Proceso 06: GESTIÓN DE PATRIMONIO HISTÓRICO					
MACROPROCESO:	**GESTIÓN INSTITUCIONAL**				**CODIGO: P01**
PROCESO:	**Gestión de Patrimonio Histórico**				**CODIGO: PM.2**
OBJETIVO:	Controlar, supervisar e inspeccionar los bienes inmuebles aplicando directivas técnicas y reglamentos relacionados en la conservación y preservación del patrimonio histórico de la región Lambayeque.				**MISIONALES**
ALCANCE:	Desde el control de bienes muebles hasta asesoría a usuarios con respecto al patrimonio histórico de la región Lambayeque.				
RESPONSABLE:	**Arquitectos DDC**				**20/05/2017**
PROVEEDORES	**ENTRADAS**	**PROCESOS, SUBPROCESOS Y ACTIVIDADES**		**SALIDAS**	**CLIENTES**
		6.1	**Control Bienes inmuebles**		
Arquitecto	Bienes inmuebles	6.1.1	Registrar Bienes inmuebles	inventario de bienes inmuebles	DDC Lambayeque
Arquitecto	Bienes inmuebles	6.1.2	Mapeo de bienes inmuebles	Informe de ubicación de bienes inmuebles	DDC Lambayeque
Arquitecto	Bienes inmuebles	6.1.3	Seguimiento de bienes inmuebles	Informe de seguimiento	DDC Lambayeque
		6.2	**Inspección de Bienes inmuebles**		
Arquitecto	Bienes inmuebles	6.2.1	Realizar inspección de bienes inmuebles	Informe de inspección ocular	DDC Lambayeque
Arquitecto	Bienes inmuebles	6.2.2	Validar estados	Informe de estados de los bienes	DDC Lambayeque
		6.3	**Asesoría a usuarios**		
Usuario	Solicitud de asesoría	6.3.1	Solicitar asesoría	Informe técnico	Usuario
Areas DDC	Informe técnico	6.3.2	Aprobación de asesoría	Informe aprobado	Usuario
NORMATIVIDAD				**INDICADORES**	
Políticas y Normas internas - Ministerio de Cultura del Perú				%Asesorias mensuales, %Inspecciones por Estados	

Anexo 10: Ficha actividades culturales

PROCESO 07: GESTIÓN ACTIVIDADES CULTURALES					
MACROPROCESO:	**GESTIÓN INSTITUCIONAL**				**CODIGO: P01**
PROCESO:	**Gestión Actividades Culturales**				**CODIGO: PM.3**
OBJETIVO:	Promocionar, difundir y desarrollar los eventos culturales organizados por la DDC de Lambayeque				**MISIONALES**
ALCANCE:	Desde la coordinación de actividades, gestión de eventos, talleres hasta la gestión de ambientes.				
RESPONSABLE:	**Gestor de Actividades**				**20/05/2017**
PROVEEDORES	**ENTRADAS**	**PROCESOS, SUBPROCESOS, ACTIVIDADES**		**SALIDAS**	**CLIENTES**
		7.1	**Coordinación de actividades**		
Gestor de Actividades	Lista de actividades	7.1.1	Generar cronograma de actividades	Cronograma de actividad	DDC Lambayeque
Gestor de Actividades	Cronograma de Actividad	7.1.2	Aprobación de actividades	Actividad (aprobada)	DDC Lambayeque
Gestor de Actividades	Actividad (aprobada)	7.1.2	Consolidar actividades	Taller / Evento	DDC Lambayeque
		7.2	**Gestionar eventos**		
Gestor de Actividades	Eventos	7.2.1	Coordinar eventos	Solicitud de participación	Usuario externo
Gestor de Actividades	Solicitud de participación	7.2.2	Solicitar participación	Correo de confirmación	Usuario externo
Gestor de Actividades	Invitaciones	7.2.3	Enviar invitaciones	Correos/Invitaciones físicas	Usuario externo
		7.3	**Gestionar talleres**		
Gestor de Actividades	Talleres	7.3.1	Publicar horarios / costos	Inscripción a talleres	Usuario externo
Gestor de Actividades	Inscripción	7.3.2	Inscribir a publico	Ingreso económico	Usuario externo
Gestor de Actividades	Ingreso económico	7.3.3	Realizar liquidación de talleres	Informe liquidación	DDC Lambayeque
		7.3	**Gestionar alquiler de ambientes**		
Gestor de Actividades	Ambientes DDC Lambayeque	7.3.1	Ofrecer alquiler	Lista de espacios disponibles	Usuario externo
Gestor de Actividades	Lista de espacios disponibles	7.3.2	Alquilar espacio	Ingreso económico	Usuario externo
Gestor de Actividades	Ingreso económico	7.3.3	Realizar liquidación de alquiler de espacio.	Informe liquidación	DDC Lambayeque
NORMATIVIDAD				**INDICADORES**	
Políticas y Normas internas - Ministerio de Cultura del Perú				%Invitacionesrealizadas, %Eventos mensuales, % Cumplimiento de Participación, %Participantes por taller	

Anexo 11: Ficha gestión de comunicaciones

PROCESO 08: GESTIÓN DE COMUNICACIONES					
MACROPROCESO:	**GESTIÓN INSTITUCIONAL**				**CODIGO: P01**
PROCESO:	**Gestión de Comunicaciones**				**CODIGO: PE.3**
OBJETIVO:	Fortalecer las comunicaciones mediante estrategias de promoción y difusión del Patrimonio Cultural de la DDC.				**ESTRATEGICOS**
ALCANCE:	Desde la gestión de materiales, coordinar el diseño y la difusión de eventos culturales con publicaciones de imprenta y digitales.				
RESPONSABLE:	**Gestor de comunicaciones**				**20/05/2017**
PROVEEDORES	**ENTRADAS**	**PROCESOS, SUB PROCESOS Y ACTIVIDADES**		**SALIDAS**	**INDICADORES**
		8.1	**Gestionar Material**		
Gestor de comunicaciones	Lista de actividades	8.1.1	Coordinar difusión	Reporte a diseñador	DDC Lambayeque
Gestor de comunicaciones	Reporte	8.1.2	Coordinar diseño	Diseños	DDC Lambayeque
Gestor de comunicaciones	Diseño físico	8.1.3	Enviar a imprenta	Impresiones	DDC Lambayeque
		8.2	**Difusión de Eventos Culturales**		
Gestor de comunicaciones	Diseño fisico / digital	8.2.1	Validar material físico/virtual	Material validado	DDC Lambayeque
Gestor de comunicaciones	Material	8.2.2	Gestionar publicaciones	Publicaciones en local y redes sociales	DDC Lambayeque
NORMATIVIDAD				**INDICADORES**	
Políticas y Normas internas - Ministerio de Cultura del Perú				% Actividades vs. Publicaciones, % Participación en redes sociales	

Anexo 12: Diagramas de los procesos de la Dirección desconcentrada de Cultura de Lambayeque.

