Máster Interuniversitario en Seguridad de las Tecnologías de la información y la Comunicación (MISTIC)

PLAN DE IMPLEMENTACIÓN DE LA ISO/IEC 27001:2013, EN LA FUNDACIÓN UNIVERSITARIA SAN MATEO

Presentado por: FELIX EDUARDO SANCHEZ ARDILA

Docentes: Profesor Carles Garrigues Olivella

Profesor colaborador: Antonio José Segovia Henares

Junio, 2018

AGRADECIMIENTOS

En primer lugar a mi esposa, mi hija, padres y familia en general. Por el apoyo incondicional y motivación constante para el crecimiento profesional y laboral que he trazado en mi vida.

La realización del presente Trabajo Final del Master es fruto de las orientaciones y desarrollo de la asignatura Sistema de Gestión de Seguridad, lo cual me incentivo a implementar un sistema de gestión en la organización para la cual trabajo, la Fundación Universitaria San Mateo.

Por otra parte agradecer a la Fundación Universitaria San Mateo, por su apoyo incondicional en la realización del Master.

Tabla de contenido

0. Descripción. ... 9
0.1 Metodología ... 10
Fase 1: Situación actual: Contextualización, Objetivos y Análisis Diferencial ... 11
1.1 Introducción ... 11
1.2 Conociendo las normas ISO/IEC 27001:2013 Y ISO/IEC 27002:2013 11
1.2.1 Origen de la Norma ISO/ IEC 27001:2013 ... 12
1.2.2 Relación entre las normas ISO/IEC 27001 Y 27002 ... 13
1.2.3 Familia ISO: 27000 ... 13
1.2.4 Ventajas de implantar un SGSI basado en la ISO/IEC 27001:2013 ... 16
1.2.5 Estructura de la Norma ISO/IEC 27001:2013 ... 17
1.2.6 Ciclo de mejora continua vs norma ISO/IEC 27001:2013 ... 18
1.2.7 Fases de Implementación del SGSI ... 19
1.2.8 ISO/IEC 27002:2013 ... 24
1.2.9 Medidas de seguridad ISO/IEC 27002:2013 ... 25
2. Situación actual: Contextualización, objetos y análisis diferencial ... 29
2.1 CONTEXTUALIZACIÓN ... 29
2.1.1 Descripción General de la Institución ... 29
2.1.2 Organización de la Institución ... 30
2.1.3 Estructura organizacional institucional ... 31
2.1.4 Infraestructura Tecnológica ... 32
2.1.5 INFRAESTRUCTURA FÍSICA ... 35
2.1.6 Procesos Estratégicos Institucionales ... 36
2.1.7 Alcance ... 39
2.2 Objetivos de seguridad de la información 39
2.2.1 Objetivo general ... 39
2.2.2 Objetivos específicos ... 39
2.3 Análisis diferencial 40
2.2.1 Análisis diferencial ISO/IEC: 27001:2013 ... 40
2.2.1 Análisis Diferencial ISO/IEC: 27002:2013 ... 48
2.3.1 Resultados ... 66
2.3.1.1 Resultados de Madurez ISO 27001:2013 ... 66
2.3.1.1 Evaluación de Madurez ISO 27002:2013 ... 68
Fase 2. Sistema de Gestión Documental ... 69
3.1 Introducción 69

3.2 Esquema Documental 70
3.2.1 Políticas de seguridad 70
3.2.2 Procedimientos de auditoria internas 71
3.2.3 Gestión de Indicadores 71
3.2.4 Procedimiento Revisión por Dirección 71
3.2.5 Gestión de roles y responsabilidades 72
3.2.7 Metodología de análisis de riesgos 72
3.2.7 Declaración de aplicabilidad 72
3.2.8 Resultados 73
Fase 3 4. Análisis de Riegos 74
4.1 Introducción 74
4.2 Inventario de activos 74
4.3 Valoración de los activos 78
4.4 Dimensiones de seguridad 80
4.5 Tabla resumen de valoración 81
4.6 Análisis de amenazas 85
4.7 Impacto potencial 95
4.8 Nivel de Riesgo Aceptable y riesgo Residual 106
Fase 4: Propuestas de Proyectos 116
5.1 Introducción 116
5.2 Propuestas ----------117
5.3 Resultados ----------123
Fase 5: 6 Auditoría de Cumplimiento 125
6.1 Introducción ----------125
6.2 Metodología ----------126
6.3 Evaluación de la madurez ISO/IEC 27001:2013 127
6.4 Evaluación de la madurez ISO/IEC 27002:2013 136
6.5 No conformidades respecto a la ISO 27002:2013 152
6.6 Observaciones respecto a la ISO/IEC 27002:2013 162
6.7 Presentación de resultados 168
6.8 Resultados 172
FASE 6 7. Presentación de Resultados y Entrega de Informes 173
7.1 Introducción 173
7.2 Objetivos 173
7.3 Entregables 173

8. Conclusiones 174
8.1 Introducción……174
8.2 Objetivos Específicos ……..174
8.3 Recomendaciones ……..174
8. Términos y Definiciones..... 174
9. Anexoas……..177
Bibliografía ……178

Índice de ilustraciones

Ilustración 1: Evolución Sistema integrado de gestión institucional. 18
Ilustración 2: Ciclo de Deming aplicado a los sistemas de gestión de seguridad de la información.18
Ilustración 3: Estructura Organizacional institucional..... 31
Ilustración 4 Estructura orgánica de Gerencia de Sistemas..... 32
Ilustración 5: Arquitectura de Software..... 33
Ilustración 6: Topología Física. 33
Ilustración 7: Infraestructura de Servidores. 34
Ilustración 8 Mapa de Ubicación San Mateo 36
Ilustración 9: Evolución Sistema integrado de gestión institucional. 37
Ilustración 10: sistema de aseguramiento de la calidad. 38
Ilustración 11: Madurez CMM de los Controles ISO..... 66
Ilustración 12: Diagrama Comparativo el estado actual con el estado deseado Controles ISO..... 67
Ilustración 13: Resumen de cumplimiento por Dominios. 68
Ilustración 14: Porcentaje de madurez de los controles implantados. 68
Ilustración 15: Porcentaje de controles Aprobados y No aprobados..... 69
Ilustración 16: Dependencias administración y monitorización..... 79
Ilustración 17: Evaluación de Madurez respecto a los controles ISO/IEC 27002:2013... 125
Ilustración 18 Grado de Madurez MMC..... 169
Ilustración 19 Porcentaje de madurez medido en la auditoría 171
Ilustración 20 Porcentaje de cumplimiento de la Norma-..... 172

Índice de tablas

Tabla 1: Fases para la implementación de SGSI en la Fundación Universitaria San Mateo..... 19
Tabla 2: Valoración de Criterios de Madurez CMM..... 40
Tabla 3: Evaluación De Efectividad De Controles - ISO 27001:2013..... 41
Tabla 4 Requerimientos obligatorios para el SGSI..... 42
Tabla 5: Madurez del control ISO..... 48
Tabla 6: Modelo de Madurez de Cumplimiento..... 50
Tabla 7: Resumen de Madurez de Cumplimento en la Fundación Universitaria San Mateo..... 51
Tabla 8: Valoración de los 114 controles..... 51
Tabla 9: Evaluación de los controles de la Normativa ISO /IEC 27002:2013Control en la normativa ISO/IEC 27002:2013..... 52
Tabla 10 Resumen de Cumplimiento por Dominios..... 65
Tabla 11: Tipos de Activos Según MAGERIT..... 74
Tabla 12: Inventario de Activos..... 75
Tabla 13: Escala de Valoración..... 79
Tabla 14: Valoración dimensiones de Seguridad..... 81
Tabla 15: Valoración de los activos..... 81
Tabla 16: Catálogo de Amenazas MAGERIT..... 85
Tabla 17: Categorías de Frecuencias de Amenazas..... 87
Tabla 18: Resumen análisis de Amenazas..... 88
Tabla 19: Impacto de Amenazas..... 95
Tabla 20: Relación impacto/ Frecuencia..... 107
Tabla 21: Valores Máximos de Frecuencia..... 107
Tabla 22: Resumen de Análisis de nivel de Riesgo..... 108
Tabla 23: Activos que superan el nivel MEDIO..... 111
Tabla 24: Resumen de cumplimiento de los dominios..... 124
Tabla 25 Modelo de Madurez de la Capacidad (CMM)..... 126
Tabla 26 Porcentaje de madurez de los dominios ISO 27002..... 170

Índice de anexos

Anexo A Autodiagnóstico 177
Anexo B Políticas de Seguridad en La Información 177
Anexo C Procedimiento Auditoria Interna 177
Anexo D Gestión de Indicadores 177
Anexo E Procedimiento Revisión por la Dirección 177
Anexo F Gestión de Roles y Responsabilidades..... 177
Anexo G Metodología de Análisis de Riesgos..... 177
Anexo H Declaración de la Aplicabilidad..... 177
Anexo I Evaluación de Madurez respecto a los controles definidos en la ISO 27002..... 177
Anexo J Declaración de Aplicabilidad San Mateo……174
Anexo K Resumen de Análisis de nivel de Riesgo……174
Anexo L Informe de Auditoria Interna……174
Anexo M Inventario San Mateo……174
Anexo N Resultado de evaluación de Madurez……174
Anexo Ñ Resultado de Evaluación de Madurez2……174

0. Descripción

El plan de implementación de la ISO/IEC 27001:2013 es un aspecto clave en cualquier organización que desea alinear sus objetivos y principios de seguridad a la normativa internacional de referencia.

El principal objetivo es establecer las bases del proceso de mejora continua en materia de seguridad de la información, permitiendo a las organizaciones conocer el estado de la misma y plantear las acciones necesarias para minimizar el impacto de los riesgos potenciales.

El proyecto busca la implementación de un SGSI (Sistema de Gestión de la Seguridad de la Información) para la Fundacion Universitaria San Mateo, para ello se ha establecido una metodología que cuenta con las siguientes fases:

- Documentación normativa sobre las mejores prácticas en seguridad de la información.
- Definición clara de la situación actual y de los objetivos del SGSI.
- Análisis de Riesgos.
    - Identificación y valoración de los activos corporativos como punto de partida a un análisis de riesgos.
    - Identificación de amenazas, evaluación y clasificación de las mismas.
- Evaluación del nivel de cumplimiento de la ISO/IEC 27002:2013 en la organización.
- Propuestas de proyectos de cara a conseguir una adecuada gestión de la seguridad.
- Esquema Documental.

Como entregables del proyecto, deberán presentarse básicamente los productos que se especifican a continuación:

- Informe Análisis Diferencial.
- Esquema Documental ISO/IEC 27001.
- Análisis de Riesgos.
- Plan de Proyectos.
- Auditoría de Cumplimiento.
- Presentación de resultados.

0.1 Metodología

A nivel metodológico, se realizará una aproximación por fases al proyecto con miras a tratar los diferentes apartados de tal forma que pueda realizarse en el tiempo estipulado.

En este sentido se relaciona a continuación el cronograma de actividades a realizar:

- **Fase 1**. Situación actual: Contextualización, objetivos y análisis diferencial
  Fecha límite de entrega: **9 de Marzo.**

  Introducción al proyecto. Enfoque y selección de la empresa que será objeto de estudio. Definición de los objetivos del plan director de seguridad y análisis diferencial de la empresa con respecto a la norma ISO/IEC 27001+ISO/IEC 27002.

- **Fase 2.** Sistema de Gestión Documental
  Fecha límite de entrega: **23 de Marzo.**

  Elaboración Política de Seguridad. Declaración de aplicabilidad y Documentación del SGS

- **Fase 3.** Análisis de riesgos

  Fecha límite de entrega: **13 de Abril.**

  Elaboración de una metodología de análisis de riesgos: Identificación y valoración de activos, amenazas, vulnerabilidades, cálculo del riesgo, nivel de riesgo aceptable y riesgo residual.

- **Fase 4:** Propuesta de Proyectos
  Fecha límite de entrega**: 27 de Abril**

  Evaluación de proyectos que debe llevar a cabo la Organización para alinearse con los objetivos planteados en el Plan Director. Cuantificación económica y temporal de los mismos.

- **Fase 5:** Auditoría de Cumplimiento de la ISO/IEC 27002:2013
  Fecha límite de entrega: **18 de Mayo**

  Evaluación de controles, madurez y nivel de cumplimiento.

- **Fase 6.** Presentación de Resultados y entrega de Informes

  Fecha límite de entrega: **6 de Junio**

  Consolidación de los resultados obtenidos durante el proceso de análisis. Realización de los informes y presentación ejecutiva a la dirección. Entrega del proyecto final.

Fase 1: Situación actual: Contextualización, Objetivos y Análisis Diferencial

1.1 Introducción

La implementación de un sistema de gestión de seguridad en la información (SGSI) es uno de los elementos clave con que debe trabajar el responsable de la seguridad de la información en una institución, empresa u organización, este sistema organiza los procedimientos para gestionar de una forma correcta la seguridad, permitiendo realizar análisis y autodiagnósticos para conocer el estado en que se encuentra, verificar falencias y establecer un plan de mejora.

Al momento de realizar una implementación de un (SGSI), teniendo en cuenta un estándar internacional ISO 27001:2013 y los controles de la ISO/IEc 27002:2013, se debe utilizar un ciclo PDCA O PHVA1 el cual cuenta con los siguientes pasos: Planificar, Hacer, Verificar y Actuar. Estos ciclos permiten realizar mejoras continuas, estableciendo objetivos de seguridad, controles, análisis y auditorias basados en herramientas como GAP, en la que su principal función es identificar las amenazas que ponen en peligro los pilares de la seguridad informática. Confidencialidad, integridad y disponibilidad de la información.

Las organizaciones deben controlar, identificar, valorar y clasificar mediante cada uno de los controles de seguridad ISO/IE 27002:2013, implementando soluciones efectivas para mitigar situaciones que puedan comprometer información importante y vulnerable como bases de datos de personas, activos e información financiera.(“ISO 27001: La implementación de un Sistema de Gestión de Seguridad de la Información)

1.2 Conociendo las normas ISO/IEC 27001:2013 Y ISO/IEC 27002:2013

La información es un activo muy valioso capaz de impulsar o destruir una empresa. Las organizaciones deben velar por garantizar su seguridad en cuanto a la integridad, disponibilidad y confidencialidad en la información, la información se ha consolidado como una parte cada vez más importante, y a la par también lo ha ido haciendo la metodología y las ‘buenas prácticas’ sobre seguridad de la información.

En este sentido organizaciones como ISO (International Organization for Standardization) y la IEC (International Electrotechnical Commission) han elaborado conjuntamente la familia ISO/IEC 27000. Esta, es un conjunto de normas desarrolladas para proveer un marco en gestión de la seguridad de la información que sirva de aplicación

1.2.1 Origen de la Norma ISO/ IEC 27001:2013

La historia del **ISO** comenzó en 1946 cuando delegados de 25 países se reunieron en el Instituto de Ingenieros Civiles en Londres y decidieron crear una nueva organización internacional 'para facilitar la coordinación internacional y la unificación de estándares industriales'. El 23 de febrero de 1947, la nueva organización, ISO, comenzó a operar oficialmente.(ISO, 2016), Su sede está en Ginebra Suiza, las normas internacionales son la columna vertebral de la sociedad, garantizan la seguridad y calidad de los productos y servicios. ISO es una organización internacional no gubernamental e independiente con una membresía de 161 organismos nacionales de normalización, (ISO, 2016).

Los estándares internacionales hacen que las cosas funcionen bien, ofrecen especificaciones de clase mundial para productos, servicios y sistemas, para garantizar la calidad, la seguridad y la eficiencia. Son fundamentales para facilitar el comercio internacional, ISO ha publicado 22070 normas internacionales y documentos relacionados, que cubren casi todas las industrias, desde la tecnología, a la seguridad alimentaria, a la agricultura y la salud.

ISO/ IEC 27001:2013 especifica los requisitos para establecer, implementar, mantener y mejorar continuamente un sistema de gestión de la seguridad de la información dentro del contexto de la organización. También incluye requisitos para la evaluación y el tratamiento de riesgos de seguridad de la información adaptados a las necesidades de la organización. Los requisitos establecidos en ISO/ IEC 27001:2013 son genéricos y están destinados a ser aplicables a todas las organizaciones, independientemente de su tipo, tamaño o naturaleza, la revisión más reciente de esta norma fue publicada en 2013 y ahora su nombre completo es ISO/IEC 27001:2013. La primera revisión se publicó en 2005 y fue desarrollada en base a la norma británica BS 7799-2.

A medida que la seguridad se ha consolidado como una parte cada vez más importante de los sistemas de información, también lo ha ido haciendo la metodología y las "buenas prácticas" sobre seguridad de la información. Por ello es relevante disponer de una primera etapa de levantamiento de información y de algunas de las mejores prácticas en seguridad de la información. Estas "mejores prácticas" serán fundamentales para realizar una aproximación sistemática al análisis de la seguridad.

Adopción del Anexo SL (lo que era antes la Guía ISO 83) dentro del SGSI. Es importante mencionar que este anexo describe los lineamientos para un sistema de gestión genérico; ayudando a las empresas que por alguna razón deben certificar múltiples normas de sistemas de gestión. De esta forma ISO 27001 cumple con los requisitos comunes a todo sistema de gestión, facilitando la implementación y auditoria de varios sistemas en la misma organización.

1.2.2 Relación entre las normas ISO/IEC 27001 Y 27002

La norma ISO/IEC: 27001:2013 es una norma que define como ejecutar un Sistema de Gestión de la Seguridad ISO/IEC: 27001:2013 de la información (SGSI), indicando que la seguridad de la información debe ser planificada, implementada, supervisada, revisada y mejorada. De estos hitos, se extraen una serie de objetivos para su cumplimiento y que están establecidos en la norma. Por lo tanto, es una norma de certificación de cumplimiento de dichos objetivos.

En cambio, la norma ISO/IEC/27002:2013 es una guía de buenas prácticas para mejorar la seguridad de la información de tal manera que ayuda a alcanzar los objetivos marcados en la ISO/IEC: 27001:2013. Estas buenas prácticas se presentan en forma de controles diferenciados por dominios relativos a la seguridad de la información. Dichos controles ya aparecen nombrados en la norma ISO/IEC: 27001:2013 en su Anexo A, pero sin ser desarrollados, y es en la 27002 donde se desarrollan. (ISO, 2016).

Por tanto, se puede concluir que la norma ISO/IEC 27002 ofrece las herramientas para ayudar a alcanzar los objetivos que se establecen en la norma ISO/27001.

1.2.3 Familia ISO: 27000

ISO 27000 es una agrupación de normas desarrolladas o en fase de desarrollo que facilitan un marco de gestión de la seguridad de la información aplicable a cualquier tipo de empresa, privada o pública, pequeña o grande.(“famila iso 27001 - Buscar con Google,”)

ISO / IEC 27000: 2018 proporciona una descripción general de los sistemas de gestión de la seguridad de la información (SGSI). También proporciona términos y definiciones comúnmente utilizados en la familia de estándares SGSI. Este documento es aplicable a todos los tipos y tamaños de organización (por ejemplo, empresas comerciales, agencias gubernamentales, organizaciones sin fines de lucro).

ISO/IEC 27001:2013 especifica los requisitos para establecer, implementar, mantener y mejorar continuamente un sistema de gestión de la seguridad de la información dentro del contexto de la organización. También incluye requisitos para la evaluación y el tratamiento de riesgos de seguridad de la información adaptados a las necesidades de la organización. Los requisitos establecidos en ISO / IEC 27001: 2013 son genéricos y están destinados a ser aplicables a todas las organizaciones, independientemente de su tipo, tamaño o naturaleza.

ISO/IEC 27002:2013 proporciona directrices para las normas de seguridad de la información organizacional y las prácticas de gestión de la seguridad de la información, incluida la selección, implementación y gestión de controles teniendo en cuenta los entornos de riesgo de seguridad de la información de la organización.

Está diseñado para ser utilizado por organizaciones que tienen la intención de:

- Seleccionar controles dentro del proceso de implementación de un Sistema de gestión de seguridad de la información basado en ISO / IEC 27001;
- implementar controles de seguridad de la información comúnmente aceptados;
- desarrollar sus propias pautas de gestión de seguridad de la información.

ISO/IEC 27003:2017 actualizada el 12 de abril de 2017. No certificable. Es una guía que se centra en los aspectos críticos necesarios para el diseño e implementación con éxito de un SGSI de acuerdo ISO/IEC 27001. Describe el proceso de especificación y diseño desde la concepción hasta la puesta en marcha de planes de implementación, así como el proceso de obtención de aprobación por la dirección para implementar un SGSI.

ISO/IEC 27004:2016 proporciona directrices destinadas a ayudar a las organizaciones a evaluar el rendimiento de la seguridad de la información y la eficacia de un sistema de gestión de seguridad de la información con el fin de cumplir con los requisitos de ISO / IEC 27001: 2013.

Establece:

a) el monitoreo y la medición del rendimiento de la seguridad de la información;
b) el monitoreo y la medición de la efectividad de un sistema de gestión de la seguridad de la información (SGSI), incluidos sus procesos y controles;
c) el análisis y evaluación de los resultados de monitoreo y medición.

ISO / IEC 27005:2011 proporciona directrices para la gestión de riesgos de seguridad de la información, es compatible con los conceptos generales especificados en ISO / IEC 27001 y está diseñado para ayudar a la implementación satisfactoria de la seguridad de la información basada en un enfoque de gestión de riesgos.

El conocimiento de los conceptos, modelos, procesos y terminologías descritos en ISO / IEC 27001 e ISO / IEC 27002 es importante para una comprensión completa de ISO / IEC 27005: 2011.

ISO / IEC 27005: 2011 es aplicable a todo tipo de organizaciones (por ejemplo, empresas comerciales, agencias gubernamentales, organizaciones sin fines de lucro) que pretenden gestionar los riesgos que podrían comprometer la seguridad de la información de la organización.

ISO/IEC 27006:2015 especifica los requisitos y proporciona una guía para los organismos que proporcionan auditoría y certificación de un sistema de gestión de seguridad de la información (ISMS), además de los requisitos contenidos en ISO / IEC 17021-1 e ISO / IEC 27001. Está destinado principalmente para apoyar la acreditación de los organismos de certificación que proporcionan la certificación ISMS.

Los requisitos contenidos en esta norma internacional deben ser demostrados en términos de competencia y confiabilidad por cualquier organismo que proporcione la certificación ISMS, y la orientación contenida en esta Norma Internacional proporciona una interpretación adicional de estos requisitos para cualquier organismo que proporcione la certificación ISMS.

NOTA: Esta norma internacional se puede usar como un documento de criterios para la acreditación, la evaluación por pares u otros procesos de auditoría ISO/IEC 27007:2011 Directrices para auditar un SGSI.

ISO / IEC 27007:2017 proporciona orientación sobre la gestión de un programa de auditoría del sistema de gestión de seguridad de la información (ISMS), sobre la realización de auditorías y sobre la competencia de los auditores de ISMS, además de la orientación contenida en ISO 19011: 2011.

ISO / IEC 27007 es aplicable a aquellos que necesitan comprender o llevar a cabo auditorías internas o externas de un ISMS o para administrar un programa de auditoría de ISMS.

ISO / IEC TR 27008: 2011 proporciona orientación sobre la revisión de la implementación y operación de controles, incluida la verificación de cumplimiento técnico de los controles del sistema de información, de conformidad con los estándares de seguridad de la información establecidos por una organización.

ISO / IEC TR 27008: 2011 es aplicable a todos los tipos y tamaños de organizaciones, incluidas empresas públicas y privadas, entidades gubernamentales y organizaciones sin fines de lucro que realizan revisiones de seguridad de la información y verificaciones técnicas de cumplimiento. No está destinado a auditorías de sistemas de gestión.

ISO / IEC 27009: 2016 define los requisitos para el uso de ISO / IEC 27001 en cualquier sector específico (campo, área de aplicación o sector de mercado). Explica cómo incluir requisitos adicionales a los de ISO / IEC 27001, cómo refinar cualquiera de los requisitos ISO / IEC 27001 y cómo incluir controles o conjuntos de control además de ISO / IEC 27001: 2013, Anexo A.

- ✓ Asegura que los requisitos adicionales o refinados no entren en conflicto con los requisitos de ISO / IEC 27001.
- ✓ Es aplicable a aquellos involucrados en la producción de estándares específicos del sector relacionados con ISO / IEC 27001.

1.2.4 Ventajas de implantar un SGSI basado en la ISO/IEC 27001:2013

- Disminuir el riesgo, con la consiguiente reducción de gastos asociados.
- Reducir la incertidumbre por el conocimiento de los riesgos e impactos asociados.
- Mejorar continuamente la gestión de la seguridad de la información.
- Garantizar la continuidad del negocio.
- Aumento de la competitividad por mejora de la imagen corporativa.
- Incremento de la confianza de las partes interesadas.
- Aumento de la rentabilidad, derivado de un control de los riesgos.
- Cumplir la legislación vigente referente a seguridad de la información.
- Aumentar las oportunidades de negocio.

- Reducir los costos asociados a los incidentes.
- Mejorar la implicación y participación del personal en la gestión de la seguridad.
- Posibilidad de integración con otros sistemas de gestión como ISO 9001, ISO14001, OHSAS 18001, entre otros.
- Mejorar los procesos y servicios prestados.
- Aumentar de la competitividad por mejora de la imagen corporativa.(Marco & Poblano, n.d.).

1.2.5 Estructura de la Norma ISO/IEC 27001:2013

El Nuevo esquema definido por International Organization for Standardization - ISO para todos los Sistemas de Gestión acorde al nuevo formato llamado "Anexo SL", que proporciona una estructura uniforme como el marco de un sistema de gestión genérico.

El Anexo SL aplica a todas las normas de sistemas de gestión, tales como las normas ISO, especificaciones de acceso público (PAS) y especificaciones técnicas (TS). Las revisiones de ISO 9001 e ISO 14001, así como la nueva norma ISO 45001 están todas basados en la estructura de alto nivel del Anexo SL.

Cláusula 1: Objeto y campo de aplicación

Cláusula 2: Referencias normativas

Cláusula 3: Términos y definiciones

Cláusula 4: Contexto de la organización

Cláusula 5: Liderazgo

Cláusula 6: Planificación

Cláusula 7: Soporte

Cláusula 8: Operación

Cláusula 9: Evaluación del desempeño

Cláusula 10: Mejora (Marco & Poblano, n.d.)

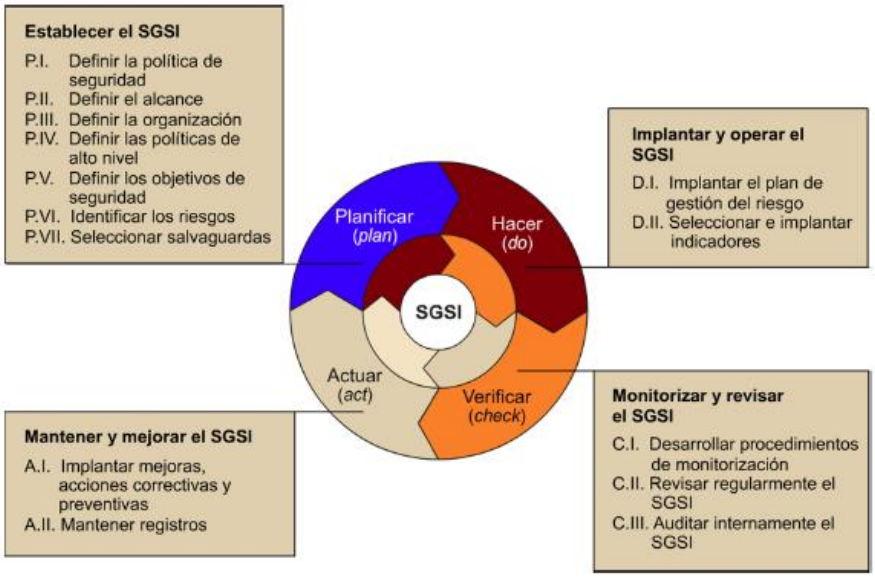
1.2.6 Ciclo de mejora continua vs norma ISO/IEC 27001:2013

Ilustración 1: Evolución Sistema integrado de gestión institucional.

Fuente: UOC. (2016). Implantación de un sistema de gestión de la seguridad de la información (SGSI).

El desarrollo de un sistema de gestión de la seguridad de la información se basa en la ISO 27001 y la ISO 27002, así como en el Ciclo de Deming, para garantizar la actualización del sistema y la mejora continua, tal y como se describe en el gráfico siguiente:

Ilustración 2: Ciclo de Deming aplicado a los sistemas de gestión de seguridad de la información.



Fuente: UOC. (2016). Implantación de un sistema de gestión de la seguridad de la información (SGSI).

- Fase PLANEAR en la norma ISO 27001:2013: Contexto de la organización de la norma ISO 27001:2013, se determina la necesidad de realizar un análisis de las cuestionas externas e internas de la organización y de su contexto, con el propósito de incluir las necesidades y expectativas de las partes interesas de la organización en el alcance del SGSI. Liderazgo, se establece las responsabilidades y compromisos de la Alta Dirección respecto al Sistema de Gestión de Seguridad de la Información.
- Fase HACER en la norma ISO 27001:2013: En el capítulo 8 - Operación de la norma ISO 27001:2013, se indica que la organización debe planificar, implementar y controlar los procesos necesarios para cumplir los objetivos y requisitos de seguridad y llevar a cabo la valoración y tratamiento de los riesgos de la seguridad de la información.
- Fase VERIFICAR en la norma ISO 27001:2013: En el capítulo 9 - Evaluación del desempeño, se define los requerimientos para evaluar periódicamente el desempeño de la seguridad de la información y eficacia del sistema de gestión de seguridad de la información.
- Fase ACTUAR en la norma ISO 27001:2013: En el capítulo 10 - Mejora20, se establece para el proceso de mejora del Sistema de Gestión de Seguridad de la Información, que a partir de las no-conformidades 30 que ocurran, las organizaciones deben establecer las acciones más efectivas para solucionarlas y evaluar la necesidad de acciones para eliminar las causas de la no conformidad con el objetivo de que no se repitan.("Ciclo PDCA (Planificar, Hacer, Verificar y Actuar): El círculo de Deming de mejora continua | PDCA Home,")

1.2.7 Fases de Implementación del SGSI

Las fases que serían necesarias para la implementación, así como el detalle de las actividades que se llevarían a cabo en cada fase en la Fundación Universitaria San Mateo

Tabla 1: Fases para la implementación de SGSI en la Fundación Universitaria San Mateo.

FASES	ACTIVIDADES A REALIZAR	JUSTIFICACION	TIEMPO DETERMINADO PARA SU EJECUCION
FASE 1 (PLANIFICAR)	Definir la política de seguridad	La institución deberá definir estrategias que busquen establecer una serie de normas, estándares o reglas que vaya de la mano con los objetivos de la empresa.	En la fase 1 (Planificación), lo que realmente se busca es que la institución realice una fotografía, un levantamiento de la información, como se encuentra actualmente y a dónde quiere llegar, con el objetivo de establecer un SGSI, una política de seguridad integral (Manejo de la información), procedimientos
	definir el alcance	Para definir el alcance la Fundación Universitaria San Mateo debe identificar donde se encuentra la organización, a donde quiere ir, con qué medios	

FASES	ACTIVIDADES A REALIZAR	JUSTIFICACION	TIEMPO DETERMINADO PARA SU EJECUCION
		cuenta y en qué áreas se quiere trabajar, a su vez podrá identificar procesos críticos en busca de establecer prioridades y delimitaciones de la implementación del SGSI.	para la gestión del riesgo, el alcance de la implementación de SGSI, la mejora de seguridad de información para obtener unos objetivos y una político global, a su vez también es importante la inclusión o no de las actividades llevadas a cabo con terceros para la organización, entre otras.
	definir la organización	La institución deberá establecer su estructura organizacional, donde se identifiquen todas las áreas de la misma, realizar una descripción general de la organización y del negocio como tal.	
	definir las políticas de alto nivel	para definir las políticas de alto nivel de la organización, esta debe cubrir un objetivo de seguridad, debe fortalecer sus recursos informáticos	
	definir los objetivos de seguridad	La empresa deberá definir los objetivos de seguridad encaminados a los objetivos del negocio en busca de una mejora no solo a nivel interno de la organización sino también para con sus clientes.	
	identificar los riesgos	Identificar cuáles son los puntos más altos de riesgos en los activos con los que cuenta la organización, esto deberá documentarse y crear una metodología donde la organización pueda revisar y	

FASES	ACTIVIDADES A REALIZAR	JUSTIFICACION	TIEMPO DETERMINADO PARA SU EJECUCION
		realizar un constante mantenimiento.	
	Seleccionar salvaguardas	Identificado los riesgos más críticos de la organización se deben seleccionar los controles necesarios para mitigar los riesgos, estas medidas deben quedar documentadas y cada control seleccionado debe tener una justificación y respectivo procedimiento en caso de ser ejecutado, para este caso en especial es importante que la organización tenga en cuenta el control del comercio electrónico dado que es su principal actividad económica.	
FASE 2 (HACER)	Implementar un plan de gestión de riesgos	Una vez planificado todas las actividades de la fase anterior la organización debe implementar el plan de gestión, como se van a implementar las salvaguardias y los controles seleccionados, en qué momento se implementaran si es a corto, mediano o largo plazo. Deberá tener en cuenta los costes de cada una de las actividades a realizar, dado que el plan de gestión de riesgos es básicamente como llevar acabo los objetivos de	La segunda fase está compuesta por dos actividades muy importantes basadas en la implementación un plan de gestión de riesgo y realizar la selección de indicadores, en esta etapa es muy importante tener en cuenta que esta fase no termina con la definición de un plan de seguridad si no una vez realizada la planificación del SGSI dentro de la organización, esta debe poner en práctica y operar el

FASES	ACTIVIDADES A REALIZAR	JUSTIFICACION	TIEMPO DETERMINADO PARA SU EJECUCION
		seguridad planificados en la fase anterior. Es muy importante que la organización conozca y este a la vanguardia de lo que actualmente ofrece el mercado en el área de la tecnología.	SGSI, implementar y operar la política, los controles, procesos y procedimientos planificados, realizar seguimiento constante a todas las subfases y actividades planificadas y por lo tanto esta segunda fase del proceso se convierte en unas de las fases más largas del SGSI y en la cual la organización tardará más tiempo.
	seleccionar e implementar indicadores	En esta actividad la compañía juega un papel fundamental pues para que el sistema vivo y actualizado deberá realizar periódicamente revisiones y evaluaciones al sistema para identificar el nivel de eficiencia de los controles implementados, En esta actividad la organización deberá elaborar un documento donde queden identificados todos los indicador implementados, indicar la frecuencia en la cual se debe ejecutar y quien es el responsable; esto nos permitirá controlar y garantizar la eficiencia de la información que proporcionan.	
FASE 3 (VERIFICAR)	Desarrollar procedimientos de monitorización	La institución deberá realizar monitorios periódicos con el fin de conocer el estado y evolución de cada uno de los indicadores de seguridad implementados, con esto; la organización evidenciara si el control constituye o no a los objetivos de seguridad	La fase de verificar permite que el SGSI se mantenga actualizado y se identifiquen debilidades que nos ayudaran a tomar acciones de mejoras pertinentes, evaluar y medir la evolución del proceso respecto a la política del SGSI, sus objetivos y alcance, esta fase

FASES	ACTIVIDADES A REALIZAR	JUSTIFICACION	TIEMPO DETERMINADO PARA SU EJECUCION
		implementados o si por lo contrario alguno de ellos requiere actuación urgente.	además permitirá obtener unos resultados los cuales se deben gestionar para su revisión. La organización gastará menos tiempo que en las demás fases, dado que en esta fase solo se debe verificar las medidas y acciones implementadas.
	revisar regularmente el SGSI	Revisar regularmente el SGSI es unas de las funciones que desde la dirección se debe realizar, esta actividad debe realizarse mínimo una vez al año pero si el presupuesto lo permite lo mejor es que estas revisiones se realicen con mayor frecuencia, esto le permitirá a la organización controlar los procedimientos, identificar posibles cambios, revisar el estado del sistema, establecer acciones preventivas, correctivas o acciones de mejora cuando a ello hubiere lugar.	
	Auditar internamente el SGSI	La organización deberá auditar internamente su SGSI, debe planificar correctamente las auditorias, incluir la objetividad en la evaluación y establecer criterios estándar para la misma, esta actividad puede ser realizada o apoyada por auditores externos lo cual podrá brindar mayor objetividad en la auditoria como tal. En resultado de esta fase deberá concluir con un informe detallado de dicha auditoria el	

FASES	ACTIVIDADES A REALIZAR	JUSTIFICACION	TIEMPO DETERMINADO PARA SU EJECUCION
		cual deberá incluir el mínimo de requisitos establecidos por la norma.	
FASE 4 (ACTUAR)	Implementar mejoras, acciones correctivas y preventivas	En esta fase la organización debe velar por mantener y mejorar su SGSI, levantar registros los cuales pueden ser legibles, identificables y trazables, estos a su vez se deberán custodiar por un mínimo de 3 años, mantener este conjunto de evidencias permitirá a la organización comprobar que los indicadores, controles y políticas de seguridad se han implementador y de los cuales hay un registro de evidencias permitirán la obtención de planes de mejoras que se deberán planificar dentro del plan de seguridad de la información.	
	Mantener registros		

1.2.8 ISO/IEC 27002:2013

La norma ISO/IEC 27002:2013 (anteriormente denominada ISO 17799) es un estándar para la seguridad de la información que ha publicado la organización internacional de normalización y la comisión electrotécnica internacional. La versión más reciente de la norma ISO 27002:2013.