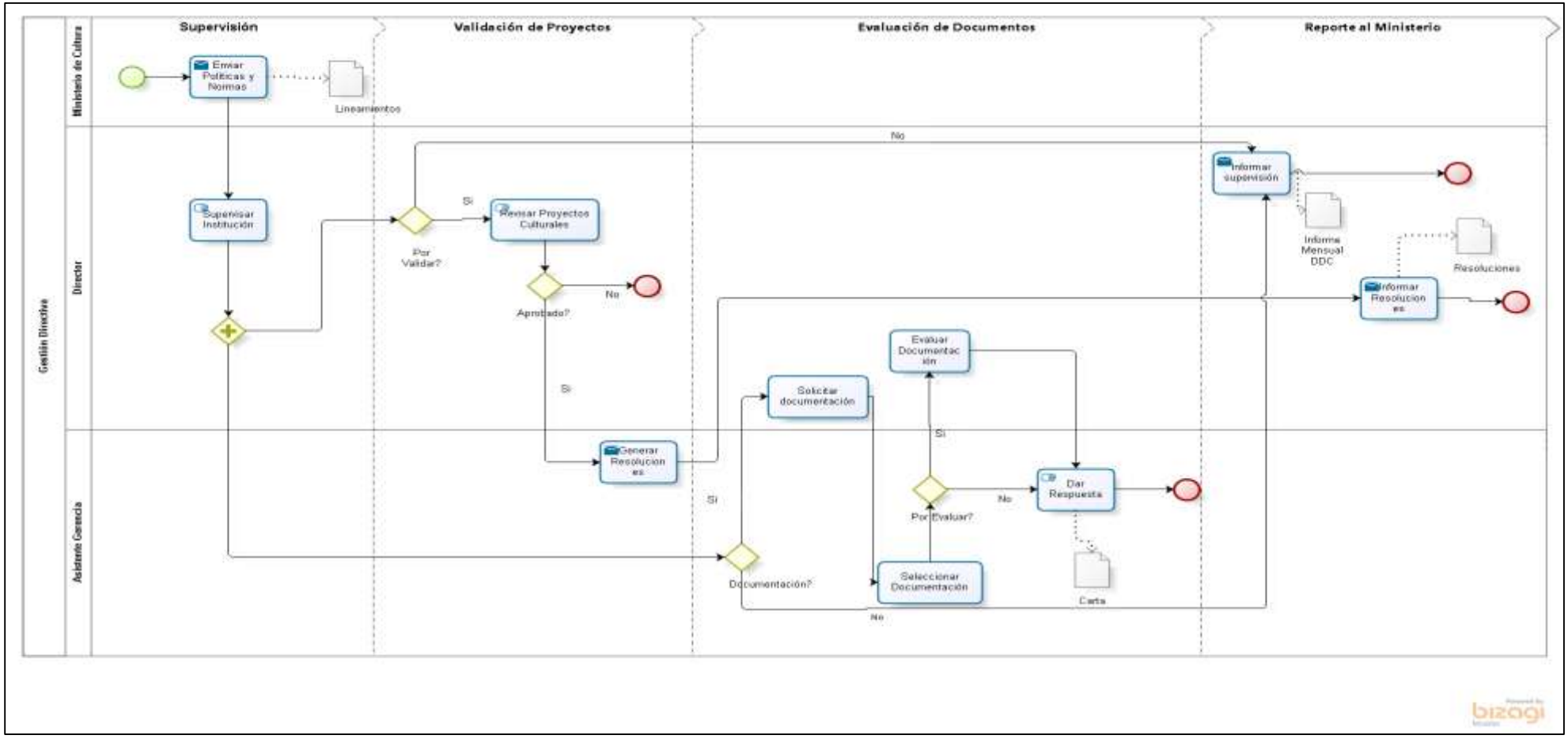


Diagrama 01: Proceso de Gestión Directiva

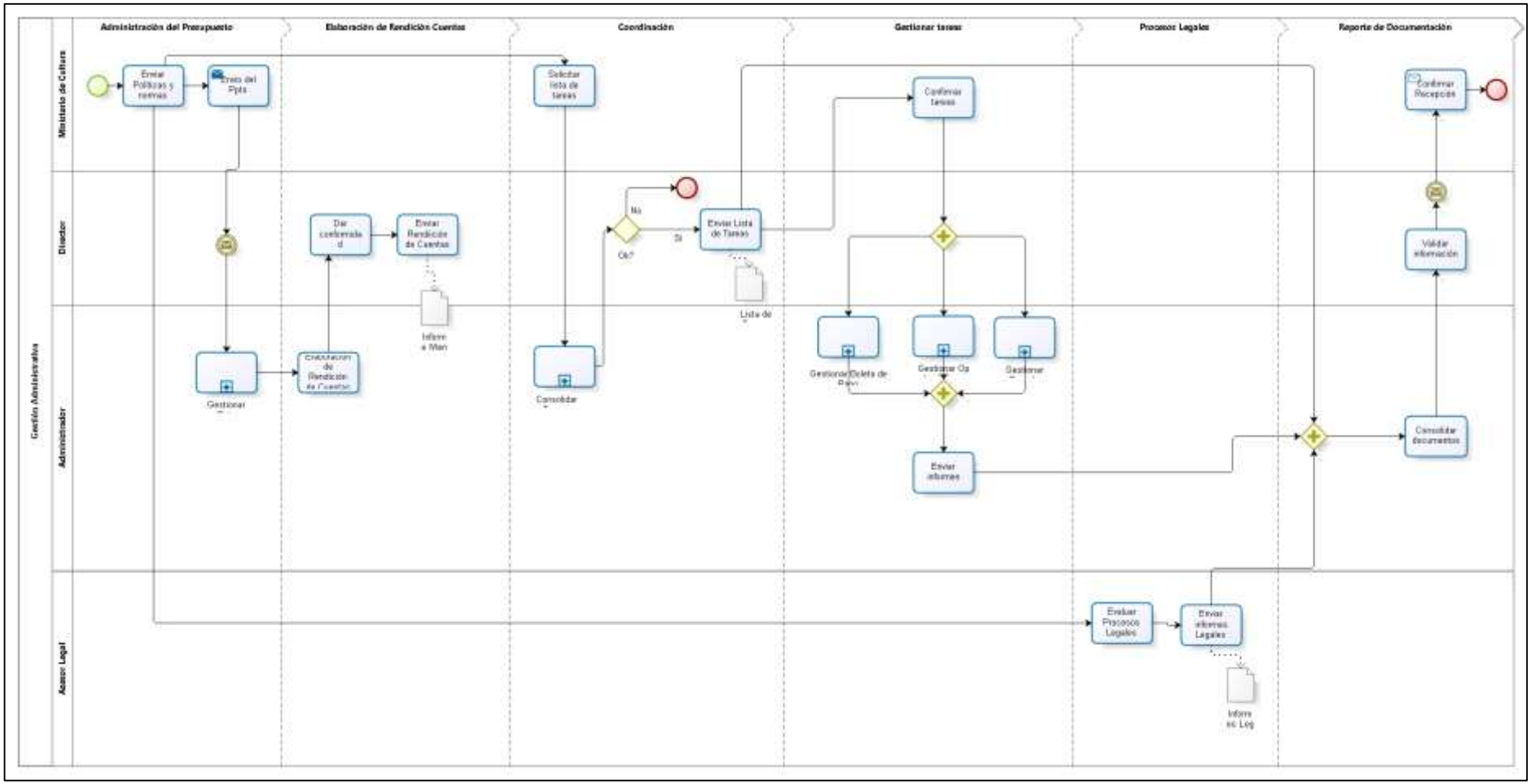


Diagrama 02: Proceso de Gestión Administrativa

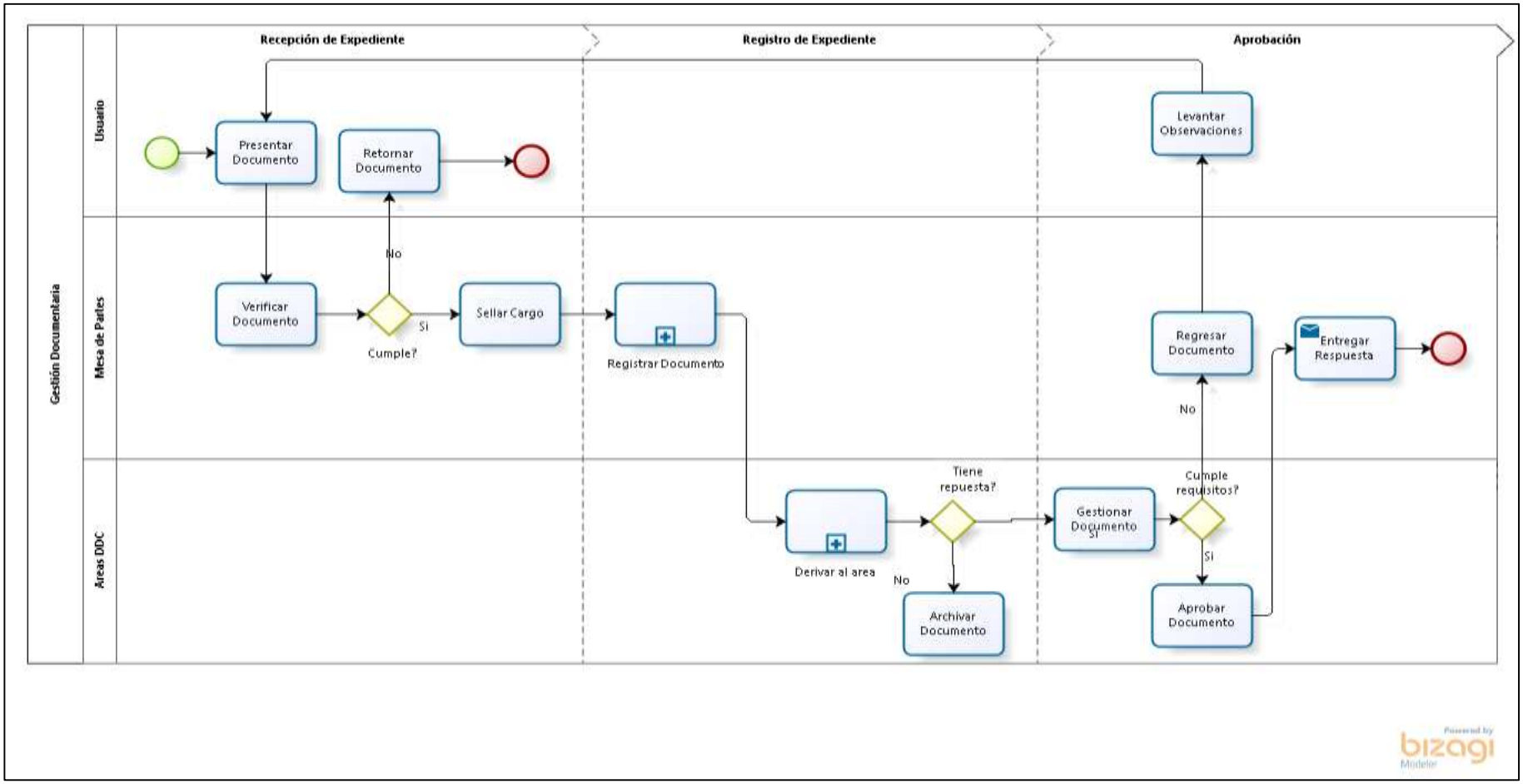


Diagrama 03: Proceso de Gestión Documentaria

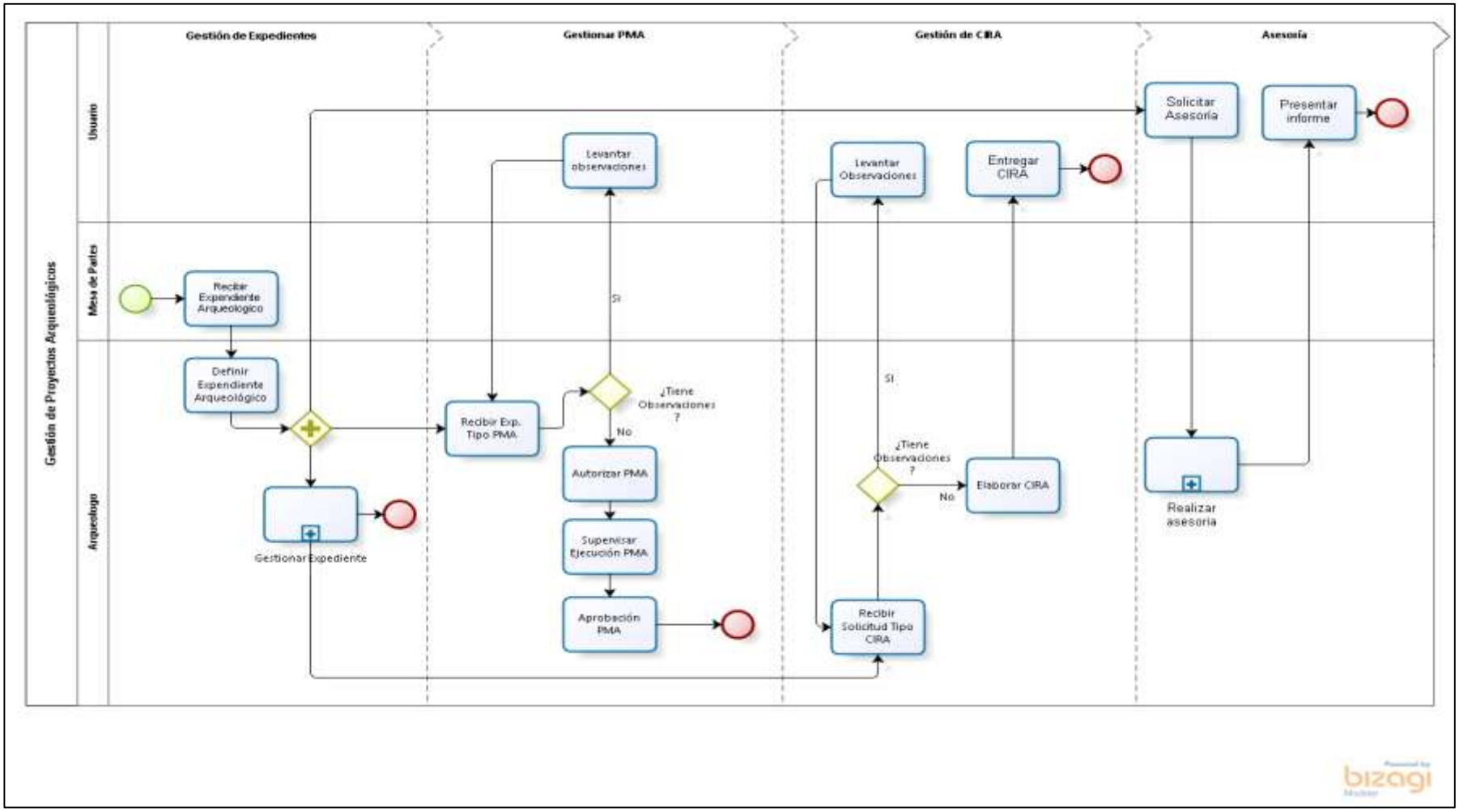


Diagrama 04: Proceso de Gestión Proyectos Arqueológicos

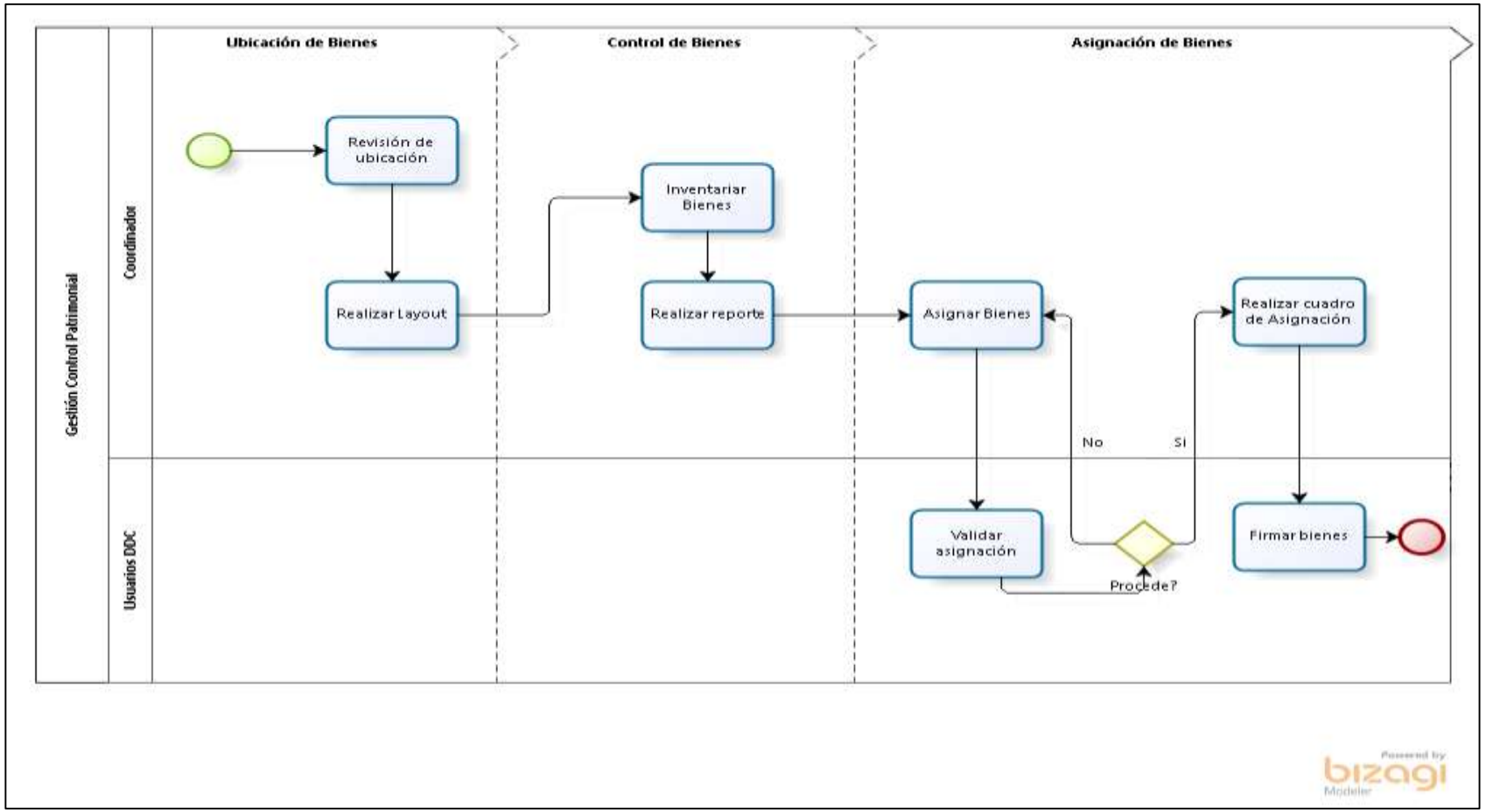


Diagrama 05: Proceso de Gestión Control Patrimonial

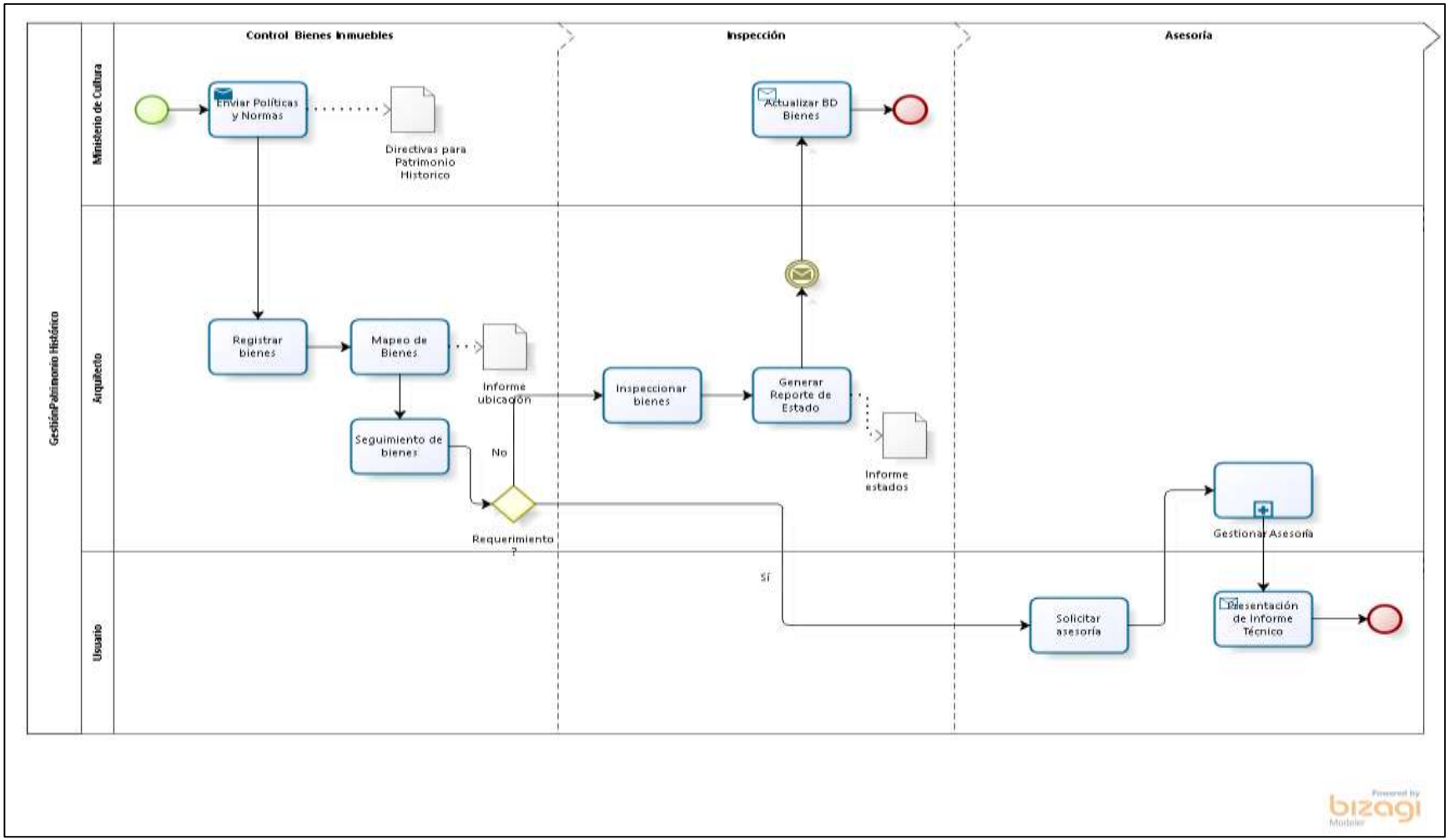


Diagrama 06: Proceso de Gestión Patrimonio Histórico

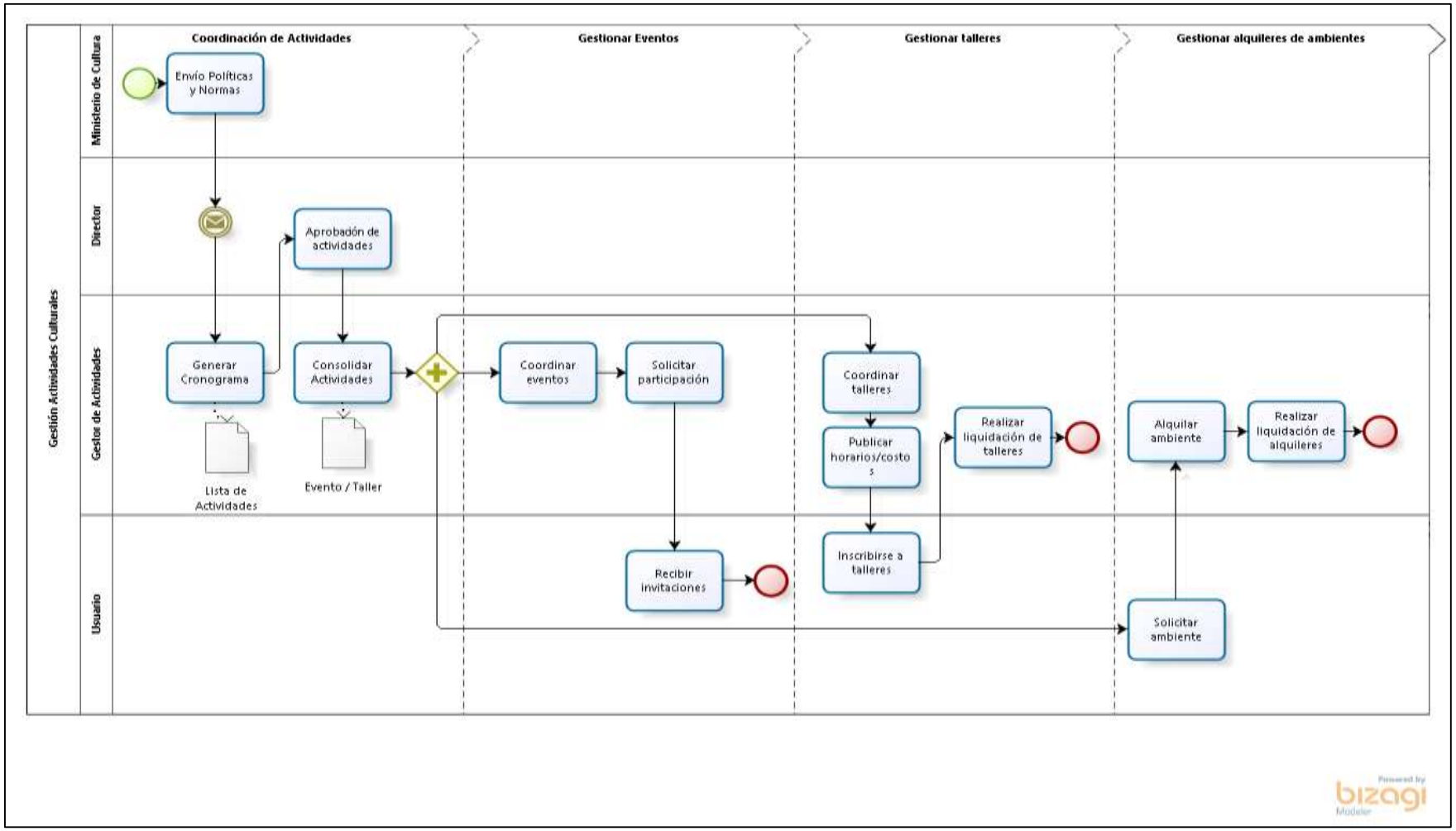


Diagrama 07: Proceso de Gestión Actividades culturales

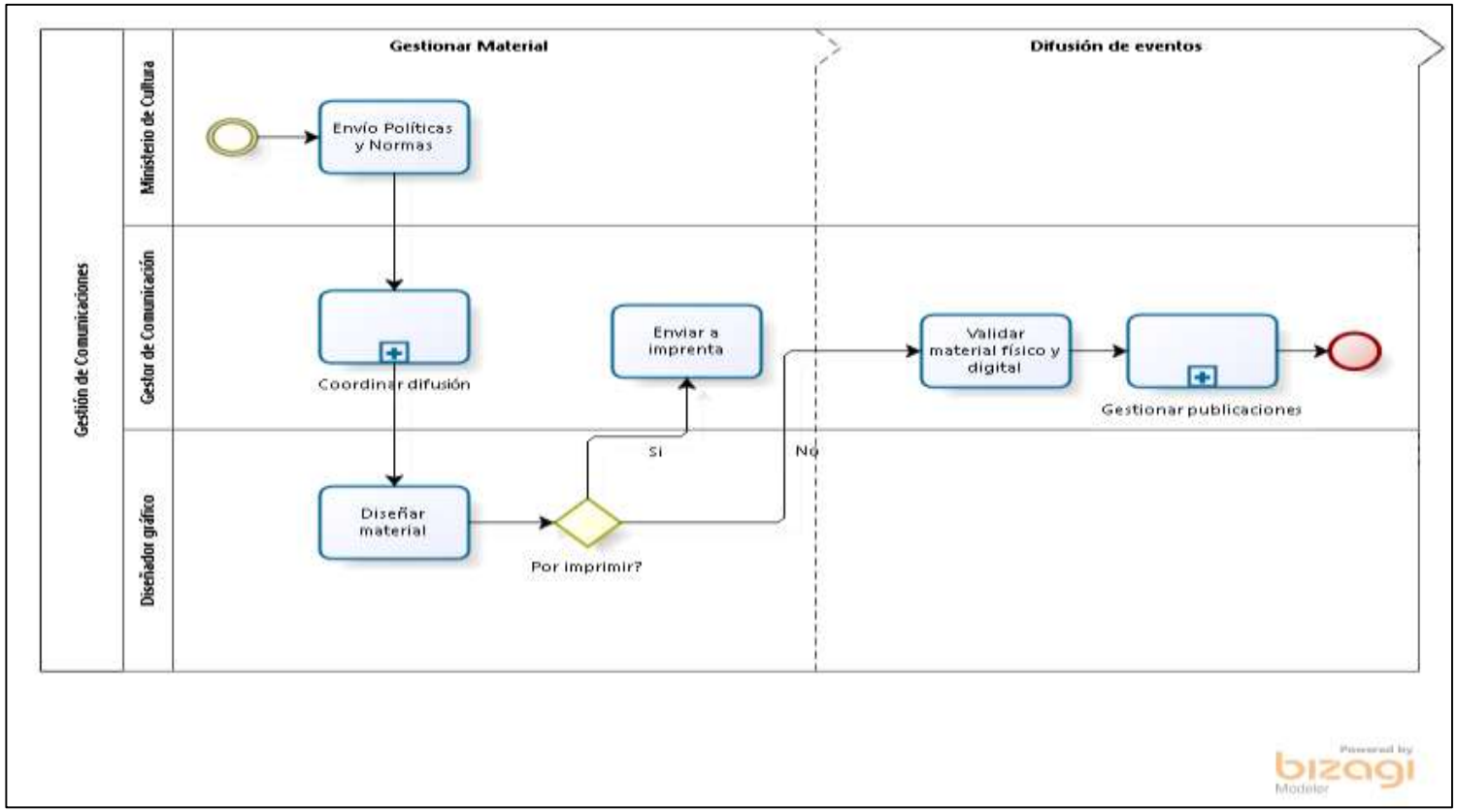


Diagrama 08: Proceso de Gestión de Comunicaciones

Anexo 13: Alcance del SGSI

ALCANCE DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA LA DIRECCIÓN DESCONCENTRADA DE CULTURA DE LAMBAYEQUE

Código:	**SGSI-001**
Versión:	0.1
Fecha de la versión:	03/07/2017
Creado por:	Clara Patricia Cubas Penas

1. Objetivo, alcance y usuarios

1.1 Objetivos

Este documento se aplica a toda la documentación y actividades dentro del SGSI.

Los usuarios de este documento son los miembros de la alta dirección, los miembros del equipo del proyecto que implementa el SGSI en la Dirección Desconcentrada de cultura de Lambayeque, y todos los colaboradores de la institución.

1.2 Alcance

Se aplica a todas las actividades que serán realizadas dentro del proyecto de implementación del SGSI.

1.3 Usuarios

- Miembros de la alta dirección
- Miembros del comité de SGSI

2. Documentos de referencia

- RESOLUCIÓN MINISTERIAL N° 004-2016-PCM
- NTP ISO/IEC 27001:2014
- ISO/IEC 27001:2013
- ISO/IEC 27002:2013

3. Definición del Alcance

La institución necesita tener establecidos los límites del SGSI para decidir qué información se quiere proteger para luego aplicar medidas de seguridad según como se administre el tratamiento de esa información.