Las normas ISO/IEC 27001:2013, ISO/IEC 27002:2013 están enfocadas a todo tipo de organizaciones (por ej. empresas comerciales, agencias, gubernamentales, organizaciones sin ánimo de lucro), tamaños (pequeña, mediana o gran empresa), tipo o naturaleza, está organizado en base a los 14 dominios, 35 objetivos de control y 114 controles de ISO/IEC 27002:2013.

Todas las futuras normas de sistemas de gestión tendrán la misma estructura de referencia, texto básico idéntico, así como términos y definiciones comunes. Aunque la estructura de referencia no se

puede modificar, se pueden añadir sub-cláusulas y texto específico de la disciplina.("Norma ISO 27002: El dominio política de seguridad,")

1.2.9 Medidas de seguridad ISO/IEC 27002:2013

A continuación se describen los controles de seguridad basados en la norma ISO 27002:2013, lo cual busca tomar medidas de seguridad en los activos informáticos de la Fundación Universitaria San Mateo teniendo en cuenta los pilares de la seguridad informática Confidencialidad, Integridad y disponibilidad.

5. POLÍTICAS DE SEGURIDAD

- ✓ 5.1 Directrices de la Dirección en seguridad de la información.
  - 5.1.1 Conjunto de políticas para la seguridad de la información.
  - 5.1.2 Revisión de las políticas para la seguridad de la información("Norma ISO 27002: El dominio política de seguridad,")

6. ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACION

- ✓ 6.1 Organización interna.
  - 6.1.1 Asignación de responsabilidades para la segur. de la información.
  - • 6.1.2 Segregación de tareas.
  - • 6.1.3 Contacto con las autoridades.
  - • 6.1.4 Contacto con grupos de interés especial.
  - 6.1.5 Seguridad de la información en la gestión de proyectos.
- ✓ 6.2 Dispositivos para movilidad y teletrabajo.
  - 6.2.1 Política de uso de dispositivos para movilidad.
  - 6.2.2 Teletrabajo

7. SEGURIDAD LIGADA A LOS RECURSOS HUMANOS

- ✓ 7.1 Antes de la contratación.
  - 7.1.1 Investigación de antecedentes.
  - 7.1.2 Términos y condiciones de contratación.
- ✓ 7.2 Durante la contratación.
  - 7.2.1 Responsabilidades de gestión.
  - 7.2.2 Concienciación, educación y capacitación en seguridad de la información
  - 7.2.3 Proceso disciplinario.
- 7.3 Cese o cambio de puesto de trabajo
- 7.3.1 Cese o cambio de puesto de trabajo

8. GESTIÓN DE ACTIVOS

- ✓ 8.1 Responsabilidad sobre los activos.
  - 8.1.1 Inventario de activos.
  - 8.1.2 Propiedad de los activos.
  - 8.1.3 Uso aceptable de los activos.

- 8.1.4 Devolución de activos.
- ✓ 8.2 Clasificación de la información.
  - 8.2.1 Directrices de clasificación.
  - 8.2.2 Etiquetado y manipulado de la información.
  - 8.2.3 Manipulación de activos.
- ✓ 8.3 Manejo de los soportes de almacenamiento
  - 8.3.1 Gestión de soportes extraíbles.
  - 8.3.2 Eliminación de soportes.
  - 8.3.3 Soportes físicos en tránsito

9. CONTROL DE ACCESOS

- ✓ 9.1 Requisitos de negocio para el control de accesos.
  - 9.1.1 Política de control de accesos.
  - 9.1.2 Control de acceso a las redes y servicios asociados.
- ✓ 9.2 Gestión de acceso de usuario.
  - 9.2.1 Gestión de altas/bajas en el registro de usuarios.
  - 9.2.2 Gestión de los derechos de acceso asignados a usuarios.
  - 9.2.3 Gestión de los derechos de acceso con privilegios especiales.
  - 9.2.4 Gestión de información confidencial de autenticación de usuarios.
  - 9.2.5 Revisión de los derechos de acceso de los usuarios.
  - 9.2.6 Retirada o adaptación de los derechos de acceso
- ✓ 9.3 Responsabilidades del usuario.
  - 9.3.1 Uso de información confidencial para la autenticación.
- ✓ 9.4 Control de acceso a sistemas y aplicaciones.
  - 9.4.1 Restricción del acceso a la información.
  - 9.4.2 Procedimientos seguros de inicio de sesión.
  - 9.4.3 Gestión de contraseñas de usuario.
  - 9.4.4 Uso de herramientas de administración de sistemas.
  - 9.4.5 Control de acceso al código fuente de los programas.

10.CIFRADO

- ✓ 10.1 Controles criptográficos.
  - 10.1.1 Política de uso de los controles criptográficos.
  - 10.1.2 Gestión de claves

11.SEGURIDAD FÍSICA Y AMBIENTAL

- ✓ 11.1 Áreas seguras.
  - 11.1.1 Perímetro de seguridad física.
  - 11.1.2 Controles físicos de entrada.
  - 11.1.3 Seguridad de oficinas, despachos y recursos.
  - 11.1.4 Protección contra las amenazas externas y ambientales.
  - 11.1.5 El trabajo en áreas seguras.
  - 11.1.6 Áreas de acceso público, carga y descarga.
- ✓ 11.2 Seguridad de los equipos.
  - 11.2.1 Emplazamiento y protección de equipos.
  - 11.2.2 Instalaciones de suministro.
  - 11.2.3 Seguridad del cableado.
  - 11.2.4 Mantenimiento de los equipos.

- 11.2.5 Salida de activos fuera de las dependencias de la empresa.
- 11.2.6 Seguridad de los equipos y activos fuera de las instalaciones.
- 11.2.7 Reutilización o retirada segura de dispositivos de almacenamiento.
- 11.2.8 Equipo informático de usuario desatendido.
- 11.2.9 Política de puesto de trabajo despejado y bloqueo de pantalla

12.SEGURIDAD EN LA OPERATIVA

- ✓ 12.1 Responsabilidades y procedimientos de operación.
  - 12.1.1 Documentación de procedimientos de operación.
  - 12.1.2 Gestión de cambios.
  - 12.1.3 Gestión de capacidades.
  - 12.1.4 Separación de entornos de desarrollo, prueba y producción.
- ✓ 12.2 Protección contra código malicioso.
  - 12.2.1 Controles contra el código malicioso.
- ✓ 12.3 Copias de seguridad.
  - 12.3.1 Copias de seguridad de la información.
- ✓ 12.4 Registro de actividad y supervisión.
  - 12.4.1 Registro y gestión de eventos de actividad.
  - 12.4.2 Protección de los registros de información.
  - 12.4.3 Registros de actividad del administrador y operador del sistema.
  - 12.4.4 Sincronización de relojes.
- ✓ 12.5 Control del software en explotación.
  - 12.5.1 Instalación del software en sistemas en producción.
- ✓ 12.6 Gestión de la vulnerabilidad técnica.
  - 12.6.1 Gestión de las vulnerabilidades técnicas.
  - 12.6.2 Restricciones en la instalación de software.
- ✓ 12.7 Consideraciones de las auditorías de los sistemas de información.
  - 12.7.1 Controles de auditoría de los sistemas de información

13.SEGURIDAD EN LAS TELECOMUNICACIONES

- ✓ 13.1 Gestión de la seguridad en las redes.
  - 13.1.1 Controles de red.
  - 13.1.2 Mecanismos de seguridad asociados a servicios en red.
  - 13.1.3 Segregación de redes.
- ✓ 13.2 Intercambio de información con partes externas.
  - 13.2.1 Políticas y procedimientos de intercambio de información.
  - 13.2.2 Acuerdos de intercambio.
  - 13.2.3 Mensajería electrónica.
  - 13.2.4 Acuerdos de confidencialidad y secreto.

14.ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN

- ✓ 14.1 Requisitos de seguridad de los sistemas de información.
  - 14.1.1 Análisis y especificación de los requisitos de seguridad.
  - 14.1.2 Seguridad de las comunicaciones en servicios accesibles por redes públicas.
  - 14.1.3 Protección de las transacciones por redes telemáticas.

- ✓ 14.2 Seguridad en los procesos de desarrollo y soporte.
  - 14.2.1 Política de desarrollo seguro de software.
  - 14.2.2 Procedimientos de control de cambios en los sistemas.
  - 14.2.3 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo.
  - 14.2.4 Restricciones a los cambios en los paquetes de software.
  - 14.2.5 Uso de principios de ingeniería en protección de sistemas.
  - 14.2.6 Seguridad en entornos de desarrollo.
  - 14.2.7 Externalización del desarrollo de software.
  - 14.2.8 Pruebas de funcionalidad durante el desarrollo de los sistemas.
  - 14.2.9 Pruebas de aceptación.
- ✓ 14.3 Datos de prueba.
  - 14.3.1 Protección de los datos utilizados en pruebas.

15.RELACIONES CON SUMINISTRADORES

- ✓ 15.1 Seguridad de la información en las relaciones con suministradores.
  - 15.1.1 Política de seguridad de la información para suministradores.
  - 15.1.2 Tratamiento del riesgo dentro de acuerdos de suministradores.
  - 15.1.3 Cadena de suministro en tecnologías de la información y comunicaciones.
- ✓ 15.2 Gestión de la prestación del servicio por suministradores.
  - • 15.2.1 Supervisión y revisión de los servicios prestados por terceros.
  - • 15.2.2 Gestión de cambios en los servicios prestados por terceros

16.GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN

- ✓ 16.1 Gestión de incidentes de seguridad de la información y mejoras.
  - 16.1.1 Responsabilidades y procedimientos.
  - 16.1.2 Notificación de los eventos de seguridad de la información.
  - 16.1.3 Notificación de puntos débiles de la seguridad.
  - 16.1.4 Valoración de eventos de seguridad de la información y toma de decisiones.
  - 16.1.5 Respuesta a los incidentes de seguridad.
  - 16.1.6 Aprendizaje de los incidentes de seguridad de la información.
  - 16.1.7 Recopilación de evidencias.

17.ASPECTOS DE SEGURIDAD DE LA INFORMACION EN LA GESTIÓN DE 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.
  - 17.1.2 Implantación de la continuidad de la seguridad de la información.
  - 17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información.
- ✓ 17.2 Redundancias.
  - 17.2.1 Disponibilidad de instalaciones para el procesamiento de la información.

18.CUMPLIMIENTO

- 18.1 Cumplimiento de los requisitos legales y contractuales.

- 18.1.1 Identificación de la legislación aplicable.
- 18.1.2 Derechos de propiedad intelectual (DPI).
- 18.1.3 Protección de los registros de la organización.
- 18.1.4 Protección de datos y privacidad de la información personal.
- 18.1.5 Regulación de los controles criptográficos.
- 18.2 Revisiones de la seguridad de la información.
- 18.2.1 Revisión independiente de la seguridad de la información.
- 18.2.2 Cumplimiento de las políticas y normas de seguridad.
- 18.2.3 Comprobación del cumplimiento.(PCS, 2017)

2. Situación actual: Contextualización, objetos y análisis diferencial

La Fundación Universitaria San Mateo objeto de este plan Director de seguridad es una institución dedicada a la prestación de servicios de educación en metodología presencial en la ciudad de Bogotá y en la modalidad virtual en Colombia.

2.1 CONTEXTUALIZACIÓN

A continuación se realizará una contextualización de la institución; Fundación Universitaria San Mateo, con lo cual se trabajará el plan de implementación de la ISO/IEC/27001:2013, según las necesidades y requerimientos de la Institución

2.1.1 Descripción General de la Institución

La organización seleccionada como objeto estudio del Trabajo Final del Master es la "Fundación Universitaria San Mateo", cuenta con 30 años de experiencia en el sector educativo, inculcando los principales elementos de su Misión los cuales son: servicio educativo, compromiso social, formación integral y articulación con el sector productivo. Igualmente centrada en su Visión proyectada al 2021 lo cual será una institución de educación superior reconocida a nivel nacional y con proyección internacional centrada en cada uno de sus elementos Modelo Educativo, Formación Pertinente, compromiso social, innovación y desarrollo tecnológico, inculcando los valores institucionales: Honestidad, Respeto, Trabajo en Equipo, Tolerancia, Confianza Liderazgo y lealtad (Fundación Universitaria San Mateo, 2018).

Existen dos facultades; Ciencias Administrabas y Facultad de Ingenierías y Afines, estas dos facultades ofrecen programas en modalidad presencial en las jornadas Diurnas, Nocturnas y sábados, y ofrece programas en la modalidad virtual.

Los programas asociados a esta facultad de ingenierías son: Ingeniería de Sistemas, Ingeniería de Telecomunicaciones, Ingeniería Industrial, Ingeniería en Seguridad y Salud para el Trabajo, Diseño Gráfico.

La Facultad de Ciencias administrativas cuenta con los siguientes programas: Negocios Internacionales, Administración de Empresas, Contaduría Pública y Gastronomía

La implementación del Sistema de Gestión de Seguridad en la Información va abarcar el área de Tecnología de la Fundación Universitaria San Mateo.

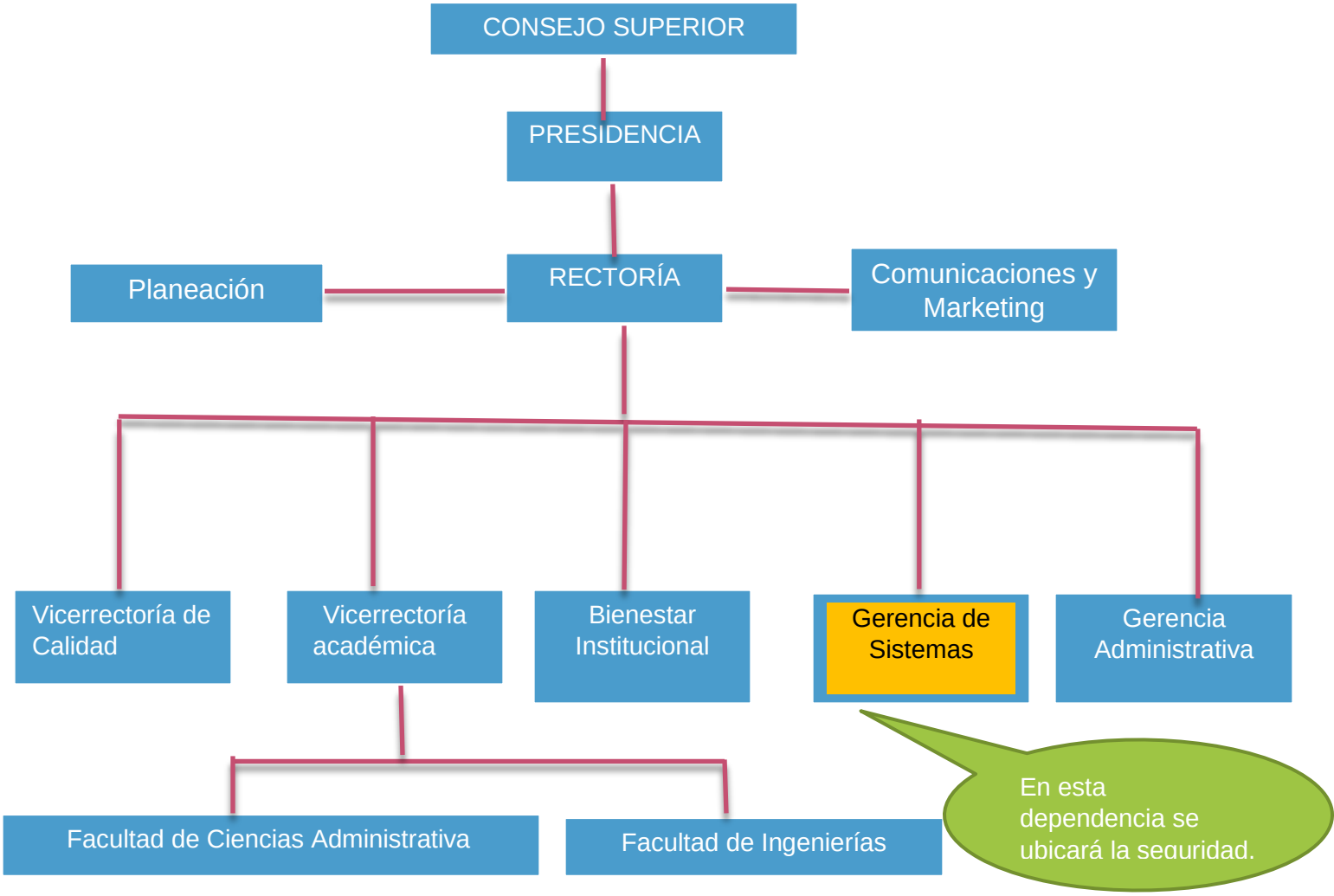
2.1.2 Organización de la Institución

La Fundación Universitaria San Mateo en coherencia con su crecimiento, proyectos y plan de desarrollo, cuenta con una estructura académico administrativa actualizada, organizada y conformada mediante resolución presidencial de Febrero de 2014.

La estructura académico administrativa del programa se enmarca en lo académico desde la vicerrectoría académica. Enseguida están las facultades que son lideradas por las Decanaturas; en la institución existen dos Facultadas es como se observa en la Figura 1, cada facultad gestiona los procesos y procedimientos relacionados con las funciones sustantivas direccionando y orientando estratégicamente en el grupo de programas, las dimensiones de extensión, proyección social, docencia, investigación e internacionalización en coherencia con los objetivos y políticas institucionales.(“organigrama.png (2846×1722)

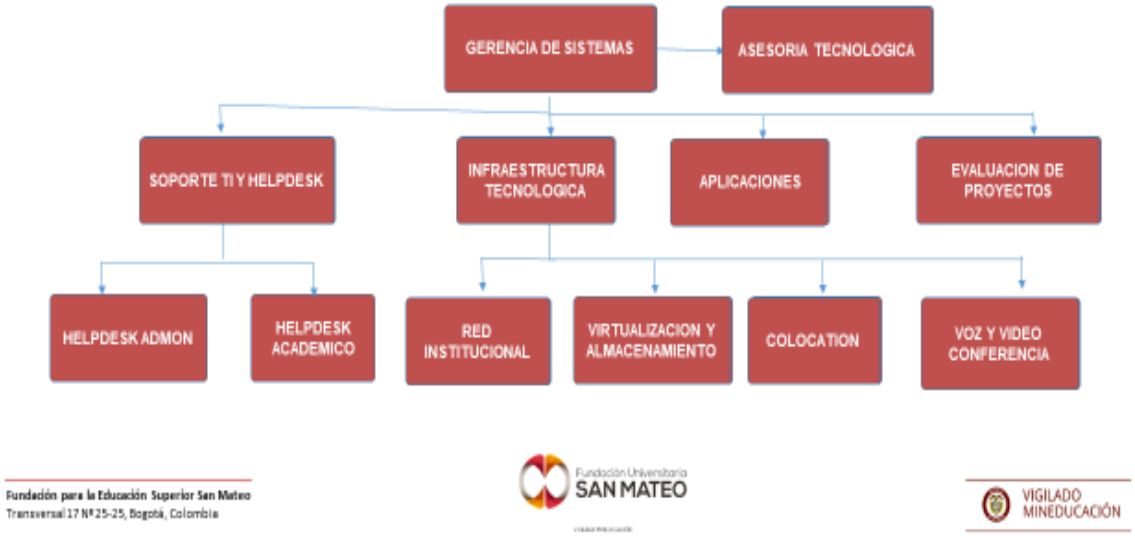
2.1.3 Estructura organizacional institucional

Ilustración 3: Estructura Organizacional institucional.



FUENTE: http://www.sanmateo.edu.co/img/organigrama.png.

Ilustración 4 Estructura orgánica de Gerencia de Sistemas

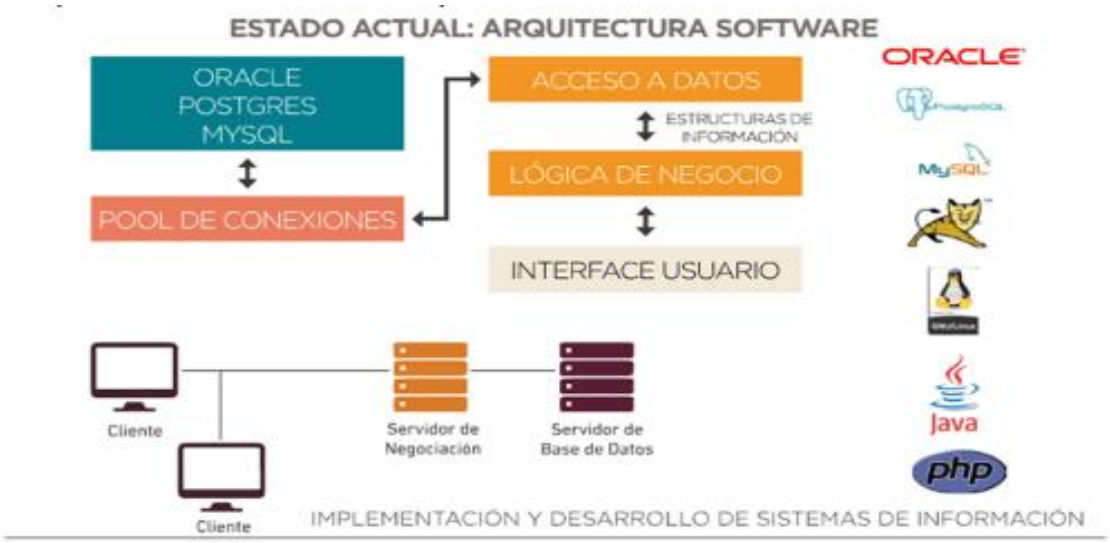


Fuente: Fundación Universitaria San Mateo.

2.1.4 Infraestructura Tecnológica

La Fundación Universitaria San Mateo cuenta con una infraestructura informática acorde a sus necesidades presentes y futuras entre ellas una infraestructura de red de datos que permite transferir y recibir cualquier tipo de información dentro o fuera de ella, esta red interconecta los diferentes edificios y Centros de Atención al estudiante con que cuenta la institución, formado por un anillo de fibra e interconectado por equipos de alta tecnología; una solución implementada de virtualización de servidores y almacenamiento que consolida el centro de datos que permite tener una solución redundante, de alta disponibilidad, y de respaldo; un número adecuado y actualizado de medios audiovisuales; aplicaciones informáticas al servicio de su comunidad académica y administrativa y un número adecuado en cantidad y calidad de computadores personales. ("FUNDACIÓN UNIVERSITARIA SAN MATEO," 2014).

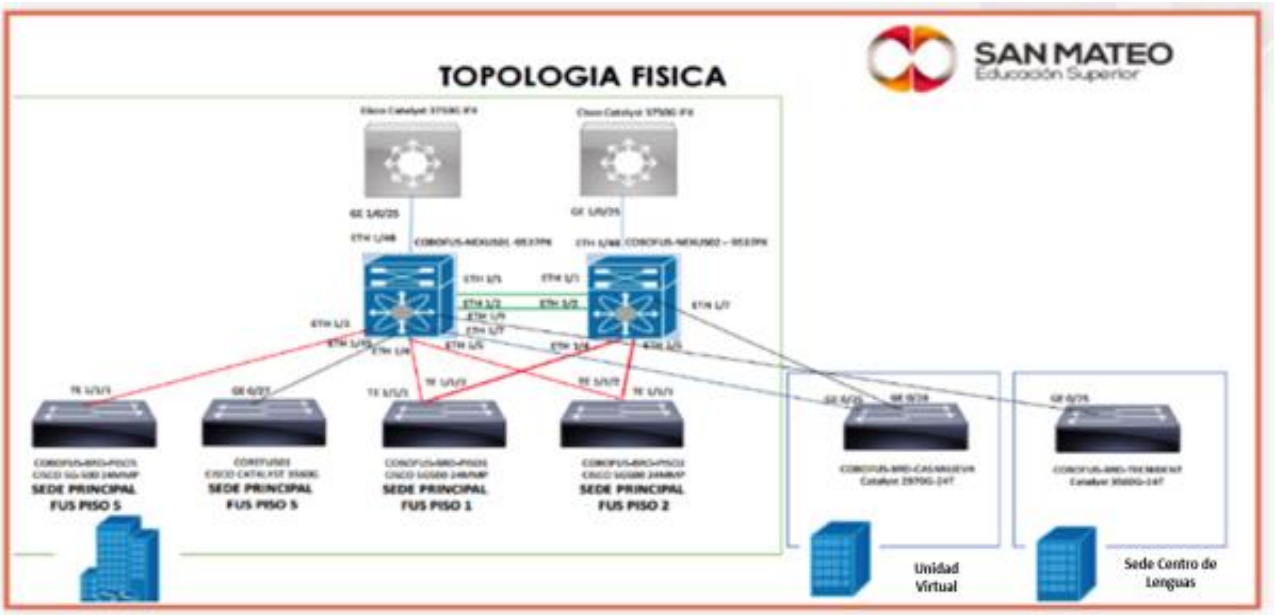
Ilustración 5: Arquitectura de Software.



Fuente: Fundación Universitaria San Mateo.

La Fundación Universitaria San Mateo cuenta con diferentes aplicativos para llevar a cabo los procesos académicos administrativos, se cuenta con software licenciado y de uso libre para los diferentes servicios como son Bases de Datos, Servidor de Dominio, servidores de Telefonía, servidor de aplicaciones etc..

Ilustración 6: Topología Física.

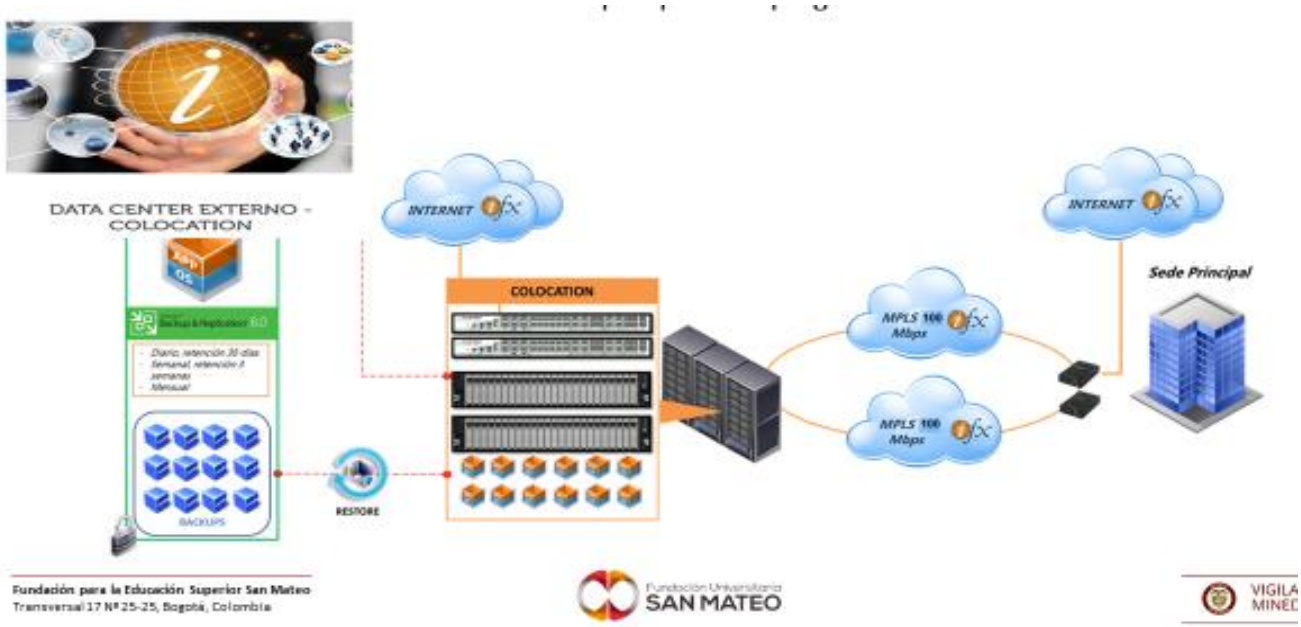


Fuente: Fundación Universitaria San Mateo.

La ilustración anterior podemos identificar la infraestructura tecnológica de switching, está basada en tecnológica NEXUS de Cisco Systems, la cual está conformada por 2 switches Cisco Nexus 9372PX, los cuales están configurados e instalados en esquema redundante.

Actualmente para los diferentes programas de la Fundación para la Educación Superior San Mateo se cuenta con un canal dedicado de 110 MBPS con reusó 1:1 (Ampliable a Capacidades Superiores) este canal garantizará el ancho de banda contratado la totalidad del tiempo así como en todos sus segmentos: última milla, NAP Colombia y salida internacional.

Ilustración 7: Infraestructura de Servidores.



Fuente: Fundación Universitaria San Mateo.

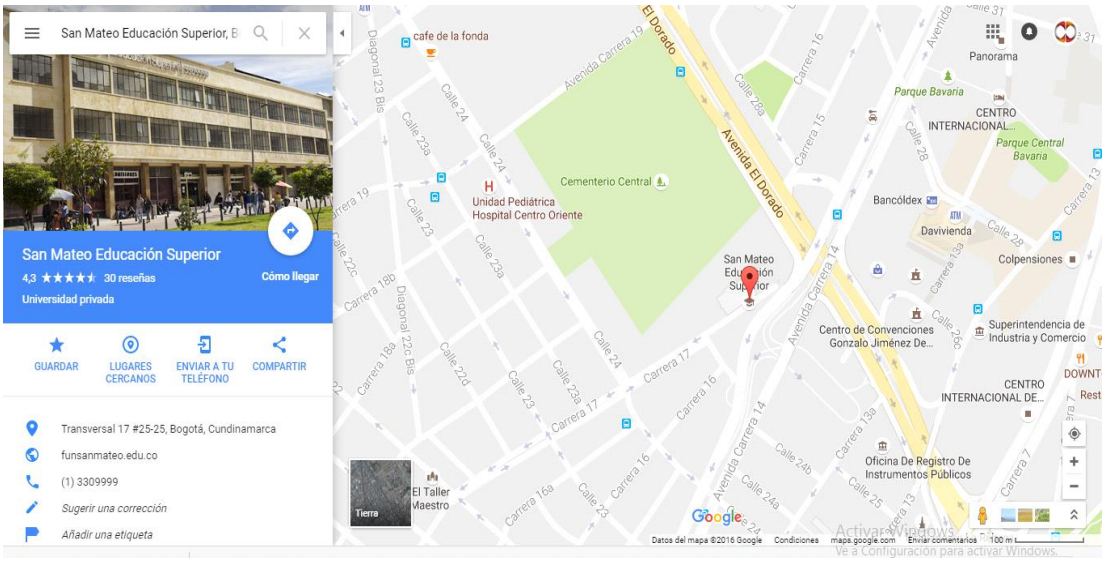
La institución cuenta con una gama de servidores con el fin de proveer todos los servicios informáticos y de comunicaciones hacia la comunidad Manteísta, cuenta con servidores virtualizados en el cual se alojan los principales que son: bases de datos, contenedores, aplicaciones, dominio, asterisk etc…

2.1.5 INFRAESTRUCTURA FÍSICA

El Edificio ubicado en la Transversal 17 No. 25-25 es la Sede Principal y las otras edificaciones se encuentran en sus alrededores a pocos metros de éste, frente a una amplia zona común de aproximadamente 2000 m2, en los que se cuenta con una zona verde y un parque, separados por una calle adoquinada cerrada, con entrada exclusiva al parqueadero, lo cual privilegia a las instalaciones al estar aisladas del ruido y alejadas de la contaminación vehicular y la polución en general. De igual forma, en el costado occidental se colinda con el parque cementerio británico que ubica a la institución en condiciones aisladas de ruido y contaminación.

Su cercanía a principales vías de la ciudad como son la Avenida Caracas y la Calle 26, permite el fácil desplazamiento desde diferentes partes de la ciudad, lo que garantiza un fácil acceso a través de los diferentes medios de transporte como el Sistema de Transporte Masivo Transmilenio al cual se puede acceder por las estaciones Calle 26 y Calle 22 de la troncal caracas y las diferentes rutas del SITP y próximamente el metro con su estación de la calle 26. El acceso vehicular a la sede principal de la Fundación para la Educación Superior San Mateo se hace por la transversal 17 sobre la que encontramos un espacio de parqueadero con un área total de 1400 metros cuadrados, de propiedad de la institución y administrado por un tercero, el cual ofrece el servicio de parqueadero para 60 vehículos y 200 motocicletas, para los estudiantes, docentes, personal administrativo y público visitante. Además, sobre esta misma transversal y a menos de 200 metros se encuentran ubicados 4 parqueaderos con capacidad total aproximada de 120 vehículos, los cuales son utilizados por nuestra comunidad Mateista. A continuación se observa el mapa con la ubicación estratégica de la institución.

Ilustración 8 Mapa de Ubicación San Mateo

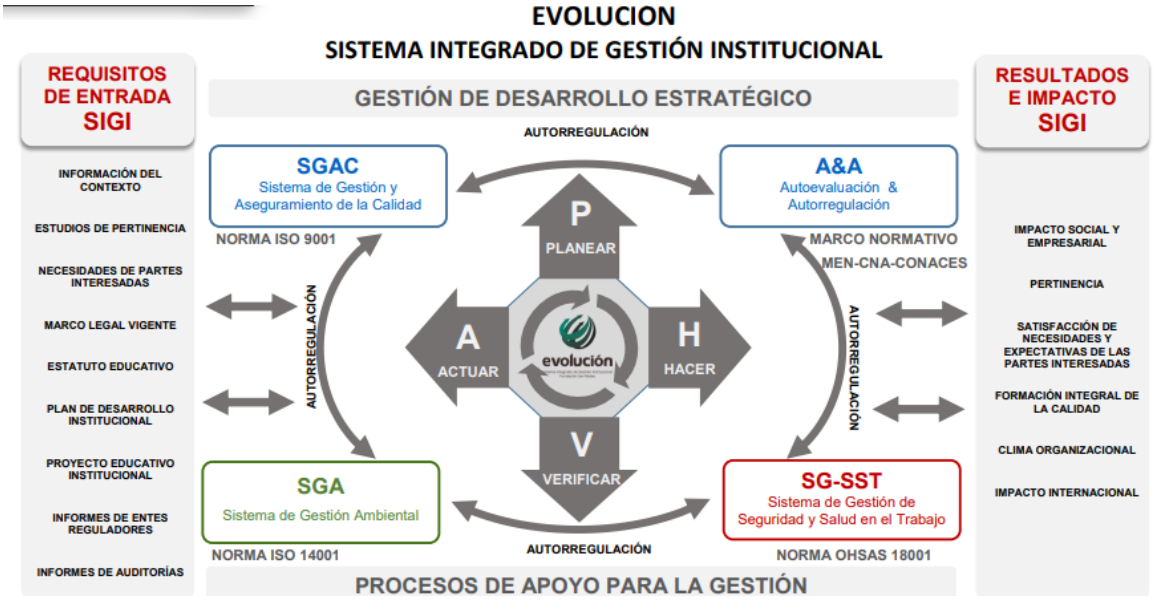


Fuente: Fundación San Mateo. (2018), disponible en el sitio http://www.sanmateo.edu.co/.

2.1.6 Procesos Estratégicos Institucionales

La institución cuenta con un sistema integrado de gestión institucional como se muestra en la siguiente ilustración. (SGAG) Sistema de Gestión y Aseguramiento de la Calidad, (A&A) Autoevaluación y Autorregulación, (SGA) sistema de Gestión Ambienta y (SG-SST) Sistema de Gestión de Seguridad y Salud en el Trabajo.

Ilustración 9: Evolución Sistema integrado de gestión institucional.



Fuente: (San Mateo)

Teniendo en cuenta la figura N° 2, en el sistema integrado de gestión institucional está pendiente integrar los Sistemas de Gestión de Seguridad en la Información (SGSI), lo cual es muy importante para la institución, es un tema que ha venido cobrando fuerza gracias a las diferentes políticas de protección de datos que han venido adoptando los diferentes países. Sin embargo la institución ha iniciado desde el departamento de tecnología el proceso de concientización y asignación de responsabilidades en estos temas.

La institución cuenta con un sistema de aseguramiento de la calidad de los procesos institucionales con el fin de garantizar la calidad, excelencia y mejoramiento continuo de nuestros programas.

Ilustración 10: sistema de aseguramiento de la calidad.

Fuente: http://sanmateo.edu.co/sgac.html

Contamos con 12 procesos clasificados en estratégicos, misiones y de apoyo los cuales gestionados articuladamente garantizan la planeación y administración de las funciones sustantivas del programa (Docencia, investigación y extensión, internacionalización) su ejecución, evaluación seguimiento y autorregulación.

2.1.7 Alcance

El propósito del siguiente plan director de seguridad en la Fundación Universitaria San Mateo, es implementar la norma ISO/IEC 27001:2013 Y ISO/IEC 27002:2013, todos los activos procesos y procedimientos que intervienen en los diferentes servicios en cuanto a gestión de la información del área de Gerencia de sistemas de institución.

Se define dentro del alcance los siguientes puntos

- Activos relacionados al tratamiento de información dela gerencia de sistemas
- Procesos y procedimientos relacionados con el tratamiento de la información
- Procesos y procedimientos para el personal interno y externo que tengan acceso algún activo de la institución.

En definitiva, el alcance son todos los sistemas de información que dan soporte a los procesos, actividades y servicios de la institución mencionados y que son llevados a cabo y ofrecidos de acuerdo a la declaración de la aplicabilidad vigente.

2.2 Objetivos de seguridad de la información

2.2.1 Objetivo general

Implementar estrategias de la seguridad en la información basados en la norma ISO/IEC 27001:2013, en el área donde mayor riegos se presenta que es el área gerencia de sistemas, dado los diferentes sistemas de información que maneja.

2.2.2 Objetivos específicos

Presentar en forma vigente las políticas de seguridad de la información, la documentación y procedimientos de un Sistema de Gestión de Seguridad en la información (SGSI) al personal administrativo de la Fundación Universitaria San Mateo

Planear los procedimientos y manuales que involucran el uso de información, de todas las personas en relación con el área de gerencia de sistemas de la institución.

Evaluar de manera clara los requisitos de seguridad de la información que la institución debe cumplir, con el fin identificar los riesgos y proteger la información y las bases de datos de la institución.

Presentar los pilares de la seguridad informática, Integridad, Disponibilidad y confidencialidad en los sistemas de información de la Institución con el fin de brindar la confianza a todos los miembros de la institución.

Establecer al interior de la compañía los roles y responsabilidades en términos de Seguridad de la Información.

2.3 Análisis diferencial

2.2.1 Análisis diferencial ISO/IEC: 27001:2013

Teniendo como base esta definición de la norma ISO27001:2013, este Trabajo Final de Master se enfocara en analizar los controles y requerimientos de seguridad de la ISO/IEC 27002:2013 con los procesos de la Fundación Universitaria San Mateo, para lo cual se mirara en el (**Anexo A**) la evaluación de efectividad de los Controles.(Oberta De Catalunya Autor & Rojas Valduciel, 2014)

El estudio debe realizar una revisión de 114 controles planteados por la norma para cumplir los diferentes objetivos de control, esta estimación la realizaremos según la siguiente tabla, que se basa en el Modelo de Madurez de capacidad (CMM):

Tabla 2: Valoración de Criterios de Madurez CMM.

Valor	Efectividad	Significado	Descripción
L0	0%	Inexistente	Carencia completa de cualquier proceso reconocible. No se ha reconocido siquiera que existe un problema a resolver.
L1	10%	Inicial / Ad-hoc	Estado inicial donde el éxito de las actividades de los procesos se basa la mayoría de las veces en el esfuerzo personal. Los procedimientos son inexistentes o localizados en áreas concretas.
L2	50%	Reproducible, pero intuitivo	Los procesos similares se llevan en forma similar por diferentes personas con la misma tarea. Se normalizan las buenas prácticas en base a la experiencia y al método.
L3	90%	Proceso definido	La organización entera participa en el proceso. Los procesos están implantados, documentados y comunicados
L4	95%	Gestionado y medible	Se puede seguir con indicadores numéricos y estadísticos la evolución de los procesos. Se dispone de tecnología para automatizar el flujo de trabajo, se
L5	100%	Optimizado	Los procesos están bajo constante mejora.

Teniendo en cuenta la tabla anterior se procede a realizar la evaluación de la efectividad de los controles correspondientes a la ISO 27001:2013,

Como resultados sintéticos, es interesante evaluar el nivel de madurez porcentual de los diferentes controles. Es decir, para los 114 controles, qué grado de madurez tiene cada uno, cosa que nos da una visión del estado de la seguridad en la Fundación universitaria San Mateo.

Ver detalle en el anexo: TFM SGSI (ANEXO A Autodiagnóstico)

Tabla 3: Evaluación De Efectividad De Controles - ISO 27001:2013.

	DOMINIOS	**Calificación Actual**	**Calificación Objetivo**	**EVALUACIÓN DE EFECTIVIDAD DE CONTROL**
A.5	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	70	100	**GESTIONADO**
A.6	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	30	100	**REPETIBLE**
A.7	SEGURIDAD DE LOS RECURSOS HUMANOS	40	100	**REPETIBLE**
A.8	GESTIÓN DE ACTIVOS	70	100	**GESTIONADO**
A.9	CONTROL DE ACCESO	70	100	**GESTIONADO**
A.10	CRIPTOGRAFÍA	30	100	**REPETIBLE**
A.11	SEGURIDAD FÍSICA Y DEL ENTORNO	60	100	**EFECTIVO**
A.12	SEGURIDAD DE LAS OPERACIONES	30	100	**REPETIBLE**
A.13	SEGURIDAD DE LAS COMUNICACIONES	40	100	**REPETIBLE**
A.14	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	60	100	**EFECTIVO**
A.15	RELACIONES CON LOS PROVEEDORES	70	100	**GESTIONADO**
A.16	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	40	100	**REPETIBLE**
A.17	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	50	100	**EFECTIVO**
A.18	CUMPLIMIENTO	30	100	**REPETIBLE**
PROMEDIO EVALUACIÓN DE CONTROLES		**49**	**100**	**EFECTIVO**

En la tabla anterior se puede evaluar los 14 dominios de la ISO 27001:2013, en los cuales se califica la efectividad de cada control. Este análisis nos muestra el estado actual de la Fundación Universitaria San Mateo, a cada dominio se agregara un valor en base al estado en que se encuentra.

Tabla 4 Requerimientos obligatorios para el SGSI

Control de ISO /IEC 27001	Requerimientos obligatorios para el SGSI	Valoración
4	**SGSI**	
4.1	**Requerimientos Generales**	
4.1	La organización debe establecer, implementar, operar, monitorizar, revisar, mantener y mejorar un SGSI documentado.	L2
4.2	**Establecer y Gestionar el SGSI**	
4.2.1	**Establecer el SGSI**	
4.2.1 (a)	Definir el alcance y los límites del SGSI.	L2
4.2.1 (b)	Definir una política de SGSI.	L2
4.2.1 (c)	Definir el enfoque de la evaluación de Riesgos.	L2
4.2.1 (d)	Identificar los riesgos.	L2
4.2.1 (e)	Analizar y evaluar los riesgos.	L2
4.2.1 (f)	Identificar y evaluar opciones para el tratamiento de riesgos.	L1
4.2.1 (g)	Seleccionar objetivos de control y controles para los tratamientos de riesgos.	L1
4.2.1 (h)	Obtener la aprobación por parte de la dirección de los riesgos residuales propuestos.	L2
4.2.1 (i)	Obtener la autorización de la Dirección para implementar y operar el SGSI.	L2
4.2.1 (j)	Preparar una Declaración de aplicabilidad.	L2
4.2.2	**Implementar el SGSI**	
4.2.2 (a)	Elaborar un plan de tratamiento de riesgos.	L1
4.2.2 (b)	Implementar el plan de tratamiento de riesgos para lograr los objetivos de control identificados.	L1
4.2.2 (c)	Implementar los controles seleccionados en 4.2.1g para llegar a los objetivos de control.	L1
4.2.2 (d)	Definir cómo medir la efectividad de los controles o grupos de controles seleccionados y especificar cómo estas mediciones van a ser utilizadas para evaluar la efectividad del control para producir resultados comparables y reproducibles (ver 4.2.3c) .	L1
4.2.2 (e)	Implementar programas de formación y concienciación (ver 5.2.2) .	L2
4.2.2 (f)	Gestionar la operación del SGSI.	L2
4.2.2 (g)	Gestionar los recursos para el SGSI (ver 5.2).	L2

4.2.2 (h)	Implementar procedimientos y otros controles capaces de permitir una rápida detección de eventos de seguridad y respuesta a incidentes de seguridad (ver 4.2.3[a]).	L0
4.2.3	**Monitorizar y Revisar el SGSI**	
4.2.3 (a)	Ejecutar procedimientos de monitorización y revisión y otros controles.	L2
4.2.3 (b)	Llevar a cabo revisiones periódicas de la efectividad del SGSI.	L1
4.2.3 (c)	Medir la efectividad de los controles para verificar que se cumplen los requerimientos de seguridad.	L1
4.2.3 (d)	Revisar las evaluaciones de riesgos en intervalos planificados y revisar los riesgos residuales y los niveles aceptables de riesgos identificados.	L1
4.2.3 (e)	Llevar a cabo auditorías internas del SGSI de manera regular (ver 6).	L0
4.2.3 (f)	Llevar a cabo una revisión por la dirección del SGSI de manera regular (ver 7.1).	L2
4.2.3 (g)	Actualizar los planes de seguridad para tener en cuenta los hallazgos de las actividades de monitorización y revisión.	L3
4.2.3 (h)	Registrar acciones y eventos que podrían tener impacto en la efectividad o el rendimiento del SGSI (ver 4.3.3).	L2
4.2.4	**Mantener y mejorar el SGSI**	
4.2.4 (a)	Implementar las mejoras identificadas en el SGSI.	L2
4.2.4 (b)	Llevar a cabo las acciones correctivas y preventivas de acuerdo con 8.2 y 8.3.	L2
4.2.4 (c)	Comunicar las acciones y mejoras a todas las partes interesadas.	L3
4.2.4 (d)	Asegurar que las mejoras consiguen sus objetivos propuestos.	L2
4.3	**Requerimientos de Documentación**	
4.3.1	**Documentación General del SGSI**	
4.3.1 (a)	Documentar los procedimientos y objetivos de la política del SGSI (ver 4.2.1b)	L3
4.3.1 (b)	Alcance del SGSI (ver 4.2.1A)	L3
4.3.1 (c)	Procedimientos y controles de apoyo al SGSI.	L2
4.3.1 (d)	Descripción de la metodología de evaluación de Riesgos (ver 4.2.1c)	L1
4.3.1 (e)	Informe de evaluación de Riesgos (ver desde el 4.2.1c al 4.2.1g)	L0
4.3.1 (f)	Plan de Tratamiento de Riesgos (ver 4.2.2b)	L2
4.3.1 (g)	Procedimientos necesitados por la organización para asegurar la planificación efectiva, la operación y el control de sus procesos de seguridad de la información y describir cómo medir la efectividad de los controles (ver 4.2.3c)	L1
4.3.1 (h)	Registros requeridos por este Estándar Internacional (ver 4.3.3)	L2
4.3.1 (i)	Declaración de Aplicabilidad.	L1

4.3.2	**Control de Documentos**	
4.3.2	Los Documentos requeridos por el SGSI deberán ser protegidos y controlados. Un procedimiento documentado deberá ser establecido para definir las acciones de la dirección necesitadas para:	
4.3.2 (a)	Aprobar documentos para su adecuación antes de su emisión.	L2
4.3.2 (b)	Revisar y actualizar documentos cuando sea necesario y re-aprobar documentos.	L1
4.3.2 (c)	Asegurar que los cambios y que los estados de revisión actual de los documentos están identificados	L2
4.3.2 (d)	Asegurar que las versiones pertinentes de documentos aplicables están disponible y a punto para ser usados.	L1
4.3.2 (e)	Asegurar que los documentos permanecen legibles y fácilmente identificables.	L3
4.3.2 (f)	Asegurar que los documentos están disponibles para aquellos que lo necesiten y son transferidos, almacenados y en última instancia, eliminados de acuerdo a los procedimientos aplicables en base a su clasificación.	L2
4.3.2 (g)	Asegurar que los documentos de procedencia externa están identificados.	L2
4.3.2 (h)	Asegurar que la distribución de los documentos está controlada.	L3
4.3.2 (i)	Prevenir el uso no intencionado de documentos obsoletos.	L3
4.3.2 (j)	Aplicar una identificación adecuada a los documentos si éstos son retenidos para cualquier propósito.	L3
4.3.3	**Control de los Registros**	
4.3.3 (a)	Los registros deben establecerse y mantenerse para proporcionar evidencias de conformidad a los requerimientos y a la eficacia del SGSI.	L3
4.3.3 (b)	Los registros serán protegidos y controlados	L3
4.3.3 (c)	El SGSI debe tener en cuenta los requisitos legales o reglamentarios y las obligaciones contractuales.	L5
4.3.3 (d)	Los registros deben permanecer legibles, fácilmente identificables y recuperables.	L4
4.3.3 (e)	Los controles necesarios para la identificación, almacenamiento, protección, recuperación, tiempo de retención y desechado de los registros serán documentados e implementados.	L5
4.3.3 (f)	Se mantendrán registros de los resultados del proceso, como se indica en el apartado 4.2 y de todas las ocurrencias de incidentes de seguridad significativos relacionados con el SGSI.	L3
5	**Gestión de la Responsabilidad**	
5.1	Compromiso de la dirección.	
5.1	La dirección debe proporcionar evidencia de su compromiso con el establecimiento, implementación, operación, monitoreo, revisión, mantenimiento y mejora del SGSI por:	L4
5.1 (a)	Establecer una política de SGSI.	L3

5.1 (b)	Asegurar de que se establecen los objetivos y los planes del ISMS.	L3
5.1 (c)	Establecer roles y responsabilidades para la seguridad de la información.	L4
5.1 (d)	Comunicar a la organización la importancia de satisfacer los objetivos de seguridad de la información y conforme a la política de seguridad de la información, sus responsabilidades en virtud de la ley así como la necesidad de la mejora continua.	L3
5.1 (e)	Proporcionar recursos suficientes para establecer, implementar, operar, monitorizar, revisar, mantener y mejorar el SGSI (ver 5.2.1)	L4
5.1 (f)	Decidir los criterios de aceptación de riesgos y los niveles de riesgo aceptables.	L3
5.1 (g)	Asegurarse de que las auditorías internas del SGSI se llevan a cabo (ver 6)	L2
5.1 (h)	La realización de revisiones por la dirección del SGSI (ver 7)	L3
5.2	Gestión de los recursos.	
5.2.1	Provisión de Recursos.	
5.2.1	La organización deberá determinar y proveer los recursos necesarios para:	
5.2.1 (a)	Establecer, implementar, operar, monitorizar, revisar, mantener y mejorar un SGSI.	L4
5.2.1 (b)	Asegurar que los procedimientos de seguridad de la información son compatibles con los requerimientos del negocio.	L2
5.2.1 (c)	Identificar y abordar los requisitos legales y reglamentarios y las obligaciones contractuales de seguridad.	L3
5.2.1 (d)	Mantener la seguridad adecuada mediante la aplicación correcta de todos los controles implementados.	L2
5.2.1 (e)	Llevar a cabo revisiones cuando sea necesario, y dar una respuesta adecuada a los resultados de estas revisiones.	L3
5.2.1 (f)	Cuando sea necesario, mejorar la eficacia del SGSI.	L3
5.2.2	Formación, sensibilización y competencia.	
5.2.2	La organización debe asegurarse de que todo el personal al que se le asigna responsabilidades definidas en el SGSI sean competentes para desempeñar las tareas requeridas por:	
5.2.2 (a)	Determinar las competencias necesarias para el personal que realiza trabajo efectivo en el SGSI.	L3
5.2.2 (b)	Proporcionar formación o tomar otras acciones (por ejemplo, el empleo de personal competente) para satisfacer estas necesidades.	L3
5.2.2 (c)	Evaluar la efectividad de las acciones llevadas a cabo.	

5.2.2 (d)	El mantenimiento de los registros de educación, formación, habilidades, experiencia y calificaciones (véase 4.3.3)	L2
5.2.2	La organización también debe asegurar que todo el personal pertinente es consciente de la relevancia e importancia de sus actividades de seguridad de la información y de cómo contribuyen al logro de los objetivos del SGSI.	L3
6	**Auditoría Interna del SGSI**	
6	La organización debe llevar a cabo auditorías internas del SGSI a intervalos planificados para determinar si los objetivos del control, controles, procesos y procedimientos de su SGSI:	
6 (a)	Cumplir con los requisitos de este Estándar Norma y la legislación o los reglamentos pertinentes.	L4
6 (b)	Cumplir con los requisitos de seguridad de la información identificados.	L3
6 (c)	Que está efectivamente implementado y mantenido.	L3
6 (d)	Desempeñe según lo esperado	L2
6 (e)	Que sea planificado un programa de auditoría.	L3
6 (f)	La dirección responsable del área que esté siendo auditada debe asegurarse de que se toman acciones sin demora injustificada para eliminar las no conformidades detectadas y sus causas. Las actividades de seguimiento deben incluir la verificación de las acciones llevadas a cabo y el informe de resultados de la verificación (ver 8).	L1
7	**Revisión por la dirección del SGSI**	
7.1	General	
7.1	La dirección revisará SGSI de la organización a intervalos planificados (por lo menos una vez al año) para asegurar su continua idoneidad, adecuación y eficacia	L3
7.2 (a)	Información para la Revisión.	
7.2	La información para una revisión incluirá:	
7.2 (a)	Resultados de Auditorías y revisiones del SGSI.	L3
7.2 (b)	Los comentarios de las partes interesadas.	L1
7.2 (c)	Técnicas, productos o procedimientos, que podrían ser utilizados en la organización para mejorar el rendimiento y la eficacia del SGSI.	L3
7.2 (d)	Estado de las acciones preventivas y correctivas.	L3
7.2 (e)	Las vulnerabilidades o amenazas no tratadas adecuadamente en la evaluación de riesgos anterior.	L2

7.2 (f)	Los resultados de las mediciones de la eficacia.	L1
7.2 (g)	Las acciones de seguimiento de revisiones previas de la dirección.	L3
7.2 (h)	Todos los cambios que podrían afectar al SGSI.	L2
7.2 (i)	Recomendaciones de mejora.	L3
7,3	Resultados de la Revisión.	
7,3	El resultado de la revisión por la dirección deben incluir todas las decisiones y acciones relacionadas con lo siguiente:	
7.3 (a)	Mejora de la eficacia del SGSI.	L4
7.3 (b)	Actualización del plan de tratamiento de riesgos y evaluación de riesgos.	L2
7.3 (c)	Modificación de los procedimientos y controles que la seguridad efecto la información, según sea necesario, para responder a eventos internos o externos que pueden influir en el SGSI.	L3
7.3 (d)	Necesidades de Recursos.	L3
7.3 (e)	Mejoras de cómo la efectividad de los controles está siendo medida.	L3
8	**Mejora del SGSI**	
8.1	Mejora continua.	
8.1	La organización debe mejorar continuamente la eficacia del SGSI a través del uso de la política de seguridad de la información, los objetivos de seguridad de la información, resultados de las auditorías, el análisis de los eventos monitorizados, acciones correctivas y preventivas y la revisión por la dirección (véase 7).	L2
8.2 (a)	Acción Correctiva.	
8.2	La organización deberá tomar acciones para eliminar la causa de no conformidades con los requisitos del SGSI con el fin de prevenir la recurrencia de éstas. El procedimiento documentado de acciones correctivas debe definir requisitos para:	
8.2 (a)	Identificar las no conformidades.	L2
8.2 (b)	Determinar las causas de las no conformidades.	L2
8.2 (c)	Evaluar la necesidad de adoptar medidas para asegurar que las no conformidades no vuelvan a ocurrir.	L1
8.2 (d)	Determinar y aplicar las medidas correctivas necesarias.	L1
8.2 (e)	Registrar los resultados de las acciones tomadas (véase 4.3.3) .	L3

8.2 (f)	Revisar las acciones correctivas tomadas.	L1
8.3 (a)	Acción Preventiva.	
8.3	La organización determinará acciones para eliminar las causas de no conformidades potenciales con los requisitos del SGSI con el fin de prevenir su ocurrencia. Las acciones preventivas tomadas deben ser apropiadas a los efectos de los problemas potenciales. El procedimiento documentado para las acciones preventivas deben definir requisitos para:	
8.3 (a)	Identificar no conformidades potenciales y sus causas	L1
8.3 (b)	Evaluar la necesidad de actuar para prevenir la ocurrencia de no conformidades.	L2
8.3 (c)	Determinar e implementar las acciones preventivas necesarias.	L2
8.3 (d)	Registrar los resultados de las acciones tomadas (véase 4.3.3) .	L2
8.3 (e)	Revisar las acciones preventivas tomadas.	L2
8,3	La organización debe identificar cambios en los riesgos y determinar las necesidades de acciones preventivas centrando la atención en los riesgos que han cambiado significativamente.	L2

Tabla 5: Madurez del control ISO.

Significado	Número
Inexistente	3
Inicial / Ad-hoc	21
Reproducible, pero intuitivo	41
Proceso definido	35
Gestionado y medible	7
Optimizado	2
No aplica	3

2.2.1 Análisis Diferencial ISO/IEC: 27002:2013

En esta sección se realizará el análisis diferencial con respecto la ISO/IEC 27002, este análisis nos permitirá conocer de manera global el estado actual de la empresa en relación a los requisitos que establece la norma para un Sistema de Gestión de la Seguridad de la Información (“FUNDACIÓN UNIVERSITARIA SAN MATEO,” 2014).

La ISO/IEC: 27002:2013 Proporciona directrices para las normas de seguridad de la información organizacional y las prácticas de gestión de la seguridad de la información, incluida la selección, implementación y gestión de controles teniendo en cuenta los entornos de riesgo de seguridad de la información de la organización.("POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN," n.d.).

A continuación se describe cada control:

Políticas de seguridad de la Información: controles acerca de cómo deben ser escritas y revisadas las políticas.

Organización de la seguridad de la información: controles acerca de cómo se asignan las responsabilidades; también incluye los controles para los dispositivos móviles y el teletrabajo.

Seguridad de los Recursos Humanos: controles antes, durante y después de emplear.

Gestión de recursos: controles acerca de lo relacionado con el inventario de recursos y su uso aceptable, también la clasificación de la información y la gestión de los medios de almacenamiento.

Control de Acceso: controles para las políticas de control de acceso, gestión de acceso de los usuarios, control de acceso para el sistema y las aplicaciones, y responsabilidades del usuario.

Criptografía: controles relacionados con la gestión de inscripción y claves.

Seguridad física y ambiental: controles que definen áreas seguras, controles de entrada, protección contra amenazas, seguridad de equipos, descarte seguro, políticas de escritorio y pantalla despejadas, etc.

Seguridad Operacional: muchos de los controles relacionados con la gestión de la producción en TI: gestión de cambios, gestión de capacidad, malware, respaldo, bitácoras, espejos, instalación, vulnerabilidades, etc.

Seguridad de las Comunicaciones: controles relacionados con la seguridad de redes, segregación, servicios de redes, transferencia de información, mensajería, etc.

Adquisición, desarrollo y mantenimiento de Sistemas: controles que definen los requerimientos de seguridad y la seguridad en los procesos de desarrollo y soporte.

Relaciones con los proveedores: controles acerca de qué incluir en los contratos, y cómo hacer el seguimiento a los proveedores.

Gestión de Incidentes en Seguridad de la Información: controles para reportar los eventos y debilidades, definir responsabilidades, procedimientos de respuesta, y recolección de evidencias.

Aspectos de Seguridad de la Información de la gestión de la continuidad del negocio: controles que requieren la planificación de la continuidad del negocio, procedimientos, verificación y revisión, y redundancia de TI.

Cumplimiento: controles que requieren la identificación de las leyes y regulaciones aplicables, protección de la propiedad intelectual, protección de datos personales, y revisiones de la seguridad de la información.

A continuación, se muestra una tabla explicativa con la escala de madurez usada para la evaluación del cumplimiento de los 114 controles establecidos en la norma ISO/IEC 27002:2013.

Tabla 6: Modelo de Madurez de Cumplimiento.

Valor	Efectividad	Significado	Descripción
L0	0%	Inexistente	Carencia completa de cualquier proceso conocido.
L1	10%	Inicial / Ad-hoc	Procedimientos inexistentes o localizados en áreas concretas. El éxito de las tareas se debe a esfuerzos personales.
L2	50%	Reproducible, pero intuitivo	Existe un método de trabajo basado en la experiencia, aunque sin comunicación formal. Dependencia del conocimiento individual
L3	90%	Proceso definido	La organización en su conjunto participa en el proceso. Los procesos están implantados, documentados y comunicados.
L4	95%	Gestionado y medible	Se puede seguir la evolución de los procesos mediante indicadores numéricos y estadísticos. Hay herramientas para mejorar la calidad y la eficiencia
L5	100%	Optimizado	Los procesos están bajo constante mejora. En base a criterios cuantitativos se determinan las desviaciones más comunes y se optimizan los procesos
L6	N/A	No aplica	

Una vez contrastados los controles de la norma ISO/27002:2013, se identifica el nivel de madurez de la Fundación Universitaria San Mateo.

A continuación se muestra el porcentaje de efectividad para los 114 controles, donde se puede evidenciar que 65 controles no están aprobados en la valoración realizada a la Fundación Universitaria San Mateo, equivalentes a un 57% de los controles que poseen entre un 0% y 50% de efectividad,

lo cual indica que carecen completamente de un determinado procesos o existen casos de éxito en determinadas tareas pero depende de esfuerzos personales o existe trabajo basado en experiencias.

El 43% restante se valora como Aprobados, ya que hay 49 controles entre el 90% y 100% en la valoración de efectividad.

Tabla 7: Resumen de Madurez de Cumplimento en la Fundación Universitaria San Mateo.

Valor	Efectividad	Significado	Número
L0	0%	Inexistente	3
L1	10%	Inicial / Ad-hoc	14
L2	50%	Reproducible, pero intuitivo	48
L3	90%	Proceso definido	40
L4	95%	Gestionado y medible	8
L5	100%	Optimizado	1
L6	N/A	No aplica	0

Tabla 8: Valoración de los 114 controles.

Valor	Número
Aprobados	49
No Aprobados	65

En la siguiente tabla se presenta un resumen detallado de cada uno de los dominios, el % de efectividad y los 114 controles debidamente identificados en su nivel de madurez respecto a los controles definidos en la ISO/27002:2013.

Tabla 9: Evaluación de los controles de la Normativa ISO /IEC 27002:2013*Control en la normativa ISO/IEC 27002:2013.*

5	**POLÍTICA DE SEGURIDAD**		
5.1	**Directrices de la Dirección en seguridad de la información**		
5.1.1	Políticas para la seguridad de la información	Control: Se debe definir un conjunto de políticas para la seguridad de la información, aprobada por la dirección, publicada y comunicada a los empleados y a las partes externas pertinentes.	L2
5.1.2	Revisión de las políticas para la seguridad de la información.	Control: Las políticas para la seguridad de la información se deben revisar a intervalos planificados o si ocurren cambios significativos, para para asegurar su conveniencia, adecuación y eficacia continuas.	L2

6	**ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACION**		
6.1	**Organización interna**		
A6.1.1	Roles y responsabilidades para la seguridad de la información	Control: Se deben definir y asignar todas las responsabilidades de la seguridad de la información.	L1
A6.1.2	Separación de deberes	Control: Los deberes y áreas de responsabilidad en conflicto se deben separar para reducir las posibilidades de modificación no autorizada o no intencional, o el uso indebido de los activos de la organización.	L2
A6.1.3	Contacto con las autoridades	Control: Se deben mantener contactos apropiados con las autoridades pertinentes.	L2
A6.1.4	Contacto con grupos de interés especial	Control: Se deben mantener contactos apropiados con grupos de interés especial u otros foros y asociaciones profesionales especializadas en seguridad	L2
A6.1.5	Seguridad de la información en la gestión de proyectos.	Control: La seguridad de la información se debe tratar en la gestión de proyectos, independientemente del tipo de proyecto.	L3
6.2	**Dispositivos móviles y teletrabajo**		
A6.2.1	Política para dispositivos móviles	Control: Se deben adoptar una política y unas medidas de seguridad de soporte, para gestionar los riesgos introducidos por el uso de dispositivos móviles.	L1

A6.2.2	Teletrabajo	Control: Se deben implementar una política y unas medidas de seguridad de soporte, para proteger la información a la que se tiene acceso, que es procesada o almacenada en los lugares en los que se realiza teletrabajo.	L3

7	**SEGURIDAD DE LOS RECURSOS HUMANOS**		
7.1	**Antes de asumir el empleo**		
A7.1.1	Selección	Control: Las verificaciones de los antecedentes de todos los candidatos a un empleo se deben llevar a cabo de acuerdo con las leyes, reglamentaciones y ética pertinentes y deben ser proporcionales a los requisitos de negocio, a la clasificación de la información a que se va a tener acceso y a los riesgos percibidos.	L3
A7.1.2	Términos y condiciones del empleo	Control: Los acuerdos contractuales con empleados y contratistas deben establecer sus responsabilidades y las de la organización en cuanto a la seguridad de la información.	L3
7.2	**Durante la ejecución del empleo**		
A7.2.1	Responsabilidades de la dirección.	Control: La dirección debe exigir a todos los empleados y contratista la aplicación de la seguridad de la información de acuerdo con las políticas y procedimientos establecidos por la organización.	L3
A7.2.2	Toma de conciencia, educación y formación en la seguridad de la información.	Control: Todos los empleados de la organización, y en donde sea pertinente, los contratistas, deben recibir la educación y la formación en toma de conciencia apropiada, y actualizaciones regulares sobre las políticas y procedimientos de la organización pertinentes para su cargo.	L3
A7.2.3	Proceso disciplinario.	Control: Se debe contar con un proceso formal, el cual debe ser comunicado, para emprender acciones contra empleados que hayan cometido una violación a la seguridad de la información.	L3
7.2	**Terminación y cambio de empleo**		
A7.3.1	Terminación o cambio de responsabilidades de empleo.	Control: Las responsabilidades y los deberes de seguridad de la información que permanecen validos después de la terminación o cambio de empleo de deben definir, comunicar al empleado o contratista y se deben hacer cumplir.	L3

8	GESTION DE ACTIVOS		
8.1	**Responsabilidad por los activos**		
A8.1.1	Inventario de activos	Control: Se deben identificar los activos asociados con información e instalaciones de procesamiento de información, y se debe elaborar y mantener un inventario de estos activos.	L2
A8.1.2	Propiedad de los activos	Control: Los activos mantenidos en el inventario deben tener un propietario.	L3
A8.1.3	Uso aceptable de los activos	Control: Se deben identificar, documentar e implementar reglas para el uso aceptable de información y de activos asociados con información e instalaciones de procesamiento de información.	L3
A8.1.4	Devolución de activos	Control: Todos los empleados y usuarios de partes externas deben devolver todos los activos de la organización que se encuentren a su cargo, al terminar su empleo, contrato o acuerdo.	L3
A8.2	**Clasificación de la información**		
A8.2.1	Clasificación de la información	Control: La información se debe clasificar en función de los requisitos legales, valor, criticidad y susceptibilidad a divulgación o a modificación no autorizada.	L2
A8.2.2	Etiquetado de la información	Control: Se debe desarrollar e implementar un conjunto adecuado de procedimientos para el etiquetado de la información, de acuerdo con el esquema de clasificación de información adoptado por la organización.	L3
A8.2.3	Manejo de activos	Control: Se deben desarrollar e implementar procedimientos para el manejo de activos, de acuerdo con el esquema de clasificación de información adoptado por la organización.	L3
A8.2	**Manejo de medios**		
A8.3.1	Gestión de medio removibles	Control: Se deben implementar procedimientos para la gestión de medio removibles, de acuerdo con el esquema de clasificación adoptado por la organización.	L2
A8.3.2	Disposición de los medios	Control: Se debe disponer en forma segura de los medios cuando ya no se requieran, utilizando procedimientos formales.	L3
A8.3.3	Transferencia de medios físicos	Control: Los medios que contienen información se deben proteger contra acceso no autorizado, uso indebido o corrupción durante el transporte.	L2

9	**CONTROL DE ACCESO**		
9.1	**Requisitos del negocio para el control de acceso**		
A9.1.1	Política de control de acceso	Control: Se debe establecer, documentar y revisar una política de control de acceso con base en los requisitos del negocio y de la seguridad de la información.	L2
A9.1.2	Acceso a redes y a servicios en red	Control: Solo se debe permitir acceso de los usuarios a la red y a los servicios de red para los que hayan sido autorizados específicamente.	L4
9.2	**Gestión de acceso de usuarios**		
A9.2.1	Registro y cancelación del registro de usuarios	Control: Se debe implementar un proceso formal de registro y de cancelación de registro de usuarios, para posibilitar la asignación de los derechos de acceso.	L3
A9.2.2	Suministro de acceso de usuarios	Control: Se debe implementar un proceso de suministro de acceso formal de usuarios para asignar o revocar los derechos de acceso para todo tipo de usuarios para todos los sistemas y servicios.	L3
A9.2.3	Gestión de derechos de acceso privilegiado	Control: Se debe restringir y controlar la asignación y uso de derechos de acceso privilegiado	L3
A9.2.4	Gestión de información de autenticación secreta de usuarios	Control: La asignación de información de autenticación secreta se debe controlar por medio de un proceso de gestión formal.	L4
A9.2.5	Revisión de los derechos de acceso de usuarios	Control: Los propietarios de los activos deben revisar los derechos de acceso de los usuarios, a intervalos regulares.	L3
A9.2.6	Retiro o ajuste de los derechos de acceso	Control: Los derechos de acceso de todos los empleados y de usuarios externos a la información y a las instalaciones de procesamiento de información se deben retirar al terminar su empleo, contrato o acuerdo, o se deben ajustar cuando se hagan cambios.	L4
A9.3	Responsabilidades de los usuarios		
A9.3.1	Uso de información de autenticación secreta	Control: Se debe exigir a los usuarios que cumplan las prácticas de la organización para el uso de información de autenticación secreta.	L2
A9.4	Control de acceso a sistemas y aplicaciones		
A9.4.1	Restricción de acceso a la información	Control: El acceso a la información y a las funciones de los sistemas de las aplicaciones se debe restringir de acuerdo con la política de control de acceso.	L4

A9.4.2	Procedimiento de ingreso seguro	Control: Cuando lo requiere la política de control de acceso, el acceso a sistemas y aplicaciones se debe controlar mediante un proceso de ingreso seguro.	L4
A9.4.3	Sistema de gestión de contraseñas	Control: Los sistemas de gestión de contraseñas deben ser interactivos y deben asegurar la calidad de las contraseñas.	L2
A9.4.4	Uso de programas utilitarios privilegiados	Control: Se debe restringir y controlar estrictamente el usos de programas utilitarios que podrían tener capacidad de anular el sistema y los controles de las aplicaciones.	L1
A9.4.5	Control de acceso a códigos fuente de programas	Control: Se debe restringir el acceso a los códigos fuente de los programas.	L4

10	**CIFRADO**		
10.1	**Controles criptográficos**		
A10.1.1	Política sobre el uso de controles criptográficos	Control: Se debe desarrollar e implementar una política sobre el uso de controles criptográficos para la protección de la información.	L1
A10.1.2	Gestión de llaves	Control: Se debe desarrollar e implementar una política sobre el uso, protección y tiempo de vida de las llaves criptográficas, durante todo su ciclo de vida.	L0

A11	**SEGURIDAD FISICA Y DEL ENTORNO**		
11.1	**Áreas seguras**		
A11.1.1	Perímetro de seguridad física	Control: Se deben definir y usar perímetros de seguridad, y usarlos para proteger áreas que contengan información confidencial o critica, e instalaciones de manejo de información.	L2
A11.1.2	Controles de acceso físicos	Control: Las áreas seguras deben estar protegidas con controles de acceso apropiados para asegurar que sólo se permite el acceso a personal autorizado.	L3
A11.1.3	Seguridad de oficinas, recintos e instalaciones.	Control: Se debe diseñar y aplicar la seguridad física para oficinas, recintos e instalaciones.	L2
A11.1.4	Protección contra amenazas externas y ambientales.	Control: Se deben diseñar y aplicar protección física contra desastres naturales, ataques maliciosos o accidentes.	L2
A11.1.5	Trabajo en áreas seguras.	Control: Se deben diseñar y aplicar procedimientos para trabajo en áreas seguras.	L1

A11.1.6	Áreas de carga, despacho y acceso público	Control: Se deben controlar los puntos de acceso tales como las áreas de despacho y carga y otros puntos por donde pueden entrar personas no autorizadas y, si es posible, aislarlos de las instalaciones de procesamiento de información para evitar el acceso no autorizado.	L3
A11.2	**Equipos**		
A11.2.1	Ubicación y protección de los equipos	Control: Los equipos deben de estar ubicados y protegidos para reducir los riesgos de amenazas y peligros del entorno, y las posibilidades de acceso no autorizado.	L3
A11.2.2	Servicios de suministro	Control: Los equipos se deben proteger contra fallas de energía y otras interrupciones causadas por fallas en los servicios de suministro.	L3
A11.2.3	Seguridad en el cableado.	Control: El cableado de energía eléctrica y de telecomunicaciones que porta datos o brinda soporte a los servicios de información se debe proteger contra interceptación, interferencia o daño.	L5
A11.2.4	Mantenimiento de los equipos.	Control: Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.	L4
A11.2.5	Retiro de activos	Control: Los equipos, información o software no se deben retirar de su sitio sin autorización previa.	L4
A11.2.6	Seguridad de equipos y activos fuera de las instalaciones	Control: Se deben aplicar medidas de seguridad a los activos que se encuentran fuera de las instalaciones de la organización, teniendo en cuenta los diferentes riesgos de trabajar fuera de dichas instalaciones.	L3
A11.2.7	Disposición segura o reutilización de equipos	Control: Se deben verificar todos los elementos de equipos que contengan medios de almacenamiento para asegurar que cualquier dato confidencial o software licenciado haya sido retirado o sobrescrito en forma segura antes de su disposición o reúso.	L2
A11.2.8	Equipos de usuario desatendido	Control: Los usuarios deben asegurarse de que a los equipos desatendidos se les da protección apropiada.	L3
A11.2.9	Política de escritorio limpio y pantalla limpia	Control: Se debe adoptar una política de escritorio limpio para los papeles y medios de almacenamiento removibles, y una política de pantalla limpia en las instalaciones de procesamiento de información.	L2