El alcance del SGSI se define de acuerdo a los siguientes aspectos:

3.1. Procesos y Sub procesos

Los procesos y sub procesos definidos de la institución son los siguientes:

1. Gestión Directiva

    1.1 Supervisar las actividades de la institución
    1.2 Dar conformidad de los proyectos culturales en la región.

1.3 Solicitar documentación dirigida a DDC Lambayeque
1.4 Reportar al ministerio las incidencias DDC Lambayeque

2. Gestión Administrativa

2.1 Administración del presupuesto
2.2 Elaboración de informe Rendición de cuentas
2.3 Coordinación con Sede Central
2.4 Gestionar tareas
2.5 Seguimiento procesos legales (judiciales y policiales)
2.6 Reportar documentación a Director DDC

3. Gestión documentaria

3.1 Recepción de Expedientes
3.2 Registro de Expedientes
3.3 Aprobación de Recepción

4. Gestión de Proyectos Arqueológicos

4.1 Gestionar de Expedientes Arqueológico
4.2 Gestionar PMA
4.3 Gestionar CIRA
4.4 Asesoría de Proyectos Arqueológicos

5. Gestión de Control Patrimonial

5.1 Ubicación de Bienes Muebles
5.2 Control de Bienes Muebles
5.3 Asignación de bienes Muebles

6. Gestión del Patrimonio Histórico

6.1 Control Bienes inmuebles
6.2 Inspección de Bienes inmuebles
6.3 Asesoría a usuarios

7. Gestión Actividades Culturales

7.1 Coordinación de actividades
7.2 Gestionar eventos
7.3 Gestionar talleres
7.4 Gestionar alquiler de ambientes

8. Gestión de Comunicaciones

8.1 Gestionar Material
8.2 Difusión de Eventos Culturales

3.2. Unidades Organizativas

El presente alcance abarcará todas las oficinas de la Dirección Desconcentrada de cultura de Lambayeque.

- Dirección Regional

- Oficina de Asesoría Legal
- Oficina de Administración
- Oficina de Control Patrimonial
- Oficina de Almacén
- Oficina de Arquitectura/Patrimonio Histórico
- Oficina de Arqueología
- Oficina de Actividades Culturales
- Oficina de Trámite Documentario
- Oficina de Comunicaciones e Imagen Institucional

3.3. Ubicación

El sistema cubrirá los procesos y activos de información de la Dirección Desconcentrada de Cultura de Lambayeque ubicado en la Avenida Luis Gonzáles N° 345 en la ciudad de Chiclayo, departamento de Lambayeque.

3.2. Exclusiones del Alcance

El alcance abarca toda la institución, sin exclusiones de procesos o actividades por ser una pequeña organización.

9 Validez y Gestión de Documentos

El uso del presente documento solo puede aprobarse por el director de la Dirección desconcentrada de cultura de Lambayeque, quien podrá determinar su validez y el plazo de vigencia del documento.

La mejora continua de este documento depende directamente del comité de Seguridad de la información de la Dirección Desconcentrada de cultura de Lambayeque.

El presente documento se ha realizado con fines académicos como parte de una investigación de tesis para obtener el título profesional.

Anexo 14: Política del SGSI

POLÍTICA DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA LA DIRECCIÓN DESCONCENTRADA DE CULTURA DE LAMBAYEQUE

Código:	**SGSI-002**
Versión:	0.1
Fecha de la versión:	03/07/2017
Creado por:	Clara Patricia Cubas Penas

1. Objetivo, alcance y usuarios

El propósito de esta política es definir el objetivo, dirección, principios y reglas básicas para la gestión de la seguridad de la información.

Esta Política se aplica a todo el Sistema de gestión de seguridad de la información de la Dirección desconcentrada de cultura de Lambayeque, según se define en el Documento del Alcance del SGSI.

Los usuarios de este documento son todos los colaboradores de la Dirección desconcentrada de cultura de Lambayeque, como también terceros externos a la organización.

2. Documentos de referencia

- RESOLUCIÓN MINISTERIAL Nº 004-2016-PCM
- NTP ISO/IEC 27001:2014
- ISO/IEC 27001:2013
- ISO/IEC 27002:2013
- SGSI-001 - Documento sobre el alcance del SGSI
- Metodología de evaluación y tratamiento de riesgos - MEHARI
- Declaración de aplicabilidad

3. Terminología básica sobre seguridad de la información

A continuación la terminología más importante con respecto a seguridad de la información:

- **Confidencialidad**: característica de la información que está disponible solo para personas o sistemas autorizados.
- **Integridad**: característica de la información que es modificada solo por personas o sistemas autorizados y de una forma permitida.
- **Disponibilidad**: característica de la información a la cual pueden acceder solo las personas autorizadas cuando sea necesario.
- **Seguridad de la información**: es la preservación de la confidencialidad, integridad y disponibilidad de la información.

- **Sistema de gestión de seguridad de la información**: parte de los procesos generales de gestión que se encarga de planificar, implementar, mantener, revisar y mejorar la seguridad de la información.

4. Gestión de la seguridad de la información

4.1 Objetivos y medición

Se han definido los siguientes objetivos del SGSI:

- Proteger adecuadamente la información de la institución con el fin de asegurar el cumplimiento de la confidencialidad, integridad y disponibilidad de la información.
- Definir las reglas generales que aseguren el tratamiento adecuado de los riesgos.
- Fortalecer una cultura en seguridad de la información, concientizando a los colaboradores de la institución.
- Asegurar la implementación de las medidas de seguridad, identificando recursos necesarios para su cumplimiento.
- Preparar a la institución para el cumplimiento de la resolución ministerial N° 004-2016-PCM que solicita el uso obligatorio de la Norma Técnica Peruana "ISO NTP/IEC 27001:2014.

4.2 Requisitos para la seguridad de la información

Los requisitos necesarios para la seguridad de la información deben incluir las decisiones de la Dirección desconcentrada de cultura de Lambayeque, que asegure que las acciones que realizadas respondan a las normas establecidas.

La documentación del Sistema de Gestión de Seguridad de la información deberá incluir lo siguiente:

- Alcance del SGSI
- Informe de inventario de Activos
- Informe de evaluación de riesgos
- Plan de tratamiento de riesgos
- Declaración de aplicabilidad
- Procedimientos documentados de la institución.

4.3 Responsabilidades

Para el cumplimiento de la presente política de seguridad de la información en la Dirección Desconcentrada de Cultura de Lambayeque, se establecen las siguientes responsabilidades:

- Dirección Regional: Aprobar la política de seguridad y sus futuras modificación con el visto bueno del Comité de Seguridad de la información de la Dirección desconcentrada de cultura de Lambayeque.

- Comité de Gestión de Seguridad de la información: Dirigir, coordinar y supervisar la implementación y funcionamiento de la seguridad de la información en la Dirección desconcentrada de Cultura.

- Oficial de Seguridad de la Información: Supervisar el cumplimiento de la presente política en coordinación con las oficinas de la institución.

- Usuario: Ser responsables del uso de los activos de información a los que tiene acceso autorizado.

4.4 Controles

- Proceso disciplinario: Se determina que ante el incumplimiento de la presente política es necesario aplicar un proceso disciplinario, teniendo en cuenta que los colaboradores tienen conocimiento y el compromiso de cumplir todas las políticas y procedimientos. El detalle del proceso disciplinario lo decidirá el director de la institución.
- Derecho de propiedad intelectual: Se determina que todos los colaboradores cuentan con el derecho de la propiedad intelectual, derecho que debe ser respetado por todos los colaboradores de la institución.
- Privacidad y protección de la información de identificación personal: La institución se responsabiliza de toda la información otorgada por los colaboradores con el compromiso del buen manejo por ser información sensible.

5. Validez y Gestión de Documentos

El uso del presente documento solo puede aprobarse por el director de la Dirección desconcentrada de cultura de Lambayeque, quien podrá determinar su validez y el plazo de vigencia del documento.

La mejora continua de este documento depende directamente del comité de Seguridad de la información de la Dirección Desconcentrada de cultura de Lambayeque.

El presente documento se ha realizado con fines académicos como parte de una investigación de tesis para obtener el título profesional.

Anexo 15: Metodología de gestión de riesgos para SGSI

METODOLOGÍA PARA LA GESTIÓN DE RIESGOS EN LA DIRECCIÓN DESCONCENTRADA DE CULTURA DE LAMBAYEQUE

Código:	**SGSI-003**
Versión:	0.1
Fecha de la versión:	03/07/2017
Creado por:	Clara Patricia Cubas Penas

1. Objetivo, alcance y usuarios

El objetivo del presente documento es definir la metodología para evaluar y tratar los riesgos de la información en la Dirección desconcentrada de cultura de Lambayeque y definir el nivel aceptable de riesgo según la norma ISO/IEC 27001.

La evaluación y tratamiento de riesgos se aplica a todo el alcance del Sistema de gestión de seguridad de la información (SGSI); es decir, a todos los activos que se utilizan dentro de la organización o que pueden tener un impacto sobre la seguridad de la información en el ámbito del SGSI.

Los usuarios de este documento son todos los colaboradores de la Dirección desconcentrada de cultura de Lambayeque.

2. Documentos de referencia

- RESOLUCIÓN MINISTERIAL Nº 004-2016-PCM
- NTP ISO/IEC 27001:2014
- Norma ISO/IEC 27001, capítulos A.9.1.1, A.9.1.2, A.9.2.1, A.9.2.2, A.9.2.3, A.9.2.4, A.9.2.5
- SGSI-001 - Documento sobre el alcance del SGSI
- SGSI-002 – Política del SGSI
- Declaración de aplicabilidad

3. Metodología de evaluación de riesgos

La metodología MEHARI acrónimo de Método para el Análisis Armonizado del Riesgo (MEthod for Harmonized Analysis of RIsk) tiene 3 fases para la administración de riesgos como parte de la implementación del SGSI.

3.1 Fase 1: Análisis de Riesgos

La evaluación de los riesgos consiste en identificar, de la manera más exhaustiva posible, todos los riesgos a los que está expuesta una empresa u organización, estimar la gravedad de cada riesgo y juzgar si cada riesgo se evalúa como aceptable o no.

a. Identificación de riesgos

Este paso apunta no sólo a buscar y reconocer situaciones de riesgo, sino también a caracterizar cada uno de estos riesgos con suficiente precisión para lograr estimar su gravedad.

b. Estimación de riesgos:

Este paso tiene por objeto estimar la gravedad de cada riesgo previamente identificado, teniendo en cuenta las diferentes medidas de seguridad implementadas.

c. Evaluación de riesgos:

La gravedad de cada escenario o situación de riesgo es una función de su probabilidad e impacto residual.

Para ello es necesario desarrollar una tabla de aceptabilidad del riesgo considerando 4 tipos de riesgo:

- Riesgos intolerables.
- Riesgos inadmisibles.
- Riesgos tolerables.
- Riesgos aceptables.

3.2 Fase 2: Tratamiento de Riesgos

Hay diferentes opciones disponibles para tratar los riesgos una vez que se han identificado, enumerado y evaluado, es decir, una vez que cada riesgo se ha considerado aceptable o no.

En esta fase se examinarán las cuatro principales opciones disponibles para el tratamiento de riesgos, las cuales se describen en la norma ISO/IEC 27005 y se representan en el siguiente diagrama. Estas opciones son: Retener, Reducir, Transferir y Evitar.

3.3 Fase 3: Gestión de Riesgos

Implica todos los procesos que facilitan la implementación de las decisiones tomadas anteriormente en relación con el tratamiento de los riesgos, el seguimiento del efecto de estas decisiones y su mejora si es necesario.

a. Elaboración de planes de acción

Como tal, los planes de acción deben desarrollarse de acuerdo con los siguientes pasos:

- Elija objetivos prioritarios en términos de servicios de seguridad para implementar y optimizar esta elección,
- Transformar la (s) elección (es) de servicios de seguridad en planes de acción concretos (contar previamente con un manual de referencia de los servicios de seguridad).
- Elija posibles medidas estructurales y medidas de prevención del riesgo.
- Validar las decisiones anteriores.

b. Implementación de planes de acción

La implementación de los planes de acción puede plantear problemas de aplicación en contextos específicos.

En este caso, es importante poder referirse a los riesgos que cada plan de acción debía reducir para determinar la mejor respuesta.

c. Seguimiento y gestión directa de los riesgos

El primer nivel de monitoreo consiste en verificar que las soluciones y mecanismos de seguridad planificados y seleccionados corresponden efectivamente a los niveles de calidad de servicio escogidos durante la fase de tratamiento de riesgos.

La segunda verificación está relacionada con el cumplimiento de la implementación.

La dirección general de la gestión directa de riesgos es similar a toda la dirección del proyecto e incluye:

- Indicadores y un cuadro de indicadores,
- Un sistema de presentación de informes,
- Un sistema para revisiones periódicas y toma de decisiones sobre las acciones correctivas necesarias.

Anexo 16: Declaración de aplicabilidad del SGSI

DECLARACIÓN DE APLICABILIDAD DEL SGSI PARA LA DIRECCIÓN DESCONCENTRADA DE CULTURA DE LAMBAYEQUE

Código:	**SGSI-004**
Versión:	0.1
Fecha de la versión:	03/07/2017
Creado por:	Clara Patricia Cubas Penas

1. Objetivo, alcance y usuarios

El objetivo del presente documento es presentar la declaración de aplicabilidad en la Dirección desconcentrada de cultura de Lambayeque y definir el nivel aceptable de riesgo según la norma ISO/IEC 27001.

La declaración de aplicabilidad se aplica a todo el alcance del Sistema de gestión de seguridad de la información (SGSI); es decir, a todos los activos que se utilizan dentro de la organización o que pueden tener un impacto sobre la seguridad de la información en el ámbito del SGSI.

Los usuarios de este documento son todos los colaboradores de la Dirección desconcentrada de cultura de Lambayeque.

2. Documentos de referencia

- RESOLUCIÓN MINISTERIAL Nº 004-2016-PCM
- NTP ISO/IEC 27001:2014
- Norma ISO/IEC 27001, capítulos A.9.1.1, A.9.1.2, A.9.2.1, A.9.2.2, A.9.2.3, A.9.2.4, A.9.2.5
- SGSI-001 - Documento sobre el alcance del SGSI
- SGSI-002 – Política del SGSI

3. Declaración de aplicabilidad

Según la documentación solicitada por el sistema de gestión de seguridad de la información, basado en la ISO 27001:2013, se propone también el siguiente listado de controles detallados en el Anexo A de la norma, eligiendo que controles pueden ser implementados o deben implementarse según el requerimiento de seguridad de la institución, este importante documento es la "Declaración de aplicabilidad".

En este documento se presenta el listado de los 114 controles, eligiendo que controles si son aplicables en la institución, su justificación y un breve comentario de lo que sería su implementación.

Clausula	Sección	Objetivo de Control / Control	Es Aplicable a la organización	Justificación	Comentarios (Sobre la implementación en DDC Lambayeque)
5. Políticas de Seguridad	5.1	Dirección de la Alta Gerencia para la Seguridad de la Información			
	5.1.1	Políticas de Seguridad de la Información	Aplica	Actualmente la institución no cuenta con políticas de Seguridad de la información.	Para iniciar un Sistema de gestión de seguridad de la información es necesario establecer una Política de Seguridad de la información, se ha realizado una propuesta.
	5.1.2	Revisión de las Políticas de Seguridad de la Información	Aplica	Actualmente la institución no cuenta con políticas de Seguridad de la información, cómo parte del diseño del SGSI se ha realizado dentro de esta propuesta.	Es necesario que la política de seguridad de la información sea revisada y aprobada.
6. Organización de la seguridad de la información	6.1	Organización interna			
	6.1.1	Roles y Responsabilidad de Seguridad de la Información	Aplica	Actualmente no existen roles de seguridad de la información, esta responsabilidad estará a cargo por el administrador.	Es necesario que la institución apruebe los roles indicados en la política de seguridad de la información.
	6.1.2	Segregación de deberes	Aplica	Actualmente no existen roles de seguridad de la información, esta responsabilidad estará a cargo por el administrador.	Es necesario que se revise y apruebe lo indicado en las políticas de seguridad de la información establecida en esta propuesta.
	6.1.3	Contacto con autoridades	Aplica	Anteriormente no se ha realizado el contacto para este proceso.	Es importante realizar reuniones para la aprobación del SGSI.
	6.1.4	Contacto con grupos de interés especial	Aplica	Anteriormente no se ha realizado el contacto para este proceso.	Es importante realizar reuniones para la aprobación del SGSI.
	6.1.5	Seguridad de la Información en la gestión de proyectos	Aplica	Una de las principales funciones de la institución es gestionar proyectos.	Es necesario implementar un sistema de seguridad de la información.
	6.2	Dispositivos móviles y teletrabajo			
	6.2.1	Política de dispositivos móviles	No Aplica	-	Los principales riesgos de la institución no están vinculados a dispositivos móviles.

Anexo 17: Plan de tratamiento de riesgos del SGSI

PLAN DE TRATAMIENTO DE RIESGOS DEL SISTEMA DE GESTIÓN DE SEGURIDAD LA INFORMACIÓN DE LA DIRECCIÓN DESCONCENTRADA DE CULTURA DE LAMBAYEQUE

Código:	**SGSI-005**
Versión:	0.1
Fecha de la versión:	03/07/2017
Creado por:	Clara Patricia Cubas Penas

1. Objetivo, alcance y usuarios

El objetivo del presente documento es garantizar el funcionamiento correcto y seguro de la tecnología de la información y de la comunicación.

Este documento se aplica a todo el alcance del Sistema de gestión de seguridad de la información (SGSI).

Los usuarios de este documento son todos los colaboradores de la Dirección desconcentrada de cultura de Lambayeque.

2. Documentos de referencia

- RESOLUCIÓN MINISTERIAL Nº 004-2016-PCM
- NTP ISO/IEC 27001:2014
- SGSI-001 - Documento sobre el alcance del SGSI
- SGSI-002 – Política del SGSI
- Declaración de aplicabilidad

3. Tratamiento de Riesgos

Según la metodología MEHARI, las medidas de seguridad implementadas pueden actuar como factores de reducción del riesgo. Para manejar los riesgos, es necesario entender cómo, en qué nivel estas medidas reducen el riesgo.

3.1 Factores de reducción de la probabilidad

Medidas adecuadas pueden reducir la probabilidad de riesgo a través de diversos mecanismos que pueden actuar de forma independiente o acumulativa.

- **Medidas disuasorias**, dirigidas a las acciones humanas y destinadas a hacer menos probable que un actor realice la acción.
- **Medidas preventivas**, cuyo objetivo es hacer menos probable que cualquier acción, ya sea humana o no, conduzca a la aparición del riesgo.

3.2 Factores de reducción del impacto

Medidas adecuadas pueden reducir el impacto del riesgo (el nivel de sus consecuencias) a través de diversos mecanismos que pueden actuar de forma independiente o acumulativa y no se aplican a los mismos tipos de consecuencias.

- **Las medidas de protección**, que tienen por objeto limitar la magnitud de las consecuencias directas.
- **Las medidas de mitigación**, cuyo objetivo es minimizar las consecuencias indirectas de un riesgo, anticipando la gestión de crisis.

4. Plan Tratamiento de Riesgos

A continuación un modelo para realizar un plan de tratamiento según tipo de medida:

TIPO DE MEDIDA	MEDIDAS POR IMPLEMENTAR
Disuasoria	Elaboración de declaración de confidencialidad
	Elaboración de política del SGSI
	Elaboración de declaraciones y compromisos.
	Sensibilización y capacitación
Mitigación	Elaboración de política de control de acceso del SGSI.
	Elaboración de política de transferencia de información
Preventiva	Adquisición de Software open source
	Elaboración de política de continuidad
	Elaboración de política de gestión de activos del SGSI
	Elaboración de procedimiento gestión de incidentes
	Elaboración de procedimiento TI
	Elaboración de procedimiento zonas seguras
	Validación del sistema de vigilancia y monitoreo
Protección	Adquisición de licencia software propietario
	Adquisición de Software open source
	Elaboración de política
	Propuesta de cableado estructurado
	Elaboración de procedimiento TI

El plan de tratamiento del sistema de gestión de seguridad de la información se puede visualizar en el anexo 01: Plan de tratamiento de Riesgos.