A12	**SEGURIDAD DE LAS OPERACIONES**	
A12.1	**Procedimientos operacionales y responsabilidades**	

A12.1.1	Procedimientos de operación documentados	Control: Los procedimientos de operación se deben documentar y poner a disposición de todos los usuarios que los necesitan.	L3
A12.1.2	Gestión de cambios	Control: Se deben controlar los cambios en la organización, en los procesos de negocio, en las instalaciones y en los sistemas de procesamiento de información que afectan la seguridad de la información.	L3
A12.1.3	Gestión de capacidad	Control: Se debe hacer seguimiento al uso de recursos, hacer los ajustes, y hacer proyecciones de los requisitos de capacidad futura, para asegurar el desempeño requerido del sistema.	L2
A12.1.4	Separación de los ambientes de desarrollo, pruebas y operación	Control: Se deben separar los ambientes de desarrollo, pruebas y operación, para reducir los riesgos de acceso o cambios no autorizados al ambiente de operación.	L2
A12.2	**Protección contra códigos maliciosos**		
A12.2.1	Controles contra códigos maliciosos	Control: Se deben implementar controles de detección, de prevención y de recuperación, combinados con la toma de conciencia apropiada de los usuarios, para proteger contra códigos maliciosos.	L2
A12.2	**Protección contra códigos maliciosos**		
A12.3.1	Respaldo de la información	Control: Se deben hacer copias de respaldo de la información, software e imágenes de los sistemas, y ponerlas a prueba regularmente de acuerdo con una política de copias de respaldo acordadas.	L2
A12.2	**Protección contra códigos maliciosos**		
A12.4.1	Registro de eventos	Control: Se deben elaborar, conservar y revisar regularmente los registros acerca de actividades del usuario, excepciones, fallas y eventos de seguridad de la información.	L1
A12.4.2	Protección de la información de registro	Control: Las instalaciones y la información de registro se deben proteger contra alteración y acceso no autorizado.	L3
A12.4.3	Registros del administrador y del operador	Control: Las actividades del administrador y del operador del sistema se deben registrar, y los registros se deben proteger y revisar con regularidad.	L3
A12.4.4	Sincronización de relojes	Control: Los relojes de todos los sistemas de procesamiento de información pertinentes dentro de una organización o ámbito de seguridad se deben sincronizar con una única fuente de referencia de tiempo.	L1
A12.2	**Protección contra códigos maliciosos**		

A12.5.1	Instalación de software en sistemas operativos	Control: Se deben implementar procedimientos para controlar la instalación de software en sistemas operativos.	L3
A12.6	**Gestión de la vulnerabilidad técnica**		
A12.6.1	Gestión de las vulnerabilidades técnicas	Control: Se debe obtener oportunamente información acerca de las vulnerabilidades técnicas de los sistemas de información que se usen; evaluar la exposición de la organización a estas vulnerabilidades, y tomar las medidas apropiadas para tratar el riesgo asociado.	L1
A12.6.2	Restricciones sobre la instalación de software	Control: Se deben establecer e implementar las reglas para la instalación de software por parte de los usuarios.	L3
A12.7	**Consideraciones sobre auditorias de sistemas de información**		
A12.7.1	Controles de auditorías de sistemas de información	Control: Los requisitos y actividades de auditoria que involucran la verificación de los sistemas operativos se deben planificar y acordar cuidadosamente para minimizar las interrupciones en los procesos del negocio.	L2

A13	**SEGURIDAD DE LAS COMUNICACIONES**		
A13.1	**Gestión de la seguridad de las redes**		
A13.1.1	Controles de redes	Control: Las redes se deben gestionar y controlar para proteger la información en sistemas y aplicaciones.	L2
A13.1.2	Seguridad de los servicios de red	Control: Se deben identificar los mecanismos de seguridad, los niveles de servicio y los requisitos de gestión de todos los servicios de red, e incluirlos en los acuerdos de servicio de red, ya sea que los servicios se presten internamente o se contraten externamente.	L3
A13.1.3	Separación en las redes	Control: Los grupos de servicios de información, usuarios y sistemas de información se deben separar en las redes.	L2
A13.2	**Transferencia de información**		
A13.2.1	Políticas y procedimientos de transferencia de información	Control: Se debe contar con políticas, procedimientos y controles de transferencia información formales para proteger la transferencia de información mediante el uso de todo tipo de instalaciones de comunicaciones.	L2
A13.2.2	Acuerdos sobre transferencia de información	Control: Los acuerdos deben tratar la transferencia segura de información del negocio entre la organización y las partes externas.	L1

A13.2.3	Mensajería Electrónica	Control: Se debe proteger adecuadamente la información incluida en la mensajería electrónica.	L2
A13.2.4	Acuerdos de confidencialidad o de no divulgación	Control: Se deben identificar, revisar regularmente y documentar los requisitos para los acuerdos de confidencialidad o no divulgación que reflejen las necesidades de la organización para la protección de la información.	L3

14	**Adquisición, desarrollo y mantenimiento de sistemas**		
14.1	**Requisitos de seguridad de los sistemas de información**		
A.14.1.1	Análisis y especificación de requisitos de seguridad de la información	Control: Los requisitos relacionados con seguridad de la información se deben incluir en los requisitos para nuevos sistemas de información o para mejoras a los sistemas de información existentes.	L2
A.14.1.2	Seguridad de servicios de las aplicaciones en redes públicas	Control: La información involucrada en los servicios de las aplicaciones que pasan sobre redes públicas se debe proteger de actividades fraudulentas, disputas contractuales y divulgación y modificación no autorizadas.	L2
A.14.1.3	Protección de transacciones de los servicios de las aplicaciones.	Control: La información involucrada en las transacciones de los servicios de las aplicaciones se debe proteger para evitar la transmisión incompleta, el enrutamiento errado, la alteración no autorizada de mensajes, la divulgación no autorizada, y la duplicación o reproducción de mensajes no autorizada.	L3
A14.2	**Seguridad en los procesos de Desarrollo y de Soporte**		
A.14.2.1	Política de desarrollo seguro	Control: Se debe establecer y aplicar reglas para el desarrollo de software y de sistemas, a los desarrollos dentro de la organización.	L3
A.14.2.2	Procedimientos de control de cambios en sistemas	Control: Los cambios a los sistemas dentro del ciclo de vida de desarrollo se deben controlar mediante el uso de procedimientos formales de control de cambios.	L2
A.14.2.3	Revisión técnica de las aplicaciones después de cambios en la plataforma de operación	Control: Cuando se cambian las plataformas de operación, se deben revisar las aplicaciones críticas del negocio, y someter a prueba para asegurar que no haya impacto adverso en las operaciones o seguridad de la organización.	L2

A.14.2.4	Restricciones en los cambios a los paquetes de software	Control: Se deben desalentar las modificaciones a los paquetes de software, los cuales se deben limitar a los cambios necesarios, y todos los cambios se deben controlar estrictamente.	L3
A.14.2.5	Principio de Construcción de los Sistemas Seguros.	Control: Se deben establecer, documentar y mantener principios para la construcción de sistemas seguros, y aplicarlos a cualquier actividad de implementación de sistemas de información.	L0
A.14.2.6	Ambiente de desarrollo seguro	Control: Las organizaciones deben establecer y proteger adecuadamente los ambientes de desarrollo seguros para las actividades de desarrollo e integración de sistemas que comprendan todo el ciclo de vida de desarrollo de sistemas.	L3
A.14.2.7	Desarrollo contratado externamente	Control: La organización debe supervisar y hacer seguimiento de la actividad de desarrollo de sistemas contratados externamente.	L2
A.14.2.8	Pruebas de seguridad de sistemas	Control: Durante el desarrollo se deben llevar a cabo pruebas de funcionalidad de la seguridad.	L2
A.14.2.9	Prueba de aceptación de sistemas	Control: Para los sistemas de información nuevos, actualizaciones y nuevas versiones, se deben establecer programas de prueba para aceptación y criterios de aceptación relacionados.	L2
A14.3	**Datos de prueba**		
A.14.3.1	Protección de datos de prueba	Control: Los datos de prueba se deben seleccionar, proteger y controlar cuidadosamente.	L2

A15	**RELACIONES CON LOS PROVEEDORES**		
A15.1	**Seguridad de la información en las relaciones con los proveedores.**		
A15.1.1	Política de seguridad de la información para las relaciones con proveedores	Control: Los requisitos de seguridad de la información para mitigar los riesgos asociados con el acceso de proveedores a los activos de la organización se deben acordar con estos y se deben documentar.	L2
A15.1.2	Tratamiento de la seguridad dentro de los acuerdos con proveedores	Control: Se deben establecer y acordar todos los requisitos de seguridad de la información pertinentes con cada proveedor que pueda tener acceso, procesar, almacenar, comunicar o suministrar componentes de infraestructura de TI para la información de la organización.	L1

A15.1.3	Cadena de suministro de tecnología de información y comunicación	Control: Los acuerdos con proveedores deben incluir requisitos para tratar los riesgos de seguridad de la información asociados con la cadena de suministro de productos y servicios de tecnología de información y comunicación.	L2
A15.2	**Gestión de la prestación de servicios de proveedores**		
A15.2.1	Seguimiento y revisión de los servicios de los proveedores	Control: Las organizaciones deben hacer seguimiento, revisar y auditar con regularidad la prestación de servicios de los proveedores.	L0
A15.2.2	Gestión del cambio en los servicios de los proveedores	Control: Se deben gestionar los cambios en el suministro de servicios por parte de los proveedores, incluido el mantenimiento y las mejoras de las políticas, procedimientos y controles de seguridad de la información existentes, teniendo en cuenta la criticidad de la información, sistemas y procesos de negocio involucrados, y la revaluación de los riesgos.	L2

A16	**GESTION DE INCIDENTES DE SEGURIDAD DE LA INFORMACION**		
A16.1	**Gestión de incidentes y mejoras en la seguridad de la información**		
A16.1.1	Responsabilidades y procedimientos	Control: Se deben establecer las responsabilidades y procedimientos de gestión para asegurar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información.	L2
A16.1.2	Reporte de eventos de seguridad de la información	Control: Los eventos de seguridad de la información se deben informar a través de los canales de gestión apropiados, tan pronto como sea posible.	L2
A16.1.3	Reporte de debilidades de seguridad de la información	Control: Se debe exigir a todos los empleados y contratistas que usan los servicios y sistemas de información de la organización, que observen y reporten cualquier debilidad de seguridad de la información observada o sospechada en los sistemas o servicios.	L3
A16.1.4	Evaluación de eventos de seguridad de la información y decisiones sobre ellos	Control: Los eventos de seguridad de la información se deben evaluar y se debe decidir si se van a clasificar como incidentes de seguridad de la información.	L2
A16.1.5	Respuesta a incidentes de seguridad de la información	Control: Se debe dar respuesta a los incidentes de seguridad de la información de acuerdo con procedimientos documentados.	L1
A16.1.6	Aprendizaje obtenido de los incidentes de seguridad de la información	Control: El conocimiento adquirido al analizar y resolver incidentes de seguridad de la información se debe usar	L2

		para reducir la posibilidad o impacto de incidentes futuros.	
A16.1.7	Recolección de evidencia	Control: La organización debe definir y aplicar procedimientos para la identificación, recolección, adquisición y preservación de información que pueda servir como evidencia.	L3

A17	**ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTION DE CONTINUIDAD DE NEGOCIO**		
A17.1	**Continuidad de Seguridad de la información**		
A17.1.1	Planificación de la continuidad de la seguridad de la información	Control: La organización debe determinar sus requisitos para la seguridad de la información y la continuidad de la gestión de la seguridad de la información en situaciones adversas, por ejemplo, durante una crisis o desastre.	L2
A17.1.2	Implementación de la continuidad de la seguridad de la información	Control: La organización debe establecer, documentar, implementar y mantener procesos, procedimientos y controles para asegurar el nivel de continuidad requerido para la seguridad de la información durante una situación adversa.	L1
A17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información	Control: La organización debe verificar a intervalos regulares los controles de continuidad de la seguridad de la información establecidos e implementados, con el fin de asegurar que son válidos y eficaces durante situaciones adversas.	L1
A17.2	**Redundancias**		
A17.2.1	Disponibilidad de instalaciones de procesamiento de información	Control: Las instalaciones de procesamientos de información se deben implementar con redundancia suficiente para cumplir los requisitos de disponibilidad.	L2

A18	**CUMPLIMIENTO**		
A18.1	**Cumplimiento de requisitos legales y contractuales**		
A18.1.1	Identificación de la legislación aplicable.	Control: Todos los requisitos estatutarios, reglamentarios y contractuales pertinentes y el enfoque de la organización para cumplirlos, se deben identificar y documentar explícitamente y mantenerlos actualizados para cada sistema de información y para la organización.	L3

A18.1.2	Derechos propiedad intelectual (DPI)	Control: Se deben implementar procedimientos apropiados para asegurar el cumplimiento de los requisitos legislativos, de reglamentación y contractuales relacionados con los derechos de propiedad intelectual y el uso de productos de software patentados.	L2
A18.1.3	Protección de registros	Control: Los registros se deben proteger contra perdida, destrucción, falsificación, acceso no autorizado y liberación no autorizada, de acuerdo con los requisitos legislativos, de reglamentación, contractuales y de negocio.	L2
A18.1.4	Privacidad y protección de información de datos personales	Control: Se deben asegurar la privacidad y la protección de la información de datos personales, como se exige e la legislación y la reglamentación pertinentes, cuando sea aplicable.	L2
A18.1.5	Reglamentación de controles criptográficos.	Control: Se deben usar controles criptográficos, en cumplimiento de todos los acuerdos, legislación y reglamentación pertinentes.	L1
A18.2	**Revisiones de seguridad de la información**		
A18.2.1	Revisión independiente de la seguridad de la información	Control: El enfoque de la organización para la gestión de la seguridad de la información y su implementación (es decir los objetivos de control, los controles, las políticas, los procesos y los procedimientos para seguridad de la información), se deben revisar independientemente a intervalos planificados o cuando ocurran cambios significativos.	L2
A18.2.2	Cumplimiento con las políticas y normas de seguridad	Control: Los directores deben revisar con regularidad el cumplimiento del procesamiento y procedimientos de información dentro de su área de responsabilidad, con las políticas y normas de seguridad apropiadas, y cualquier otro requisito de seguridad.	L3
A18.2.3	Revisión del cumplimiento técnico	Control: Los sistemas de información se deben revisar periódicamente para determinar el cumplimiento con las políticas y normas de seguridad de la información.	L2

Tabla 10 Resumen de Cumplimiento por Dominios

Dominio	% de Efectividad	# NC Mayores	# NC Menores	<
5 - POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN	50%	0	2	0
6 - ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	50%	2	5	0
7 - SEGURIDAD DE LOS RECURSOS HUMANOS	90%	0	6	0
8 - GESTIÓN DE ACTIVOS	73%	0	10	0
9 - CONTROL DE ACCESO	71%	1	7	6
10 - CRIPTOGRAFÍA	5%	2	0	0
11 - SEGURIDAD FÍSICA Y DEL ENTORNO	70%	1	11	3
12 - SEGURIDAD DE LAS OPERACIONES	57%	3	11	0
13 - SEGURIDAD DE LAS COMUNICACIONES	57%	1	6	0
14 - ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	57%	1	12	0
15 - RELACIÓN CON LOS PROVEEDORES	31%	2	3	0
16 - GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	0%	1	6	0
17 - ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTION DE CONTINUIDAD DE NEGOCIO	37%	2	2	0
18 - SEGURIDAD DE LAS COMUNICACIONES	57%	1	7	0

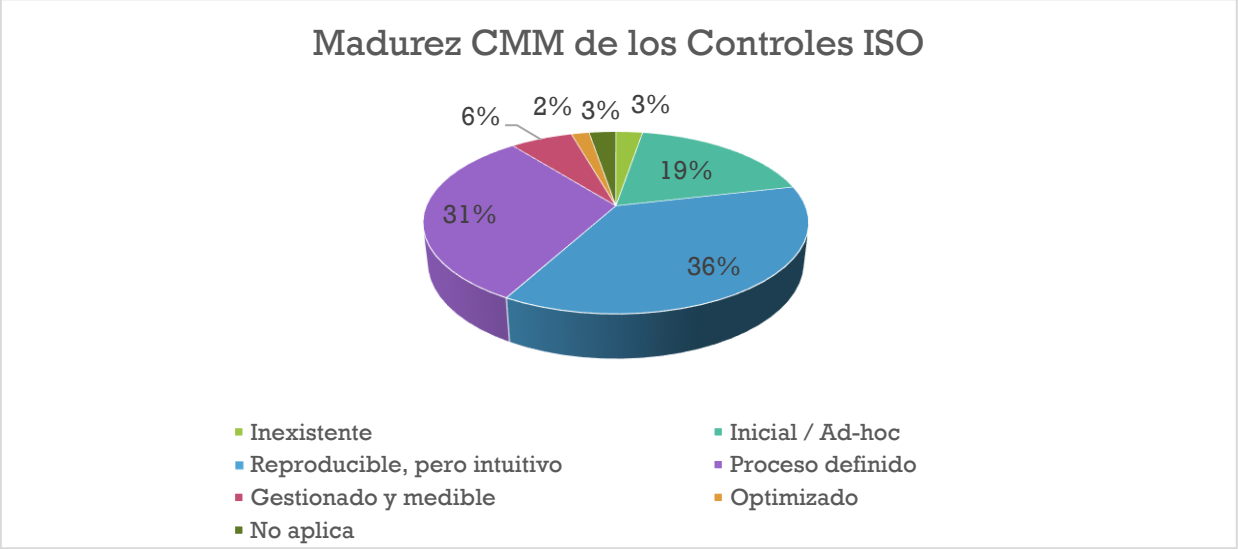
En la tabla anterior se presenta un resumen de los 14 Dominios y de los 114 controles valorados en % de efectividad y número de controles que cumple y no cumple la Fundación Universitaria San Mateo.

2.3.1 Resultados

2.3.1.1 Resultados de Madurez ISO 27001:2013

Los siguientes resultados muestra el estado de madurez en cuanto a los controles de la Norma ISO, y el grado de cumplimiento en los controles establecidos.

Ilustración 11: Madurez CMM de los Controles ISO.



Fuentes: Resultado de Anexo A.

Como resultado de la ilustración, se evalúa el nivel de madurez porcentual de los diferentes controles, se identifica el grado de madurez que tiene cada uno, lo cual nos da un estado de la seguridad en la Fundación Universitaria San Mateo, Podemos ver que el 36% Los procesos similares se llevan en forma similar por diferentes personas con la misma tarea, se normalizan las buenas prácticas en base a la experiencia y al método, No hay comunicación o entrenamiento formal, las responsabilidades quedan a cargo de cada individuo y depende del grado de conocimiento de cada individuo.

A continuación se presenta una visión más detallada que mostrara el nivel de cumplimiento pro el capítulo ISO, Anticipándonos a las medidas, compara el estado actual con el estado deseado.

Ilustración 12: Diagrama Comparativo el estado actual con el estado deseado Controles ISO.

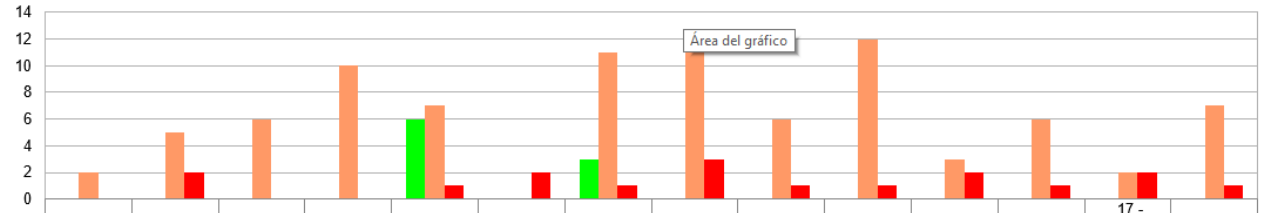
Fuentes: ANEXO A Autodiagnóstico.

En la ilustración anterior, vale la pena destacar que el domino que tiene un nivel mayor de nivel de madures es son las políticas de seguridad, seguido de la seguridad física y del entorno, la institución ha trabajado en estos aspectos y ha sido los controles que se han trabajado con diferentes controles de acceso por medio de huella, control biométrico, circuitos cerrado de televisión, controles de acceso segmentados, restricciones en áreas de las tecnologías, y protección de la información en cuanto a los servidores ya que son administrados por un proveedor y están virtual izados en otra localidad.

2.3.1.1 Evaluación de Madurez ISO 27002:2013

Ilustración 13: Resumen de cumplimiento por Dominios.

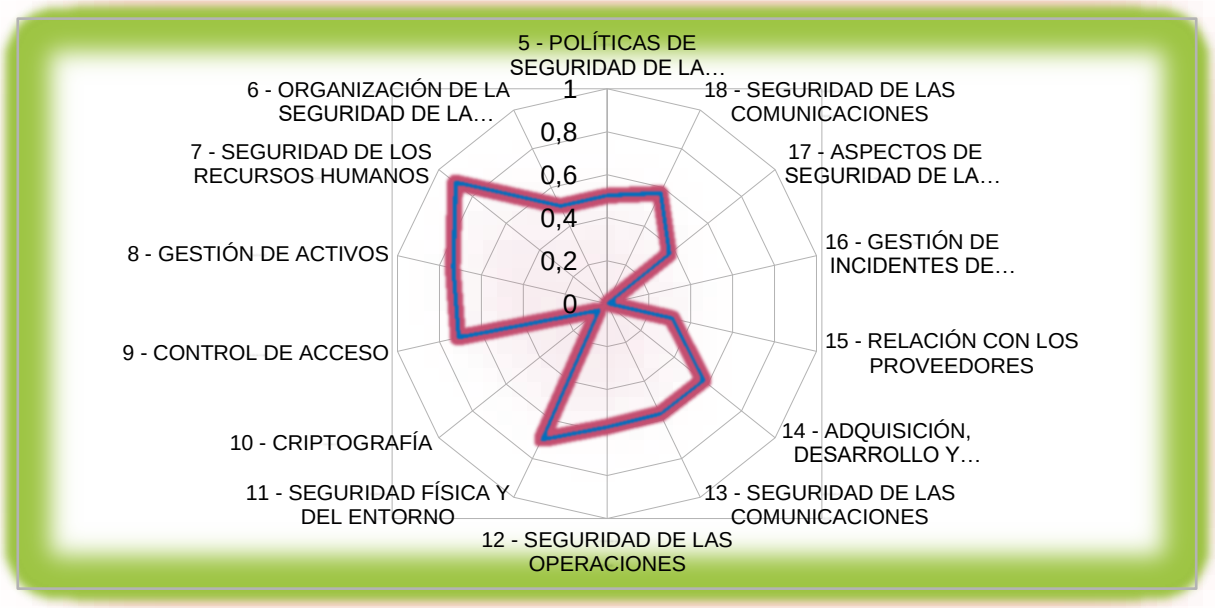
En las siguientes imagen se puede observar el resumen de cumplimento por dominio de forma gráfica.



	5 - POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN	6 - ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	7 - SEGURIDAD DE LOS RECURSOS HUMANOS	8 - GESTIÓN DE ACTIVOS	9 - CONTROL DE ACCESO	10 - CRIPTOGRAFÍA	11 - SEGURIDAD FÍSICA Y DEL ENTORNO	12 - SEGURIDAD DE LAS OPERACIONES	13 - SEGURIDAD DE LAS COMUNICACIONES	14 - ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	15 - RELACIÓN CON LOS PROVEEDORES	16 - GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	17 - ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTION DE CONTINUIDAD DE NEGOCIO	18 - SEGURIDAD DE LAS COMUNICACIONES
Control OK	0	0	0	0	6	0	3	0	0	0	0			
# NC Menores	2	5	6	10	7	0	11	11	6	12	3	6	2	7
# NC Mayores	0	2	0	0	1	2	1	3	1	1	2	1	2	1

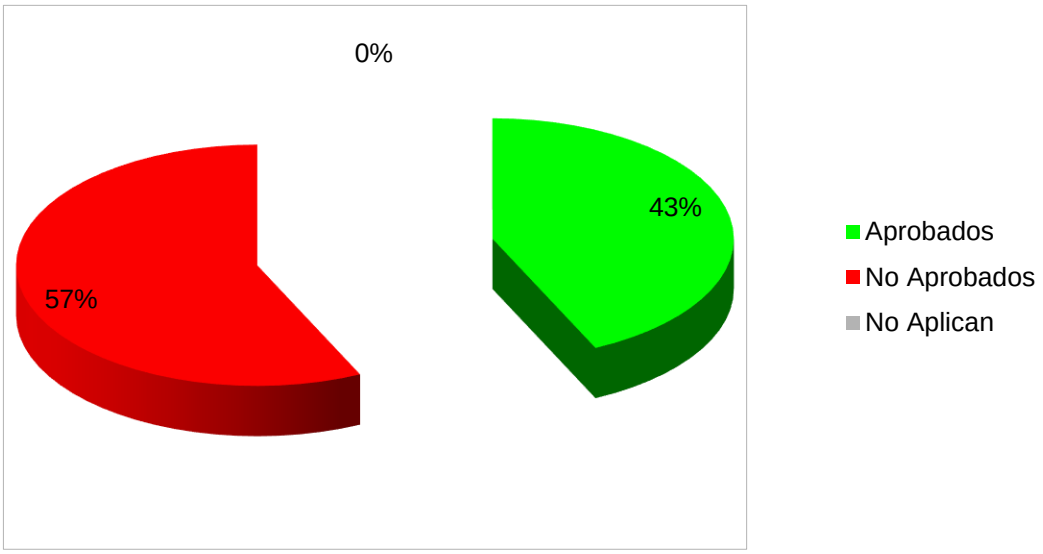
Fuente: Estado de valoración de la madurez ISO27002 Anexo A2 Madurez ISO 27002 2013

Ilustración 14: Porcentaje de madurez de los controles implantados.



En las gráficas anterior podemos observar que el dominio mejor valorado en cuanto la efectividad es la seguridad de los recursos Humanos, y el dominio con el menor porcentaje de efectividad son la Gestión de incidentes de seguridad en la información y la criptografía

Ilustración 15: Porcentaje de controles Aprobados y No aprobados.



Fuente: Estado de valoración de la madurez ISO27002 Anexo A2 Madurez ISO 27002 2013,

Como se puede observar en la gráfica anterior, la Fundación Universitaria San Mateo presenta en la actualidad una implementación baja del 57% de los 114 controles, teniendo en cuenta la norma ISO/IEC: 27002:2013, y una madurez del 43% de los controles ya implantados.

Fase 2. Sistema de Gestión Documental

3.1 Introducción

Todos los Sistemas de Gestión se apoyan en un cuerpo documental para el cumplimiento normativo, esto significa que en nuestro Sistema de Gestión de Seguridad de la Información tendremos que tener una serie de documentos para alcanzar los objetivos de un SGSI. Los cuales vienen establecidos en la propia norma ISO/IEC 27001:2013.

A continuación, se muestra los documentos de la norma que serán explicados en el siguiente apartado.

- Política de Seguridad
- Procedimiento de Auditorías Internas
- Gestión de Indicadores
- Procedimiento Revisión por Dirección
- Gestión de Roles y Responsabilidades
- Metodología de Análisis de Riesgos
- Declaración de Aplicabilidad

3.2 Esquema Documental

3.2.1 Políticas de seguridad

Normativa interna que debe conocer y cumplir todo el personal afectado por el alcance del Sistema de Gestión de Seguridad de la Información. El contenido de la Política debe cubrir aspectos relativos al acceso de la información, uso de recursos de la Organización, comportamiento en caso de incidentes de seguridad, etc.

A continuación de describirá la política de seguridad de la información para la Fundación Universitaria San mateo, con el fin de organizar la seguridad de la información de los sistemas y garantizar la protección de cualquier perdida de su confidencialidad, integridad y disponibilidad.

Con la socialización se busca que toda la organización incluyendo Directivos, consejos superiores, individuales y colectivos brinde apoyo para que la institución disponga de información con niveles apropiados de seguridad.(“Norma ISO 27002: El dominio política de seguridad,” n.d.-b).

Se ha definido la política institucional para la Fundación Universitaria San Mateo los cuales hacen parte del SGSI y se encuentra en el **Anexos B** de este Documento.

3.2.2 Procedimientos de auditoria internas

El propósito del documento del procedimiento de auditoria interna es incluir una planificación de las auditorías que se llevarán a cabo durante la vigencia de la certificación (una vez se obtenga), para verificar que todos los aspectos del SGSI funcionen como se diseñaron y para ser correctamente evolucionados.

En este documentos es establecen los requisitos a los auditores internos y se definirá el modelo de informe de auditoría.

Se ha definido el procedimiento de auditoria interna para la Fundación Universitaria San Mateo los cuales hacen parte del SGSI y se encuentra en el **Anexo C** de este documento.

3.2.3 Gestión de Indicadores

En la Fundación Universitaria San Mateo es necesario definir indicadores para medir la eficacia de los controles de seguridad implantados. Igualmente es importante definir la sistemática para medir el nivel de madurez respecto a los objetivos planteados, para disponer de esta información, es necesario implantar indicadores que nos dé información para valorarlos.

Se ha planteado el procedimiento de gestión de indicadores que indica cómo se realizaran las mediciones para la Fundación Universitaria San Mateo y se encuentra en el **Anexo D** de este documento.

3.2.4 Procedimiento Revisión por Dirección

El propósito de la dirección de la organización es revisar anualmente las cuestiones más importantes que han sucedido en relación al Sistema de Gestión de Seguridad de la Información. Para esta revisión, la ISO/IEC 27001 define tanto los puntos de entrada, como los puntos de salida que se deben obtener de estas revisiones.

Se ha planteado el procedimiento de revisión por la dirección para la Fundación Universitaria San Mateo y se encuentra en el **Anexo E** de este documento.

3.2.5 Gestión de roles y responsabilidades

El Sistema de Gestión de Seguridad de la Información tiene que estar compuesto por un equipo que se encargue de crear, mantener, supervisar y mejorar el Sistema. Este equipo de trabajo, conocido habitualmente como Comité de Seguridad, debe estar compuesto al menos por una persona de la Dirección, para que de esta manera las decisiones que se tomen puedan estar respaldadas por alguien de la Dirección.

Se ha planteado el procedimiento para la Gestión de Roles y Responsabilidades para la Fundación Universitaria San Mateo y se encuentra en el **Anexo F** de este documento.

3.2.7 Metodología de análisis de riesgos

Establece la sistemática que se seguirá para calcular el riesgo, lo cual deberá incluir básicamente la identificación y valoración de los activos, amenazas y vulnerabilidades.

La metodología de análisis de riesgos establece la sistemática que se seguirá para calcular el riesgo, lo cual deberá incluir básicamente la identificación y valoración de los activos, amenazas y vulnerabilidades.

Se utilizará MAGERIT como metodología de análisis de riesgo, la cual tiene como característica fundamental que los riesgos que se plantean para la Fundación Universitaria San Mateo, se expresan en valores económicos directamente.

Se ha planteado el procedimiento para la Gestión de Roles y Responsabilidades para la Fundación Universitaria San Mateo y se encuentra en el **Anexo G** de este documento.

3.2.7 Declaración de aplicabilidad

Documento que incluye todos los controles de Seguridad establecidos en la Fundación Universitaria San Mateo Basados en la norma ISO/IEC 27002:2013, con el detalle de su aplicabilidad, estado y documentación relacionada.

Se ha creado el documento de declaración de la aplicabilidad para la Fundación Universitaria San Mateo y se encuentra en el **Anexo H** de este documento.("Documentación requerida por la ISO 27001,")

Análisis de porcentaje de efectividad: Resultado de declaración de la aplicabilidad.

Dominio	% de Efectividad
5 - POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN	50%
6 - ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	50%
7 - SEGURIDAD DE LOS RECURSOS HUMANOS	90%
8 - GESTIÓN DE ACTIVOS	73%
9 - CONTROL DE ACCESO	71%
10 - CRIPTOGRAFÍA	5%
11 - SEGURIDAD FÍSICA Y DEL ENTORNO	70%
12 - SEGURIDAD DE LAS OPERACIONES	57%
13 - SEGURIDAD DE LAS COMUNICACIONES	57%
14 - ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	57%
15 - RELACIÓN CON LOS PROVEEDORES	31%
16 - GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	0%
17 - ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTION DE CONTINUIDAD DE NEGOCIO	37%
18 - SEGURIDAD DE LAS COMUNICACIONES	57%

3.2.8 Resultados

Con el esquema documental básico que establece la norma preparada, tendremos establecidas las bases de nuestro Sistema de Gestión de Seguridad de la Información, ya que sobre estos documentos y/o políticas/procedimientos se llevarán a cabo las diferentes actividades de implantación (realización del análisis de riesgos, implantación de controles necesarios, implantación de proyectos, realización de auditoría interna, etc.

Fase 3 4. Análisis de Riegos

4.1 Introducción

Para nadie es un secreto que desde hace varias décadas la información se ha convertido en el activo con más valor de una organización, pasando por el ciclo continuo de ser insumo de alto valor, convirtiéndose en producto del desarrollo de las actividades, o viceversa, siendo esta fundamental para el cumplimiento de los objetivos y subsistencia de las organizaciones.

No es posible proteger aquello que no se conoce, es por ello, que la primera etapa hacia la consecución del plan de implementación de un SGSI consistirá en la evaluación de los activos, considerando las dependencias existentes entre ellos y realizando una valoración de los mismos.

Se identifican los activos de la Institución relacionados con la seguridad de la información cuyo objetivo del SGSI es protegerlos y se calcula el valor, amenazas y vulnerabilidades.

4.2 Inventario de activos

El primer punto a tratar es analizar los activos vinculados a la información, es habitual agrupar los activos por grupos, en este caso, podemos agrupar los activos en grupos acordes con la metodología MAGERIT, el enfoque está dado en:

Tabla 11: Tipos de Activos Según MAGERIT.

A	*Descripción*
Instalaciones [L]	Lugares donde se hospedan los sistemas de información y comunicaciones.
Hardware [HW]	Los medios materiales, físicos, destinados a soportar directa o indirectamente los servicios que presta la organización.
Software [SW]	Tareas que han sido automatizadas para su desempeño por un equipo informático. Las aplicaciones gestionan, analizan y transforman los datos permitiendo la explotación de la información para la prestación de servicios.
Datos[D]	La información que permite a la organización prestar sus servicios.
Redes de comunicaciones [COM]	Son los medios de transporte que llevan datos de un sitio a otro. Se incluyen tanto instalaciones dedicadas como servicios de comunicaciones contratados a terceros.
Equipamiento Auxiliar [AUX]	Otros equipos que sirven de soporte a los sistemas de información, sin estar directamente relacionados con éstos.
Personal [P]	Personas relacionadas con los sistemas de información.
Soportes de información [Media]	Dispositivos físicos que permiten almacenar información de forma permanente o, al menos, durante largos periodos de tiempo.

Tabla 12: Inventario de Activos.