5. Validez y Gestión de Documentos

El uso del presente documento solo puede aprobarse por el director de la Dirección desconcentrada de cultura de Lambayeque, quien podrá determinar su validez y el plazo de vigencia del documento.

La mejora continua de este documento depende directamente del comité de Seguridad de la información de la Dirección Desconcentrada de cultura de Lambayeque.

El presente documento se ha realizado con fines académicos como parte de una investigación de tesis para obtener el título profesional.

ANEXO 01: Plan de tratamiento de Riesgos.

CONTROLES	DESCRIPCIÓN DE CONTROLES	RIESGOS	TIPO DE MEDIDA	MEDIDAS POR IMPLEMENTAR	ACCIONES
7.2.2	Concientización, educación y capacitación en materia de seguridad de la información.	R16,R21,R22,R23,R48	Disuasoria	Sensibilización y capacitación	Presentación en auditorio de la institución, sensibilización con afiches y folletos, Publicidad en computadoras, capacitaciones
7.2.3	Proceso disciplinario	R17,R22,R23,R51,R52	Disuasoria	Elaboración de política del SGSI, declaraciones y compromisos.	Firmas de declaraciones y compromisos, inducción de políticas del SGSI.
8.1.1	Inventario de activos	R17,R51,R52	Preventiva	Adquisición de Software open source	Instalación de Software open source
8.1.2	Propiedad de los activos	R17,R51,R52	Preventiva	Elaboración de política de gestión de activos del SGSI.	Firmar documentación e implementar política.
8.1.3	Uso aceptable de los activos	R12,R16,R29,R48	Preventiva	Elaboración de política de gestión de activos del SGSI.	Firmar documentación e implementar política.
8.3.1	Gestión de medios extraíbles	R12,R70,R17	Preventiva	Elaboración de política de gestión de activos del SGSI.	Firmar documentación e implementar política.
8.3.3	Transferencia de medios físicos	R09	Preventiva	Elaboración de política de gestión de activos del SGSI.	Firmar documentación e implementar política.
9.1.1	Política de control de acceso	R16,R29,R48,R62,R66,R70	Mitigación	Elaboración de política de control de acceso del SGSI.	Firma de documentación e implementación de política.
9.1.2	Acceso a redes y servicios de red	R19,R48,R62,R62,R66	Protección	Elaboración de política, propuesta de cableado estructurado	Implementación de cableado estructurado.

9.2.1	Gestión de altas/bajas en el registro de usuarios	R22,R34,R62,R66	Mitigación	Elaboración de política de control de acceso del SGSI.	Firma de documentación e implementación de política.
9.2.2	Gestión de los derechos de acceso asignados a usuarios	R30,R33,R34,R35,R48,R49,R50,R54	Mitigación	Elaboración de política de control de acceso del SGSI.	Firma de documentación e implementación de política.
9.2.3	Gestión de derechos de acceso privilegiados	R34,R62,R66,R62	Mitigación	Elaboración de política de control de acceso del SGSI.	Firma de documentación e implementación de política.
9.2.4	Gestión de la información de autenticación secreta de los usuarios	R48,R60	Mitigación	Elaboración de política de control de acceso del SGSI.	Firma de documentación e implementación de política.
9.2.5	Revisión de derechos de acceso de usuario	R48	Mitigación	Elaboración de política de control de acceso del SGSI.	Firma de documentación e implementación de política.
9.2.6	Eliminación o ajuste de los derechos de acceso	R48	Mitigación	Elaboración de política de control de acceso del SGSI.	Firma de documentación e implementación de política.
9.3.1	Uso de la información confidencial para la autenticación	R30,R35,R54	Disuasoria	Elaboración de declaración de confidencialidad	Firma de declaración
9.4.1	Restricción de acceso a la información	R60,R62,R66,R70	Mitigación	Elaboración de política de control de acceso del SGSI.	Firma de documentación e implementación de política.
9.4.3	Sistema de gestión de contraseñas	R30,R35,R54	Mitigación	Elaboración de política de control de acceso del SGSI.	Firma de documentación e implementación de política.
9.4.4	Uso de programas de utilidad privilegiada	R32,R60,R70	Mitigación	Elaboración de política de control de acceso del SGSI.	Firma de documentación e implementación de política.
10.1.2	Gestión de claves	R29	Mitigación	Elaboración de política de control de acceso del SGSI.	Firma de documentación e implementación de política.
11.1.1	Perímetro de seguridad física	R17,R21,R23,R34,R50,R51,R52,R55,R57	Preventiva	Elaboración de procedimiento zonas seguras	Firma e implementación de procedimiento.

11.1.2	Controles físicos de entrada	R16,R17,R21,R23,R34,R51,R52,R56,R55,R57	Preventiva	Elaboración de procedimiento zonas seguras	Firma e implementación de procedimiento.
11.1.3	Asegurar oficinas, habitaciones e instalaciones	R16,R21,R23,R34,R50,R51,R52,R55,R56,R57	Preventiva	Elaboración de procedimiento zonas seguras, validación del sistema de vigilancia y monitoreo	Firma e implementación de procedimiento, contrato de un personal externo para validación y mantenimiento del sistema de vigilancia.
11.1.4	Protección contra las amenazas externas y ambientales	R71	Preventiva	Elaboración de procedimiento zonas seguras	Firma e implementación de procedimiento.
11.1.5	Trabajo en áreas seguras	R17,R21,R23,R51,R52	Preventiva	Elaboración de procedimiento zonas seguras, validación del sistema de vigilancia y monitoreo	Firma e implementación de procedimiento, contrato de un personal externo para validación y mantenimiento del sistema de vigilancia.
11.1.6	Zonas de entrega y carga	R09	Preventiva	Elaboración de procedimiento zonas seguras	Firma e implementación de procedimiento.
11.2.1	Ubicación y protección del equipo	R17,R49,R69	Preventiva	Elaboración de procedimiento zonas seguras	Firma e implementación de procedimiento.
11.2.2	Instalaciones de suministro	R71	Preventiva	Elaboración de procedimiento zonas seguras	Firma e implementación de procedimiento.
11.2.4	Mantenimiento de equipo	R69,R70	Preventiva	Elaboración de procedimiento TI	Firma e implementación de procedimiento.
11.2.6	Seguridad de equipos y activos fuera de las instalaciones	R17	Preventiva	Elaboración de procedimiento zonas seguras	Firma e implementación de procedimiento.
11.2.8	Equipo de usuario desatendido	R69, R70	Protección	Elaboración de procedimiento TI	Firma e implementación de procedimiento.
12.2.1	Controles contra el código malicioso	R12,R70	Protección	Adquisición de licencia software propietario	Instalación de software en todos los equipos
12.3.1	Copia de seguridad de la información	R09, R33, R16	Protección	Adquisición de Software open source	Instalación y uso de Software open source por comité de seguridad
			Protección	Elaboración de procedimiento TI	Firma e implementación de procedimiento.

13.1.1	Controles de red	R29,R30,R33,R74	Protección	Elaboración de política, propuesta de cableado estructurado	Implementación de cableado estructurado.
13.1.2	Seguridad de los servicios de red	R19,R29,R30,R33,R49,R62,R74,	Protección	Elaboración de política, propuesta de cableado estructurado	Implementación de cableado estructurado.
13.2.1	Políticas y procedimientos de transferencia de información	R09,R35,R48,R54,R55,R56	Mitigación	Elaboración de política de transferencia de información.	Firmar documentación e implementar política.
13.2.2	Acuerdos sobre transferencia de información	R19,R47,R48,R54,R55,R56	Mitigación	Elaboración de política de transferencia de información.	Firmar documentación e implementar política.
13.2.3	Mensajería electrónica	R19,R35,R54,	Mitigación	Elaboración de política de transferencia de información.	Firmar documentación e implementar política.
13.2.4	Acuerdos de confidencialidad o no divulgación	R22,R47,R48,R49,R50,R54,R55,R56	Disuasoria	Elaboración de declaración de confidencialidad	Firma de declaración
16.1.5	Respuesta a incidentes de seguridad de la información	R62,R71	Preventiva	Adquisición de Software open source	Instalación y uso de Software open source por comité de seguridad
			Preventiva	Elaboración de procedimiento gestión de incidentes	Firma e implementación de procedimiento.
17.1.1	Planificación de la continuidad de la seguridad de la información	R62,R66,R69,R70,R71	Preventiva	Elaboración de política de continuidad.	Firmar documentación e implementar política.
18.1.2	Derechos de propiedad intelectual	R29	Disuasoria	Elaboración de política del SGSI, declaraciones y compromisos.	Firmar documentación e implementar política.
18.1.4	Privacidad y protección de la información de identificación personal	R29, R34	Disuasoria	Elaboración de política del SGSI, declaraciones y compromisos.	Firmar documentación e implementar política.

Anexo 18: Procedimiento de gestión de activos

PROCEDIMIENTO DE GESTIÓN DE ACTIVOS PARA LA DIRECCIÓN DESCONCENTRADA DE CULTURA DE LAMBAYEQUE

Código:	**SGSI-006**
Versión:	0.1
Fecha de la versión:	03/07/2017
Creado por:	Clara Patricia Cubas Penas

1. Objetivo, alcance y usuarios

El objetivo del presente documento es definir reglas claras para el uso de los sistemas y de otros activos de información en la Dirección desconcentrada de Cultura de Lambayeque.

Este documento se aplica a todo el alcance del Sistema de gestión de seguridad de la información (SGSI); es decir, a todos los sistemas, equipos, instalaciones e información utilizados dentro del alcance del SGSI.

Los usuarios de este documento son todos los colaboradores de la Dirección desconcentrada de cultura de Lambayeque.

2. Documentos de referencia

- RESOLUCIÓN MINISTERIAL N° 004-2016-PCM
- NTP ISO/IEC 27001:2014
- SGSI-001 - Documento sobre el alcance del SGSI
- SGSI-002 – Política del SGSI

3. Responsabilidades

Todos los colaboradores de la Dirección desconcentrada de Lambayeque, deben conocer y poner en práctica las disposiciones dadas por el presente procedimiento.

4. Gestión de Activos de la Información

4.1 Definiciones

Activos de información: en el contexto de esta Política, el término activos de información se aplica a los sistemas de información y demás información o equipos, incluyendo documentos en papel, teléfonos móviles, ordenadores portátiles, soportes de almacenamiento de datos, etc.

4.2 Políticas de Uso Aceptable

1. Todas las actividades y funciones dentro de la Dirección desconcentrada de cultura de Lambayeque que se realicen involucrando activos de la información deben estar alineados con la misión de la institución.

2. El comité de seguridad de la institución debe mantener actualizado el inventario de activos.
3. Todos los colaboradores pueden dar alerta de algún evento que perjudique la integridad, disponibilidad y confidencialidad de los activos.
4. Todos los colaboradores deben tener en cuenta las buenas prácticas que se detallen en toda la documentación del SGSI.
5. Los colaboradores tienen prohibido instalar software que no corresponda a sus actividades laborales y además que no cuenten con licencia.
6. Los colaboradores no pueden instalar software interno de la institución en equipos externos.
7. Con respecto a la información sensible de la institución, se le pondrá parámetros de acceso restringido.
8. Ningún colaborador debe compartir usuarios y contraseñas de los sistemas de información.

4.3 Propiedad de los activos

1. Es necesario que el comité de seguridad realice una tabla de asignaciones de activos por usuario.
2. Los colaboradores deberán devolver los activos asignados al finalizar su contrato.
3. Todo colaborador deberá cerrar la sesión de la computadora en la cual se encuentra trabajando si necesita salir de oficina o realizar otra actividad.
4. No está permitido cambiar debe cambiar ni alterar de ninguna forma el hardware o el software de los sistemas de información de la institución, a menos que tenga autorización.
5. Los activos de información de la institución deben usarse única y exclusivamente para el propósito para el que fueron asignados.

4.4 Políticas de gestión de medios extraíbles

1. Están permitidos los medios extraíbles para uso interno y únicamente laboral.
2. Los colaboradores utilizaran sus medios extraíbles previa revisión del antivirus.

4.5 Políticas de transferencia de medios físicos

Es responsabilidad exclusiva del colaborador a quien se le ha dado la custodia, la protección de los medios físicos que están bajo su manejo, debe velar por cuidar los medios dentro y también cuando no se encuentre dentro de las instalaciones de la institución.

Anexo 19: Política de gestión de accesos del SGSI

POLÍTICA DE CONTROL DE ACCESO DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA LA DIRECCIÓN DESCONCENTRADA DE CULTURA DE LAMBAYEQUE

Código:	**SGSI-007**
Versión:	0.1
Fecha de la versión:	03/07/2017
Creado por:	Clara Patricia Cubas Penas

1. Objetivo, alcance y usuarios

El objetivo del presente documento es definir reglas de acceso para diversos sistemas, equipos, instalaciones e información en base a los requerimientos de la institución y de la seguridad.

Este documento se aplica a todo el alcance del Sistema de gestión de seguridad de la información (SGSI); es decir, a todos los sistemas, equipos, instalaciones e información utilizados dentro del alcance del SGSI.

Los usuarios de este documento son todos los colaboradores de la Dirección desconcentrada de cultura de Lambayeque.

2. Documentos de referencia

- RESOLUCIÓN MINISTERIAL Nº 004-2016-PCM
- NTP ISO/IEC 27001:2014
- Norma ISO/IEC 27001, capítulos A.9.1.1, A.9.1.2, A.9.2.1, A.9.2.2, A.9.2.3, A.9.2.4, A.9.2.5
- SGSI-001 - Documento sobre el alcance del SGSI
- SGSI-002 – Política del SGSI
- Declaración de aplicabilidad

3. Control de Acceso

3.1 Introducción

El principio básico es que el acceso a todos los sistemas, redes, servicios e información está prohibido salvo que sea expresamente permitido a usuarios individuales o a grupos de usuarios.

3.2 Objetivos

El control de acceso tiene como principales objetivos:

- Controlar los accesos a la información, evitar accesos no autorizados a los sistemas de información.
- Evitar el acceso de usuarios no autorizados, proteger los servicios en red.
- Evitar accesos no autorizados a ordenadores, el acceso no autorizado a la información contenida en los sistemas.

- Detectar actividades no autorizadas.
- Garantizar la seguridad de la información cuando se usan dispositivos informáticos.

3.3 Definiciones

- Proteger la información valiosa o considerada confidencial con un sistema basado en contraseñas.
- Tener listas de control de acceso, ubicadas en los lugares sensibles para diferenciar los grupos de usuarios.
- Generar funciones de acceso a los recursos en función a las actividades de los grupos de usuarios.
- Determinar los privilegios de usuario, cada usuario debe recibir los derechos mínimos
- para que sean capaces de realizar sus funciones.
- Los usuarios deben tener claro que deben evitar de tratar de forzar o evadir los controles de acceso con el fin de obtener un mayor nivel de acceso.
- Todo personal externo (clientes, proveedores, visitas, etc.) deberá pasar por un control previa solicitud.

3.4 Gestión de accesos

3.4.1 Administración de usuarios

- Las altas y bajas serán gestionadas por cada jefe de oficina a través del sistema de gestión de incidencias, solicitando un ticket de alta o baja de usuario.
- Los derechos de los usuarios serán determinados por los perfiles de usuario definidos por el comité de seguridad.
- Las cuentas que no hayan sido utilizadas en los últimos sesenta días deben ser eliminadas.
- El nivel de acceso debe ser definido por funciones específicas dentro de cada aplicación y para cada usuario.
- La creación, eliminación y revisión de privilegios de los usuarios de la red y las aplicaciones, deberán ser validadas por la oficina de informática del Ministerio de Cultura para luego ser comunicadas a la Dirección desconcentrada de Cultura de Lambayeque.
- La institución deberá enviar mensualmente a la Oficina de informática la lista actualizada de altas, bajas, vacaciones, incapacidades o licencias de la institución.

3.4.2 Gestión de contraseñas

- Cada personal de la dirección desconcentrada de cultura de Lambayeque debe tener asociada una contraseña, de la que será responsable.
- No está permitido que las demás personas (naturales, jurídicas, consultores, contratistas u otros no colaboradores) utilicen contraseñas asignadas al personal de la institución.
- Las contraseñas deberán permanecer enmascaradas en todos los medios tecnológicos en los cuales son digitadas.
- Es responsabilidad directa del personal el velar por la confidencialidad y buen uso de su contraseña.

3.4.3 Revisión de derechos de acceso de usuario

- Se debe revisar los derechos de acceso de los usuarios cada 6 meses.
- Revisar los usuarios y cuentas dobles.
- Revisión de cambios en los usuarios por los puestos de trabajo.

3.4.4 Controles de accesos a la red

- El comité de seguridad de la institución, garantizará a la institución los niveles de acceso del personal, a excepción de los que se encuentren de vacaciones o licencia.

3.4.5 Controles de acceso a aplicaciones

- Las aplicaciones incluirán un adecuado control de acceso basado en el análisis de las funciones que la aplicación tiene desarrolladas y las autorizaciones por grupos de usuarios, roles y perfiles.

4. Validez y Gestión de Documentos

El uso del presente documento solo puede aprobarse por el director de la Dirección desconcentrada de cultura de Lambayeque, quien podrá determinar su validez y el plazo de vigencia del documento.

La mejora continua de este documento depende directamente del comité de Seguridad de la información de la Dirección Desconcentrada de cultura de Lambayeque.

El presente documento se ha realizado con fines académicos como parte de una investigación de tesis para obtener el título profesional.

Anexo 20: Procedimiento Trabajo en zonas seguras

PROCEDIMIENTO TRABAJO EN ZONAS SEGURAS DE LA DIRECCIÓN DESCONCENTRADA DE CULTURA DE LAMBAYEQUE

Código:	**SGSI-008**
Versión:	0.1
Fecha de la versión:	03/07/2017
Creado por:	Clara Patricia Cubas Penas

1. Objetivo, alcance y usuarios

El objetivo del presente documento es garantizar el funcionamiento correcto y seguro de la tecnología de la información y de la comunicación.

Este documento se aplica a todo el alcance del Sistema de gestión de seguridad de la información (SGSI); es decir, a todos los sistemas, equipos, instalaciones e información utilizados dentro del alcance del SGSI.

Los usuarios de este documento son todos los colaboradores de la Dirección desconcentrada de cultura de Lambayeque.

2. Documentos de referencia

- RESOLUCIÓN MINISTERIAL N° 004-2016-PCM
- NTP ISO/IEC 27001:2014
- SGSI-001 - Documento sobre el alcance del SGSI
- SGSI-002 – Política del SGSI

3. Reglas para Zonas Seguras

3.1 Lista de zonas seguras

1. Determinar las áreas con información sensible y tener una lista de las oficinas con los usuarios involucrados.
2. Realizar un formato de firmas de accesos a áreas con información sensible.

3.2. Derechos de Acceso

1. Los accesos los determinará el comité de seguridad de la institución.
2. En zonas de acceso restringido, solo las personas con permisos podrán acceder.
3. Las áreas seguras se deberían proteger mediante controles de entrada apropiados para asegurar que solamente se permite el acceso a personal autorizado.

3.3. Controles de Ingreso

1. El control del ingreso de personal interno o externo está a cargo del personal de seguridad en portería.
2. El acceso de visitantes es validado por el personal de vigilancia, solicitando documento de identificación y realizando la consulta del motivo de la visita, el personal de vigilancia pedirá el visto bueno al área involucrada y registrará el ingreso del usuario.
3. La portería cuenta con un sistema de vigilancia y un servicio de contrato externo que deberá ser periódicamente validado y solicitado por el comité de seguridad de la institución.

3.4 Ubicación y protección del equipo

1. La ubicación será determinada por el encargado de control patrimonial de la institución.
2. Los colaboradores deben respetar la ubicación de los equipos como se encuentren en el lay out de distribución.
3. Cada colaborador es responsable de los equipos asignados durante sus términos de contrato laboral.

4. Validez y Gestión de Documentos

El uso del presente documento solo puede aprobarse por el director de la Dirección desconcentrada de cultura de Lambayeque, quien podrá determinar su validez y el plazo de vigencia del documento.

La mejora continua de este documento depende directamente del comité de Seguridad de la información de la Dirección Desconcentrada de cultura de Lambayeque.

El presente documento se ha realizado con fines académicos como parte de una investigación de tesis para obtener el título profesional.

Anexo 21: "Procedimientos operativos para la gestión de TI

PROCEDIMIENTOS OPERATIVOS PARA LA GESTIÓN DE TI EN LA DIRECCIÓN DESCONCENTRADA DE CULTURA DE LAMBAYEQUE

Código:	**SGSI-009**
Versión:	0.1
Fecha de la versión:	03/07/2017
Creado por:	Clara Patricia Cubas Penas

1. Objetivo, alcance y usuarios

El objetivo del presente documento es garantizar el funcionamiento correcto y seguro de la tecnología de la información y de la comunicación.

Este documento se aplica a todo el alcance del Sistema de gestión de seguridad de la información (SGSI); es decir, a todos los sistemas, equipos, instalaciones e información utilizados dentro del alcance del SGSI.

Los usuarios de este documento son todos los colaboradores de la Dirección desconcentrada de cultura de Lambayeque.

2. Documentos de referencia

- RESOLUCIÓN MINISTERIAL Nº 004-2016-PCM
- NTP ISO/IEC 27001:2014
- SGSI-001 - Documento sobre el alcance del SGSI
- SGSI-002 – Política del SGSI

3. Procedimientos operativos para tecnología de la información y de la comunicación

3.1 Documentación operativa

Los procedimientos físicos estarán documentados y a disposición de los usuarios vinculados a esas funciones, por el comité de seguridad.
Es responsabilidad del Comité de Seguridad, mantener debidamente actualizada toda la documentación referente al sistema de gestión de seguridad de la información de la Dirección desconcentrada de cultura de Lambayeque.

3.1 Control de Cambios

Cualquier cambio relacionado a la información deberá ser completamente documentado y controlado por el Comité de Seguridad de la institución.
Cualquier cambio en la plataforma de las estaciones de trabajo deberá ser autorizado por el Comité de Seguridad.

3.2 Uso de la Tecnología

El Comité de Seguridad de información definirá los criterios de utilización de los servicios de tecnología y el adecuado uso de los equipos, que deben ser usados solo a beneficio de la institución.

3.3 Servicios de red

Es tarea del Comité de Seguridad de la institución notificar el correcto funcionamiento de los servicios de red, manteniendo un constante monitoreo sobre la red interna.

Ante algún incidente, el Comité de Seguridad deberá comunicarse con la para una pronta solución a los servicios de red.

3.4 Servicios Web

La administración supervisará el correcto funcionamiento de la página de la Dirección desconcentrada de cultura de Lambayeque: wwww.facebook.com/DDCLambayeque.

3.5 Software

Todo el personal de la Dirección desconcentrada de cultura de Lambayeque tiene prohibido instalar o utilizar software o productos sin licencias autorizadas por la institución.

3.6 Equipos de cómputo

Los equipos de cómputo utilizados fuera de la institución y en funciones asignadas, deben ser exclusivamente utilizados para brindar apoyo a las actividades de la institución.

Las computadoras personales, pueden conectarse a la red de la institución previa autorización del Comité de Seguridad.

Durante los viajes, los equipos y medios magnéticos deben cuidarse con el fin de no exponerlos a pérdidas o robos con el fin de prevenir el acceso no autorizado.

La utilización de elementos removibles de almacenamiento (DVD's, memorias USB, CD's reescribirles, discos duros portátiles, etc.) por parte de los usuarios, deberán ser usados responsablemente, cabe resaltar que el Comité de Seguridad (custodia, reutilización y destrucción) adecuada de estos, tanto para su conservación como la destrucción, cuando fuera necesario, estará determinada con autorización del Comité de Seguridad.

El ingreso y/o salida de los equipos de cómputo deben ser autorizados por la Administración y registrado por el Comité de Seguridad.

El usuario deberá cerrar la sesión de su equipo de cómputo, si necesita salir de oficina o realizar otra actividad.

3.6.1 Mantenimiento de equipos

El mantenimiento de equipo se debe solicitar mediante ticket en el sistema de gestión de incidentes y atendidos según su prioridad.

Se realizará un plan de mantenimiento anual para todos los equipos de la institución, a cargo del comité de seguridad.

3.7 Control de código Malicioso

La institución contará permanentemente con un antivirus que será administrado bajo la responsabilidad del Comité de Seguridad, que coordinará las licencias y uso con la Oficina de Tecnologías de la Información y Comunicaciones del Ministerio de Cultura.
Los usuarios deberán cumplir con las mejores prácticas establecidas por el Comité de Seguridad con respecto al uso del Antivirus.
Es responsabilidad de todo el personal de la institución revisar que todos los medios extraíbles con el antivirus provisto antes de procesarlos en los equipos de cómputo.
Es responsabilidad del Comité de Seguridad, mantener en buen funcionamiento las aplicaciones que le permitan prevenir, detectar y corregir problemas producidos por virus.

3.8 Telefonía

La entidad contará con el servicio telefónico local, nacional, internacional y de celulares, con lo cual autorizará su uso de manera particular a todo el personal de la institución según lo requieran sus funciones.

Anexo 22: "Política de Transferencia de la información

POLÍTICA DE TRANSFERENCIA DE LA INFORMACIÓN DE LA DIRECCIÓN DESCONCENTRADA DE CULTURA DE LAMBAYEQUE

Código:	**SGSI-010**
Versión:	0.1
Fecha de la versión:	03/07/2017
Creado por:	Clara Patricia Cubas Penas

1. Objetivo, alcance y usuarios

El objetivo del presente documento es asegurar la seguridad de la información cuando son intercambiados dentro o fuera de la institución.

Este documento se aplica a todo el alcance del Sistema de gestión de seguridad de la información (SGSI); es decir, a todos los sistemas, equipos, instalaciones e información utilizados dentro del alcance del SGSI.

Los usuarios de este documento son todos los colaboradores de la Dirección desconcentrada de cultura de Lambayeque.

2. Documentos de referencia

- RESOLUCIÓN MINISTERIAL Nº 004-2016-PCM
- NTP ISO/IEC 27001:2014
- SGSI-001 - Documento sobre el alcance del SGSI
- SGSI-002 – Política del SGSI

3. Transferencia de la información

3.1 Canales de comunicación electrónica

La información de la institución puede ser intercambiada a través de los siguientes canales de comunicación electrónica: correo electrónico, descarga de archivos desde Internet, transferencia de datos, teléfonos, mensajes de texto por teléfonos móviles o redes sociales, en beneficio de la institución y solo en función de las actividades laborales.

3.2 Políticas de uso del correo electrónico

- El uso del correo electrónico es solo para fines de gestión laboral, debiendo ser responsable de la protección contra archivos adjuntos y mensajes no autorizados.
- Con respecto a la creación del correo electrónico, la solicitud la realiza el jefe del área a través de un ticket del sistema de gestión de incidencias, indicando los datos del colaborador.
- Con respecto a la baja del correo electrónico, la solicitud la realiza el jefe del área a través de un ticket del sistema de gestión de incidencias, indicando la baja y el motivo.
- Los mensajes masivos solo puede ser utilizado para notificaciones y comunicaciones laborales, está prohibido el envío de cadenas.

- Está prohibido enviar o recibir el correo electrónico, usando la identidad de otro usuario.
- Está prohibido enviar o recibir mediante correo electrónico contenido que genere desprestigio a la institución.
- Está prohibido el envío de material con contenido malicioso o virus utilizando correo electrónico.
- Todo correo electrónico que contenga información confidencial deberá indicar en el asunto la palabra "CONFIDENCIAL".
- Los usuarios pueden estar sujetos a auditorías por parte del comité de seguridad en cuanto al manejo seguro de la información enviada, considerada como información sensible.

4. Validez y Gestión de Documentos

El uso del presente documento solo puede aprobarse por el director de la Dirección desconcentrada de cultura de Lambayeque, quien podrá determinar su validez y el plazo de vigencia del documento.

La mejora continua de este documento depende directamente del comité de Seguridad de la información de la Dirección Desconcentrada de cultura de Lambayeque.

El presente documento se ha realizado con fines académicos como parte de una investigación de tesis para obtener el título profesional.

Anexo 23: Procedimiento “Gestión de incidentes”

PROCEDIMIENTO DE GESTIÓN DE INCIDENTES PARA LA DIRECCIÓN DESCONCENTRADA DE CULTURA DE LAMBAYEQUE

Código:	**SGSI-011**
Versión:	0.1
Fecha de la versión:	03/07/2017
Creado por:	Clara Patricia Cubas Penas

1. Objetivo, alcance y usuarios

El objetivo del presente documento es garantizar la detección temprana de eventos y debilidades de seguridad, como también la rápida reacción y respuesta ante incidentes de seguridad.

Este documento se aplica a todo el alcance del Sistema de gestión de seguridad de la información (SGSI); es decir, a todos los sistemas, equipos, instalaciones e información utilizados dentro del alcance del SGSI.

Los usuarios de este documento son todos los colaboradores de la Dirección desconcentrada de cultura de Lambayeque.

2. Documentos de referencia

- RESOLUCIÓN MINISTERIAL Nº 004-2016-PCM
- NTP ISO/IEC 27001:2014
- SGSI-001 - Documento sobre el alcance del SGSI
- SGSI-002 – Política del SGSI

3. Gestión de Incidentes de Seguridad

3.1 Reporte de incidencias y eventos de seguridad

Todo el personal debería tener la facultad de identificar, clasificar y reportar los incidentes de seguridad, utilizando herramientas de reporte.

El sistema de gestión de seguridad de la información (SGSI) debe recibir información y eventos sucedidos ayudando a identificar cuáles son los que más se repiten o de gran impacto para la institución, con la finalidad que el sistema mejoré continuamente e implementando mejores controles para disminuir daños futuros.

Todo el personal de la institución está en la obligación de reportar cualquier incidente de seguridad que detecte, al Oficial de Seguridad de la Información, mediante una herramienta de soporte o vía correo electrónico institucional, quien analizará el evento y derivará su tratamiento.

El asunto del correo electrónico debe seguir el siguiente formato: Incidente Seguridad de la Información – "Área Usuaria", su envío depende directamente del Oficial de Seguridad de la institución.

3.2 Administración de incidencias de seguridad

El oficial de Seguridad de la Información debe realizar el debido estudio y seguimiento de todos los incidentes de seguridad, valiéndose de la asistencia de todos los usuarios involucrados cuando éste lo requiera.

El oficial de Seguridad de la información debe realizar la recolección de información sobre el incidente y analizar los antecedentes, el resultado de dicho análisis puede tener las siguientes opciones:

- El evento no es a una amenaza: Se cierra el registro de eventos, informando a la persona que reportó.
- El evento corresponde a una debilidad: Se gestiona las actividades de mitigación (con los propietarios de los activos comprometidos, área y/o comité de seguridad), dejando registro en la plantilla de incidentes.
- El evento ocurrió y debe ser gestionado como incidente de seguridad.

Es responsabilidad del Oficial de Seguridad de la Información mantener actualizados los reportes de incidencias.

3.2.1 Registro de incidencias

La institución contará con una herramienta de soporte de gestión de incidencias internas en la que los colaboradores podrán notificar su incidencia.
El oficial de seguridad revisará diariamente las notificaciones de incidente y realizará la gestión necesaria a cada una, iniciando por el registro del incidente en la plantilla de incidentes.
Finalmente enviará la plantilla de incidentes a la oficina de informática para su tratamiento, esta plantilla se irá completando según el avance del tratamiento (registro, clasificación, escalamiento, respuesta inmediata).
Si la incidencia es de atención directa, el oficial de seguridad puede darle solución inmediata reportando solo la aparición del incidente pero gestionándolo desde la institución.

3.2.2 Clasificación de incidencias

Se considerará la siguiente clasificación:

Tipo de incidentes

a. Informático: Incidentes que afecten las tecnologías de la información.
b. No informático: Todo aquello no considerado informático.

Nivel de criticidad

a. **Impacto:** Importancia del incidente dependiendo de los procesos y usuarios afectados puede ser: Insignificante, Bajo, Medio, Alto.
b. **Urgencia:** Tiempo máximo de demora que puede aceptar el proceso para la resolución del incidente, puede ser: Insignificante, Bajo, Medio, Alto.

Cualquier cambio relacionado a la información deberá ser completamente documentado y controlado por la Administración de la institución.

3.2.3 Escalamiento

Si se determina que el incidente detectado requiere un tratamiento urgente, deberá procederse con la mayor rapidez posible. Si la urgencia es alta, deberá informarse a la Oficina de informática del Ministerio de Cultura.

Para esto es necesario:

- Tipo de incidente, nivel de criticidad, alcance del incidente.
- Que origino el incidente.
- Como ocurrió (o está ocurriendo el incidente).

El criterio principal de escalar es transferir a una persona de soporte más elevado con las siguientes características:

- Mayor conocimiento o experiencia
- Recursos para solucionar problemas
- Mayor cargo para la toma de decisiones.

En general dependiendo el tipo de incidente los responsables de la respuesta serían:

Tipo de Activo	Tipo de Activo involucrado en el incidente	Jefatura responsable de la respuesta
D01	Documentos informáticos (datos de las aplicaciones)	Administración de la institución
D02	Datos de aplicaciones (sensibles o transferibles)	
D04	E-mail	
D06	Información publicada o servicios disponibles en un servidor de Internet	
S01	TI y servicios de telecomunicaciones	
S02	Disposición de Equipos (PC, impresoras locales, periféricos, interfaces específicas, etc.)	
S03	Los servicios ofrecidos en los sitios web	
G01	Entorno de trabajo del usuario	
D03	Archivos de Oficina	Jefe de área donde ocurrió incidente
D05	Documentos no informáticos, impresos o escritos a mano	

3.2.4 Respuesta inmediata

La jefatura designada para la respuesta inmediata del incidente deberá seguir estas acciones:

- Minimizar el riesgo: Coordinar las actividades necesarias para la disminución de las consecuencias y probabilidades futuras.
- Reclasificación de incidentes.
- Notificación externa: Si es necesario notificar a instituciones externas.
- Consolidación de documentos: Recopilar antecedentes.

PROCEDIMIENTO DE GESTIÓN DE LA CONTINUIDAD PARA LA DIRECCIÓN DESCONCENTRADA DE CULTURA DE LAMBAYEQUE

Código:	**SGSI-012**
Versión:	0.1
Fecha de la versión:	03/07/2017
Creado por:	Clara Patricia Cubas Penas

1. Objetivo, alcance y usuarios

El propósito de esta Política es definir el objetivo, alcance y reglas básicas para la gestión de la continuidad del negocio

Este documento se aplica a todo el alcance del Sistema de gestión de seguridad de la información (SGSI); es decir, a todos los sistemas, equipos, instalaciones e información utilizados dentro del alcance del SGSI.

Los usuarios de este documento son todos los colaboradores de la Dirección desconcentrada de cultura de Lambayeque.

2. Documentos de referencia

- RESOLUCIÓN MINISTERIAL N° 004-2016-PCM
- NTP ISO/IEC 27001:2014
- SGSI-001 - Documento sobre el alcance del SGSI
- SGSI-002 – Política del SGSI

3. Políticas de la Gestión de continuidad

El objetivo de la gestión de la continuidad del negocio es identificar potenciales amenazas en una organización y los impactos que esas amenazas podrían tener sobre las operaciones de negocios; también sirven para proporcionar un marco de referencia para construir resiliencia organizacional con la capacidad de una respuesta efectiva.

Las políticas de la gestión de continuidad:

- El plan de continuidad considera el mapeo de todos los procesos de la institución.
- El plan de continuidad incluye el organigrama, los roles y funciones bien establecidos.
- El plan de continuidad debe ser probado para comprobar su eficacia.
- Los resultados deben ser registrados.
- El plan de continuidad debe identificar los principales eventos que puedan afectar la continuidad o los procesos considerados como críticos tales como: Impactos directos (financiero, normativo, tiempos de interrupción) e Impactos indirectos (daño de imagen o falta de credibilidad).
- El plan de continuidad deberá conseguir que los procesos críticos sean estableces en máximo 1 a 2 horas.
- Es responsabilidad directa del comité de seguridad, realizar el plan de continuidad según los eventos.
- Es responsabilidad de los colaboradores entender el plan de continuidad.

Anexo 25: Plan de Sensibilización y capacitación

PLAN DE SENSIBILIZACIÓN Y CAPACITACIÓN PARA LA DIRECCIÓN DESCONCENTRADA DE CULTURA DE LAMBAYEQUE

Código:	**SGSI-011**
Versión:	0.1
Fecha de la versión:	03/07/2017
Creado por:	Clara Patricia Cubas Penas

1. Objetivo, alcance y usuarios

Este documento tiene como objetivo establecer el plan de capacitación, sensibilización y comunicación de la seguridad de la información, para así asegurar que la información llegue en su totalidad los colaboradores de la Dirección desconcentrada de cultura de Lambayeque, asegurando que cada uno cumpla con sus roles y responsabilidades de seguridad y privacidad de la información dentro de la institución.

Este documento se aplica a todo el alcance del Sistema de gestión de seguridad de la información (SGSI); es decir, a todos los sistemas, equipos, instalaciones e información utilizados dentro del alcance del SGSI.

Los usuarios de este documento son todos los colaboradores de la Dirección desconcentrada de cultura de Lambayeque.

2. Documentos de referencia

- RESOLUCIÓN MINISTERIAL N° 004-2016-PCM
- NTP ISO/IEC 27001:2014
- SGSI-001 - Documento sobre el alcance del SGSI
- SGSI-002 – Política del SGSI
- SGSI-003 - Metodología de Riesgos
- SGSI-004 – Declaración de aplicabilidad
- SGSI-005 – Plan de tratamiento de riesgos
- SGSI-006 – Gestión de Activos
- SGSI-007 – Política de control de Accesos
- SGSI-008 – Procedimiento Trabajo en zonas seguras
- SGSI-009 – Procedimientos operativos para la gestión de TI
- SGSI-010 – Política de transferencia de información
- SGSI-011 – Procedimiento de gestión de incidentes
- SGSI-012 – Procedimiento de gestión de la continuidad

3. Descripción general

Un plan de sensibilización, capacitación y comunicación en seguridad de la información debe explicar las reglas del uso de los sistemas y de la información, que se detallan en las políticas y procedimientos de seguridad de la información de la institución, requiere que sean cumplidos por parte de todos los colaboradores.

3.1 Sensibilización

Es un proceso que tiene como objetivo impactar sobre el comportamiento de los colaboradores y reforzar buenas prácticas sobre la seguridad de la información.