Tipo de Activo Descripción	ID	ACTIVO
Instalaciones [L]	L1	Centro de proceso de Datos
	L2	Oficina Director Administrativo
	L3	Oficina Director de Contabilidad
	L4	Oficina Director de Planeación
	L5	Oficina Gerencia de Sistemas
	L6	Oficina de Decanaturas
	L7	Oficina de Direcciones de Programa
	L8	Oficina de Rectoría
	L9	Oficina de Vicerrectoría académica
	L10	Oficina Recepción
	L11	Oficina de Calidad
	L12	Oficina de Investigación
	L13	Oficina de Proyección Social
	L14	Oficina de Bienestar Institucional
	L15	Oficina de Registro y Control
	L16	Oficina de Mercadeo
	L17	Sala de Docentes
	L18	Salas Especialidad
	L19	Laboratorios
Hardware [HW]	HW1	servidor de aplicaciones
	HW2	Servidor de Bases de Datos
	HW3	Servidor Telefonía
	HW4	Servidor Proxy
	HW5	Servidor Web
	HW6	Servidor de Dominio
	HW7	Equipos Sala 1 (30) equipos
	HW8	Equipos Sala 2 (30) equipos
	HW9	Equipos Sala 3 (30) equipos
	HW10	Equipos Sala 4 (30) equipos
	HW11	Equipos Sala 5 (30) equipos
	HW12	Equipos Sala docentes 15
	HW13	Equipos de Oficinas Administrativas 16
	HW14	Equipos de Laboratorios 120
	HW15	Equipos de Laboratorios Telecomunicaciones 120
	HW16	Equipos de Laboratorios Electrónica 1 10

	HW17	Equipos de Laboratorios Electrónica 1 20
	HW18	Equipos de Laboratorios electrónica 3 20
	HW19	Equipos de Laboratorios de Antenas 10
	HW20	Equipos de Laboratorios de Hardware 20
Software [SW]	SW1	Windows Server 2012
	SW2	Office 2013
	SW3	Sistema Operativo Windows 10
	SW4	Matlab
	SW5	Paquect Tracer
	SW6	Microsoft active Directory
	SW7	Apache Tomcat
	SW8	Antivirus
	SW9	Academusoft
	SW10	Sistemas de Grados
	SW11	Sistema de Homologaciones
	SW12	Moodle
	SW13	Bibliofus
	SW14	SSE
	SW15	Asistencia
	SW16	Evaluación Docente
	SW17	Seguimiento Docente
	SW18	Sistema Presupuesto
	SW19	Sistema Eventos
	SW20	Mesa de Ayuda
	SW21	Ficheros Estadísticos
	SW22	Gestión de Talento Humano
	SW23	Helisa
	SW24	Tutorías
	SW25	Facturación y Cartera
Datos[D]	D1	Bases de Datos Administrativos
	D2	Bases de Datos Estudiantes
	D3	Bases de Datos Docente
	D4	Bases de Datos Proveedores, Empresarios
	D5	Backus generadas de Bases de datos
	D6	Bases de Datos Correos Institucionales
	D7	Respaldo de Aplicaciones Institucionales
	D8	Centro de proceso de Datos
Redes de comunicaciones [COM]	COM1	Acceso a inter Oficinas (14)

	COM2	Líneas Telefónicas (24)
	COM3	1 Fax
	COM4	Acceso Inalámbrico (8)
Servicios (S)	S1	Backup de usuarios
	S2	Video vigilancia
	S3	Virtualización (Servidor Moodle)
	S4	Correo electrónico Institucional
Equipamiento Auxiliar	AUXI	Sistema Eléctrico General
		Aire Acondicionado (Datacenter)
		Sistema de Detección de incendios
		Sistema de primeros Auxilios
		Fibra óptica
		Cableado estructurado Oficina
		Cableado estructurado Salas de informática
		Cableado estructurado laboratorios
		Ups Principal
		Planta Eléctrica
Personal [P]	P1	Rector
	P2	Vicerrectorías (5)
	P3	Gerente Administrativo
	P4	Decanatura (2)
	P5	Directores de Programa (6)
	P6	Director de Extensión
	P7	Director de Bienestar
	P8	Director de Investigación
	P9	Director de Talento Humano
	P10	Director Contabilidad
	P11	Asistentes de Secretaria (12)
	P12	Docentes (156)
	P13	Coordinador de Tecnología
	P14	Coordinador Registro y Control
	P15	Secretaria académica 3)
	P16	Soporte Técnico 5()
	P17	Estudiantes (4300)
	P18	Mercadeo (5)
	P19	Comunicaciones (2)
	P20	Personal de Servicios Generales (8)
	P21	Área de Desarrollo (4)

	P22	Recepción
	P23	Auxiliara Administrativo (4)
	P24	Auxiliar Contabilidad (3)
Soportes de información [Media]	M1	Discos Duros Backup (4)
	M2	Nas
	M3	USB (5)

Fuente: ("FUNDACIÓN SAN MATEO,")

4.3 Valoración de los activos

Si pensamos en el proceso en conjunto, el objetivo final es tomar un conjunto de medidas que garanticen nuestros activos. El sentido común indica que el coste de las medidas no deberá ser superior al coste del activo protegido. Empezaremos por tanto por determinar el valor de los diferentes activos

Esta valoración es sin duda complicada en muchos casos. ¿Cuánto vale - por ejemplo - la base de datos de cliente de una empresa? Nos basaremos en el análisis que propone MAGERIT en su Libro III (punto 2.1), completándolo con una estimación cuantitativa. La propuesta anterior realiza una clasificación según las siguientes categorías.

- **Valor real**: Valor que tiene para la empresa la reposición del activo en las condiciones anteriores a la acción de la amenaza
- **Valor estimada:** medida subjetiva de la empresa que, considerando la importancia del activo, asignan un valor económico
- **El valor de reposición**: es el valor que tiene para la empresa reponer ese activo en el caso de que se pierda o de que no pueda ser utilizado
- **El valor de configuración:** es el tiempo que se necesita desde que se adquiere el nuevo activo hasta que se configura o se pone a punto para que pueda utilizarse para la función que desarrollaba el anterior activo.
- **El valor de uso del activo:** es el valor que pierde la organización durante el tiempo que no puede utilizar dicho activo para la función que desarrolla
- **El valor de pérdida de oportunidad:** es el valor que pierde potencialmente la organización por no poder disponer de dicho activo durante un tiempo.

Para realizar la valoración se establecen diferentes grupos de activos según su valor y a cada grupo se le asigna un valor económico estimado que se utilizará para todos los activos que pertenezcan a ese grupo. En la siguiente tabla se presenta los grupos desvaloración para el análisis de riesgos de la Fundación Universitaria San Mateo.

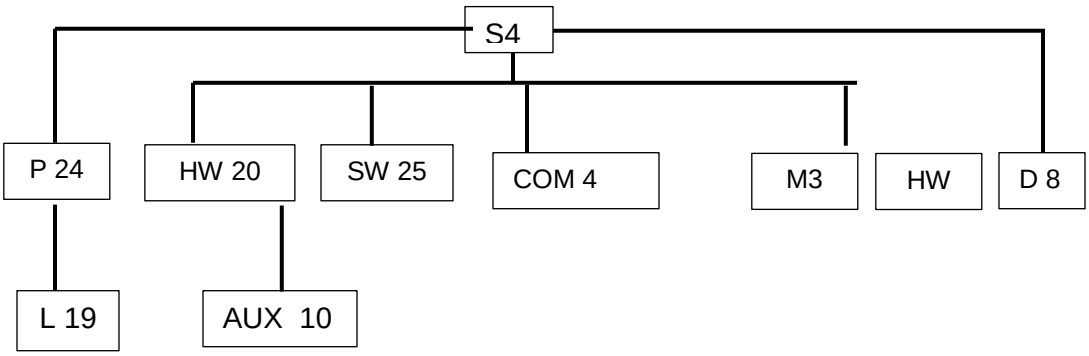
Tabla 13: Escala de Valoración.

ID	Valoración	Rango	Valor Estimado
MA	Muy Alto	Valor > 200.000.000	300.000.000
A	Alto	100.000.000<Valor>200.000.000	150.000.000
M	Medio	50.000.000<Valor>100.000.000	75.000.000
B	Bajo	10.000.000<Valor>50.000.000	30.000000
MB	Muy Bajo	Valor>10.000.000	10.000

Adicionalmente, debe tenerse en cuenta que los activos están en realidad jerarquizados. Es decir, debemos identificar y valorar las dependencias entre activos. Se dice que un "activo superior" depende de otro "activo inferior" cuando las necesidades de seguridad del superior se reflejan en las necesidades de seguridad del inferior, dicho en otras palabras, cuando la materialización de una amenaza en el activo inferior tiene como consecuencia un perjuicio sobre el activo superior, deberá por tanto analizarse el árbol de dependencias o jerarquía entre los activos.

A continuación, se presentan las jerarquías de la dependencia de los servicios de monitorización y administración de la Fundación Universitaria San Mateo

Ilustración 16: Dependencias administración y monitorización.



4.4 Dimensiones de seguridad

Desde el punto de vista de la seguridad, junto a la valoración en sí de los activos debe indicarse cuál es el aspecto de la seguridad más crítico. Esto será de ayuda en el momento de pensar en posibles salvaguardas, ya que estas se enfocarán en los aspectos que más interesen.

Una vez identificados los activos, debe realizarse la valoración ACIDA de los mismos. Dicha valoración viene a medir la criticidad en las cinco dimensiones de la seguridad de la información manejada por el proceso de negocio. Esta valoración permitirá a posteriori valorar el impacto que tendrá la materialización de una amenaza sobre la parte de activo expuesto (no cubierto por las salvaguardas en cada una de las dimensiones).

Autenticidad [A]: Propiedad o característica consistente en que una entidad es quien dice ser o bien que garantiza la fuente de la que proceden los datos.

Confidencialidad [C]: Propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados

Integridad [I]: Propiedad de la información relativa a su exactitud y completitud

Disponibilidad [D]: Propiedad o característica de los activos consistente en que las entidades o procesos autorizados tienen acceso a los mismos cuando lo requieren.

Amenaza: [D]: Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización

El valor que reciba un activo puede ser propio o acumulado, el valor propio se asignará a la información, quedando los demás activos subordinados a las necesidades de explotación y protección de la información. Así pues, los activos inferiores en un esquema de dependencias acumulan el valor de los activos que se apoyan en ellos. Cada activo de información puede poseer un valor diferente en cada una de las diferentes dimensiones para la organización que se desee analizar, para ello se ha de tener presente siempre que representa cada dimensión.

Una vez explicadas las cinco dimensiones se tiene en cuenta la escala en la que se realizarán las valoraciones. En este caso se usa una escala de valoración de diez valores siguiendo los siguientes criterios:

Tabla 14: Valoración dimensiones de Seguridad.

VALOR	CRITERIO
10	Daño muy grave a la organización
7-9	Daño grave a la organización
4-6	Daño importante a la organización
1-3	Daño menor a la organización
0	Irrelevante para la organización

A la hora de realizar las ponderaciones para cada activo se ha de tener presente la importancia o participación del activo en la cadena de valor del servicio, evitando situaciones del tipo "todo es muy importante" y obligando así al o a los responsables de realizar dicha valoración a discernir entre lo que es realmente importante y lo que no lo es tanto.

Se valorarán los activos como de importancia "Muy Alta", "Alta", "Media", "Baja" o "Despreciable" a la vez que se le asignará a cada activo en cada dimensión una valoración del [0-10].(Larrahondo Nuñez & Alexander Larrahondo)

4.5 Tabla resumen de valoración

De forma resumida, lo visto hasta ahora debe permitir generar una tabla donde se reflejará tanto la valoración de activos como los aspectos críticos del mismo. A la tabla resultante se le llamará Valoración de los activos.

Tabla 15: Valoración de los activos.

Tipo de Activo Descripción	ID	ACTIVO	VALOR	A	C	I	D	A
Instalaciones [L]	L1	Centro de proceso de Datos	MA	10	10	10	10	10
	L2	Oficina Director Administrativo	A	9	7	8	8	8
	L3	Oficina Director de Contabilidad	A	9	9	9	8	8
	L4	Oficina Director de Planeación	A	8	8	7	7	8
	L5	Oficina Gerencia de Sistemas	MA	10	10	10	10	10
	L6	Oficina de Decanaturas	M	4	6	4	4	5
	L7	Oficina de Direcciones de Programa	M	4	6	5	4	4
	L8	Oficina de Rectoría	A	8	8	8	8	8
	L9	Oficina de Vicerrectoría académica	A	8	8	7	8	7

	L10	Oficina Recepción	MB	2	3	2	2	2
	L11	Oficina de Calidad	A	8	7	9	8	8
	L12	Oficina de Investigación	M	4	6	6	6	6
	L13	Oficina de Proyección Social	M	4	5	5	6	6
	L14	Oficina de Bienestar Institucional	M	5	6	4	6	6
	L15	Oficina de Registro y Control	A	9	9	9	8	7
	L16	Oficina de Mercadeo	M	5	6	4	6	6
	L17	Sala de Docentes	MB	2	3	2	3	1
	L18	Salas de informática	M	6	6	6	6	6
	L19	Laboratorios	M	4	6	5	6	6
Hardware [HW]	HW1	servidor de aplicaciones	MA	10	10	10	10	10
	HW2	Servidor de Bases de Datos	MA	10	10	10	10	10
	HW3	Servidor Telefonía	A	7	9	9	8	7
	HW4	Servidor Proxy	MB	3	3	2	3	3
	HW5	Servidor Web	A	9	9	7	8	7
	HW6	Servidor de Dominio	M	6	6	5	4	4
	HW7	Equipos Sala 1 (30) equipos	A	8	9	7	8	7
	HW8	Equipos Sala 2 (30) equipos	A	8	9	7	8	7
	HW9	Equipos Sala 3 (30) equipos	A	8	9	7	8	7
	HW10	Equipos Sala 4 (30) equipos	A	8	9	7	8	7
	HW11	Equipos Sala 5 (30) equipos	A	8	9	7	8	7
	HW12	Equipos Sala docentes 15	A	8	9	7	8	7
	HW13	Equipos de Oficinas Administrativas 16	A	9	9	7	8	9
	HW14	Equipos de Laboratorios 120	A	8	9	7	8	7
	HW15	Equipos de Laboratorios Telecomunicaciones 120	A	8	9	7	8	7
	HW16	Equipos de Laboratorios Electrónica 1 10	A	8	9	7	8	7
	HW17	Equipos de Laboratorios Electrónica 1 20	A	8	9	7	8	7
	HW18	Equipos de Laboratorios electrónica 3 20	A	8	9	7	8	7
	HW19	Equipos de Laboratorios de Antenas 10	A	8	9	7	8	7
	HW20	Equipos de Laboratorios de Hardware 20	A	8	9	7	8	7
Software [SW]	SW1	Windows Server 2012	A	7	9	8	7	7
	SW2	Office 2013	MB	3	3	2	3	3
	SW3	Sistema Operativo Windows 10	A	8	7	9	9	9
	SW4	Matlab	MB	3	2	3	2	1
	SW5	Paquect Tracer	MB	3	2	3	2	1
	SW6	Microsoft active Directory	A	8	9	7	7	8
	SW7	Apache Tomcat	MA	10	10	10	10	10
	SW8	Antivirus	A	9	9	8	8	7
	SW9	Academusoft	A	8	9	7	7	8

	SW10	Sistemas de Grados	M	4	4	4	5	4
	SW11	Sistema de Homologaciones	M	4	4	4	5	4
	SW12	Moodle	A	7	8	8	9	7
	SW13	Bibliofus	MB	3	2	3	2	3
	SW14	SSE	A	9	7	8	8	7
	SW15	Asistencia	MB	3	3	2	3	1
	SW16	Evaluación Docente	M	4	6	4	5	6
	SW17	Seguimiento Docente	M	5	4	4	5	6
	SW18	Sistema Presupuesto	A	8	9	8	8	7
	SW19	Sistema Eventos	MB	3	2	3	3	3
	SW20	Mesa de Ayuda	M	5	6	6	5	6
	SW21	Ficheros Estadísticos	A	8	9	8	7	7
	SW22	Gestión de Talento Humano	A	8	8	9	8	7
	SW23	Helisa	A	9	9	8	8	9
	SW24	Tutorías	MB	3	2	3	3	3
	SW25	Facturación y Cartera	MA	10	10	10	10	10
Datos[D]	D1	Bases de Datos Administrativos	A	8	8	9	8	9
	D2	Bases de Datos Estudiantes	MA	10	10	10	10	10
	D3	Bases de Datos Docente	MA	10	10	10	10	10
	D4	Bases de Datos Proveedores, Empresarios	MA	10	10	10	10	10
	D5	Backus generadas de Bases de datos	A	9	9	9	9	9
	D6	Bases de Datos Correos Institucionales	A	9	9	8	9	8
	D7	Respaldo de Aplicaciones Institucionales	A	9	8	8	7	9
	D8	Centro de proceso de Datos	A	8	9	8	9	9
Redes de comunicaciones [COM]	COM1	Acceso a inter Oficinas (14)	A	9	8	8	9	9
	COM2	Líneas Telefónicas (24)	M	6	4	6	5	4
	COM3	Fax	MB	2	2	1	3	2
	COM4	Acceso Inalámbrico (8)	M	5	4	6	4	5
Servicios (S)	S1	Backup de usuarios	M	4	6	5	5	4
	S2	Video vigilancia	A	7	9	9	9	8
	S3	Virtualización (Servidor Moodle)	A	9	8	8	9	8
	S4	Correo electrónico Institucional	M	4	6	5	5	4
Equipamiento Auxiliar	AUXI	Sistema Eléctrico General	MA	10	10	10	10	10
		Aire Acondicionado (Datacenter)	M	6	6	6	6	6
		Sistema de Detección de incendios	A	7	8	8	9	9
		Sistema de primeros Auxilios	A	8	8	8	8	8
		Fibra óptica	A	8	8	8	7	7
		Cableado estructurado Oficina	M	6	6	6	6	5
		Cableado estructurado Salas de informática	M	6	6	6	6	6
		Cableado estructurado laboratorios	M	6	6	6	6	6

		Ups Principal	A	8	8	7	9	7
		Planta Eléctrica	A	7	7	7	7	7
Personal [P]	P1	Rector	MA	10	10	10	10	10
	P2	Vicerrectorías (5)	A	9	9	9	9	9
	P3	Gerente Administrativo	A	9	8	9	8	9
	P4	Decanatura (2)	A	8	8	9	8	7
	P5	Directores de Programa (6)	A	8	8	7	8	7
	P6	Director de Extensión	A	8	8	7	8	7
	P7	Director de Bienestar	M	5	5	6	4	4
	P8	Director de Investigación	A	7	8	7	9	7
	P9	Director de Talento Humano	A	9	9	9	8	9
	P10	Director Contabilidad	A	9	8	9	8	8
	P11	Asistentes de Secretaria (12)	M	6	6	4	4	6
	P12	Docentes (156)	A	9	9	9	9	9
	P13	Coordinador de Tecnología	A	8	9	9	9	9
	P14	Coordinador Registro y Control	A	8	9	9	8	9
	P15	Secretaria académica 3)	A	8	9	9	9	9
	P16	Soporte Técnico 5()	A	8	9	7	8	9
	P17	Estudiantes (4300)	A	9	9	9	9	9
	P18	Mercadeo (5)	A	8	9	8	9	9
	P19	Comunicaciones (2)	M	6	5	4	5	6
	P20	Personal de Servicios Generales (8)	M	6	6	4	6	6
	P21	Área de Desarrollo (4)	A	8	9	8	9	9
	P22	Recepción	M	6	4	6	6	4
	P23	Auxiliara Administrativo (4)	M	6	6	6	6	5
	P24	Auxiliar Contabilidad (3)	M	5	5	6	5	6
Soportes de información [Media]	M1	Discos Duros Backup (4)	A	8	8	9	8	9
	M2	Nas	A	7	8	9	8	9
	M3	USB (5)	A	7	8	7	8	9

4.6 Análisis de amenazas

Los activos están expuestos a amenazas y estas pueden afectar a los distintos aspectos de la seguridad. A nivel metodológico, se quiere analizar qué amenazas pueden afectar a qué activos de la Fundación Universitaria San Mateo. Una vez estudiado, estimar cuán vulnerable es el activo a la materialización de la amenaza así como la frecuencia estimada de la misma.

Lo más habitual en un enfoque metodológico es disponer de una tabla inicial de amenazas. Muchas metodologías disponen de tablas con algunas de las más comunes, en este caso, y por un tema de homogeneidad, se utilizarán también las usadas en MAGERIT (en concreto Libro 2 "Catálogo de Elementos" (Punto 5)).

Las amenazas están clasificadas en los siguientes grandes bloques:

- Desastres naturales [N]
- De origen industrial [I]
- Errores y fallos no intencionados [E]
- Ataques intencionados [A]

En la siguiente tabla se muestra el catálogo de amenazas según MAGERIT para la Fundación Universitaria San Mateo.

Tabla 16: Catálogo de Amenazas MAGERIT.

Tipo de Activo Descripción	ID	ACTIVO
Desastres Naturales [N]	N1	Fuego
	N2	Daños por agua
	N3	Tormenta Eléctrica
	N4	Terremoto
Origen Industrial [I]	I1	Fuego
	I2	Daños por agua
	I3	Sobrecarga eléctrica
	I4	Explosión
	I5	Derrumbe
	I6	Contaminación mecánica
	I7	Contaminación electromagnética
	I8	Avería de origen física o lógica

	I9	Corte eléctrico
	I10	Condiciones inadecuadas de temperatura y/o humedad
	I11	Fallo del servicio de comunicaciones
	I12	Interrupción de otros servicios y suministros esenciales
	I13	Degradación de los soportes de almacenamiento de la información
	I14	Emanaciones electromagnéticas
Errores y fallos no intencionados [E]	E1	Errores de usuarios
	E2	Errores de los técnicos de TI
	E3	Errores de los administradores de sirio
	E4	Errores de monitorización (log)
	E5	Errores de configuración
	E6	Deficiencias en la organización
	E7	Difusión de software dañino
	E8	Errores de [re-]encaminamiento
	E9	Errores de secuencia
	E10	Escapes de información
	E11	Alteración accidental de la información
	E12	Destrucción de información
	E13	Fugas de información
	E14	Vulnerabilidad de los programas (software)
	E15	Errores de mantenimiento / actualización de programas (software)
	E16	Errores de mantenimiento / actualización de equipos (hardware)
	E17	Caída del sistema por agotamiento de recursos
	E18	Pérdida de equipos
	E19	Indisponibilidad del personal
Ataques intencionados [A]	A1	Manipulación de los registros de actividad (log)
	A2	Manipulación de la configuración
	A3	Suplantación de la identidad del usuario
	A4	Abuso de privilegios de acceso
	A5	Uso no previsto
	A6	Difusión de software dañino
	A7	[Re-]encaminamiento de mensajes
	A8	Alteración de secuencia
	A9	Acceso no autorizado
	A10	Análisis de tráfico
	A11	Repudio
	A12	Interceptación de información (escucha)
	A13	Modificación deliberada de la información

	A14	Destrucción de información
	A15	Divulgación de información
	A16	Manipulación de programas
	A17	Manipulación de los equipos
	A18	Denegación de servicio
	A19	Robo
	A20	Ataque destructivo
	A21	Ocupación enemiga
	A22	Indisponibilidad del personal
	A23	Extorsión
	A24	Ingeniería social (picaresca)

Para la estimación de la vulnerabilidad hay que estimar la frecuencia de ocurrencia de las amenazas en una escala de tiempos.

Tabla 17: Categorías de Frecuencias de Amenazas.

Vulnerabilidad	ID	Rango	valor
Extrema Frecuencia	MA	1 vez al día	1
Alta Frecuencia	A	1 vez cada 2 semanas	26/365=0.071233
Frecuencia Media	M	1 vez cada 2 meses	6/365=0.016438
Baja Frecuencia	B	1 vez cada 6 meses	2/365=0.005479
Muy Baja Frecuencia	MB	1 vez al año	1/365=0.002739

El valor numérico del rango de vulnerabilidad se extrae mediante estimaciones anuales basadas en días, es decir, asignando un número de veces por año:

Valor Vulnerabilidad = Frecuencia estimada en días al año/ 365 (Nº de días de un año

Y la valoración del impacto que la ocurrencia de una amenaza producirá en las dimensiones de seguridad se basará en la siguiente tabla:

Impacto	*ID*	*Valor*
Muy Alto	MA	Valor > 95%
Alto	A	75%<Valor>95%
Medio	M	50%<Valor>75%

Bajo	B	30%<Valor>50%
Muy Bajo	MB	10%<Valor>30%

A continuación, se muestra una tabla resumen del análisis de amenazas de la Fundación Universitaria San Mateo, se puede apreciar que para cada amenaza que afecta un activo se analiza la frecuencia con que puede producirse la amenaza, así como su impacto en las distintas dimensiones de la seguridad del activo.

En definitiva, para cada tipo de activo se analizará la frecuencia con que puede producirse la amenaza, así como su impacto en las distintas dimensiones de la seguridad del activo.

Tabla 18: Resumen análisis de Amenazas.

GRUPO	AMENZA	Activo afectado	Frecuencia	% Impacto dimensiones				
				A	C	I	D	T
Desastres Naturales [N]	Fuego [N1]	Hardware [HW]	MB				100	
		Instalaciones [L]	MB				100	
		Red de Comunicaciones [COM]	MB				100	
		Equipamiento Auxiliar [AUX]	MB				75	
	Daños por agua [N2]	Hardware [HW]	MB				75	
		Instalaciones [L]	MB				75	
		Red de Comunicaciones [COM]	MB				75	
		Equipamiento Auxiliar [AUX]	MB				75	
	Tormenta Eléctrica [N3]	Hardware [HW]	MB				75	
		Red de Comunicaciones [COM]	MB				50	
		Equipamiento Auxiliar [AUX]	MB				50	
	Terremoto [N4]	Instalaciones [L]	MB				100	
		Hardware [HW]	MB				75	
		Equipamiento Auxiliar [AUX]	MB				75	
De origen industrial [I]	Fuego [I1]	Hardware [HW]	MB				100	
		Instalaciones [L]	MB				100	
		Red de Comunicaciones [COM]	MB				100	

		Equipamiento Auxiliar [AUX]	MB				100	
	Daños por agua [l2]	Hardware [HW]	MB				75	
		Instalaciones [L]	MB				75	
		Red de Comunicaciones [COM]	MB				75	
		Equipamiento Auxiliar [AUX]	MB				75	
	Sobrecarga eléctrica [l3]	Hardware [HW]	B				75	
		Red de Comunicaciones [COM]	B				50	
		Equipamiento Auxiliar [AUX]	B				50	
	Explosión [l4]	Hardware [HW]	MB				100	
		Instalaciones [L]	MB				100	
		Red de Comunicaciones [COM]	MB				100	
		Equipamiento Auxiliar [AUX]	MB				100	
	Derrumbe [l5]	Hardware [HW]	MB				75	
		Instalaciones [L]	MB				100	
		Red de Comunicaciones [COM]	MB				60	
		Equipamiento Auxiliar [AUX]	MB				60	
	Contaminación mecánica [l6]	Hardware [HW]	MB				50	
		Equipamiento Auxiliar [AUX]	MB				50	
	Contaminación electromagnética [l7]	Red de Comunicaciones [COM]	MB				75	
		Hardware [HW]	MB				75	
		Datos [D]	MB				75	
		Equipamiento Auxiliar [AUX]	MB				775	
	Avería de origen física o lógica [l]	Red de Comunicaciones [COM]	M				75	
		Hardware [HW]	M				75	
		Equipamiento Auxiliar [AUX]	M				40	
		Instalaciones [L]	B				20	
		Software [SW]	M				75	
		Servicios [S]	M				80	
		Datos [D]	B				30	
		Hardware [HW]	B				100	

	Corte eléctrico [l9]	Red de Comunicaciones [COM]	B				100	
		Equipamiento Auxiliar [AUX]	B				100	
	Condiciones inadecuadas de temperatura y/o humedad [l]	Hardware [HW]	B				60	
		Red de Comunicaciones [COM]	B				60	
		Equipamiento Auxiliar [AUX]	B				60	
	Fallo del servicio de comunicaciones [I]	Acceso a Internet Principal Oficinas [COM]	M				100	
		Acceso a Internet Secundario Oficinas[COM]	M				100	
		Acceso a Internet Nave [COM]	M				100	
		Líneas Móviles (COM]	M				100	
		Línea voz fija principal oficinas [COM]	M				100	
		Línea voz fija secundaria oficinas [COM]	M				100	
		Línea voz fija nave oficinas [COM]	M				100	
		Acceso de Voz Fijo [COM]	M				100	
		Acceso a Internet Plantas [COM]	M				100	
		Servicios [S]	M				100	
	Interrupción de otros servicios y suministros esenciales I12	Sistema de climatización CPD	B				60	
		Sistema de alimentación Ininterrumpida	B				30	
	Degradación de los soportes de almacenamiento de la información [I13]	Servidores [HW]	MB				75	
		Cabina de Almacenamiento [HW 11]	MB				100	
		PC'S [HW]	B				10	
	Emanaciones electromagnéticas I14	Instalaciones [L]	MB			20	20	
		Hardware [HW]	MB			50	50	
		Equipamiento Auxiliar [AUX]	MB			20	20	
Errores y fallos no intencionados [E]	Errores de usuarios E1	Instalaciones [L]	M		20	50	10	
		PC'S [HW]	M		20	20	50	
		Móviles [HW]	M		20	20	50	

		Datos [D]	M		75	40	75	
Errores y fallos no intencionados [E]	Errores de los técnicos de TI E2	Instalaciones [L]	M		20	20	50	
		Hardware [HW]	M		20	20	75	
		Software [SW]	M		20	20	75	60
		Datos [D]	M		20	20	75	
		Equipamiento Auxiliar [AUX]	M				75	
		Servicios [S]	M				80	
	Errores de monitorización (E4	Datos [D]	M				75	
	Errores de configuración E5	Hardware [HW]	B				50	
		Software [SW]	B				50	
		Datos [D]	B				50	
		Equipamiento Auxiliar [AUX]	B				50	
	Deficiencias en la organización E6	Personal [P]	M		50	30	75	
		Datos [D]	M		50	30	75	
		Instalaciones [L]	M		50	30	75	
		Servicios [S]	M		50	30	75	
	Difusión de Software dañino E7	Software [SW]	B		75	75	75	
		Datos [D]	B		50	50	50	
	Errores de [re-]encaminamiento E8	Servicios [S]	MB		50		75	
		Red de Comunicaciones [COM]	MB		40		75	
		Software [SW]	B				100	
	Errores de secuencia E9	Servicios [S]	MB		50		75	
		Red de Comunicaciones [COM]	MB		50		75	
		Software [SW]	B		50		75	
	Escapes de información E10	Servicios [S]	MB		50			
		Software [SW]	B		50			
		Datos [D]	B		100			
	Alteración accidental de la información E11	Datos [D]	M			75		
	Destrucción de información E12	Datos [D]					100	

	Fugas de información E13	Servicios [S]	MB		30			
		Software [SW]	B		65			
		Datos [D]	B		100			
	Vulnerabilidad de los programas (software) E14	Software [SW]	M		75	20	75	
		Datos [D]	M		75	20	75	
	Errores de mantenimiento / actualización de programas (software) E15	Software [SW]	B			50	75	
	Errores de mantenimiento / actualización de equipos (hardware) E16	Hardware [HW]	B				75	
	Caída del sistema por agotamiento de recursos E17	Servicios [S]	MB				100	
		Red de Comunicaciones [COM]	MB				100	
	Pérdida de equipos E18	PC's	B		50		100	
		Móviles	M					
	Indisponibilidad del personal E19	Personal [P]	A				100	
Ataques intencionados [A]	Manipulación de los registros de actividad (log) A1	Datos [D]	MB					75
		Servicios [S]	MB					80
	Manipulación de la configuración A2	Datos [D]	MB	75	75	75		
		Servicios [S]	MB	75	75	75		
	Suplantación de la identidad del usuario [A3]	Software [SW]	B	75	100	80		
		Datos [D]	B	100	100	80		
		Red de Comunicaciones [COM]	B	75	75	75		
		Servicios [S]	B	85	75	75		
	Abuso de privilegios de acceso A4	Instalaciones [L]	B		75	50	50	
		Software [SW]	B		75	50	50	
		Red de Comunicaciones [COM]	B		75	50	50	
		Servicios [S]	B		75	50	50	

	Uso no previsto A5	Instalaciones [L]	MB		25	25	25	
		Software [SW]	MB		25	25	25	
		Red de Comunicaciones [COM]	MB		25	25	25	
		Servicios [S]	MB		25	25	25	
		Hardware [HW]	MB		25	25	25	
	Difusión de software dañino A6	Software [SW]	B		75	20	75	
		Datos [D]	B		75	20	75	
	[Re-]encaminamiento de mensajes A7	Red de Comunicaciones [COM]	MB		50		75	
		Software [SW]	MB		50		75	
		Servicios [S]	MB		50		75	
	Alteración de secuencia A8	Servicios [S]	MB		50		75	
		Red de Comunicaciones [COM]	MB		50			
		Software [SW]	B		50		75	
	Acceso no autorizado A9	Servicios [S]	B		75	50	75	
		Red de Comunicaciones [COM]	B		30	30	75	
		Software [SW]	B		75	75	50	
		Hardware [HW]	MB				50	
		Datos [D]	B		100	100	100	
		Equipamiento Auxiliar [AUX]	B				50	
		Instalaciones [L]	B		20	20	20	
	Análisis de tráfico A10	Datos [D]	MB		50			
	Repudio A11	Servicios [S]	MB					80
	Interceptación de información (escucha) A12	Datos [D]	B		100			
	Modificación deliberada de la información A13	Datos [D]	B			100		
		Software [SW]	B			100		
	Destrucción de información A14	Datos [D]	B				100	
		Software [SW]	B				100	
	Divulgación de información A15	Datos [D]	B		100			
		Software [SW]	B		100			
	Manipulación de programas A16	Software [SW]	B				100	

	Manipulación de los equipos A17	Hardware [HW]	B				100	
	Denegación de servicio A18	Servicios [S]	B				100	
		Red de Comunicaciones [COM]	B				100	
	Robo A19	Hardware [HW]	B				75	
		Equipamiento Auxiliar [AUX]	MB				75	
		Datos [D]	MB		100		100	
		Software [SW]	MB		100		75	
	Ataque destructivo A20	Instalaciones [L]	MB				100	
		Hardware [HW]	MB				100	
		Software [SW]	MB				100	
		Equipamiento Auxiliar [AUX]	MB				100	
		Red de Comunicaciones [COM]	MB				100	
		Servicios [S]	MB				100	
		Datos [D]	MB				100	
	Ataque destructivo A20	Instalaciones [L]	MB				100	
		Hardware [HW]	MB				100	
		Software [SW]	MB				100	
		Equipamiento Auxiliar [AUX]	MB				100	
		Red de Comunicaciones [COM]	MB				100	
		Servicios [S]	MB				100	
		Datos [D]	MB				100	
	Ocupación enemiga A21	Instalaciones [L]	MB		20		100	
		Hardware [HW]	MB		20		100	
		Software [SW]	MB		75		100	
		Equipamiento Auxiliar [AUX]	MB		20		100	
		Red de Comunicaciones [COM]	MB		30		100	
		Servicios [S]	MB		80		100	
		Datos [D]	MB		100		100	
	Indisponibilidad del personal A22	Personal [P]	M				100	
	Extorsión A23	Personal [P]	B		25	25	25	
	Ingeniería social (picaresca) A24	Personal [P]	B		25	25	25	

4.7 Impacto potencial

Una vez realizada la tabla anterior, y dado que se conocen los valores de los diferentes activos, se puede determinar el impacto potencial que puede suponer para la Fundación Universitaria San Mateo la materialización de las amenazas. Se trata de un dato relevante, ya que permitirá priorizar el plan de acción, y a su vez, evaluar cómo se ve modificado dicho valor una vez se apliquen contramedidas.

Como ya se conoce el valor de los activos en las diferentes dimensiones y la degradación que causan las amenazas en estas mismas dimensiones, es inmediato derivar el impacto que estas tendrían sobre el sistema a través de la siguiente formula.

Impacto potencial = Valor del activo x Valor del impacto de la amenaza

Se ha realizado una eficiencia en al análisis de activos agrupando los activos cuando las amenazas impactaban en un grupo, a continuación, se presenta una tabla con los valores absolutos máximos de impacto de amenazas obtenidos en el análisis anterior que serán los valores que serían para la obtención del impacto potencial (Director de Seguridad de Ícaro Luis Rodríguez Conde Página, Luis Rodríguez Conde Dirección Antonio José Segovia Henares, & Rodríguez Conde Página, 2700)

Tabla 19: Impacto de Amenazas.

	IMPACTOR POR DIMENSIONES				
Tipo de Activo Descripción	**A**	**C**	**I**	**D**	**T**
Instalaciones [L]	0	7,5	5	10	0
Hardware [HW]	0	2,5	5	10	0
Software [SW]	7,5	10	10	10	6
Datos[D]	10	10	10	10	7,5
Redes de comunicaciones [COM]	7,5	7,5	7,5	10	0
Servicios [S]	8	7,5	7,5	10	8
Equipamiento Auxiliar [AUX]	0	2	0	10	0
Personal [P]	0	5	3	10	0

A continuación, se presenta una tabla resumen con los resultados de aplicar la fórmula del impacto potencial a cada activo.