El éxito de la sensibilización es la facilidad en que la información es entregada, para captar la atención de los involucrados.

3.2 Capacitación

Es un proceso que tiene como objetivo brinda conocimientos, habilidades y aptitudes para orientar al personal de la institución a tener un mejor desempeño en sus actividades con respecto a la seguridad de la información.

3.3 Comunicación

Es un proceso que tiene como objetivo trasmitir la documentación e implementación del sistema de seguridad de la información en la institución.

La comunicación es una herramienta fundamental para mantener la transparencia y el contacto directo sobre la importancia de la aplicación de políticas y procedimientos, de esta manera mantener el sistema de gestión de seguridad de la información.

4. Diseño del plan

4.1. Plan de Sensibilización

Se determina que el plan de sensibilización se realizará con respecto a la información que es manipulada por todos los colaboradores por ejemplo: usuarios y contraseñas, y también la información que es utilizada en cada una de sus funciones.

El plan será empleado durante 4 meses con la intención de dar a conocer el sistema de gestión de seguridad de la información.

4.1.1 Herramientas para la sensibilización

Reunión: Se convocará a reunión para la presentación del sistema de gestión de seguridad de la información de la institución en el auditorio principal.

Folletos: Se entregarán en la presentación del sistema de gestión de la seguridad con todo el personal de institución presente.

Afiches: Se exhibirán afiches de manera interna y áreas comunes de los colaboradores.

Uso de tecnología: Se realizará una campaña interna a través de los fondos de pantalla.

4.1.2 Campañas de sensibilización:

Para toda la institución:

- Contraseñas seguras: Publicidad con mensajes con mensajes alusivos a cuidar la información personal, contraseñas, equipos de cómputo y usuarios.
- Internet seguro: Publicidad con mensajes alusivos a cuidar los accesos de internet y correos electrónicos de usuarios no conocidos.
- Sesiones: Publicidad con respecto a inicio y cierre de sesión, buenas prácticas de accesos al sistema y equipos de cómputo.

4.1. Plan de Capacitación

Se propone desarrollar módulos según los temas que se necesiten trasmitir de los sistemas de gestión de seguridad de la información.

4.2.1 Herramientas para la capacitación:

Manuales: Se realizaran manuales con información especifica de lo que se necesita dar a conocer.

Cartillas: Tendrán información detallada según las funciones del colaborador con respecto a seguridad de la información.

Otras herramientas: Las capacitaciones serán realizadas con proyecto dentro del auditorio principal si son para todos los colaboradores o en cada oficina si los módulos son dedicados para una sola área.

4.2.2 Módulos y duración:

Para el comité de seguridad:

Módulos	Temas	Comité
I	Políticas claves para la Seguridad de la información	24.07.2017
II	Riesgos de la información	24.07.2017
III	Metodología de riesgos	25.07.2017
	Tratamiento de riesgos	25.07.2017
IV	Uso aceptable de Activos	26.07.2017
V	Trabajo en Áreas seguras	31.07.2017
VI	Transferencia de la información	31.07.2017
VII	Gestión de incidentes	01.08.2017
	Gestión de la continuidad	01.08.2017
VIII	Auditoría de Seguridad de la información	02.08.2017

Para toda la institución:

Módulos	Temas	Grupo 1	Grupo 2
I	Políticas claves para la Seguridad de la información	08.08.2017	09.08.2017
	Riesgos de la información		
II	Uso aceptable de Activos	10.08.2017	11.08.2017
	Trabajo en Áreas seguras		
	Transferencia de la información		
III	Gestión de incidentes	14.08.2017	15.08.2017

Al finalizar los módulos se les tomará evaluaciones tanto a los colaboradores que pertenecen al comité de seguridad así como todos los demás, si es necesario realizar más inducciones se realizaran las coordinaciones para un nuevo cronograma y reforzar lo aprendido.

5. Seguimiento e indicadores

Para considerar el éxito del plan de sensibilización y capacitaciones es necesario realizar el seguimiento con los siguientes indicadores:

- % Asistencia de colaboradores a capacitaciones.
- Resultados de Test de evaluación de módulos.
- % Registro de incidentes en sistema de gestión.

Anexo 26: Acta de Reunión del comité

PERÚ | Ministerio de Cultura

Acta de Reunión N°.... del Comité de Seguridad de la Información de la Dirección Desconcentrada de Cultura de Lambayeque

Fecha: .....

Asisten:

- Director de la institución
- Administrador de la institución
- Ing. Computación e informática

I. Tema a tratar:

Implementación del Sistema de Gestión de Seguridad de la información en la Dirección desconcentrada de Cultura de Lambayeque

II. Puntos de reunión:

- Definir las coordinaciones para el presupuesto
- Establecer un cronograma para la implementación del sistema de gestión de la seguridad de la información en la institución.
- Decisión sobre el comité de seguridad.
- Primeros pasos para el inicio del SGSI.

III. Acuerdos:

1. Coordinaciones para el presupuesto

Para determinar el presupuesto del sistema de gestión de seguridad de la información es importante realizar las coordinaciones con el Ministerio de Cultura considerando la resolución ministerial que indica que todas las instituciones del estado deben implementar un sistema que proteja sus activos de información como parte de sus obligaciones principales.

El administrador será el que se encargue de esta coordinación previa cita con el encargado de la oficina de informática y telecomunicaciones del Ministerio de Cultura.

Se acuerda tener una respuesta en el máximo de 4 días laborables.

Se determina también el presupuesto indicando que la inversión tendrá una recuperación inmediata por las mejoras que presentara en los niveles de confidencialidad, integridad y disponibilidad de la información.

2. **Cronograma de implementación**

   Se determinó el siguiente cronograma de implementación, siendo la presentación oficial del SGSI el día 4 de Agosto del 2017.

3. **Sobre el comité de seguridad**

   Se acuerda que el comité será precedido por el Director de la institución como Director del comité, el administrador será el oficial de seguridad y el encargado de la oficina de Proyectos arqueológicos será el propietario de la información.

   La fecha oficial de creación de comité con resolución de la institución será el 15 de Mayo del 2017.

4. **Primeros pasos para el Sistema de Gestión de Seguridad de la información**

   Se acuerda que la institución dará las facilidades a la bachiller en ingeniería de Computación e informática Clara Patricia Cubas Penas para el análisis del contexto de la institución y empezar con establecer los requerimientos necesarios para el inicio del Sistema de Gestión de Seguridad de la información.

IV. Conclusiones:

- El administrador se hará cargo de las coordinaciones para el presupuesto.
- Se generó el plan de implementación del SGSI.
- La fecha oficial de creación del comité de seguridad será el 15 de Mayo del 2017, siendo la fecha de presentación del sistema de gestión de seguridad de la información el día 04 de Agosto del 2017.
- La parte inicial del sistema de gestión de seguridad de la información estará a cargo de la bachiller Clara Patricia Cubas Penas.

Anexo 27: Declaración de aceptación

PERÚ | Ministerio de Cultura

Declaración de aceptación de los documentos del Sistema de gestión de seguridad de la Información de la Dirección Desconcentrada de Cultura de Lambayeque

Yo, ... con DNI ....., declaro conocer y aceptar todos los términos y condiciones que surgen de los documentos del Sistema de gestión de la seguridad de la información, definidas por la Dirección desconcentrada de cultura de Lambayeque, a través del comité de seguridad de la información.

Mediante la aceptación del presente documento, me comprometo a cumplir con las políticas y procedimientos implementados en este proceso.

Los documentos son los siguientes:

Código	Descripción del Documento
SGSI_001	Alcance del Sistema de Seguridad de Gestión de la Información de la Dirección Desconcentrada de Cultura de Lambayeque
SGSI_002	Política del Sistema de Seguridad de Gestión de la Información de la Dirección Desconcentrada de Cultura de Lambayeque
SGSI_003	Metodología de Riesgos del Sistema de Seguridad de Gestión de la Información para la Dirección Desconcentrada de Cultura de Lambayeque
SGSI_004	Declaración de Aplicabilidad para la Dirección Desconcentrada de Cultura de Lambayeque
SGSI_005	Plan de tratamiento de riesgos del Sistema de Seguridad de Gestión de la Información para la Dirección Desconcentrada de Cultura de Lambayeque
SGSI_006	Política de Gestión de Activos de Información de la Dirección Desconcentrada de Cultura de Lambayeque
SGSI_007	Política de Control de Acceso del Sistema de Seguridad de Gestión de la Información para la Dirección Desconcentrada de Cultura de Lambayeque
SGSI_008	Procedimiento para Trabajo en Zonas Seguras de la Dirección Desconcentrada de Cultura de Lambayeque
SGSI_009	Procedimientos Operativos para TI
SGSI_010	Política de Trasferencia de la Información de la Dirección Desconcentrada de Cultura de Lambayeque
SGSI_011	Procedimiento para Gestión de Incidentes de la Dirección Desconcentrada de Cultura de Lambayeque
SGSI_012	Política de la Continuidad del Negocio de la Dirección Desconcentrada de Cultura de Lambayeque
SGSI_013	Plan de Sensibilización y Capacitación

_____

Nombre:

DNI:

Anexo 28: Declaración de confidencialidad

PERÚ Ministerio de Cultura

Declaración de confidencialidad de la Información de la Dirección Desconcentrada de Cultura de Lambayeque

Yo,..... con DNI ....., en mi capacidad de empleado y en consideración de la relación laboral que mantengo con la institución, así como del acceso que se me permite a su información, constato que:

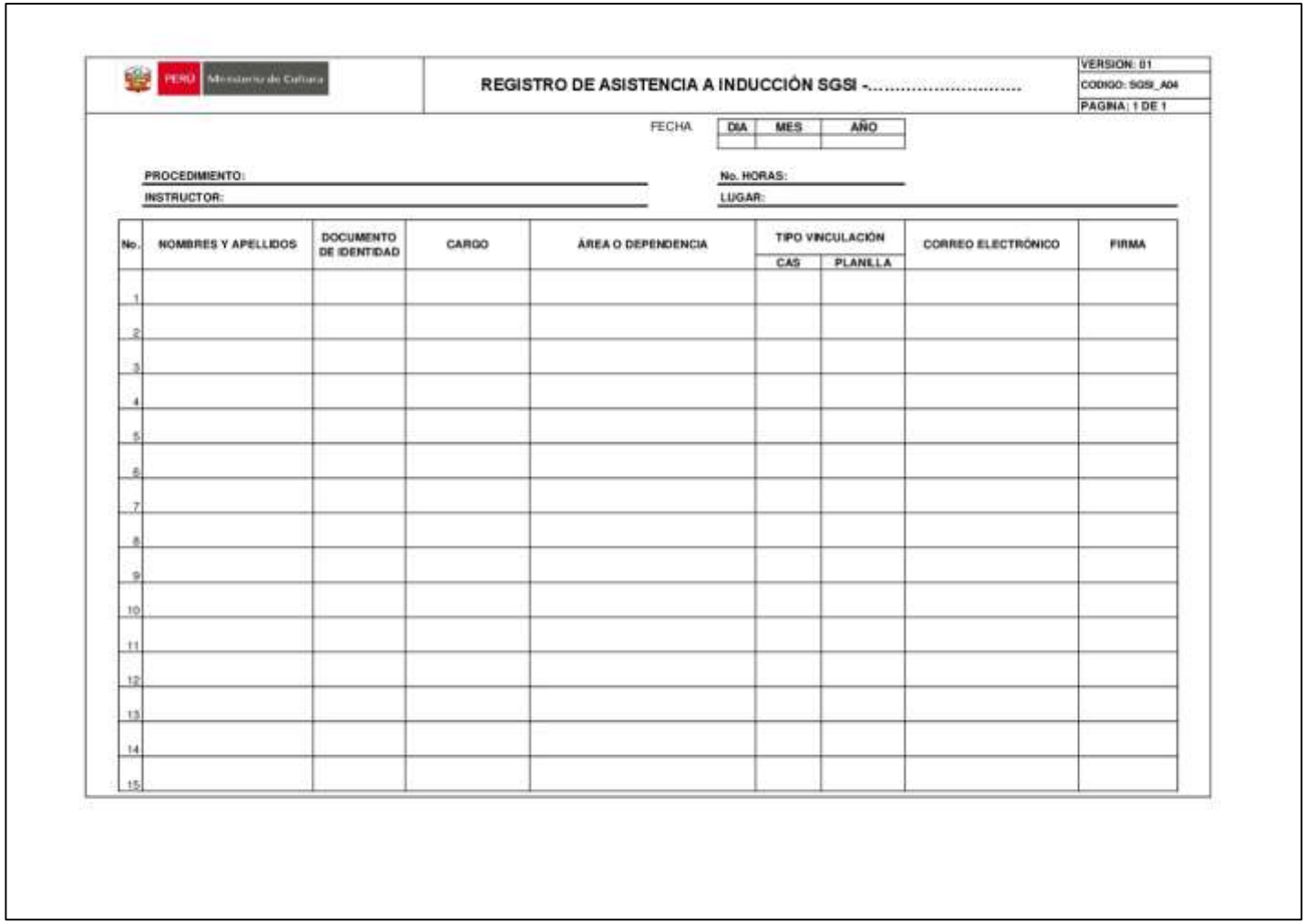
1) Soy consciente de la importancia de mis responsabilidades en cuanto a no exponer la integridad, disponibilidad y confidencialidad de la información que maneja la institución.
2) En concreto he leído, entiendo y me comprometo a cumplir con los procedimientos y políticas de Seguridad de los Sistemas de Información que corresponden a mi función en la institución.
3) Me comprometo a cumplir, asimismo, todas las disposiciones relativas a la política de la institución en materia de uso y divulgación de información, y a no divulgar la información que reciba a lo largo de mi relación con la institución, manteniendo este compromiso, aún después de que finalice dicha relación, cualquiera que sea la forma de acceso a tales datos o información, quedando absolutamente prohibido obtener copias sin previa autorización.
4) Entiendo que el incumplimiento de las obligaciones que constan en el presente documento, intencionadamente o por negligencia, podrían implicar en su caso, las sanciones disciplinarias correspondientes por parte de la institución.

_____

Nombre:

DNI:

Anexo 29: Registro de inducción



PERÚ Ministerio de Cultura

REGISTRO DE ASISTENCIA A INDUCCIÓN SGSI -.....

VERSION: 01
CODIGO: SGSI_A04
PAGINA: 1 DE 1

FECHA

DIA	MES	AÑO

PROCEDIMIENTO:

No. HORAS:

INSTRUCTOR:

LUGAR:

No.	NOMBRES Y APELLIDOS	DOCUMENTO DE IDENTIDAD	CARGO	ÁREA O DEPENDENCIA	TIPO VINCULACIÓN		CORREO ELECTRÓNICO	FIRMA
					CAS	PLANILLA		
1								
2								
3								
4								
5								
6								
7								
8								
9								
10								
11								
12								
13								
14								
15								

Anexo 30: Niveles de criticidad por valores

El nivel de criticidad se puede definir con los valores de confidencialidad, integridad y disponibilidad, estos valores van de escala del 1 al 4.

Cuando se evalúa un solo valor, la criticidad se define:

1 valor	Criticidad
1	Riesgo insignificante
2	Riesgo tolerable
3	Riesgo inadmisible
4	Riesgo intolerable

Cuando se evalúan dos valores, la criticidad se define con la suma de ambos valores:

Suma de 2 valores	Criticidad
1	Riesgo insignificante
2	Riesgo insignificante
3	Riesgo tolerable
4	Riesgo tolerable
5	Riesgo inadmisible
6	Riesgo inadmisible
7	Riesgo intolerable
8	Riesgo intolerable

Cuando se evalúan tres valores, la criticidad se define con la suma de todos valores:

Suma de 3 valores	Criticidad
1	Riesgo insignificante
2	Riesgo insignificante
3	Riesgo insignificante
4	Riesgo tolerable
5	Riesgo tolerable
6	Riesgo tolerable
7	Riesgo inadmisible
8	Riesgo inadmisible
9	Riesgo inadmisible
10	Riesgo intolerable
11	Riesgo intolerable
12	Riesgo intolerable

Anexo 31: Objetivos COBIT

Objetivos del Negocio:

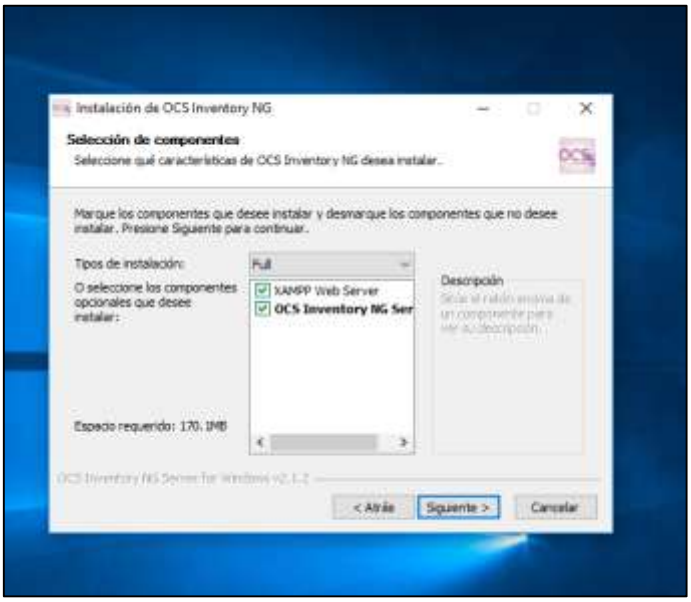
COBIT 5 - Objetivos del Negocio		
Dimensiones	**Objetivos**	
Financiero	1	Valor de las partes interesadas de las inversiones del negocio
	2	Cartera de productos y servicios competitivos
	3	Gestión de riesgos del negocio (salvaguarda de activos)
	4	Cumplimiento con leyes externas y reglamentos
	5	Transparencia financiera
Cliente	6	Cultura de servicio orientada al cliente
	7	Continuidad y disponibilidad de servicios del negocio
	8	Respuestas ágiles a un entorno cambiante del negocio
	9	Toma de decisiones estratégicas basadas en información
	10	Optimización de los costes de la prestación de servicios
Interno	11	Optimización de la funcionalidad de los procesos del negocio
	12	Optimización de los costes de los procesos del negocio
	13	Gestión de los negocios de programas de cambio
	14	Productividad operativa y de personal
	15	Cumplimiento de las políticas internas
Aprendizaje y crecimiento	16	Personas cualificadas y motivadas
	17	Cultura de innovación de productos y negocios