Tipo de Activo Descripción	ID	ACTIVO	VALOR	ASPECTOS CRITICOS				
				A	C	I	D	A
Instalaciones [L]	L1	Centro de proceso de Datos	MA	$ -	$ 225,00	150	300	$ -
	L2	Oficina Director Administrativo	A	$ -	$ 112,50	$ 75,00	$ 150,00	$ -
	L3	Oficina Director de Contabilidad	A	$ -	$ 112,50	$ 75,00	$ 150,00	$ -
	L4	Oficina Director de Planeación	A	$ -	112,5	$ 75,00	$ 150,00	$ -
	L5	Oficina Gerencia de Sistemas	MA	$ -	$ 225,00	$ 150,00	$ 300,00	$ -
	L6	Oficina de Decanaturas	M	$ -	$ 56,25	$ 37,50	$ 75,00	$ -
	L7	Oficina de Direcciones de Programa	M	$ -	$ 56,25	$ 37,50	$ 75,00	$ -
	L8	Oficina de Rectoría	A	$ -	$ 112,50	$ 75,00	$ 150,00	$ -
	L9	Oficina de Vicerrectoría académica	A	$ -	$ 112,50	$ 75,00	$ 150,00	$ -
	L10	Oficina Recepción	MB	$ -	$ 0,00	$ 0,00	$ 0,00	$ -
	L11	Oficina de Calidad	A	$ -	$ 112,50	$ 75,00	$ 150,00	$ -
	L12	Oficina de Investigación	M	$ -	$ 56,25	$ 37,50	$ 75,00	$ -

Tipo de Activo Descripción	ID	ACTIVO	VALOR	ASPECTOS CRITICOS				
				A	C	I	D	A
	L13	Oficina de Proyección Social	M	$ -	$ 56,25	$ 37,50	$ 75,00	$ -
	L14	Oficina de Bienestar Institucional	M	$ -	$ 56,25	$ 37,50	$ 75,00	$ -
	L15	Oficina de Registro y Control	A	$ -	$ 112,50	$ 75,00	$ 150,00	$ -
	L16	Oficina de Mercadeo	M	$ -	$ 56,25	$ 37,50	$ 75,00	$ -
	L17	Sala de Docentes	MB	$ -	$ 0,001	$ 0,00	$ 0,00	$ -
	L18	Salas de informática	M	$ -	$ 56,25	$ 37,50	$ 75,00	$ -
	L19	Laboratorios	M	$ -	$ 56,25	$ 37,50	$ 75,00	$ -
Hardware [HW]	HW1	servidor de aplicaciones	MA	$ -	$ 7,50	$ 150,00	$ 300,00	$ -
	HW2	Servidor de Bases de Datos	MA	$ -	$ 7,50	$ 150,00	$ 300,00	$ -
	HW3	Servidor Telefonía	A	$ -	$ 3,75	$ 75,00	$ 150,00	$ -
	HW4	Servidor Proxy	MB	$ -	$ 0,00	$ 0,00	$ 0,00	$ -
	HW5	Servidor Web	A	$ -	$ 3,75	$ 75,00	$ 150,00	$ -
	HW6	Servidor de Dominio	M	$ -	$ 1,88	$ 37,50	$ 75,00	$ -

Tipo de Activo Descripción	ID	ACTIVO	VALOR	ASPECTOS CRITICOS				
				A	C	I	D	A
	HW7	Equipos Sala 1 (30) equipos	A	$ -	$ 3,75	$ 75,00	$ 150,00	$ -
	HW8	Equipos Sala 2 (30) equipos	A	$ -	$ 3,75	$ 75,00	$ 150,00	$ -
	HW9	Equipos Sala 3 (30) equipos	A	$ -	$ 3,75	$ 75,00	$ 150,00	$ -
	HW10	Equipos Sala 4 (30) equipos	A	$ -	$ 3,75	$ 75,00	$ 150,00	$ -
	HW11	Equipos Sala 5 (30) equipos	A	$ -	$ 3,75	$ 75,00	$ 150,00	$ -
	HW12	Equipos Sala docentes 15	A	$ -	$ 3,75	$ 75,00	$ 150,00	$ -
	HW13	Equipos de Oficinas Administrativas 16	A	$ -	$ 3,75	$ 75,00	$ 150,00	$ -
	HW14	Equipos de Laboratorios 120	A	$ -	$ 3,75	$ 75,00	$ 150,00	$ -
	HW15	Equipos de Laboratorios Telecomunicaciones 120	A	$ -	$ 3,75	$ 75,00	$ 150,00	$ -
	HW16	Equipos de Laboratorios Electrónica 1 10	A	$ -	$ 3,75	$ 75,00	$ 150,00	$ -
	HW17	Equipos de Laboratorios Electrónica 1 20	A	$ -	$ 3,75	$ 75,00	$ 150,00	$ -

Tipo de Activo Descripción	ID	ACTIVO	VALOR	ASPECTOS CRITICOS				
				A	C	I	D	A
	HW18	Equipos de Laboratorios electrónica 3 20	A	$ -	$ 3,75	$ 75,00	$ 150,00	$ -
	HW19	Equipos de Laboratorios de Antenas 10	A	$ -	$ 3,75	$ 75,00	$ 150,00	$ -
	HW20	Equipos de Laboratorios de Hardware 20	A	$ -	$ 3,75	$ 75,00	$ 150,00	$ -
Software [SW]	SW1	Windows Server 2012	A	$ 112,50	$ 150,00	$ 150,00	$ 150,00	$ 90,00
	SW2	Office 2013	MB	$ 0,00	$ 0,00	$ 0,00	$ 0,00	$ 0,00
	SW3	Sistema Operativo Windows 10	A	$ 112,50	$ 150,00	$ 150,00	$ 150,00	$ 90,00
	SW4	Matlab	MB	$ 0,00	$ 0,00	$ 0,00	$ 0,00	$ 0,00
	SW5	Paquect Tracer	MB	$ 0,00	$ 0,00	$ 0,00	$ 0,00	$ 0,00
	SW6	Microsoft active Directory	A	$ 112,50	$ 150,00	$ 150,00	$ 150,00	$ 90,00
	SW7	Apache Tomcat	MA	$ 225,00	$ 300,00	$ 300,00	$ 300,00	$ 180,00
	SW8	Antivirus	A	$ 112,50	$ 150,00	$ 150,00	$ 150,00	$ 90,00
	SW9	Academusoft	A	$ 112,50	$ 150,00	$ 150,00	$ 150,00	$ 90,00

Tipo de Activo Descripción	ID	ACTIVO	VALOR	ASPECTOS CRITICOS				
				A	C	I	D	A
	SW10	Sistemas de Grados	M	$ 56,25	$ 75,00	$ 75,00	$ 75,00	$ 45,00
	SW11	Sistema de Homologaciones	M	$ 56,25	$ 75,00	$ 75,00	$ 75,00	$ 45,00
	SW12	Moodle	A	$ 112,50	$ 150,00	$ 150,00	$ 150,00	$ 90,00
	SW13	Bibliofus	MB	$ 0,00	$ 0,00	$ 0,00	$ 0,00	$ 0,00
	SW14	SSE	A	$ 112,50	$ 150,00	$ 150,00	$ 150,00	$ 90,00
	SW15	Asistencia	MB	$ 0,00	$ 0,00	$ 0,00	$ 0,00	$ 0,00
	SW16	Evaluación Docente	M	$ 56,25	$ 75,00	$ 75,00	$ 75,00	$ 45,00
	SW17	Seguimiento Docente	M	$ 56,25	$ 75,00	$ 75,00	$ 75,00	$ 45,00
	SW18	Sistema Presupuesto	A	$ 112,50	$ 150,00	$ 150,00	$ 150,00	$ 90,00

Tipo de Activo Descripción	ID	ACTIVO	VALOR	ASPECTOS CRITICOS				
				A	C	I	D	A
	SW19	Sistema Eventos	MB	$ 0,00	$ 0,00	$ 0,00	$ 0,00	$ 0,00
	SW20	Mesa de Ayuda	M	$ 56,25	$ 75,00	$ 75,00	$ 75,00	$ 45,00
	SW21	Ficheros Estadísticos	A	$ 112,50	$ 150,00	$ 150,00	$ 150,00	$ 90,00
	SW22	Gestión de Talento Humano	A	$ 112,50	$ 150,00	$ 150,00	$ 150,00	$ 90,00
	SW23	Helisa	A	$ 112,50	$ 150,00	$ 150,00	$ 150,00	$ 90,00
	SW24	Tutorías	MB	$ 0,00	$ 0,00	$ 0,00	$ 0,00	$ 0,00
	SW25	Facturación y Cartera	MA	$ 225,00	$ 300,00	$ 300,00	$ 300,00	$ 180,00
Datos[D]	D1	Bases de Datos Administrativos	A	$ 150,00	$ 150,00	$ 150,00	$ 150,00	$ 112,50
	D2	Bases de Datos Estudiantes	MA	$ 300,00	$ 300,00	$ 300,00	$ 300,00	$ 225,00
	D3	Bases de Datos Docente	MA	$ 300,00	$ 300,00	$ 300,00	$ 300,00	$ 225,00

Tipo de Activo Descripción	ID	ACTIVO	VALOR	ASPECTOS CRITICOS				
				A	C	I	D	A
	D4	Bases de Datos Proveedores, Empresarios	MA	$ 300,00	$ 300,00	$ 300,00	$ 300,00	$ 225,00
	D5	Backus generadas de Bases de datos	A	$ 150,00	$ 150,00	$ 150,00	$ 150,00	$ 112,50
	D6	Bases de Datos Correos Institucionales	A	$ 150,00	$ 150,00	$ 150,00	$ 150,00	$ 112,50
	D7	Respaldo de Aplicaciones Institucionales	A	$ 150,00	$ 150,00	$ 150,00	$ 150,00	$ 112,50
	D8	Centro de proceso de Datos	A	$ 150,00	$ 150,00	$ 150,00	$ 150,00	$ 112,50
Redes de comunicaciones [COM]	COM1	Acceso a inter Oficinas (14)	A	$ 150,00	$ 150,00	$ 675,00	$ 800,00	$ -
	COM2	Líneas Telefónicas (24)	M	$ 75,00	$ 75,00	$ 450,00	$ 400,00	$ -
	COM3	Fax	MB	$ 0,00	$ 0,00	$ 150,00	$ 200,00	$ -
	COM4	Acceso Inalámbrico (8)	M	$ 75,00	$ 75,00	$ 375,00	$ 400,00	$ -
Servicios (S)	S1	Backup de usuarios	M	$ 60,00	$ 56,25	$ 56,25	$ 75,00	$ 60,00
	S2	Video vigilancia	A	$ 120,00	$ 112,50	$ 112,50	$ 150,00	$ 120,00
	S3	Virtualización (Servidor Moodle)	A	$ 120,00	$ 112,50	$ 112,50	$ 150,00	$ 120,00

Tipo de Activo Descripción	ID	ACTIVO	VALOR	ASPECTOS CRITICOS				
				A	C	I	D	A
	S4	Correo electrónico Institucional	M	$ 60,00	$ 56,25	$ 56,25	$ 75,00	$ 60,00
Equipamiento Auxiliar	AUX I	Sistema Eléctrico General	MA	$ -	$ 60,00	$ -	$ 300,00	$ -
		Aire Acondicionado (Datacenter)	M	$ -	$ 15,00	$ -	$ 75,00	$ -
		Sistema de Detección de incendios	A	$ -	$ 30,00	$ -	$ 150,00	$ -
		Sistema de primeros Auxilios	A	$ -	$ 30,00	$ -	$ 150,00	$ -
		Fibra óptica	A	$ -	$ 30,00	$ -	$ 150,00	$ -
		Cableado estructurado Oficina	M	$ -	$ 15,00	$ -	$ 75,00	$ -
		Cableado estructurado Salas de informática	M	$ -	$ 15,00	$ -	$ 75,00	$ -
		Cableado estructurado laboratorios	M	$ -	$ 15,00	$ -	$ 75,00	$ -
		Ups Principal	A	$ -	$ 30,00	$ -	$ 150,00	$ -

Tipo de Activo Descripción	ID	ACTIVO	VALOR	ASPECTOS CRITICOS				
				A	C	I	D	A
		Planta Eléctrica	A	$ -	$ 30,00	$ -	$ 150,00	$ -
Personal [P]	P1	Rector	MA	$ -	$ 60,00	$ 90,00		$ -
	P2	Vicerrectorías (5)	A	$ -	$ 30,00	$ 45,00		$ -
	P3	Gerente Administrativo	A	$ -	$ 30,00	$ 45,00		$ -
	P4	Decanatura (2)	A	$ -	$ 30,00	$ 45,00		$ -
	P5	Directores de Programa (6)	A	$ -	$ 30,00	$ 45,00		$ -
	P6	Director de Extensión	A	$ -	$ 30,00	$ 45,00		$ -
	P7	Director de Bienestar	M	$ -	$ 15,00	$ 22,50		$ -
	P8	Director de Investigación	A	$ -	$ 30,00	$ 45,00		$ -
	P9	Director de Talento Humano	A	$ -	$ 30,00	$ 45,00		$ -
	P10	Director Contabilidad	A	$ -	$ 75,00	$ 45,00	$ 150,00	$ -
	P11	Asistentes de Secretaria (12)	M	$ -	$ 37,50	$ 22,50	$ 75,00	$ -
	P12	Docentes (156)	A	$ -	$ 75,00	$ 45,00	$ 150,00	$ -
	P13	Coordinador de Tecnología	A	$ -	$ 75,00	$ 45,00	$ 150,00	$ -

Tipo de Activo Descripción	ID	ACTIVO	VALOR	ASPECTOS CRITICOS				
				A	C	I	D	A
	P14	Coordinador Registro y Control	A	$ -	$ 75,00	$ 45,00	$ 150,00	$ -
	P15	Secretaria académica 3)	A	$ -	$ 75,00	$ 45,00	$ 150,00	$ -
	P16	Soporte Técnico 5()	A	$ -	$ 75,00	$ 45,00	$ 150,00	$ -
	P17	Estudiantes (4300)	A	$ -	$ 75,00	$ 45,00	$ 150,00	$ -
	P18	Mercadeo (5)	A	$ -	$ 75,00	$ 45,00	$ 150,00	$ -
	P19	Comunicaciones (2)	M	$ -	$ 37,50	$ 22,50	$ 75,00	$ -
	P20	Personal de Servicios Generales (8)	M	$ -	$ 37,50	$ 22,50	$ 75,00	$ -
	P21	Área de Desarrollo (4)	A	$ -	$ 37,50	$ 22,50	$ 75,00	$ -
	P22	Recepción	M	$ -	$ 37,50	$ 22,50	$ 75,00	$ -
	P23	Auxiliara Administrativo (4)	M	$ -	$ 37,50	$ 22,50	$ 75,00	$ -
	P24	Auxiliar Contabilidad (3)	M	$ -	$ 37,50	$ 22,50	$ 75,00	$ -

4.8 Nivel de Riesgo Aceptable y riesgo Residual

Sabiendo que la eliminación absoluta del riesgo es una situación casi imposible de alcanzar, es necesario definir un límite a partir del cual se pueda decidir si asumir un riesgo o por el contrario no asumirlo y por tanto aplicar controles.

Una vez presentado el análisis de riesgos a la Rectoría de la Fundación Universitaria San Mateo, esta ha decidido y aprobado que el nivel de riesgo aceptable para la empresa será de MEDIO y equivale a **0,016438**.

Los activos que estén por debajo o igual a este umbral no supondrán una amenaza importante para la seguridad de la empresa, su riesgo asociado será aceptable y no se tomarán medidas para su mitigación.

Por el contrario, los activos cuyo riesgo supere este umbral supondrán una amenaza para la seguridad de la empresa y se implantarán controles para mitigar su riesgo asociado. Una vez establecidos los controles de seguridad a los activos cuyo riesgo supere el valor este valor se reducirá, pero difícilmente podrá desaparecer, seguirá existiendo un riesgo al que se denomina residual.

El cálculo de cada uno de los activos la usaremos con la información de los análisis anteriores y aplicaremos la siguiente Formula. (Director de Seguridad de Ícaro Luis Rodríguez Conde Página et al., 2700)

Nivel de Riesgo= Impacto Potencial X frecuencia de la amenaza.

En la siguiente Tabla se muestra la relación entre el impacto y la frecuencia de la que se deduce el nivel de riesgo.

Tabla 20: Relación impacto/ Frecuencia.

RIESGO		FRECUENCIA				
		MB(0.002739)	B (0.005479)	M (0.016438)	A (0.071233)	MA (1)
IMPACTO	MA (3)	A	MA	MA	MA	MA
	A (1,5)	M	A	A	MA	MA
	M (0,75)	B	M	M	A	A
	B (0,3)	MB	B	B	M	M
	MB (0,0001)	MB	MB	MB	B	B

En la siguiente tabla mostramos el valor máximo de las frecuencias de cada grupo de activos del ejercicio anterior

Tabla 21: Valores Máximos de Frecuencia.

Grupo Activos	Valor	Valor Numérico
Instalaciones [L]	**MEDIA**	**0,016438**
Hardware [HW]		
Software [SW]		
Datos [D]		
Redes de comunicación [COM]		
Servicios [S]		
Equipamiento Auxiliar [AUX]		
Personal [P]		

En la siguiente tabla se muestra un resumen del análisis del nivel de riesgo por activo.

Tabla 22: Resumen de Análisis de nivel de Riesgo.

Tipo de Activo Descripción	ID	ACTIVO	ASPECTOS CRITICOS				
			A	C	I	D	T
Instalaciones [L]	L1	Centro de proceso de Datos	0	3,698550	2,4657	4,9314	0
	L2	Oficina Director Administrativo	0	1,849275	1,23285	2,4657	0
	L3	Oficina Director de Contabilidad	0	1,849275	1,23285	2,4657	0
	L4	Oficina Director de Planeación	0	1,849275	1,23285	2,4657	0
	L5	Oficina Gerencia de Sistemas	0	3,69855	2,4657	4,9314	0
	L6	Oficina de Decanaturas	0	0,9246375	0,616425	1,23285	0
	L7	Oficina de Direcciones de Programa	0	0,9246375	0,6164250	1,23285	0
	L8	Oficina de Rectoría	0	1,849275	1,23285	2,4657	0
	L9	Oficina de Vicerrectoría académica	0	1,849275	1,23285	2,4657	0
	L10	Oficina Recepción	0	0,000012	0,000008	0,000016	0,000000
	L11	Oficina de Calidad	0	1,849275	1,232850	2,465700	0,000000
	L12	Oficina de Investigación	0	0,924638	0,616425	1,232850	0,000000
	L13	Oficina de Proyección Social	0	0,924638	0,616425	1,232850	0,000000
	L14	Oficina de Bienestar Institucional	0	0,924638	0,616425	1,232850	0,000000
	L15	Oficina de Registro y Control	0	1,849275	1,232850	2,465700	0,000000
	L16	Oficina de Mercadeo	0	0,924638	0,616425	1,232850	0,000000
	L17	Sala de Docentes	0	0,000012	0,000008	0,000016	0,000000
	L18	Salas de informatica	0	0,924638	0,616425	1,232850	0,000000
	L19	Laboratorios	0	0,924638	0,616425	1,232850	0,000000
Hardware [HW]	HW1	servidor de aplicaciones	0	0,123285	2,465700	4,931400	0,000000
	HW2	Servidor de Bases de Datos	0	0,123285	2,465700	4,931400	0,000000
	HW3	Servidor Telefonía	0	0,061643	1,232850	2,465700	0,000000
	HW4	Servidor Proxy	0	0,000000	0,000008	0,000016	0,000000
	HW5	Servidor Web	0	0,061643	1,232850	2,465700	0,000000
	HW6	Servidor de Dominio	0	0,030821	0,616425	1,232850	0,000000
	HW7	Equipos Sala 1 (30) equipos	0	0,061643	1,232850	2,465700	0,000000
	HW8	Equipos Sala 2 (30) equipos	0	0,061643	1,232850	2,465700	0,000000
	HW9	Equipos Sala 3 (30) equipos	0	0,061643	1,232850	2,465700	0,000000
	HW10	Equipos Sala 4 (30) equipos	0	0,061643	1,232850	2,465700	0,000000
	HW11	Equipos Sala 5 (30) equipos	0	0,061643	1,232850	2,465700	0,000000
	HW12	Equipos Sala docentes 15	0	0,061643	1,232850	2,465700	0,000000
	HW13	Equipos de Oficinas Administrativas 16	0	0,061643	1,232850	2,465700	0,000000

	HW14	Equipos de Laboratorios 120	0	0,061643	1,232850	2,465700	0,000000
	HW15	Equipos de Laboratorios Telecomunicaciones 120	0	0,061643	1,232850	2,465700	0,000000
	HW16	Equipos de Laboratorios Electrónica 1 10	0	0,061643	1,232850	2,465700	0,000000
	HW17	Equipos de Laboratorios Electrónica 1 20	0	0,061643	1,232850	2,465700	0,000000
	HW18	Equipos de Laboratorios electrónica 3 20	0	0,061643	1,232850	2,465700	0,000000
	HW19	Equipos de Laboratorios de Antenas 10	0	0,061643	1,232850	2,465700	0,000000
	HW20	Equipos de Laboratorios de Hardware 20	0	0,061643	1,232850	2,465700	0,000000
Software [SW]	SW1	Windows Server 2012	1,849275	2,465700	2,465700	2,465700	1,479420
	SW2	Office 2013	0,000012	0,000016	0,000016	0,000016	0,000010
	SW3	Sistema Operativo Windows 10	1,849275	2,465700	2,465700	2,465700	1,479420
	SW4	Matlab	0,000012	0,000016	0,000016	0,000016	0,000010
	SW5	Paquect Tracer	0,000012	0,000016	0,000016	0,000016	0,000010
	SW6	Microsoft active Directory	1,849275	2,465700	2,465700	2,465700	1,479420
	SW7	Apache Tomcat	3,698550	4,931400	4,931400	4,931400	2,958840
	SW8	Antivirus	1,849275	2,465700	2,465700	2,465700	1,479420
	SW9	Academusoft	1,849275	2,465700	2,465700	2,465700	1,479420
	SW10	Sistemas de Grados	0,924638	1,232850	1,232850	1,232850	0,739710
	SW11	Sistema de Homologaciones	0,924638	1,232850	1,232850	1,232850	0,739710
	SW12	Moodle	1,849275	2,465700	2,465700	2,465700	1,479420
	SW13	Bibliofus	0,000012	0,000016	0,000016	0,000016	0,000010
	SW14	SSE	1,849275	2,465700	2,465700	2,465700	1,479420
	SW15	Asistencia	0,000012	0,000016	0,000016	0,000016	0,000010
	SW16	Evaluación Docente	0,924638	1,232850	1,232850	1,232850	0,739710
	SW17	Seguimiento Docente	0,924638	1,232850	1,232850	1,232850	0,739710
	SW18	Sistema Presupuesto	1,849275	2,465700	2,465700	2,465700	1,479420
	SW19	Sistema Eventos	0,000012	0,000016	0,000016	0,000016	0,000010
	SW20	Mesa de Ayuda	0,924638	1,232850	1,232850	1,232850	0,739710
	SW21	Ficheros Estadísticos	1,849275	2,465700	2,465700	2,465700	1,479420
	SW22	Gestión de Talento Humano	1,849275	2,465700	2,465700	2,465700	1,479420
	SW23	Helisa	1,849275	2,465700	2,465700	2,465700	1,479420
	SW24	Tutorías	0,000012	0,000016	0,000016	0,000016	0,000010
	SW25	Facturación y Cartera	3,698550	4,931400	4,931400	4,931400	2,958840
Datos[D]	D1	Bases de Datos Administrativos	2,465700	2,465700	2,465700	2,465700	1,849275
	D2	Bases de Datos Estudiantes	4,931400	4,931400	4,931400	4,931400	3,698550
	D3	Bases de Datos Docente	4,931400	4,931400	4,931400	4,931400	3,698550

	D4	Bases de Datos Proveedores, Empresarios	4,931400	4,931400	4,931400	4,931400	3,698550
	D5	Backus generadas de Bases de datos	2,465700	2,465700	2,465700	2,465700	1,849275
	D6	Bases de Datos Correos Institucionales	2,465700	2,465700	2,465700	2,465700	1,849275
	D7	Respaldo de Aplicaciones Institucionales	2,465700	2,465700	2,465700	2,465700	1,849275
	D8	Centro de proceso de Datos	2,465700	2,465700	2,465700	2,465700	1,849275
Redes de comunicaciones [COM]	COM1	Acceso a inter Oficinas (14)	2,465700	2,465700	11,095650	13,150400	0,000000
	COM2	Líneas Telefónicas (24)	1,232850	1,232850	7,397100	6,575200	0,000000
	COM3	Fax	0,000016	0,000016	2,465700	3,287600	0,000000
	COM4	Acceso Inalámbrico (8)	1,23285	1,23285	6,164250	6,5752	0
Servicios (S)	S1	Backup de usuarios	0,98628	0,9246375	0,924638	1,23285	0,98628
	S2	Video vigilancia	1,97256	1,849275	1,849275	2,4657	1,97256
	S3	Virtualización (Servidor Moodle)	1,97256	1,849275	1,849275	2,4657	1,97256
	S4	Correo electrónico Institucional	0,98628	0,9246375	0,924638	1,23285	0,98628
Equipamiento Auxiliar	AUXI	Sistema Eléctrico General	0	0,98628	0,000000	4,9314	0
		Aire Acondicionado (Datacenter)	0	0,24657	0,000000	1,23285	0
		Sistema de Detección de incendios	0	0,49314	0,000000	2,4657	0
		Sistema de primeros Auxilios	0	0,49314	0,000000	2,4657	0
		Fibra óptica	0	0,49314	0,000000	2,4657	0
		Cableado estructurado Oficina	0	0,24657	0,000000	1,23285	0
		Cableado estructurado Salas de informática	0	0,24657	0,000000	1,23285	0
		Cableado estructurado laboratorios	0	0,24657	0,000000	1,23285	0
		Ups Principal	0	0,49314	0,000000	2,4657	0
		Planta Eléctrica	0	0,49314	0,000000	2,4657	0
Personal [P]	P1	Rector	0	0,98628	1,479420	0	0
	P2	Vicerrectorías (5)	0	0,49314	0,739710	0	0
	P3	Gerente Administrativo	0	0,49314	0,739710	0	0
	P4	Decanatura (2)	0	0,49314	0,739710	0	0
	P5	Directores de Programa (6)	0	0,49314	0,739710	0	0
	P6	Director de Extensión	0	0,49314	0,739710	0	0
	P7	Director de Bienestar	0	0,24657	0,369855	0	0
	P8	Director de Investigación	0	0,49314	0,739710	0	0
	P9	Director de Talento Humano	0	0,49314	0,739710	0	0
	P10	Director Contabilidad	0	1,23285	0,739710	2,4657	0
	P11	Asistentes de Secretaria (12)	0	0,616425	0,369855	1,23285	0
	P12	Docentes (156)	0	1,23285	0,739710	2,4657	0
	P13	Coordinador de Tecnología	0	1,23285	0,739710	2,4657	0

	P14	Coordinador Registro y Control	0	1,23285	0,739710	2,4657	0
	P15	Secretaria académica 3)	0	1,23285	0,739710	2,4657	0
	P16	Soporte Técnico 5()	0	1,23285	0,739710	2,4657	0
	P17	Estudiantes (4300)	0	1,23285	0,739710	2,4657	0
	P18	Mercadeo (5)	0	1,23285	0,739710	2,4657	0
	P19	Comunicaciones (2)	0	0,616425	0,369855	1,23285	0
	P20	Personal de Servicios Generales (8)	0	0,616425	0,369855	1,23285	0
	P21	Área de Desarrollo (4)	0	0,616425	0,369855	1,23285	0
	P22	Recepción	0	0,616425	0,369855	1,23285	0
	P23	Auxiliara Administrativo (4)	0	0,616425	0,369855	1,23285	0
	P24	Auxiliar Contabilidad (3)	0	0,616425	0,369855	1,23285	0

Una vez expuestos el nivel de riesgo de todos los activos, se muestra aquellos que superan el nivel MEDIO que serán sobre los que se implante las medidas correctivas.

En la siguiente tabla se muestra el nivel de riesgos que superan el nivel medio.

Tabla 23: Activos que superan el nivel MEDIO.

Tipo de Activo Descripción	ID	ACTIVO	ASPECTOS CRITICOS				
			A	C	I	D	T
Instalaciones [L]	L1	Centro de proceso de Datos	0	0,9246375	0,616425	1,23285	0
	L2	Oficina Director Administrativo	0	0,9246375	0,6164250	1,23285	0
	L3	Oficina Director de Contabilidad	0	3,698550	2,4657	4,9314	0
	L4	Oficina Director de Planeación	0	1,849275	1,23285	2,4657	0
	L5	Oficina Gerencia de Sistemas	0	1,849275	1,23285	2,4657	0
	L6	Oficina de Decanaturas	0	1,849275	1,23285	2,4657	0
	L7	Oficina de Direcciones de Programa	0	3,69855	2,4657	4,9314	0
	L8	Oficina de Rectoría	0	1,849275	1,23285	2,4657	0
	L9	Oficina de Vicerrectoría académica	0	1,849275	1,23285	2,4657	0

	L10	Oficina Recepción	0	0,000012	0,000008	0,000016	0,000000
	L11	Oficina de Calidad	0	0,000012	0,000008	0,000016	0,000000
	L12	Oficina de Investigación	0	0,000000	0,000008	0,000016	0,000000
	L13	Oficina de Proyección Social	0	0,98628	0,000000	4,9314	0
	L14	Oficina de Bienestar Institucional	0	0,24657	0,000000	1,23285	0
	L15	Oficina de Registro y Control	0	0,49314	0,000000	2,4657	0
	L16	Oficina de Mercadeo	0	0,49314	0,000000	2,4657	0
	L17	Sala de Docentes	0	0,49314	0,000000	2,4657	0
	L18	Salas de informática	0	0,24657	0,000000	1,23285	0
	L19	Laboratorios	0	0,24657	0,000000	1,23285	0
Hardware [HW]	HW1	servidor de aplicaciones	0	0,24657	0,000000	1,23285	0
	HW2	Servidor de Bases de Datos	0	0,49314	0,000000	2,4657	0
	HW3	Servidor Telefonía	0	0,49314	0,000000	2,4657	0
	HW4	Servidor Proxy	0	1,23285	0,739710	2,4657	0
	HW5	Servidor Web	0	0,616425	0,369855	1,23285	0
	HW6	Servidor de Dominio	0	1,23285	0,739710	2,4657	0
	HW7	Equipos Sala 1 (30) equipos	0	1,23285	0,739710	2,4657	0
	HW8	Equipos Sala 2 (30) equipos	0	1,23285	0,739710	2,4657	0
	HW9	Equipos Sala 3 (30) equipos	0	1,23285	0,739710	2,4657	0
	HW10	Equipos Sala 4 (30) equipos	0	1,23285	0,739710	2,4657	0
	HW11	Equipos Sala 5 (30) equipos	0	1,23285	0,739710	2,4657	0
	HW12	Equipos Sala docentes 15	0	1,23285	0,739710	2,4657	0
	HW13	Equipos de Oficinas Administrativas 16	0	0,616425	0,369855	1,23285	0
	HW14	Equipos de Laboratorios 120	0	0,616425	0,369855	1,23285	0
	HW15	Equipos de Laboratorios Telecomunicaciones 120	0	0,616425	0,369855	1,23285	0

	HW16	Equipos de Laboratorios Electrónica 1 10	0	0,616425	0,369855	1,23285	0
	HW17	Equipos de Laboratorios Electrónica 1 20	0	0,616425	0,369855	1,23285	0
	HW18	Equipos de Laboratorios electrónica 3 20	0	0,616425	0,369855	1,23285	0
	HW19	Equipos de Laboratorios de Antenas 10	1,23285	1,23285	6,164250	6,5752	0
	HW20	Equipos de Laboratorios de Hardware 20	0	1,849275	1,232850	2,465700	0,000000
Software [SW]	SW1	Windows Server 2012	0	0,924638	0,616425	1,232850	0,000000
	SW2	Office 2013	0	0,924638	0,616425	1,232850	0,000000
	SW3	Sistema Operativo Windows 10	0	0,924638	0,616425	1,232850	0,000000
	SW4	Matlab	0	1,849275	1,232850	2,465700	0,000000
	SW5	Paquect Tracer	0	0,924638	0,616425	1,232850	0,000000
	SW6	Microsoft active Directory	0	0,924638	0,616425	1,232850	0,000000
	SW7	Apache Tomcat	0	0,924638	0,616425	1,232850	0,000000
	SW8	Antivirus	0	0,123285	2,465700	4,931400	0,000000
	SW9	Academusoft	0	0,123285	2,465700	4,931400	0,000000
	SW10	Sistemas de Grados	0	0,061643	1,232850	2,465700	0,000000
	SW11	Sistema de Homologaciones	0	0,061643	1,232850	2,465700	0,000000
	SW12	Moodle	0	0,030821	0,616425	1,232850	0,000000
	SW13	Bibliofus	0	0,061643	1,232850	2,465700	0,000000
	SW14	SSE	0	0,061643	1,232850	2,465700	0,000000
	SW15	Asistencia	0	0,061643	1,232850	2,465700	0,000000
	SW16	Evaluación Docente	0	0,061643	1,232850	2,465700	0,000000
	SW17	Seguimiento Docente	0	0,061643	1,232850	2,465700	0,000000
	SW18	Sistema Presupuesto	0	0,061643	1,232850	2,465700	0,000000

	SW19	Sistema Eventos	0	0,061643	1,232850	2,465700	0,000000
	SW20	Mesa de Ayuda	0	0,061643	1,232850	2,465700	0,000000
	SW21	Ficheros Estadísticos	0	0,061643	1,232850	2,465700	0,000000
	SW22	Gestión de Talento Humano	0	0,061643	1,232850	2,465700	0,000000
	SW23	Helisa	0	0,061643	1,232850	2,465700	0,000000
	SW24	Tutorías	0	0,061643	1,232850	2,465700	0,000000
	SW25	Facturación y Cartera	0	0,061643	1,232850	2,465700	0,000000
Datos[D]	D1	Bases de Datos Administrativos	0	0,061643	1,232850	2,465700	0,000000
	D2	Bases de Datos Estudiantes	0	0,98628	1,479420	0	0
	D3	Bases de Datos Docente	0	0,49314	0,739710	0	0
	D4	Bases de Datos Proveedores, Empresarios	0	0,49314	0,739710	0	0
	D5	Backus generadas de Bases de datos	0	0,49314	0,739710	0	0
	D6	Bases de Datos Correos Institucionales	0	0,49314	0,739710	0	0
	D7	Respaldo de Aplicaciones Institucionales	0	0,49314	0,739710	0	0
	D8	Centro de proceso de Datos	0	0,24657	0,369855	0	0
Redes de comunicaciones [COM]	COM1	Acceso a inter Oficinas (14)	0	0,49314	0,739710	0	0
	COM2	Líneas Telefónicas (24)	0	0,49314	0,739710	0	0
	COM3	Fax	1,849275	2,465700	2,465700	2,465700	1,479420
	COM4	Acceso Inalámbrico (8)	0,000012	0,000016	0,000016	0,000016	0,000010
Servicios (S)	S1	Backup de usuarios	1,849275	2,465700	2,465700	2,465700	1,479420
	S2	Video vigilancia	0,000012	0,000016	0,000016	0,000016	0,000010
	S3	Virtualización (Servidor Moodle)	0,000012	0,000016	0,000016	0,000016	0,000010
	S4	Correo electrónico Institucional	1,849275	2,465700	2,465700	2,465700	1,479420

Equipamiento Auxiliar	AUXI	Sistema Eléctrico General	3,698550	4,931400	4,931400	4,931400	2,958840
		Aire Acondicionado (Datacenter)	1,849275	2,465700	2,465700	2,465700	1,479420
		Sistema de Detección de incendios	1,849275	2,465700	2,465700	2,465700	1,479420
		Sistema de primeros Auxilios	0,924638	1,232850	1,232850	1,232850	0,739710
		Fibra óptica	0,924638	1,232850	1,232850	1,232850	0,739710
		Cableado estructurado Oficina	1,849275	2,465700	2,465700	2,465700	1,479420
		Cableado estructurado Salas de informática	0,000012	0,000016	0,000016	0,000016	0,000010
		Cableado estructurado laboratorios	1,849275	2,465700	2,465700	2,465700	1,479420
		Ups Principal	0,000012	0,000016	0,000016	0,000016	0,000010
		Planta Eléctrica	0,924638	1,232850	1,232850	1,232850	0,739710
Personal [P]	P1	Rector	0,924638	1,232850	1,232850	1,232850	0,739710
	P2	Vicerrectorías (5)	1,849275	2,465700	2,465700	2,465700	1,479420
	P3	Gerente Administrativo	0,000012	0,000016	0,000016	0,000016	0,000010
	P4	Decanatura (2)	0,924638	1,232850	1,232850	1,232850	0,739710
	P5	Directores de Programa (6)	1,849275	2,465700	2,465700	2,465700	1,479420
	P6	Director de Extensión	1,849275	2,465700	2,465700	2,465700	1,479420
	P7	Director de Bienestar	1,849275	2,465700	2,465700	2,465700	1,479420
	P8	Director de Investigación	0,000012	0,000016	0,000016	0,000016	0,000010
	P9	Director de Talento Humano	3,698550	4,931400	4,931400	4,931400	2,958840
	P10	Director Contabilidad	2,465700	2,465700	2,465700	2,465700	1,849275
	P11	Asistentes de Secretaria (12)	4,931400	4,931400	4,931400	4,931400	3,698550
	P12	Docentes (156)	4,931400	4,931400	4,931400	4,931400	3,698550
	P13	Coordinador de Tecnología	4,931400	4,931400	4,931400	4,931400	3,698550
	P14	Coordinador Registro y Control	2,465700	2,465700	2,465700	2,465700	1,849275

	P15	Secretaria académica 3)	2,465700	2,465700	2,465700	2,465700	1,849275
	P16	Soporte Técnico 5()	2,465700	2,465700	2,465700	2,465700	1,849275
	P17	Estudiantes (4300)	2,465700	2,465700	2,465700	2,465700	1,849275
	P18	Mercadeo (5)	2,465700	2,465700	11,095650	13,150400	0,000000
	P19	Comunicaciones (2)	1,232850	1,232850	7,397100	6,575200	0,000000
	P20	Personal de Servicios Generales (8)	0,000016	0,000016	2,465700	3,287600	0,000000
	P21	Área de Desarrollo (4)	0,98628	0,9246375	0,924638	1,23285	0,98628
	P22	Recepción	1,97256	1,849275	1,849275	2,4657	1,97256
	P23	Auxiliara Administrativo (4)	1,97256	1,849275	1,849275	2,4657	1,97256
	P24	Auxiliar Contabilidad (3)	0,98628	0,9246375	0,924638	1,23285	0,98628

Como se evidencia en la tabla anterior la mayoría de los activos de la Fundación Universitaria San Mateo superan el umbral de riegos impuesto por la Dirección, por lo que se debe tomar medidas que mitiguen el nivel de riesgo.

Fase 4: Propuestas de Proyectos

5.1 Introducción

Llegados a este punto, conocemos el nivel de riesgo actual en la Fundación Universitaria San Mateo, a lo relativo a los riesgos residuales a los que están expuestos, por lo cual deben plantearse proyectos que ayuden a alcanzar los niveles de seguridad que se necesiten con prioridad.

Los proyectos a trabajar a continuación son el resultado del análisis de riesgos elaborado para la Fundación Universitaria San Mateo, por tanto se plantearán proyectos en el cual se le dé prioridad a los riesgos que más impacto tiene para la Fundación Universitaria San Mateo.

5.2 Propuestas

5.2.1 Formación al personal Administrativo en seguridad informática	
Objetivo	El objetivo de este proyecto es implantar un plan de formación para concienciar a los empleados de la Fundación Universitaria San Mateo de la importancia de la seguridad de la información para el correcto funcionamiento de los procesos en los que estén involucrados.
Descripción	Con este proyecto se pretende que los empleados reciban formación y capacitación en materia de seguridad de la información para el uso de los recursos y activos a los que tienen acceso en el desempeño de sus funciones. Se trabajarán los siguientes puntos • Socialización Políticas de seguridad. • Requisitos de seguridad y responsabilidad legal • Procesos disciplinarios de las políticas de seguridad • Formación sobre amenazas y su mitigación • Protocolos de actuación en caso de incidencia o eventos que involucren un activo de la institución. • Canales seguros de comunicación • Uso de contraseñas • Equipos de usuarios desatendido, políticas de escritorio despejado
Planificación	El curso se impartirá a todos los administrativos y académicos de la institución repartida en tres sesiones al año de una semana de duración para adaptarse a la disponibilidad de los empleados. Esta formación será realizada en una sala de informática. En el mes de Mayo, Agosto y Noviembre para un total de horas de 64.
Costos asociados	$ 4.442.300 Para las tres sesiones Mayo, Agosto y Noviembre.
Indicador	Personal [P](P1, P2, P4, P5, P6, P7, P9, P10, P11, P122, P13, P14, P15, P16, P17, P18, P19, P20, P21, P22, P23, P24)
Beneficios	• Disminución de los incidentes de seguridad • Optimización del uso de los recursos • Mejora de la imagen corporativa • Incremento de calidad en seguridad por parte de la Institución
Activos Involucrados	• Rector, vicerrectorías, Gerente administrativo, directores de programa, dirección de extensión, bienestar, investigación, talento humano, contabilidad, docentes, tecnología, registro control secretaria académica, soporte técnico mercadeo, estudiantes, comunicaciones, recepción auxiliar administrativo y de contabilidad
Controles de la ISO 27001	• 5.1 Compromiso con la dirección (a,b,c,d,e,f,g,h) • 5.2.1 Gestión de los recursos (a,b,c,d,e,f,) • 5.2.2 formación, sensibilización y competencia (a,b,c,d)
Dimensiones de riesgo mitigadas	• [I] Integridad • [D] Disponibilidad • [A] Autenticidad
Responsable	• Director de Seguridad

	• Docente especialista en Seguridad

5.2.2 Instalaciones [L] Lugares donde se hospedan los sistemas de información y comunicaciones	
Objetivo	Evitar pérdida, daño, robo o puesta en peligro de los activos y la interrupción de las actividades de la organización.
Descripción	Con este proyecto se pretende trabajar las siguientes • Ubicación y protección de los Equipos • Servicio de suministro de energía • Seguridad del cableado • Mantenimiento de los Equipos • Seguridad de los equipos fuera de las Instalaciones • Seguridad en la reutilización o eliminación de equipos • Retiro de activos
Planificación	Para este proyecto se pretende trabajar en 6 meses (Iniciarán la ejecución en el mes de mayo y finalizara en el mes de Noviembre).
Costos asociados	$ 34.200.000 Asociado al pago de un ingeniero Electricista, ingeniero de sistemas y Materiales.
Indicador	Instalaciones [L] (L1, L2, L3, L4, L5, L6, L7, L8, L9, L13, L14, L15, L15, L17, L18 Y L19)
Beneficios	Reducir el riesgos debido a amenazas o peligros del entorno, acceso no autorizados, fallas de suministro de energía, protección a cableado de comunicación y de energía ante cualquier daño o interceptación, mantenimiento adecuado a equipos para su continua disponibilidad e integridad, evitar perdida de información y controlar la salida de equipos fuera de la Institución, Bakups de información y eliminación de información equipos que ya no se usan.
Activos Involucrados	Centro de proceso de Datos, director administrativo, contabilidad, planeación, gerencia de sistemas, Decanaturas, directores de programa, rectoría, vicerrectoría, recepción, calidad, investigación, proyección social, bienestar, registro y control, mercadeo Docentes, salas de informática y laboratorios.
Dimensiones de riesgo mitigadas	• [C] Confidencialidad • [I] Integridad • [D] Disponibilidad • [A] Autenticidad • [T] Trazabilidad
Controles de la ISO 27001	• A.5 Políticas de seguridad de la información • A.8 Gestión de los activos • A.9 Controles de Acceso • A.11 Seguridad Física y del Entorno
Responsable	Ingeniero Electricista, Ingeniero de Sistemas

5.2.3 Hardware [HW] Los medios materiales, físicos, destinados a soportar directa o indirectamente los servicios que presta la organización.	
Objetivo	Lograr y mantener la protección adecuada de los activos organizacionales

Descripción	Este proyecto busca mantener la protección adecuado en cuanto a los siguientes aspectos. • Inventario de activo • Propiedad de los activos • Uso aceptable de los activos • Etiqueta y manejo de información • Directrices de Clasificación
Planificación	1 año, se iniciaran actividades en el mes de Mayo, bajo la dirección de la coordinación de Sistemas y un practicante hasta el mes de Diciembre.
Costos asociados	$ 18.400.000,00 Asociados al pago de la coordinación de Soporte Tecnológico Y un practicante de apoyo.
Indicador	Hardware [HW] (HW1, HW2, HW3, HW4 ,HW5, HW5, HW7, HW8, HW9, HW10, HW11, HW12, HW13, HW14, HW15, HW16, HW17, HW18, HW19, HW20)
Beneficios	Todos los activos deben estar claramente identificados y se deben elaborar y mantener un inventario de todos los activos importantes, deben estar marcado como propiedad de un área de la Institución, todos los activos se deben identificar, documentar e implementar las reglas sobre el uso aceptable de la información y los activos asociados con los servicios de procesamiento de información, los activos se deben clasificar en términos de valor, de regiquistos legales, de la sensibilidad y la importancia, se deben implantar procedimientos adecuados para el etiquetado y el manejo de la información de acuerdo al esquema de clasificación adoptado por la Institución.
Activos Involucrados	Centro de procesos de datos, oficinas de Director administrativo, contabilidad, planeación, gerencia de sistemas direcciones de programas, rectoría vicerrectorías, recepción, calidad investigación, proyección social, bienestar, registro y control, mercadeo, docente, salas de informática y laboratorios
Controles de la ISO 27001	• A.8 Gestión de Activos • A.9 Control de Acceso • A.11 Seguridad Física y del Entorno
Dimensiones de riesgo mitigadas	• C] Confidencialidad • [I] Integridad • [D] Disponibilidad • [A] Autenticidad
Responsable	Coordinador de Soporte Tecnológico, Practicante de sistemas

5.2.4 Software [SW] Tareas que han sido automatizadas para su desempeño por un equipo informático. Las aplicaciones gestionan, analizan y transforman los datos permitiendo la explotación de la información para la prestación de servicios.	
Objetivo	Evitar el acceso no autorizado a la información contenida en los sistemas de Información, software, evitar errores, perdidas, modificaciones no autorizados o uso de la información en las aplicaciones.
Descripción	Este proyecto busca la implementación en cuanto a la restricción de acceso a la información, aislamiento de sistemas sensibles, controles contra códigos maliciosos. Políticas, procedimientos y acuerdos para el intercambio de software, validación de los datos de entrada, control de procedimiento internos,

	control de software operativo, protección de datos de prueba del sistema, control de acceso al código fuente de los programas
Planificación	Este proyecto se ejecutará en 6 meses, habrá un responsable de seguridad para
Costos asociados	**$16.800.000** Este dinero será empleado para el sueldo durante los 7 meses del proyecto a un especializasta en seguridad informática.
Indicador	Software [SW] (SW1, SW2, SW3, SW4 ,SW5, SW5, SW7, SW8, SW9, SW10, SW11, SW12, SW13, SW14, SW15, SW16, SW17, SW18, SW19, SW20, SW21, SW22, SW23, W24, SW25)
Beneficios	Se deben implantar controles detección de prevención y recuperación para proteger contra código malicioso, así como procedimientos apropiados de concientización de los usuarios, se debe restringir el acceso a la información y a las funciones del sistemas de aplicación por parte de los usuarios y del personal de soporte, de acuerdo con la política definida en el control de acceso, los sistemas sensibles deben tener un entorno informático dedicado, se deben implementar procedimientos para controlar la instalación de software en sistemas operativos, restricción al código fuente de los programas.
Activos Involucrados	Windows server 2012, office, sistema operativos, active directory, tomcat, antivirus, academusoft, sistemas de grado, sistema homologantes, Moodle, bibliofus, sse, asistencia, evaluación docente, sistema de presupuesto, eventos, mesa de ayuda, ficheros estadísticos, gestión talento humano helisa, tutorías, facturación y cartera.
Controles de la ISO 27001	• A.6 Organización de la seguridad de la información • A.12 Seguridad en las comunicaciones • A.17 Gestión de incidentes de la seguridad en la información
Dimensiones de riesgo mitigadas	• C] Confidencialidad • [I] Integridad • [D] Disponibilidad • [A] Autenticidad
Responsable	Ingeniero de sistemas / Conocimientos amplios en seguridad

5.2.5 Redes de comunicaciones [COM] Son los medios de transporte que llevan datos de un sitio a otro. Se incluyen tanto instalaciones dedicadas como servicios de comunicaciones contratados a terceros	
Objetivo	Asegurar la protección de la información en las redes y la protección de la Infraestructura de soporte.
Descripción	Este proyecto busca controlar toda la red de datos de la institución, seguridad de los servicios de red, certificación general del cableado alámbrico y actualización de la red wifi.
Planificación	Este proyecto se trabajara en 4 meses. Iniciando en el mes de Agosto.
Costos asociados	$12.000.000 estos costos son para un proveedor externo que va a trabajar en la certificación de la red y actualización de la red wifi.
Indicador	Redes de comunicaciones [COM] (COM1, COM2, COM3, COM4)

Controles de la ISO 27001	• A.8 Gestión de los activos • A.9 Controles de Acceso • A.11 Seguridad Física y del Entorno
Beneficios	Las redes deben mantener y controlar adecuadamente para protegerlas de las amenazas y mantener la seguridad de los sistemas y aplicaciones que usan la red, incluyendo la información en tránsito, se debe trabajar en los servicios de red y los requisitos de gestión de todos los servicios de la red, sin importar si los servicios s presentan en la organización o se contratan externamente.
Activos Involucrados	Acceso a internet de las oficinas, líneas telefónicas, fax, acceso inalámbrico.
Dimensiones de riesgo mitigadas	• C] Confidencialidad • [I] Integridad • [D] Disponibilidad • [A] Autenticidad • [T] Trazabilidad
Responsable	Proveedor de externo

5.2.6 Datos[D] La información que permite a la organización prestar sus servicios

Objetivo	Garantizar la seguridad de los archivos del sistema, mejorar la integridad y confidencialidad de la información de los activos de los empleados.
Descripción	Se desea cifrar la información base a: • Cifrado de los datos alojados en los discos duros de los PC's de los empleados • Cifrado de la información de los datos de los móviles de los empleados según SO que corresponda (Android o IOS) • Cifrado de los datos almacenados en la cabina habilitando una licencia del fabricante habilitado para ello. • Cifrado de la comunicación entres sistemas desplegados en las plantas y los servidores mediante el uso de certificados SSL.
Planificación	Este proyecto se trabajará en 8 meses
Costos asociados	Cifrado de las comunicaciones $ 1.000.000,00 Anuales para habilitar la opción de cifrado en el proveedor del servicio de alta disponibilidad. $ 2.000.000,00 Jornadas del departamento TI y desarrollo $ 2.000.000,00 Anuales en licencias de cifrado de cabina $ 2.000.000,00
Indicador	• Datos[D] (D1, D2, D3, D4, D5, D6, D7, D8)
Controles de la ISO 27001	• A.6. Organización de la seguridad en la información • A.10 Criptografía • A.11 Seguridad Física y del Entorno • A.13 Seguridad en las comunicaciones • A.17 Aspectos de la seguridad en la información de la gestión de la continuidad del negocio

Beneficios	Se deben identificar los requisitos para asegurar la autenticidad y proteger la integridad del mensaje en las aplicaciones, así como identificar e implementarlos controles adecuados, Se deben validar los datos de salida de una aplicación para asegurar que el procesamiento de la información almacenada es correcto y adecuado a las circunstancias.
Activos Involucrados	• Bases de datos de: Administrativos, estudiantes, docentes, proveedores, empresarios, correos institucionales, aplicaciones, centro de procesamiento de datos
Dimensiones de riesgo mitigadas	• C] Confidencialidad • [I] Integridad • [D] Disponibilidad • [A] Autenticidad • [T] Trazabilidad
Responsable	Departamento de Sistemas (coordinador, proveedores).

5.2.7 **Equipamiento Auxiliar (Auxi), SERVICIOS (S)Seguridad Física Y Del Entorno**	
Objetivo	Evitar el acceso físico no autorizado, el daño e interferencia a las instalaciones y a la información de la organización, evitar pérdida, daño, robo o puesta en peligro de los activos y la interrupción de las actividades de la organización.
Descripción	Este proyecto busca mejorar los perímetros de seguridad física, controles de acceso físico, seguridad en oficinas recinto e instalaciones, protección contra amenazas externas y ambientales, trabajo en áreas seguras, áreas de carga, despacho y acceso público, ubicación y protección de los equipos, servicios de suministro, seguridad en los equipos.
Planificación	El proyecto se ejecutara en 8 meses,
Costos asociados	Empresa de Seguridad, Personal de Mantenimiento e infraestructura $ 2.000.000,00 Equipos de video vigilancia $ 5.000.000,00 Medidas de seguridad perimetral e interna $ 2.000.000,00 Actualización Controles de acceso $ 4.000.000,00
Indicador	Servicios (S) y Equipamiento Auxiliar (AUXI)
Beneficios	Se deben utiliza perímetros de seguridad (barreras tales como paredes, puertas acceso controladas con tarjeta, o mostradores de recepción, huellero al ingreso de la institución oficinas, controles de acceso apropiados para asegurar que solo se permite al personal autorizado, seguridad física para oficina recintos e instalaciones, protecciones físicas contra daños por incendio, inundación, terremoto, explosión, manifestaciones sociales u otras formas de desastre natural o artificial, se debe diseñar y aplicar protección física y las directrices para trabajar en áreas seguras, los puntos de acceso tales como aras de carga y despacho y otros puntos por donde pueda ingresar el personal no autorizado a las instalaciones se deben controlar y si es posible aislar de los servicios de procesamiento de información para evitar el acceso no autorizado, los equipos deben estar ubicados o protegidos para reducir el riego debido a amenazas o peligros del entorno, el cableado debe estar protegido contra interceptaciones, seguridad en los equipos fuera de las instalaciones, controles para sacar e ingresar equipos a la institución

Activos Involucrados	Equipamiento Auxiliar (AUXI): Sistemas Eléctrico general, aire acondicionado, sistema de detección de incendios, sistemas de primeros auxilios, fibra óptica, cableado estructurado de oficinas, salas y laboratorios, Ups y planta eléctrica Servicios (S): Backups de usuarios, infraestructura
Controles de la ISO 27001	• A.8 Gestión de los Activos • A.9 Control de Acceso • A.12. Seguridad en las Operaciones • A.11 Seguridad Física y del Entorno • A.13 Seguridad en las comunicaciones
Dimensiones de riesgo mitigadas	• C] Confidencialidad • [I] Integridad • [D] Disponibilidad • [A] Autenticidad • [T] Trazabilidad
Responsable	Empresa de Seguridad, Personal de Mantenimiento e infraestructura

5.3 Resultados

En este punto se muestra la planificación temporal para 8 meses para los proyectos definidos en el apartado anterior, estos proyectos esta alineados con el análisis de riegos y la identificación del nivel de Madurez en seguridad de la información para la Fundación Universitaria San Mateo.

PROYECTOS PLANTEADOS (Fundación Universitaria San Mateo)												
No	**PROYECTOS**	**RESPONSABLE**	**Presupuesto**	**2018-1**		**2018-2**						
				MAY	**JUN**	**JUL**	**AGOS**	**SEP**	**OCT**	**NOV**	**DIC**
1	**5.2.1** Personal [P] Formación al personal Administrativo en seguridad informática	• Director de Seguridad • Docente especialista en Seguridad	**$ 4.442.300,00**								
2	**5.2.2** Instalaciones [L] lugares donde se hospedan los sistemas de información y comunicaciones	Ingeniero Electricistas, ingeniero de Sistema	**$ 34.200.000,00**								
3	**5.2.3** Hardware [HW] Los medios materiales, físicos, destinados a soportar directa o indirectamente los servicios que presta la organización.	Coordinador de Soporte Tecnológico, Practicante de sistemas	**$ 18.400.000,00**								
4	**5.2.4** Software [SW] Tareas que han sido automatizadas para su desempeño por un equipo informático. Las aplicaciones gestionan, analizan y transforman los datos permitiendo la explotación de la	Ingeniero de sistemas / Conocimientos amplios en seguridad	**$ 16.800.000,00**								

	información para la prestación de servicios.										
5	**5.2.5** Redes de comunicaciones [COM] Son los medios de transporte que llevan datos de un sitio a otro. Se incluyen tanto instalaciones dedicadas como servicios de comunicaciones contratados a terceros	Proveedor de externo	**$ 12.000.000,00**								
6	5.**2.6** Datos[D] La información que permite a la organización prestar sus servicios	Departamento de Sistemas (coordinador, proveedores)	**$ 56.000.000,00**								
7	**5.2.7** Equipamiento Auxiliar (Auxi), SERVICIOS (S)Seguridad Física Y Del Entorno	Empresa de Seguridad, Personal de Mantenimiento e infraestructura	**$ 27.000.000,00**								

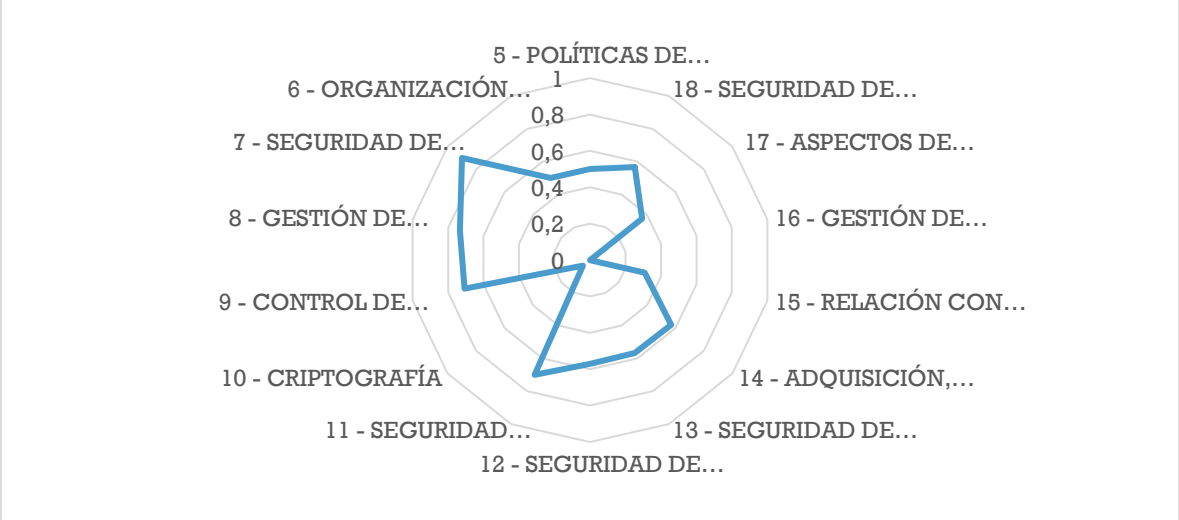
Para definir los proyectos propuestos en esta fase de Plan director de seguridad en la Fundación Universitaria san Mateo se realizó un análisis diferencial en los dominios de la ISO/IEC 27002:2013, donde se refleja la situación actual y el nivel de madurez de la institución,

Tabla 24: Resumen de cumplimiento de los dominios.

Dominio	% de Efectividad	# NC Mayores	# NC Menores	Control OK
5 - POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN	50%	0	2	0
6 - ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	50%	2	5	0
7 - SEGURIDAD DE LOS RECURSOS HUMANOS	90%	0	6	0
8 - GESTIÓN DE ACTIVOS	73%	0	10	0
9 - CONTROL DE ACCESO	71%	1	7	6
10 - CRIPTOGRAFÍA	5%	2	0	0
11 - SEGURIDAD FÍSICA Y DEL ENTORNO	70%	1	11	3
12 - SEGURIDAD DE LAS OPERACIONES	57%	3	11	0
13 - SEGURIDAD DE LAS COMUNICACIONES	57%	1	6	0
14 - ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	57%	1	12	0
15 - RELACIÓN CON LOS PROVEEDORES	31%	2	3	0
16 - GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	0%	1	6	0
17 - ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTION DE CONTINUIDAD DE NEGOCIO	37%	2	2	0
18 - SEGURIDAD DE LAS COMUNICACIONES	57%	1	7	0

En la tabla anterior podemos identificar un resumen de los 114 controles de la Norma ISO/IEC 27002:2013 para la Fundación Universitaria san Mateo.

Ilustración 17: Evaluación de Madurez respecto a los controles ISO/IEC 27002:2013.



Fase 5: 6 Auditoría de Cumplimiento

6.1 Introducción

Llegados a esta fase, hemos realizado un inventario de activos de la institución, y hemos valorado y evaluado las amenazas, se ha realizado un análisis de riesgos y hemos planteado proyectos para su mitigación,

Teniendo en cuenta los aspectos anteriores es el momento de evaluar hasta qué punto la Fundación Universitaria San Mateo cumple con los apartados de 4 al 10 de la Norma ISO/IEC 27001:2013 y verificar las buenas practicas establecidas en la Norma ISO 27002:2013 que servirá como marco de control del estado de la seguridad.

6.2 Metodología

Para evaluar correctamente la madurez de la seguridad de la información de la Fundación Universitaria San Mateo, se va a realizar una auditoria contra La norma ISO/IEC 27001:2013 evaluando los apartados del 4 al 10 y estándar ISO/IEC 27002:2013, en el cual agrupa un total de 114 controles o salvaguardas sobre buenas prácticas para la Gestión de la Seguridad de la Información organizado en 14 dominios y 35 objetivos de control. Éste estándar es internacionalmente reconocido y es perfectamente válido para la mayoría de organizaciones.

Hay diferentes aspectos en los cuales las salvaguardas actúan reduciendo el riesgo, ya hablemos de los controles ISO/IEC 27002:2013 o de cualquier otro catálogo. Estos son en general:

- Formalización de las prácticas mediante documentos escritos o aprobados.
- Política de personal.
- Solicitudes técnicas (software, hardware o comunicaciones).
- Seguridad física.

La protección integral frente a las posibles amenazas, requiere de una combinación de salvaguardas sobre cada uno de estos aspectos.(“TFM_SGSI_CASTPEC1,”)

En la siguiente tabla podemos ver los distintos niveles como recordatorio.

Tabla 25 Modelo de Madurez de la Capacidad (CMM)

Valor	Efectividad	Significado	Descripción
L0	0%	Inexistente	Carencia completa de cualquier proceso conocido.
L1	10%	Inicial / Ad-hoc	Procedimientos inexistentes o localizados en áreas concretas. El éxito de las tareas se debe a esfuerzos personales.
L2	50%	Reproducible, pero intuitivo	Existe un método de trabajo basado en la experiencia, aunque sin comunicación formal. Dependencia del conocimiento individual
L3	90%	Proceso definido	La organización en su conjunto participa en el proceso. Los procesos están implantados, documentados y comunicados.
L4	95%	Gestionado y medible	Se puede seguir la evolución de los procesos mediante indicadores numéricos y estadísticos. Hay herramientas para mejorar la calidad y la eficiencia
L5	100%	Optimizado	Los procesos están bajo constante mejora. En base a criterios cuantitativos se determinan las desviaciones más comunes y se optimizan los procesos
L6	N/A	No aplica	

6.3 Evaluación de la madurez ISO/IEC 27001:2013

A continuación se muestra el nivel de madurez adquirido durante la implementación respecto al GAP inicial

			ESTADO INICIAL ANTES DE LA IMPLEMENTACION	RESULTADO DE PRIMERA AUDITORIA
4	**CONTEXTO DE LA ORGANIZACIÓN**			
4.1	**CONOCIMIENTO DE LA ORGANIZACIÓN Y DE SU CONTEXTO**	La organización debe determinar las cuestiones externas e internas que son pertinentes para su propósito y que afectan su capacidad para lograr los resultados previstos de su sistema de gestión de la seguridad de la información.	No cumple	Cumple parcialmente
4.2	**COMPRENSIÓN DE LAS NECESIDADES Y EXPECTATIVAS DE LAS PARTES INTERESADAS**	La organización debe determinar: a) las partes interesadas que son pertinentes al sistema de gestión de la seguridad de la información; y b) los requisitos de estas partes interesadas pertinentes a seguridad de la información.	Cumple parcialmente	Cumple satisfactoriamente
4.3	**DETERMINACIÓN DEL ALCANCE DEL SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN**	La organización debe determinar los límites y la aplicabilidad del sistema de gestión de la seguridad de la información para establecer su alcance. Cuando se determina este alcance, la organización debe considerar: a) las cuestiones externas e internas referidas en el numeral 4.1, y b) los requisitos referidos en el numeral 4.2; y c) las interfaces y dependencias entre las actividades realizadas por la organización, y las que realizan otras organizaciones. El alcance debe estar disponible como información documentada.	No cumple	Cumple satisfactoriamente
4.4	**SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN**	La organización debe establecer, implementar, mantener y mejorar continuamente un sistema de	No cumple	Cumple satisfactoriamente

		gestión de la seguridad de la información, de acuerdo con los requisitos de esta Norma.		
5	**LIDERAZGO**			
5.1	**LIDERAZGO Y COMPROMISO**	La alta dirección debe demostrar liderazgo y compromiso con respecto al sistema de gestión de la seguridad de la información: a) asegurando que se establezcan la política de la seguridad de la información y los objetivos de la seguridad de la información, y que estos sean compatibles con la dirección estratégica de la organización; b) asegurando la integración de los requisitos del sistema de gestión de la seguridad de la información en los procesos de la organización; c) asegurando que los recursos necesarios para el sistema de gestión de la seguridad de la información estén disponibles; d) comunicando la importancia de una gestión de la seguridad de la información eficaz y de la conformidad con los requisitos del sistema de gestión de la seguridad de la información; e) asegurando que el sistema de gestión de la seguridad de la información logre los resultados previstos; f) dirigiendo y apoyando a las personas, para contribuir a la eficacia del sistema de gestión de la seguridad de la información; g) promoviendo la mejora continua, y h) apoyando otros roles pertinentes de la dirección, para demostrar su liderazgo aplicado a sus áreas de responsabilidad.	Cumple parcialmente	Cumple satisfactoriamente

5.2	**POLÍTICA**	La alta dirección debe establecer una política de la seguridad de la información que: a) sea adecuada al propósito de la organización; b) incluya objetivos de seguridad de la información (véase el numeral 6.2) o proporcione el marco de referencia para el establecimiento de los objetivos de la seguridad de la información; c) incluya el compromiso de cumplir los requisitos aplicables relacionados con la seguridad de la información; y d) incluya el compromiso de mejora continua del sistema de gestión de la seguridad de la información. La política de la seguridad de la información debe: e) estar disponible como información documentada; f) comunicarse dentro de la organización; y g) estar disponible para las partes interesadas, según sea apropiado.	Cumple parcialmente	Cumple satisfactoriamente
5.3	**ROLES, RESPONSABILIDADES Y AUTORIDADES EN LA ORGANIZACIÓN**	La alta dirección debe asegurarse de que las responsabilidades y autoridades para los roles pertinentes a la seguridad de la información se asignen y comuniquen. La alta dirección debe asignar la responsabilidad y autoridad para: a) asegurarse de que el sistema de gestión de la seguridad de la información sea conforme con los requisitos de esta Norma; b) informar a la alta dirección sobre el desempeño del sistema de gestión de la seguridad de la información.	No cumple	Cumple satisfactoriamente
6	**POLITICA**			
6.1	**ACCIONES PARA TRATAR RIESGOS Y OPORTUNIDADES**	6.1.1 Generalidades 6.1.2 Valoración de riesgos de la seguridad de la información 6.1.3 Tratamiento de riesgos de la seguridad de la información	No cumple	Cumple parcialmente

6.2	**OBJETIVOS DE SEGURIDAD DE LA INFORMACIÓN Y PLANES PARA LOGRARLOS**	La organización debe establecer los objetivos de seguridad de la información en las funciones y niveles pertinentes. Los objetivos de seguridad de la información deben: a) ser coherentes con la política de seguridad de la información; b) ser medibles (si es posible); c) tener en cuenta los requisitos de la seguridad de la información aplicables, y los resultados de la valoración y del tratamiento de los riesgos; d) ser comunicados; y e) ser actualizados, según sea apropiado. La organización debe conservar información documentada sobre los objetivos de la seguridad de la información. Cuando se hace la planificación para lograr sus objetivos de la seguridad de la información, la organización debe determinar: f) lo que se va a hacer; g) que recursos se requerirán; h) quién será responsable; i) cuándo se finalizará; y j) cómo se evaluarán los resultados.	No cumple	Cumple parcialmente
7	**SOPORTE**			
7.1	**RECURSOS**	La organización debe determinar y proporcionar los recursos necesarios para el establecimiento, implementación, mantenimiento y mejora continua del sistema de gestión de la seguridad de la información.	Cumple parcialmente	Cumple satisfactoriamente

7.2	**COMPETENCIA**	La organización debe: a) determinar la competencia necesaria de las personas que realizan, bajo su control, un trabajo que afecta su desempeño de la seguridad de la información, b) asegurarse de que estas personas sean competentes, basándose en la educación, formación o experiencia adecuadas; c) cuando sea aplicable, tomar acciones para adquirir la competencia necesaria y evaluar la eficacia de las acciones tomadas; y d) conservar la información documentada apropiada, como evidencia de la competencia.	No cumple	Cumple parcialmente
7.3	**TOMA DE CONCIENCIA**	Las personas que realizan el trabajo bajo el control de la organización deben tomar conciencia de: a) la política de la seguridad de la información; b) su contribución a la eficacia del sistema de gestión de la seguridad de la información, incluyendo los beneficios de una mejora del desempeño de la seguridad de la información; c) las implicaciones de la no conformidad con los requisitos del sistema de gestión de la seguridad de la información.	Cumple parcialmente	Cumple satisfactoriamente
7.4	**COMUNICACIÓN**	La organización debe determinar la necesidad de comunicaciones internas y externas pertinentes al sistema de gestión de la seguridad de la información, que incluyan: a) el contenido de la comunicación; b) cuándo comunicar; c) a quién comunicar; d) quién debe comunicar; y e) los procesos para llevar a cabo la comunicación.	Cumple parcialmente	Cumple satisfactoriamente

7.5	**INFORMACIÓN DOCUMENTADA**	*El sistema de gestión de la seguridad de la información de la organización debe incluir: a) la información documentada requerida por esta Norma; b) la información documentada que la organización ha determinado que es necesaria para la eficacia del sistema de gestión de la seguridad de la información. *Creación y actualización *Control de la información documentada	Cumple parcialmente	Cumple satisfactoriamente
8	**OPERACIÓN**			
8.1	**PLANIFICACIÓN Y CONTROL OPERACIONAL**	La organización debe planificar, implementar y controlar los procesos necesarios para cumplir los requisitos de seguridad de la información y para implementar las acciones determinadas en el numeral 6.1. La organización también debe implementar planes para lograr los objetivos de la seguridad de la información determinados en el numeral 6.2.	No cumple	Cumple satisfactoriamente
8.2	**VALORACIÓN DE RIESGOS DE LA SEGURIDAD DE LA INFORMACIÓN**	La organización debe llevar a cabo valoraciones de riesgos de la seguridad de la información a intervalos planificados o cuando se propongan u ocurran cambios significativos, teniendo en cuenta los criterios establecidos en el numeral 6.1.2 a). La organización debe conservar información documentada de los resultados de las valoraciones de riesgos de la seguridad de la información.	No cumple	Cumple parcialmente
8.3	**TRATAMIENTO DE RIESGOS DE LA SEGURIDAD DE LA INFORMACIÓN**	La organización debe implementar el plan de tratamiento de riesgos de la seguridad de la información. La organización debe conservar información documentada de los resultados del tratamiento de riesgos de la seguridad de la información.	No cumple	Cumple parcialmente

9	EVALUACIÓN DEL DESEMPEÑO			
9.1	SEGUIMIENTO, MEDICIÓN, ANÁLISIS Y EVALUACIÓN	La organización debe determinar: a) a qué es necesario hacer seguimiento y qué es necesario medir, incluidos los procesos y controles de la seguridad de la información; b) los métodos de seguimiento, medición, análisis y evaluación, según sea aplicable, para asegurar resultados válidos; NOTA Para ser considerados válidos, los métodos seleccionados deberían producir resultados comparables y reproducibles. c) cuándo se deben llevar a cabo el seguimiento y la medición; d) quién debe llevar a cabo el seguimiento y la medición; e) cuándo se deben analizar y evaluar los resultados del seguimiento y de la medición; y f) quién debe analizar y evaluar estos resultados	No cumple	Cumple parcialmente
9.2	AUDITORÍA INTERNA	La organización debe llevar a cabo auditorías internas a intervalos planificados, para proporcionar información acerca de si el sistema de gestión de la seguridad de la información: a) es conforme con: 1) los propios requisitos de la organización para su sistema de gestión de la seguridad de la información; y 2) los requisitos de esta Norma; b) está implementado y mantenido eficazmente. La organización debe: c) planificar, establecer, implementar y mantener uno o varios programas de auditoría que incluyan la frecuencia, los métodos, las responsabilidades, los requisitos de planificación, y la elaboración de informes. Los programas de auditoría deben tener en cuenta la importancia de los procesos involucrados y los resultados de las auditorías previas; d) para cada auditoría, definir los criterios y el alcance de ésta; e) seleccionar los auditores y llevar a	No cumple	Cumple parcialmente

		cabo auditorías para asegurarse de la objetividad y la imparcialidad del proceso de auditoría; f) asegurarse de que los resultados de las auditorías se informan a la dirección pertinente; y g) conservar información documentada como evidencia de la implementación del programa de auditoría y de los resultados de ésta.		
9.3	**REVISIÓN POR LA DIRECCIÓN**	La alta dirección debe revisar el sistema de gestión de la seguridad de la información de la organización a intervalos planificados, para asegurarse de su conveniencia, adecuación y eficacia continuas. La revisión por la dirección debe incluir consideraciones sobre: a) el estado de las acciones con relación a las revisiones previas por la dirección; b) los cambios en las cuestiones externas e internas que sean pertinentes al sistema de gestión de la seguridad de la información; c) retroalimentación sobre el desempeño de la seguridad de la información, incluidas las tendencias relativas a: 1) no conformidades y acciones correctivas; 2) seguimiento y resultados de las mediciones; 3) resultados de la auditoría; 4) cumplimiento de los objetivos de la seguridad de la información; d) retroalimentación de las partes interesadas; e) resultados de la valoración de riesgos y estado del plan de tratamiento de riesgos; y	No cumple	Cumple parcialmente

		f) las oportunidades de mejora continua. Los elementos de salida de la revisión por la dirección deben incluir las decisiones relacionadas con las oportunidades de mejora continua y cualquier necesidad de cambio en el sistema de gestión de la seguridad de la información. La organización debe conservar información documentada como evidencia de los resultados de las revisiones por la dirección.		
10	**MEJORA**			
10.1	**NO CONFORMIDADES Y ACCIONES CORRECTIVAS**	Cuando ocurra una no conformidad, la organización debe: a) reaccionar ante la no conformidad, y según sea aplicable 1) tomar acciones para controlarla y corregirla, y 2) hacer frente a las consecuencias; b) evaluar la necesidad de acciones para eliminar las causas de la no conformidad, con el fin de que no vuelva a ocurrir ni ocurra en otra parte, mediante: 1) la revisión de la no conformidad 2) la determinación de las causas de la no conformidad, y 3) la determinación de si existen no conformidades similares, o que potencialmente podrían ocurrir; c) implementar cualquier acción necesaria; d) revisar la eficacia de las acciones correctivas tomadas, y e) hacer cambios al sistema de gestión de la seguridad de la información, si es necesario. Las acciones correctivas deben ser apropiadas a los efectos de las no conformidades encontradas. La organización debe conservar información documentada adecuada, como evidencia de: f) la naturaleza	No cumple	Cumple parcialmente

		de las no conformidades y cualquier acción posterior tomada; y g) los resultados de cualquier acción correctiva.		
10.2	**MEJORA CONTINUA**	La organización debe mejorar continuamente la conveniencia, adecuación y eficacia del sistema de gestión de la seguridad de la información.	No cumple	Cumple parcialmente

Fuente: NTC-ISO-IEC 27001:2013
file:///C:/Users/Dir%20comercio/Downloads/document.pdf

6.4 Evaluación de la madurez ISO/IEC 27002:2013

El objetivo de esta fase del proyecto es evaluar la madurez de la seguridad de la Fundación Universitaria San Mateo en lo que respecta a los diferentes dominios de control y los 114 controles planteados por la ISO/IEC 27002:2013. Antes de abordar este aspecto se buscará profundizar al máximo en el conocimiento de la organización.