Objetivos relacionados TI

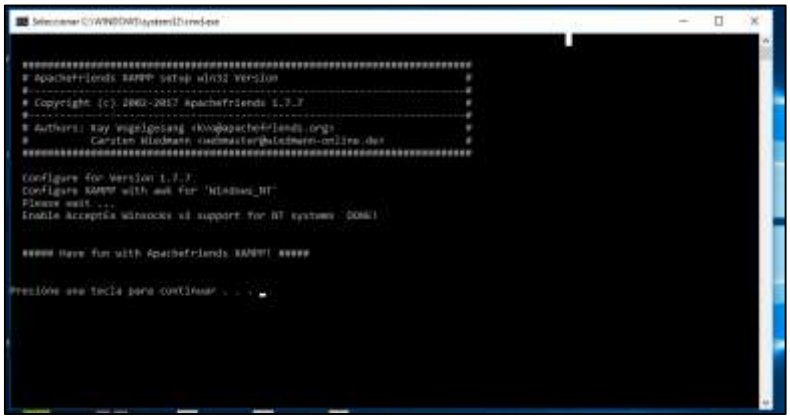
Figure 6— Objetivos relacionados a TI		
Dimensión	**Objetivos relacionados a Tecnología e información**	
Financiero	1	Alineación de TI y estrategia del negocio
	2	Cumplimiento de las TI y soporte para el cumplimiento de las leyes y reglamentos externos
	3	Compromiso de la dirección para tomar decisiones relacionadas con TI
	4	Gestión de riesgos de negocio relacionados con TI
	5	Beneficios obtenidos de la cartera de inversiones y servicios de TI
	6	Transparencia de los costos, beneficios y riesgos de TI
Cliente	7	Entrega de servicios de TI en línea con los requisitos del negocio
	8	Uso adecuado de aplicaciones, soluciones de información y tecnología
Interno	9	Agilidad de TI
	10	Seguridad de la información, infraestructura de procesamiento y aplicaciones
	11	Optimización de los recursos, recursos y capacidades de TI
	12	Capacitación y soporte de procesos de negocio integrando aplicaciones y tecnología en procesos de negocio
	13	Entrega de programas que ofrecen beneficios, puntuales, presupuestarios y cumpliendo con los requisitos y estándares de calidad.
	14	Disponibilidad de información confiable y útil para la toma de decisiones
	15	Cumplimiento de las políticas internas con las TI
Aprendizaje y crecimiento	16	Personal institucional y de TI competente y motivado
	17	Conocimiento, experiencia e iniciativas para la innovación institucional

Anexo 32: Instalación y configuración OCS Inventory

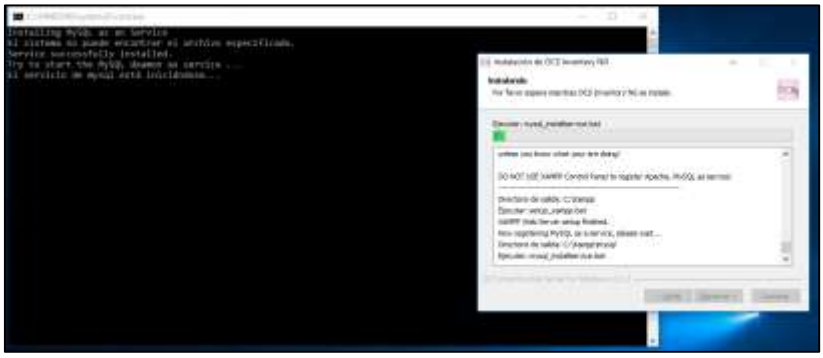
1. Instalación de OCS Inventory Server (incluye XAMPP Web Server):



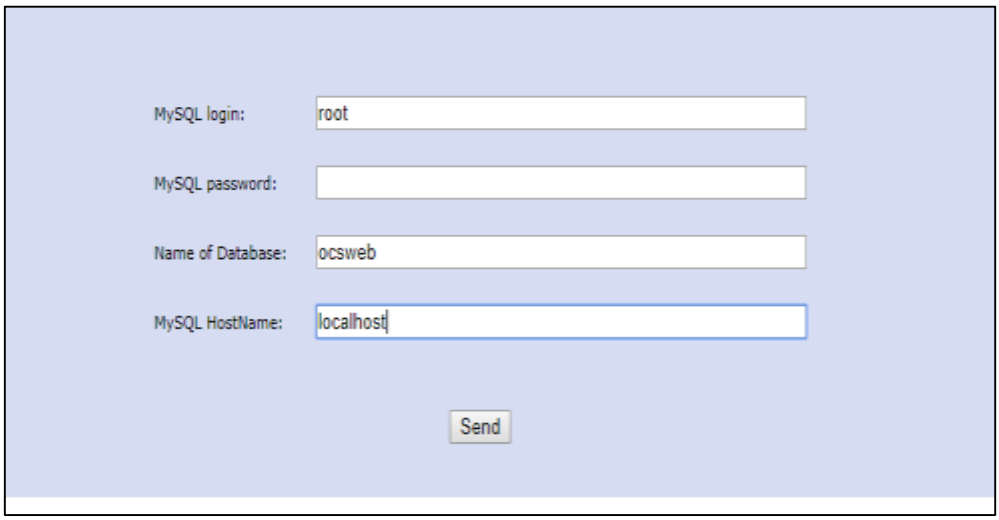
2. La herramienta instala XAMPP desde símbolo de sistema:



3. Instalación de mysql:

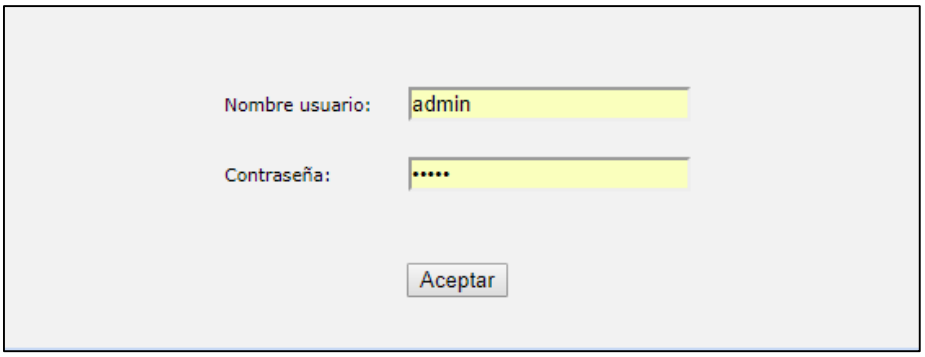


4. Acceso localhost. Configuración de usuarios:



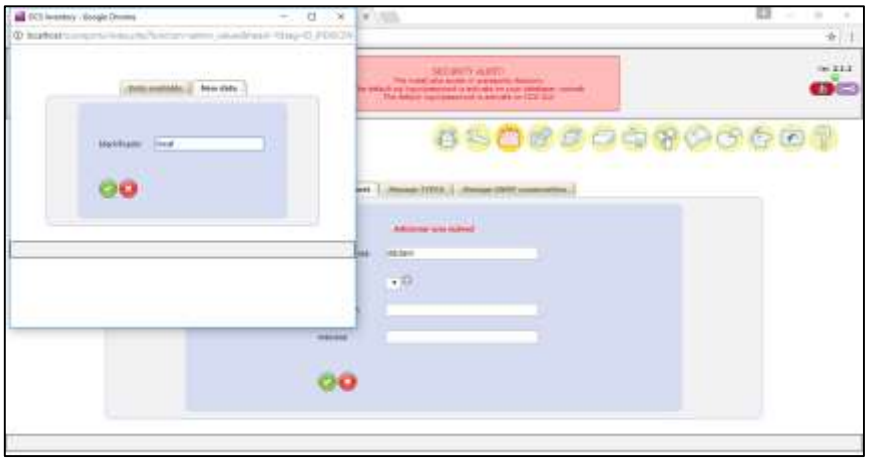
5. Configuración de OCS Inventory:

6. Acceso de administrador:



7. Panel de OCS Inventory:

8. Configuración de datos de institución:

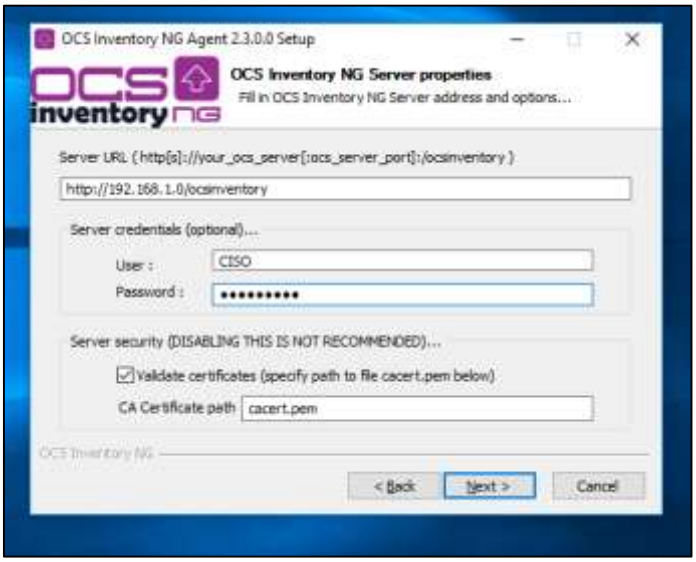


9. Configuración de administrador:

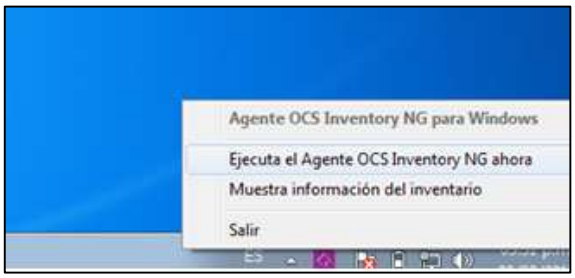
10. Configuración de red para luego enlazarlo con los agentes:

11. Instalación de Agente OCS Inventory:

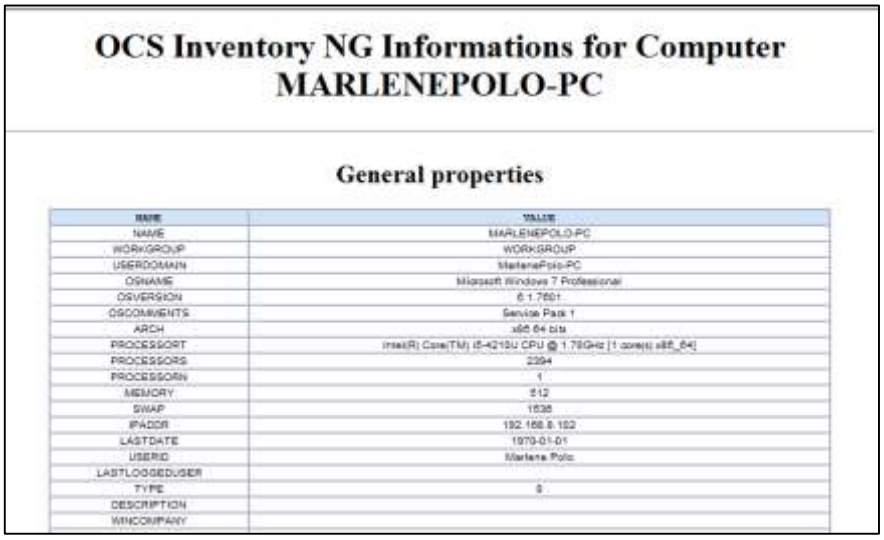
12. Enlace de agente con administrador desde la instalación:



13. Ejecución de Agente para envío de información al servidor:



14. Información consolidada de inventario:



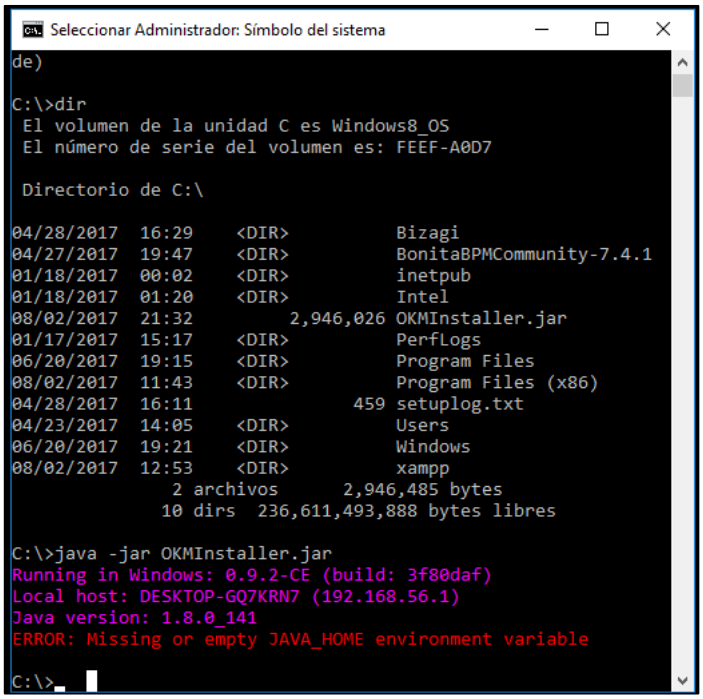
OCS Inventory NG Informations for Computer MARLENEPOLO-PC

General properties

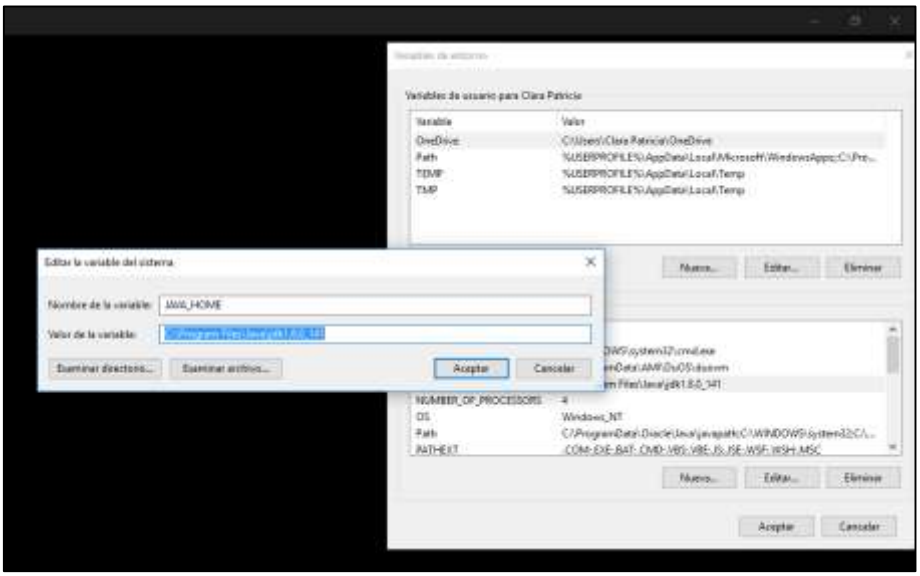
NAME	VALUE
NAME	MARLENEPOLO-PC
WORKGROUP	WORKGROUP
USERDOMAIN	MarlenePolo-PC
OSNAME	Microsoft Windows 7 Professional
OSVERSION	6.1.7601
OSCOMMENTS	Service Pack 1
ARCH	x86 64-bits
PROCESSORT	Intel(R) Core(TM) i5-4210U CPU @ 1.70GHz [1 core(s) x86_64]
PROCESSORS	2394
PROCESSORN	1
MEMORY	512
SWAP	1535
IPADDR	192.168.8.102
LASTDATE	1970-01-01
USERID	Marlene Polo
LASTLOGGEDUSER	
TYPE	0
DESCRIPTION	
WINCOMPANY	

Anexo 33: Instalación y configuración Open KM

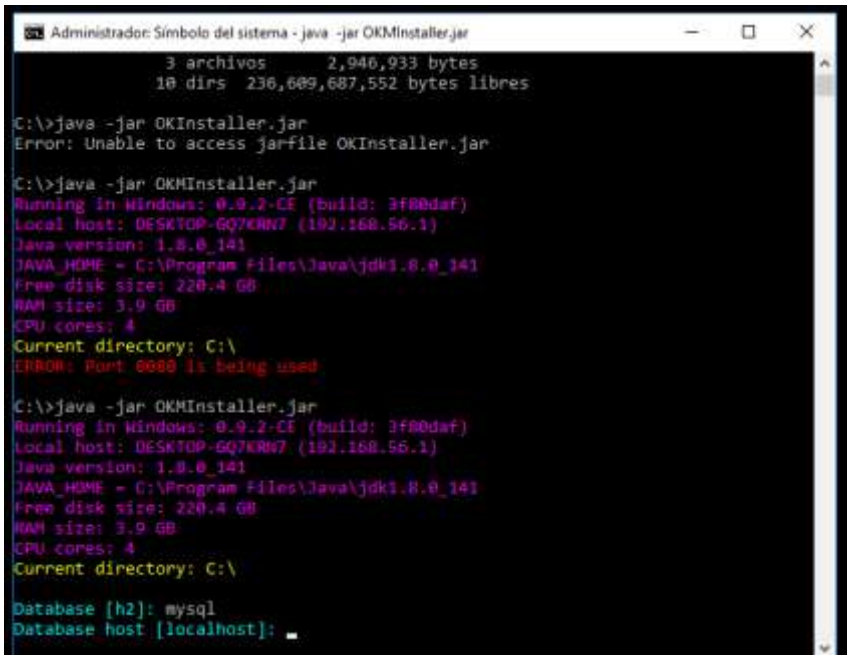
1. Después de descargar e instalar Java JDK, se descarga el archivo OKMInstaller.jar desde la página de Open KM Community edition y desde el símbolo de sistema ejecutar como administrador:
   java – jar OKMInstaller.jar



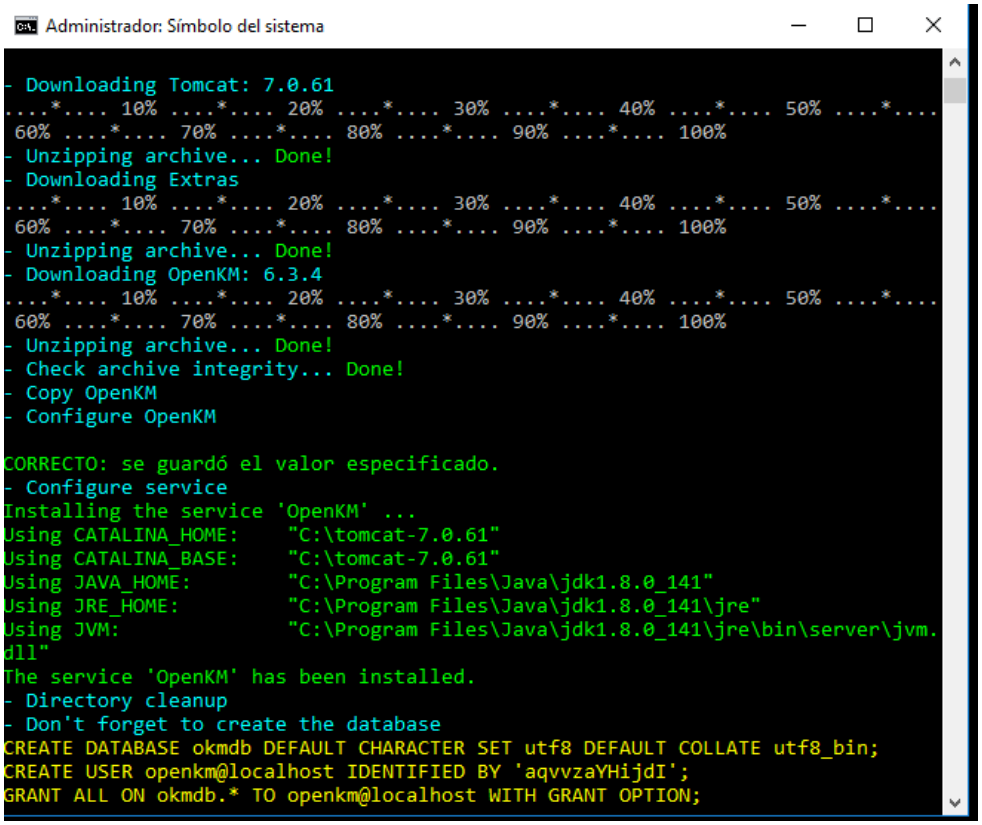
2. Se configura la variable de entorno en propiedades del sistema Windows, escribiendo la ubicación de la instalación de java JDK:



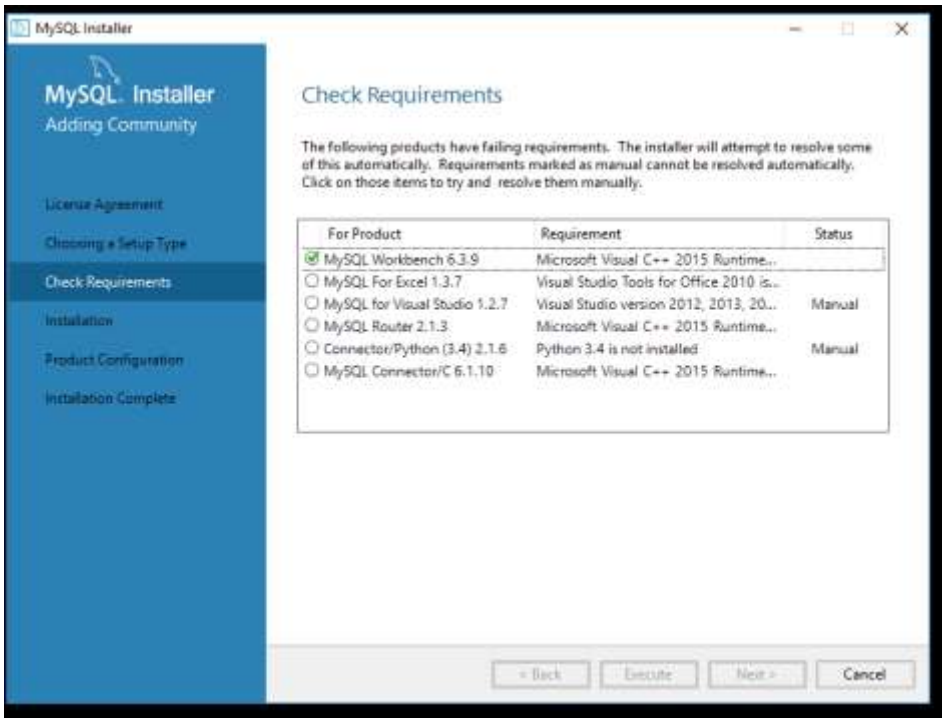
3. Se ejecuta nuevamente java –jar OKInstaller.jar:



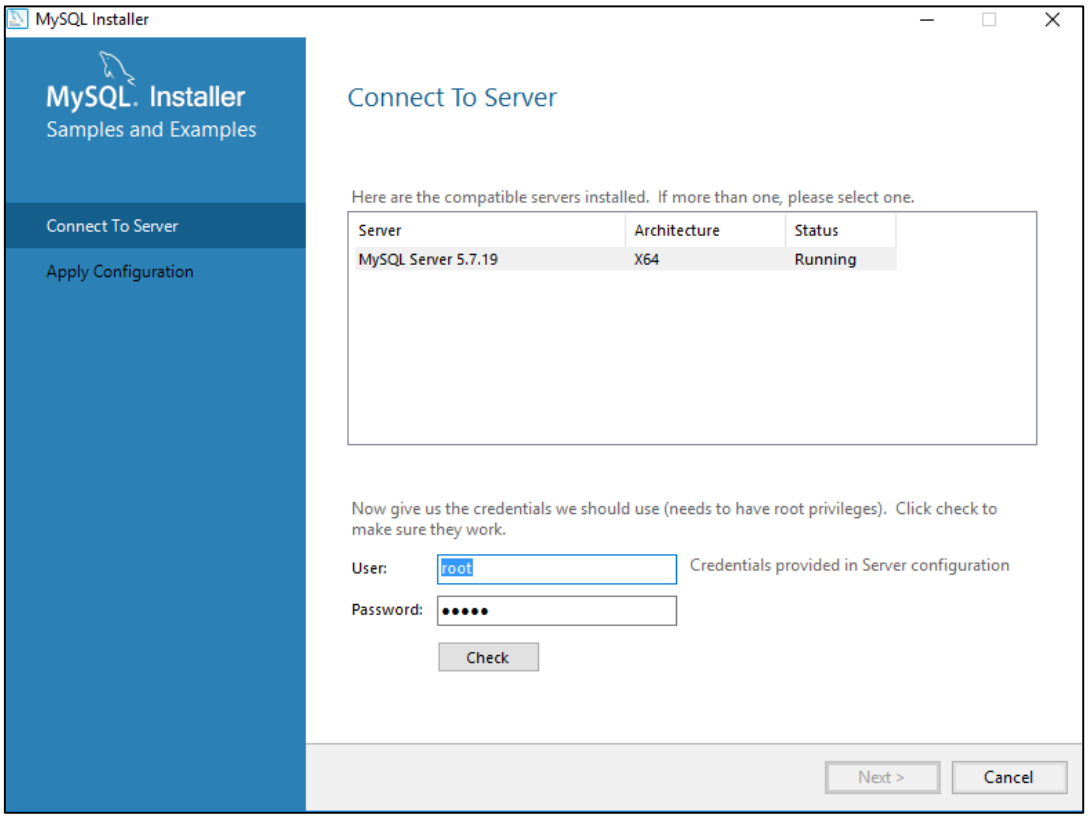
4. Se descarga TomCat, OpenKM:



5. Se descarga MySql versión Community y se instala:



6. Se configura usuario mysql:

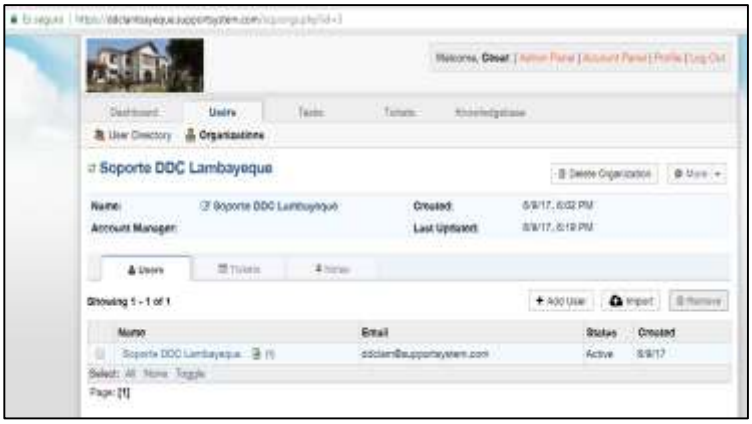


7. **Se accede a Open KM:**

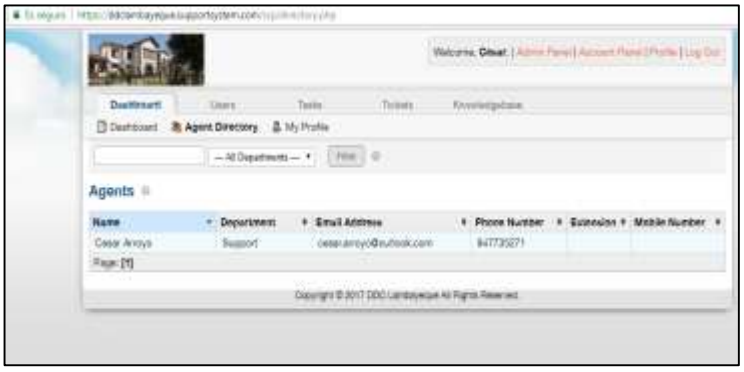
8. Configuración de usuario:

Anexo 34: Instalación y configuración OS Ticket

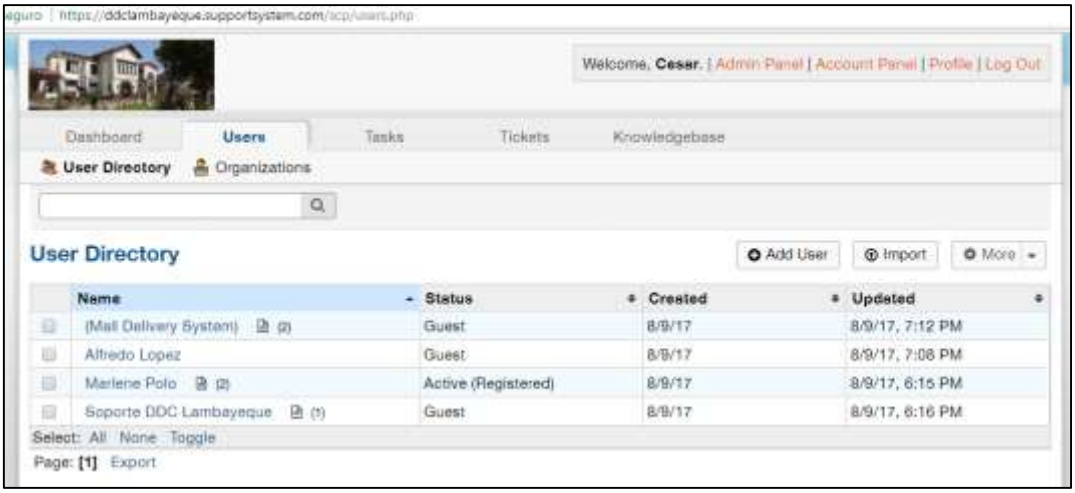
1. Se crea usuario Soporte DDC Lambayeque:



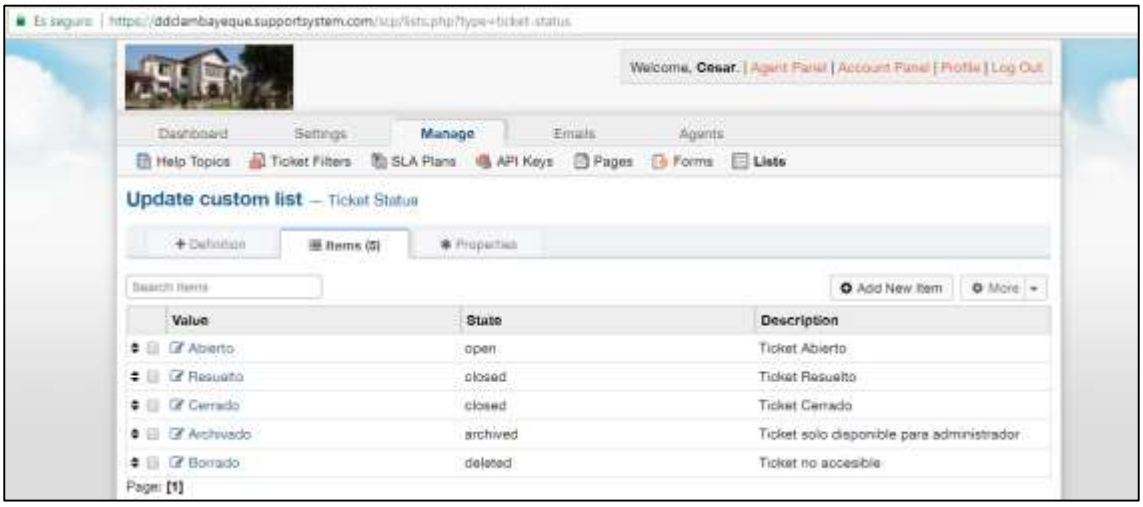
2. Se crea cuenta a CISO de la institución para administración de la herramienta:



3. Se crean usuarios y se configuran perfiles de la institución:

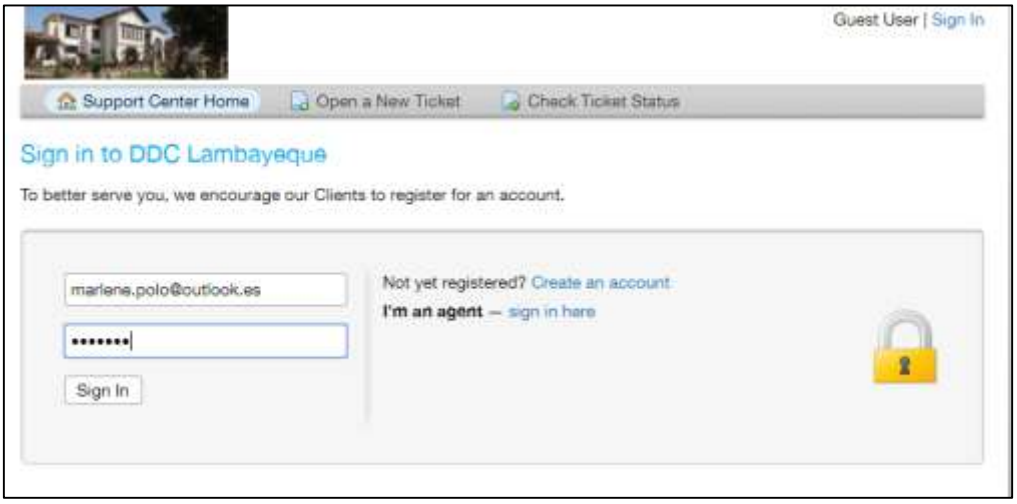


4. Se configura el estado de los tickets:

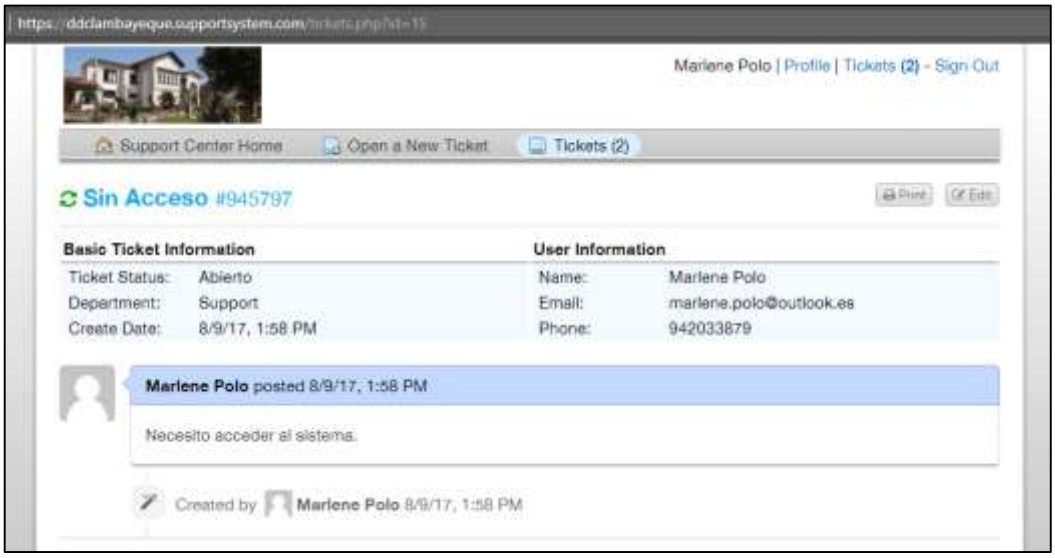


5. Se configura el “Acceso de Usuario”:

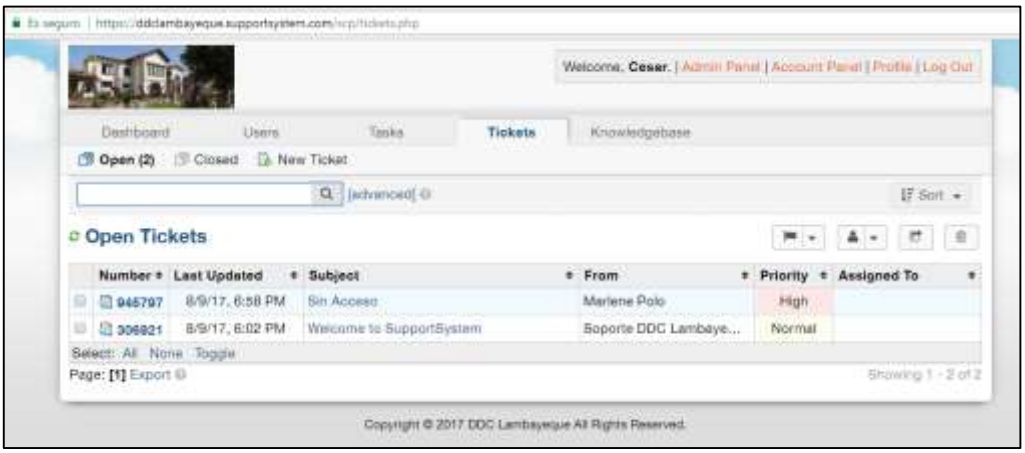
6. Acceso de usuarios finales:



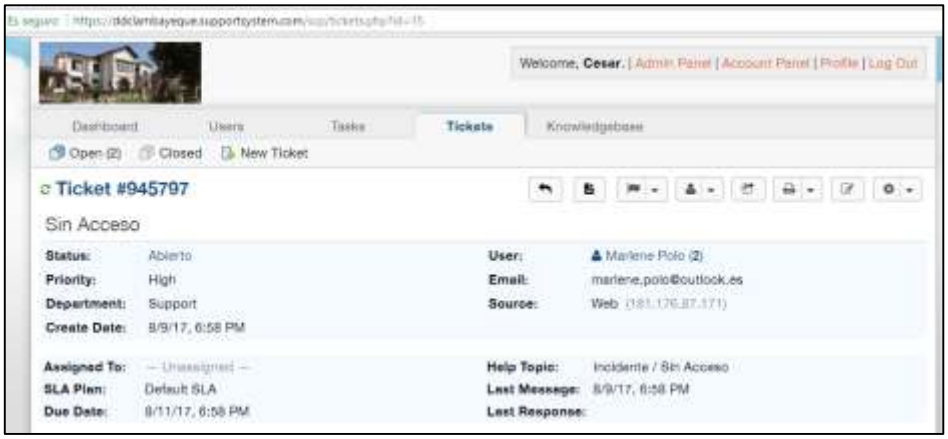
7. Usuario genera ticket:



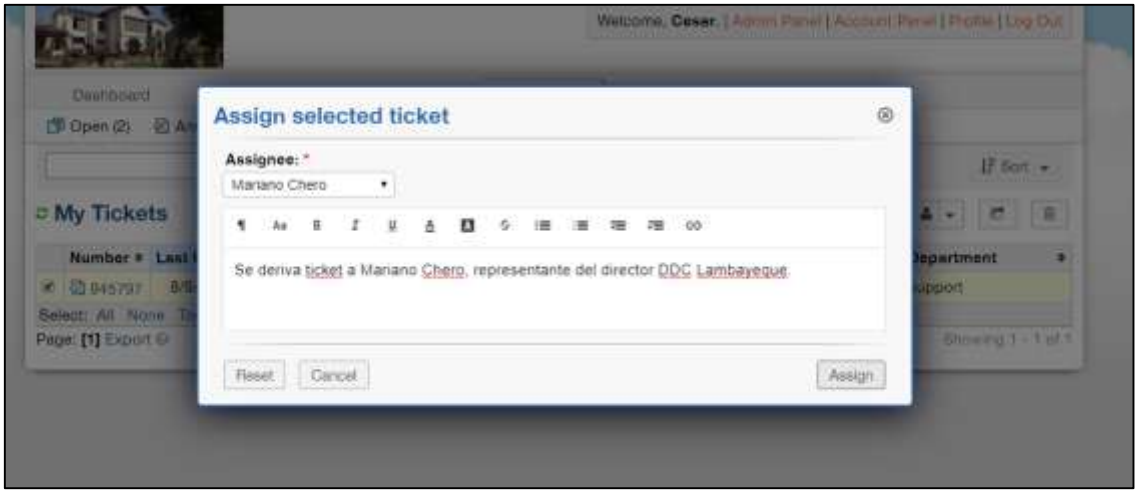
8. Ticket es recibido por el agente en este caso CISO:



9. Ticket tiene numeración y estado:



10. Ticket derivado a agente para su atención:



11. Agente recibe y confirma ticket:

12. Agente resuelve y soluciona ticket.