De forma resumida, los dominios que deben analizarse son:

Dominio
5 - POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN
6 - ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN
7 - SEGURIDAD DE LOS RECURSOS HUMANOS
8 - GESTIÓN DE ACTIVOS
9 - CONTROL DE ACCESO
10 - CRIPTOGRAFÍA
11 - SEGURIDAD FÍSICA Y DEL ENTORNO
12 - SEGURIDAD DE LAS OPERACIONES
13 - SEGURIDAD DE LAS COMUNICACIONES
14 - ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS
15 - RELACIÓN CON LOS PROVEEDORES
16 - GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN
17 - ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTION DE CONTINUIDAD DE NEGOCIO
18 - SEGURIDAD DE LAS COMUNICACIONES

A continuación, se presenta en la siguiente tabla los resultados de la auditoria de los 114 controles de la norma ISO/IEC 27002:2013

Control en la Normativa ISO 27002	Sección	Control	% de cumplimiento	Cumplimiento
5	**POLÍTICA DE SEGURIDAD**			
5.1	**Directrices de la Dirección en seguridad de la información**			
5.1.1	Políticas para la seguridad de la información	Control: Se debe definir un conjunto de políticas para la seguridad de la información, aprobada por la dirección, publicada y comunicada a los empleados y a las partes externas pertinentes.	50%	L2
5.1.2	Revisión de las políticas para la seguridad de la información.	Control: Las políticas para la seguridad de la información se deben revisar a intervalos planificados o si ocurren cambios significativos, para para asegurar su conveniencia, adecuación y eficacia continuas.	50%	L2

Control en la Normativa	Sección	Control	% de cumplimiento	Cumplimiento
6	**ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACION**			
6.1	**Organización interna**			
A6.1.1	Roles y responsabilidades para la seguridad de la información	Control: Se deben definir y asignar todas las responsabilidades de la seguridad de la información.	10%	L1

A6.1.2	Separación de deberes	Control: Los deberes y áreas de responsabilidad en conflicto se deben separar para reducir las posibilidades de modificación no autorizada o no intencional, o el uso indebido de los activos de la organización	50%	L2
A6.1.3	Contacto con las autoridades	Control: Se deben mantener contactos apropiados con las autoridades pertinentes.	50%	L2
A6.1.4	Contacto con grupos de interés especial	Control: Se deben mantener contactos apropiados con grupos de interés especial u otros foros y asociaciones profesionales especializadas en seguridad	50%	L2
A6.1.5	Seguridad de la información en la gestión de proyectos.	Control: La seguridad de la información se debe tratar en la gestión de proyectos, independientemente del tipo de proyecto.	90%	L3
6.2	**Dispositivos móviles y teletrabajo**			
A6.2.1	Política para dispositivos móviles	Control: Se deben adoptar una política y unas medidas de seguridad de soporte, para gestionar los riesgos introducidos por el uso de dispositivos móviles.	10%	L1
A6.2.2	Teletrabajo	Control: Se deben implementar una política y unas medidas de seguridad de soporte, para proteger la información a la que se tiene acceso, que es procesada o almacenada en los lugares en los que se realiza teletrabajo.	90%	L3

Control en la Normativa	Sección	Control	% de cumplimiento	Cumplimiento
7	**SEGURIDAD DE LOS RECURSOS HUMANOS**			

7.1	**Antes de asumir el empleo**			
A7.1.1	Selección	Control: Las verificaciones de los antecedentes de todos los candidatos a un empleo se deben llevar a cabo de acuerdo con las leyes, reglamentaciones y ética pertinentes y deben ser proporcionales a los requisitos de negocio, a la clasificación de la información a que se va a tener acceso y a los riesgos percibidos.	90%	L3
A7.1.2	Términos y condiciones del empleo	Control: Los acuerdos contractuales con empleados y contratistas deben establecer sus responsabilidades y las de la organización en cuanto a la seguridad de la información.	90%	L3
7.2	**Durante la ejecución del empleo**			
A7.2.1	Responsabilidades de la dirección	Control: La dirección debe exigir a todos los empleados y contratista la aplicación de la seguridad de la información de acuerdo con las políticas y procedimientos establecidos por la organización.	90%	L3
A7.2.2	Toma de conciencia, educación y formación en la seguridad de la información.	Control: Todos los empleados de la organización, y en donde sea pertinente, los contratistas, deben recibir la educación y la formación en toma de conciencia apropiada, y actualizaciones regulares sobre las políticas y procedimientos de la organización pertinentes para su cargo.	90%	L3
A7.2.3	Proceso disciplinario	Control: Se debe contar con un proceso formal, el cual debe ser comunicado, para emprender acciones contra empleados que hayan	90%	L3

		cometido una violación a la seguridad de la información.		
7.2	**Terminación y cambio de empleo**			
A7.3.1	Terminación o cambio de responsabilidades de empleo	Control: Las responsabilidades y los deberes de seguridad de la información que permanecen validos después de la terminación o cambio de empleo de deben definir, comunicar al empleado o contratista y se deben hacer cumplir.	90%	L3

Control en la Normativa	Sección	Control	% de cumplimiento	Cumplimiento
8	**GESTION DE ACTIVOS**			
8.1	**Responsabilidad por los activos**			
A8.1.1	Inventario de activos	Control: Se deben identificar los activos asociados con información e instalaciones de procesamiento de información, y se debe elaborar y mantener un inventario de estos activos.	50%	L2
A8.1.2	Propiedad de los activos	Control: Los activos mantenidos en el inventario deben tener un propietario.	90%	L3
A8.1.3	Uso aceptable de los activos	Control: Se deben identificar, documentar e implementar reglas para el uso aceptable de información y de activos asociados con información e instalaciones de procesamiento de información.	90%	L3

A8.1.4	Devolución de activos	Control: Todos los empleados y usuarios de partes externas deben devolver todos los activos de la organización que se encuentren a su cargo, al terminar su empleo, contrato o acuerdo.	90%	L3
A8.2	**Clasificación de la información**			
A8.2.1	Clasificación de la información	Control: La información se debe clasificar en función de los requisitos legales, valor, criticidad y susceptibilidad a divulgación o a modificación no autorizada.	50%	L2
A8.2.2	Etiquetado de la información	Control: Se debe desarrollar e implementar un conjunto adecuado de procedimientos para el etiquetado de la información, de acuerdo con el esquema de clasificación de información adoptado por la organización.	90%	L3
A8.2.3	Manejo de activos	Control: Se deben desarrollar e implementar procedimientos para el manejo de activos, de acuerdo con el esquema de clasificación de información adoptado por la organización.	90%	L3
A8.2	**Manejo de medios**			
A8.3.1	Gestión de medio removibles	Control: Se deben implementar procedimientos para la gestión de medio removibles, de acuerdo con el esquema de clasificación adoptado por la organización.	50%	L2
A8.3.2	Disposición de los medios	Control: Se debe disponer en forma segura de los medios cuando ya no se requieran, utilizando procedimientos formales.	90%	L3

A8.3.3	Transferencia de medios físicos	Control: Los medios que contienen información se deben proteger contra acceso no autorizado, uso indebido o corrupción durante el transporte.	50%	L2

Control en la Normativa	Sección	Control	% de cumplimiento	Cumplimiento
9	**CONTROL DE ACCESO**			
9.1	**Requisitos del negocio para el control de acceso**			
A9.1.1	Política de control de acceso	Control: Se debe establecer, documentar y revisar una política de control de acceso con base en los requisitos del negocio y de la seguridad de la información.		L2
A9.1.2	Acceso a redes y a servicios en red	Control: Solo se debe permitir acceso de los usuarios a la red y a los servicios de red para los que hayan sido autorizados específicamente.	95%	L4
9.2	**Gestión de acceso de usuarios**			
A9.2.1	Registro y cancelación del registro de usuarios	Control: Se debe implementar un proceso formal de registro y de cancelación de registro de usuarios, para posibilitar la asignación de los derechos de acceso.	90%	L3
A9.2.2	Suministro de acceso de usuarios	Control: Se debe implementar un proceso de suministro de acceso formal de usuarios para asignar o revocar los derechos de acceso para todo tipo de usuarios para todos los sistemas y servicios.	90%	L3
A9.2.3	Gestión de derechos de acceso privilegiado	Control: Se debe restringir y controlar la asignación y uso de derechos de acceso privilegiado	90%	L3
A9.2.4	Gestión de información de autenticación secreta de usuarios	Control: La asignación de información de autenticación secreta se debe controlar por medio de un proceso de gestión formal.	95%	L4
A9.2.5	Revisión de los derechos de acceso de usuarios	Control: Los propietarios de los activos deben revisar los derechos de acceso de los usuarios, a intervalos regulares.	90%	L3

A9.2.6	Retiro o ajuste de los derechos de acceso	Control: Los derechos de acceso de todos los empleados y de usuarios externos a la información y a las instalaciones de procesamiento de información se deben retirar al terminar su empleo, contrato o acuerdo, o se deben ajustar cuando se hagan cambios.	95%	L4
A9.3	**Responsabilidades de los usuarios**			
A9.3.1	Uso de información de autenticación secreta	Control: Se debe exigir a los usuarios que cumplan las prácticas de la organización para el uso de información de autenticación secreta.	50%	L2
A9.4	**Control de acceso a sistemas y aplicaciones**			
A9.4.1	Restricción de acceso a la información	Control: El acceso a la información y a las funciones de los sistemas de las aplicaciones se debe restringir de acuerdo con la política de control de acceso.	95%	L4
A9.4.2	Procedimiento de ingreso seguro	Control: Cuando lo requiere la política de control de acceso, el acceso a sistemas y aplicaciones se debe controlar mediante un proceso de ingreso seguro.	95%	L4
A9.4.3	Sistema de gestión de contraseñas	Control: Los sistemas de gestión de contraseñas deben ser interactivos y deben asegurar la calidad de las contraseñas.	50%	L2
A9.4.4	Uso de programas utilitarios privilegiados	Control: Se debe restringir y controlar estrictamente el usos de programas utilitarios que podrían tener capacidad de anular el sistema y los controles de las aplicaciones.	10%	L1
A9.4.5	Control de acceso a códigos fuente de programas	Control: Se debe restringir el acceso a los códigos fuente de los programas.	95%	L4

Control en la Normativa	Sección	Control	% de cumplimiento	Cumplimiento
10	**CIFRADO**			
10.1	**Controles criptográficos**			

A10.1.1	Política sobre el uso de controles criptográficos	Control: Se debe desarrollar e implementar una política sobre el uso de controles criptográficos para la protección de la información.	10%	L1
A10.1.2	Gestión de llaves	Control: Se debe desarrollar e implementar una política sobre el uso, protección y tiempo de vida de las llaves criptográficas, durante todo su ciclo de vida.	0%	L0

Control en la Normativa	Sección	Control	% de cumplimiento	Cumplimiento
A11	**SEGURIDAD FISICA Y DEL ENTORNO**			
11.1	**Áreas seguras**			
A11.1.1	Perímetro de seguridad física	Control: Se deben definir y usar perímetros de seguridad, y usarlos para proteger áreas que contengan información confidencial o critica, e instalaciones de manejo de información.	50%	L2
A11.1.2	Controles de acceso físicos	Control: Las áreas seguras deben estar protegidas con controles de acceso apropiados para asegurar que sólo se permite el acceso a personal autorizado.	90%	L3
A11.1.3	Seguridad de oficinas, recintos e instalaciones.	Control: Se debe diseñar y aplicar la seguridad física para oficinas, recintos e instalaciones.	50%	L2
A11.1.4	Protección contra amenazas externas y ambientales.	Control: Se deben diseñar y aplicar protección física contra desastres naturales, ataques maliciosos o accidentes.	50%	L2
A11.1.5	Trabajo en áreas seguras.	Control: Se deben diseñar y aplicar procedimientos para trabajo en áreas seguras.	10%	L1
A11.1.6	Áreas de carga, despacho y acceso público	Control: Se deben controlar los puntos de acceso tales como las áreas de despacho y carga y otros puntos por donde pueden entrar personas no autorizadas y, si es posible, aislarlos de las instalaciones de procesamiento de información para evitar el acceso no autorizado.	90%	L3
A11.2	**Equipos**			

A11.2.1	Ubicación y protección de los equipos	Control: Los equipos deben de estar ubicados y protegidos para reducir los riesgos de amenazas y peligros del entorno, y las posibilidades de acceso no autorizado.	90%	L3
A11.2.2	Servicios de suministro	Control: Los equipos se deben proteger contra fallas de energía y otras interrupciones causadas por fallas en los servicios de suministro.	90%	L3
A11.2.3	Seguridad en el cableado.	Control: El cableado de energía eléctrica y de telecomunicaciones que porta datos o brinda soporte a los servicios de información se debe proteger contra interceptación, interferencia o daño.	100%	L5
A11.2.4	Mantenimiento de los equipos.	Control: Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.	95%	L4
A11.2.5	Retiro de activos	Control: Los equipos, información o software no se deben retirar de su sitio sin autorización previa	95%	L4
A11.2.6	Seguridad de equipos y activos fuera de las instalaciones	Control: Se deben aplicar medidas de seguridad a los activos que se encuentran fuera de las instalaciones de la organización, teniendo en cuenta los diferentes riesgos de trabajar fuera de dichas instalaciones.	90%	L3
A11.2.7	Disposición segura o reutilización de equipos	Control: Se deben verificar todos los elementos de equipos que contengan medios de almacenamiento para asegurar que cualquier dato confidencial o software licenciado haya sido retirado o sobrescrito en forma segura antes de su disposición o reúso.	50%	L2
A11.2.8	Equipos de usuario desatendido	Control: Los usuarios deben asegurarse de que a los equipos desatendidos se les da protección apropiada.	90%	L3
A11.2.9	Política de escritorio limpio y pantalla limpia	Control: Se debe adoptar una política de escritorio limpio para los papeles y medios de almacenamiento removibles, y una política de pantalla limpia en las instalaciones de procesamiento de información.	50%	L2

Control en la Normativa	Sección	Control	% de cumplimiento	Cumplimiento
A12	**SEGURIDAD DE LAS OPERACIONES**			
A12.1	**Procedimientos operacionales y responsabilidades**			
A12.1.1	Procedimientos de operación documentados	Control: Los procedimientos de operación se deben documentar y poner a disposición de todos los usuarios que los necesitan.	90%	L3
A12.1.2	Gestión de cambios	Control: Se deben controlar los cambios en la organización, en los procesos de negocio, en las instalaciones y en los sistemas de procesamiento de información que afectan la seguridad de la información.	90%	L3
A12.1.3	Gestión de capacidad	Control: Se debe hacer seguimiento al uso de recursos, hacer los ajustes, y hacer proyecciones de los requisitos de capacidad futura, para asegurar el desempeño requerido del sistema.	50%	L2
A12.1.4	Separación de los ambientes de desarrollo, pruebas y operación	Control: Se deben separar los ambientes de desarrollo, pruebas y operación, para reducir los riesgos de acceso o cambios no autorizados al ambiente de operación.	50%	L2
A12.2	**Protección contra códigos maliciosos**			
A12.2.1	Controles contra códigos maliciosos	Control: Se deben implementar controles de detección, de prevención y de recuperación, combinados con la toma de conciencia apropiada de los usuarios, para proteger contra códigos maliciosos.	50%	L2
A12.2	**Protección contra códigos maliciosos**			
A12.3.1	Respaldo de la información	Control: Se deben hacer copias de respaldo de la información, software e imágenes de los sistemas, y ponerlas a prueba regularmente de acuerdo con una política de copias de respaldo acordadas.	50%	L2

A12.2	**Protección contra códigos maliciosos**			
A12.4.1	Registro de eventos	Control: Se deben elaborar, conservar y revisar regularmente los registros acerca de actividades del usuario, excepciones, fallas y eventos de seguridad de la información.	10%	L1
A12.4.2	Protección de la información de registro	Control: Las instalaciones y la información de registro se deben proteger contra alteración y acceso no autorizado.	90%	L3
A12.4.3	Registros del administrador y del operador	Control: Las actividades del administrador y del operador del sistema se deben registrar, y los registros se deben proteger y revisar con regularidad.	90%	L3
A12.4.4	Sincronización de relojes	Control: Los relojes de todos los sistemas de procesamiento de información pertinentes dentro de una organización o ámbito de seguridad se deben sincronizar con una única fuente de referencia de tiempo.	10%	L1
A12.2	**Protección contra códigos maliciosos**			
A12.5.1	Instalación de software en sistemas operativos	Control: Se deben implementar procedimientos para controlar la instalación de software en sistemas operativos.	90%	L3
A12.6	**Gestión de la vulnerabilidad técnica**			
A12.6.1	Gestión de las vulnerabilidades técnicas	Control: Se debe obtener oportunamente información acerca de las vulnerabilidades técnicas de los sistemas de información que se usen; evaluar la exposición de la organización a estas vulnerabilidades, y tomar las medidas apropiadas para tratar el riesgo asociado.	10%	L1
A12.6.2	Restricciones sobre la instalación de software	Control: Se deben establecer e implementar las reglas para la instalación de software por parte de los usuarios.	90%	L3
A12.7	**Consideraciones sobre auditorias de sistemas de información**			

A12.7.1	Controles de auditorías de sistemas de información	Control: Los requisitos y actividades de auditoria que involucran la verificación de los sistemas operativos se deben planificar y acordar cuidadosamente para minimizar las interrupciones en los procesos del negocio.	50%	L2

Control en la Normativa	Sección	Control	% de cumplimiento	Cumplimiento
A13	**SEGURIDAD DE LAS COMUNICACIONES**			
A13.1	**Gestión de la seguridad de las redes**			
A13.1.1	Controles de redes	Control: Las redes se deben gestionar y controlar para proteger la información en sistemas y aplicaciones.	50%	L2
A13.1.2	Seguridad de los servicios de red	Control: Se deben identificar los mecanismos de seguridad, los niveles de servicio y los requisitos de gestión de todos los servicios de red, e incluirlos en los acuerdos de servicio de red, ya sea que los servicios se presten internamente o se contraten externamente.	90%	L3
A13.1.3	Separación en las redes	Control: Los grupos de servicios de información, usuarios y sistemas de información se deben separar en las redes.	50%	L2
A13.2	**Transferencia de información**			
A13.2.1	Políticas y procedimientos de transferencia de información	Control: Se debe contar con políticas, procedimientos y controles de transferencia información formales para proteger la transferencia de información mediante el uso de todo tipo de instalaciones de comunicaciones.	50%	L2
A13.2.2	Acuerdos sobre transferencia de información	Control: Los acuerdos deben tratar la transferencia segura de información del negocio entre la organización y las partes externas.	10%	L1

A13.2.3	Mensajería Electrónica	Control: Se debe proteger adecuadamente la información incluida en la mensajería electrónica.	50%	L2
A13.2.4	Acuerdos de confidencialidad o de no divulgación	Control: Se deben identificar, revisar regularmente y documentar los requisitos para los acuerdos de confidencialidad o no divulgación que reflejen las necesidades de la organización para la protección de la información.	90%	L3

Control en la Normativa	Sección	Control	% de cumplimiento	Cumplimiento
14	**Adquisición, desarrollo y mantenimiento de sistemas**			
14.1	**Requisitos de seguridad de los sistemas de información**			
A.14.1.1	Análisis y especificación de requisitos de seguridad de la información	Control: Los requisitos relacionados con seguridad de la información se deben incluir en los requisitos para nuevos sistemas de información o para mejoras a los sistemas de información existentes.	50%	L2
A.14.1.2	Seguridad de servicios de las aplicaciones en redes públicas	Control: La información involucrada en los servicios de las aplicaciones que pasan sobre redes públicas se debe proteger de actividades fraudulentas, disputas contractuales y divulgación y modificación no autorizadas.	50%	L2
A.14.1.3	Protección de transacciones de los servicios de las aplicaciones.	Control: La información involucrada en las transacciones de los servicios de las aplicaciones se debe proteger para evitar la transmisión incompleta, el enrutamiento errado, la alteración no autorizada de mensajes, la divulgación no autorizada, y la duplicación o reproducción de mensajes no autorizada.	90%	L3
A14.2	**Seguridad en los procesos de Desarrollo y de Soporte**			
A.14.2.1	Política de desarrollo seguro	Control: Se debe establecer y aplicar reglas para el desarrollo de software y de sistemas, a los desarrollos dentro de la organización.	90%	L3

A.14.2.2	Procedimientos de control de cambios en sistemas	Control: Los cambios a los sistemas dentro del ciclo de vida de desarrollo se deben controlar mediante el uso de procedimientos formales de control de cambios.	50%	L2
A.14.2.3	Revisión técnica de las aplicaciones después de cambios en la plataforma de operación	Control: Cuando se cambian las plataformas de operación, se deben revisar las aplicaciones críticas del negocio, y someter a prueba para asegurar que no haya impacto adverso en las operaciones o seguridad de la organización.	50%	L2
A.14.2.4	Restricciones en los cambios a los paquetes de software	Control: Se deben desalentar las modificaciones a los paquetes de software, los cuales se deben limitar a los cambios necesarios, y todos los cambios se deben controlar estrictamente.	90%	L3
A.14.2.5	Principio de Construcción de los Sistemas Seguros.	Control: Se deben establecer, documentar y mantener principios para la construcción de sistemas seguros, y aplicarlos a cualquier actividad de implementación de sistemas de información.	0%	L0
A.14.2.6	Ambiente de desarrollo seguro	Control: Las organizaciones deben establecer y proteger adecuadamente los ambientes de desarrollo seguros para las actividades de desarrollo e integración de sistemas que comprendan todo el ciclo de vida de desarrollo de sistemas.	90%	L3
A.14.2.7	Desarrollo contratado externamente	Control: La organización debe supervisar y hacer seguimiento de la actividad de desarrollo de sistemas contratados externamente.	50%	L2
A.14.2.8	Pruebas de seguridad de sistemas	Control: Durante el desarrollo se deben llevar a cabo pruebas de funcionalidad de la seguridad.	50%	L2
A.14.2.9	Prueba de aceptación de sistemas	Control: Para los sistemas de información nuevos, actualizaciones y nuevas versiones, se deben establecer programas de prueba para aceptación y criterios de aceptación relacionados.	50%	L2
A14.3	**Datos de prueba**			
A.14.3.1	Protección de datos de prueba	Control: Los datos de prueba se deben seleccionar, proteger y controlar cuidadosamente.	50%	L2

Control en la Normativa	Sección	Control	% de cumplimiento	Cumplimiento

A15	**RELACIONES CON LOS PROVEEDORES**			
A15.1	**Seguridad de la información en las relaciones con los proveedores.**			
A15.1.1	Política de seguridad de la información para las relaciones con proveedores	Control: Los requisitos de seguridad de la información para mitigar los riesgos asociados con el acceso de proveedores a los activos de la organización se deben acordar con estos y se deben documentar.	50%	L2
A15.1.2	Tratamiento de la seguridad dentro de los acuerdos con proveedores	Control: Se deben establecer y acordar todos los requisitos de seguridad de la información pertinentes con cada proveedor que pueda tener acceso, procesar, almacenar, comunicar o suministrar componentes de infraestructura de TI para la información de la organización.	10%	L1
A15.1.3	Cadena de suministro de tecnología de información y comunicación	Control: Los acuerdos con proveedores deben incluir requisitos para tratar los riesgos de seguridad de la información asociados con la cadena de suministro de productos y servicios de tecnología de información y comunicación.	50%	L2
A15.2	**Gestión de la prestación de servicios de proveedores**			
A15.2.1	Seguimiento y revisión de los servicios de los proveedores	Control: Las organizaciones deben hacer seguimiento, revisar y auditar con regularidad la prestación de servicios de los proveedores.	0%	L0
A15.2.2	Gestión del cambio en los servicios de los proveedores	Control: Se deben gestionar los cambios en el suministro de servicios por parte de los proveedores, incluido el mantenimiento y las mejoras de las políticas, procedimientos y controles de seguridad de la información existentes, teniendo en cuenta la criticidad de la información, sistemas y procesos de negocio involucrados, y la revaluación de los riesgos.	50%	L2

Control en la Normativa	Sección	Control	% de cumplimiento	Cumplimiento
A16.1	**Gestión de incidentes y mejoras en la seguridad de la información**			

A16.1.1	Responsabilidades y procedimientos	Control: Se deben establecer las responsabilidades y procedimientos de gestión para asegurar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información.	50%	L2
A16.1.2	Reporte de eventos de seguridad de la información	Control: Los eventos de seguridad de la información se deben informar a través de los canales de gestión apropiados, tan pronto como sea posible.	50%	L2
A16.1.3	Reporte de debilidades de seguridad de la información	Control: Se debe exigir a todos los empleados y contratistas que usan los servicios y sistemas de información de la organización, que observen y reporten cualquier debilidad de seguridad de la información observada o sospechada en los sistemas o servicios.	90%	L3
A16.1.4	Evaluación de eventos de seguridad de la información y decisiones sobre ellos	Control: Los eventos de seguridad de la información se deben evaluar y se debe decidir si se van a clasificar como incidentes de seguridad de la información.	50%	L2
A16.1.5	Respuesta a incidentes de seguridad de la información	Control: Se debe dar respuesta a los incidentes de seguridad de la información de acuerdo con procedimientos documentados.	10%	L1
A16.1.6	Aprendizaje obtenido de los incidentes de seguridad de la información	Control: El conocimiento adquirido al analizar y resolver incidentes de seguridad de la información se debe usar para reducir la posibilidad o impacto de incidentes futuros.	50%	L2
A16.1.7	Recolección de evidencia	Control: La organización debe definir y aplicar procedimientos para la identificación, recolección, adquisición y preservación de información que pueda servir como evidencia.	90%	L3

6.5 No conformidades respecto a la ISO 27002:2013

En este apartado se muestran las No Conformidades (NC) con la norma ISO 27002:2013 descubiertas durante la realización del proceso de auditoría de cumplimiento, así como las acciones correctivas recomendadas. Se considera que un control es de No Conformidad cuando este ha obtenido una evaluación de MMC inferior a L3.

ID	Control	NC	DETALLE	ACCION CORRECTIVA	MMC
5.1.1	Políticas para la seguridad de la información	menor	Se debe definir un conjunto de políticas para la seguridad de la información, aprobada por la dirección, publicada y comunicada a los empleados y a las partes externas pertinentes.	Se debe socializar las políticas de seguridad con todos los miembros de la Institución	L2
5.1.2	Revisión de las políticas para la seguridad de la información.	menor	Las políticas para la seguridad de la información se deben revisar a intervalos planificados o si ocurren cambios significativos, para para asegurar su conveniencia, adecuación y eficacia continuas.	comunicar a todo el personal las políticas y los cambios significativos para su adecuación y eficacia	L2
A6.1.1	Roles y responsabilidades para la seguridad de la información	menor	No existen roles y responsabilidades para todos los usuarios	se deben definir los roles y responsabilidades para cada una de las unidades y usuarios	L1
A6.1.2	Separación de deberes	menor	Los deberes y áreas de responsabilidad en conflicto se deben separar para reducir las posibilidades de modificación no autorizada o no intencional, o el uso indebido de los activos de la organización	se deben establecer medidas y responsabilidades para el uso indebido de los activos de la organización	L2
A6.1.3	Contacto con las autoridades	menor	Se deben mantener contactos apropiados con las autoridades pertinentes.	Actualizar los contactos de emergencia para cualquier situación que se presente	L2
A6.1.4	Contacto con grupos de interés especial	menor	Se deben mantener contactos apropiados con grupos de interés especial u otros foros y asociaciones profesionales especializadas en seguridad	Actualizar los contactos de emergencia para cualquier situación que se presente	L2
A6.2.1	Política para dispositivos móviles	menor	Hay que adoptar políticas y medidas de seguridad de soporte, para gestionar los riesgos introducidos por el uso de dispositivos móviles.	se debe realizar el procedimiento para adoptar las políticas y medidas de seguridad para dispositivos móviles	L1
A8.1.1	Inventario de activos	menor	Se deben identificar los activos asociados con información e instalaciones de procesamiento de información, y se debe elaborar y	se deben actualizar los activos en todo momento	L2

			mantener un inventario de estos activos.		
A8.2.1	Clasificación de la información	menor	La información se debe clasificar en función de los requisitos legales, valor, criticidad y susceptibilidad a divulgación o a modificación no autorizada.	No toda la información está clasificada, se debe clasificar en función de requisitos de valor, criticidad y susceptibilidades	L2
A8.3.1	Gestión de medio removibles	menor	Se deben implementar procedimientos para la gestión de medio removibles, de acuerdo con el esquema de clasificación adoptado por la organización.	implementar procedimientos para la gestión de medio removibles	L2
A8.3.3	Transferencia de medios físicos	menor	Los medios que contienen información se deben proteger contra acceso no autorizado, uso indebido o corrupción durante el transporte.	Verificar y parametrizar los medios físicos para evitar la transferencia de información ante personas no autorizadas	L2
A9.1.1	Política de control de acceso	menor	Se debe establecer, documentar y revisar una política de control de acceso con base en los requisitos del negocio y de la seguridad de la información.	Establecer procedimientos para controlar el acceso de la información a través de políticas	L2
A9.3.1	Uso de información de autenticación secreta	menor	Se debe exigir a los usuarios que cumplan las prácticas de la organización para el uso de información de autenticación secreta.	Capacitar a todo el personal para que cumplan con las buenas prácticas para autenticación secreta	L2
A9.4.3	Sistema de gestión de contraseñas	menor	Los sistemas de gestión de contraseñas deben ser interactivos y deben asegurar la calidad de las contraseñas.	verificar los sistemas de gestión de contraseñas en cuanto a calidad y que deben ser interactivas	L2
A9.4.4	Uso de programas utilitarios privilegiados	menor	Se debe restringir y controlar estrictamente los usos de programas utilitarios que podrían tener capacidad de anular el sistema y los controles de las aplicaciones.	Implementar los diferentes controles para restringir el uso de programas con privilegios	L1

A10.1.1	Política sobre el uso de controles criptográficos	menor	Desarrollar e implementar una política sobre el uso de controles criptográficos para la protección de la información.	No existen políticas, se debe generar políticas para la protección de información desde la gerencia tecnológica hasta los desarrolladores	L1
A10.1.2	Gestión de llaves	Mayor	No existe ninguna política sobre el uso, protección y tiempo de vida de las llaves criptográficas, durante todo su ciclo de vida.	Crear una política para la protección de llaves criptográficas	L0
A11.1.1	Perímetro de seguridad física	menor	Se deben definir y usar perímetros de seguridad, y usarlos para proteger áreas que contengan información confidencial o crítica, e instalaciones de manejo de información.	verificar todas las áreas en el cual se tiene información crítica, y verificar los perímetros de seguridad para el acceso	L2
A11.1.3	Seguridad de oficinas, recintos e instalaciones.	menor	Se debe diseñar y aplicar la seguridad física para oficinas, recintos e instalaciones.	Verificar todos las oficinas, e instalaciones en cuanto a la seguridad	L2
A11.1.4	Protección contra amenazas externas y ambientales.	menor	Se deben diseñar y aplicar protección física contra desastres naturales, ataques maliciosos o accidentes.	Tener activos los sistemas de emergencia y detección de incendios, humedad etc...	L2
A11.1.5	Trabajo en áreas seguras.	menor	Diseñar y aplicar procedimientos para trabajo en áreas seguras.	Revisar y realizar nuevas políticas y procedimientos para el trabajo en áreas seguras	L1
A11.2.7	Disposición segura o reutilización de equipos	menor	Se deben verificar todos los elementos de equipos que contengan medios de almacenamiento para asegurar que cualquier dato confidencial o software licenciado haya sido retirado o sobrescrito en forma segura antes de su disposición o reúso.	Todos los medios de almacenamiento deben estar protegidos contra robo, copia y duplicidad de información	L2
A11.2.9	Política de escritorio limpio y pantalla limpia	menor	Se debe adoptar una política de escritorio limpio para los papeles y medios de almacenamiento removibles, y una política de	Capacitar al personal para mantener las políticas de escritorio y pantalla limpia	L2

			pantalla limpia en las instalaciones de procesamiento de información.		
A12.1.3	Gestión de capacidad	menor	Se debe hacer seguimiento al uso de recursos, hacer los ajustes, y hacer proyecciones de los requisitos de capacidad futura, para asegurar el desempeño requerido del sistema.	Se debe proyectar la capacidad de la informacion para no presentar ningún inconveniente	L2
A12.1.4	Separación de los ambientes de desarrollo, pruebas y operación	menor	Se deben separar los ambientes de desarrollo, pruebas y operación, para reducir los riesgos de acceso o cambios no autorizados al ambiente de operación.	Verificar que los ambientes de desarrollo tanto pruebas como producción estén bien definidos	L2
A12.2.1	Controles contra códigos maliciosos	menor	Se deben implementar controles de detección, de prevención y de recuperación, combinados con la toma de conciencia apropiada de los usuarios, para proteger contra códigos maliciosos.	se debe concientizar a todo el personal e implementar los controles de detección de intrusos y códigos maliciosos	L2
A12.3.1	Respaldo de la información	menor	Se deben hacer copias de respaldo de la información, software e imágenes de los sistemas, y ponerlas a prueba regularmente de acuerdo con una política de copias de respaldo acordadas.	se debe garantizar los bakups de la información institucional	L2
A12.4.1	Registro de eventos	menor	Se deben elaborar, conservar y revisar regularmente los registros acerca de actividades del usuario, excepciones, fallas y eventos de seguridad de la información.	Elaborar procedimientos para controlar los registros de eventos en cuanto a la seguridad en la información	L1
A12.4.4	Sincronización de relojes	menor	Los relojes de todos los sistemas de procesamiento de información pertinentes dentro de una organización o ámbito de seguridad se deben sincronizar con una única fuente de referencia de tiempo.	Programar y sincronizar en toda la institución los relojes de los sistemas de procesamiento de datos	L1
A12.6.1	Gestión de las vulnerabilidades técnicas	menor	Se debe obtener oportunamente información acerca de las vulnerabilidades técnicas de los sistemas de información que se usen; evaluar la exposición de la organización a estas vulnerabilidades, y tomar las	Gestionar oportunamente la información acerca de vulnerabilidades técnicas	L1

			medidas apropiadas para tratar el riesgo asociado.		
A12.7.1	Controles de auditorías de sistemas de información	menor	Los requisitos y actividades de auditoria que involucran la verificación de los sistemas operativos se deben planificar y acordar cuidadosamente para minimizar las interrupciones en los procesos del negocio.	se deben seguir los lineamientos de los procesos de auditoria en los tiempos establecidos	L2
A13.1.1	Controles de redes	menor	Las redes se deben gestionar y controlar para proteger la información en sistemas y aplicaciones.	Verificar los controles para proteger la información	L2
A13.1.3	Separación en las redes	menor	Los grupos de servicios de información, usuarios y sistemas de información se deben separar en las redes.	segmentar las redes institucionales, académicas, administrativas	L2
A13.2.1	Políticas y procedimientos de transferencia de información	menor	Se debe contar con políticas, procedimientos y controles de transferencia información formales para proteger la transferencia de información mediante el uso de todo tipo de instalaciones de comunicaciones.	implementar las políticas y procedimientos para la transferencia de información en las comunicaciones	L2
A13.2.2	Acuerdos sobre transferencia de información	menor	Los acuerdos deben tratar la transferencia segura de información del negocio entre la organización y las partes externas.	Generar procedimiento y formatos para la transferencia de información en la Institución	L1
A13.2.3	Mensajería Electrónica	menor	Se debe proteger adecuadamente la información incluida en la mensajería electrónica.	capacitar el personal en el manejo de la información en las cuentas de correo, chats	L2
A.14.1.1	Análisis y especificación de requisitos de seguridad de la información	menor	Los requisitos relacionados con seguridad de la información se deben incluir en los requisitos para nuevos sistemas de información o para mejoras a los sistemas de información existentes.	aplicar requisitos de seguridad para aplicativos existentes y aplicar requisitos a los nuevos sistemas de información	L2

A.14.1.2	Seguridad de servicios de las aplicaciones en redes públicas	menor	La información involucrada en los servicios de las aplicaciones que pasan sobre redes públicas se debe proteger de actividades fraudulentas, disputas contractuales y divulgación y modificación no autorizadas.	verificar los servidos de aplicaciones que pasar por redes públicas y protegerlas de cualquier actividad fraudulenta	L2
A.14.2.2	Procedimientos de control de cambios en sistemas	menor	Los cambios a los sistemas dentro del ciclo de vida de desarrollo se deben controlar mediante el uso de procedimientos formales de control de cambios.	Establecer procedimientos para el control de cambios en los sistemas	L2
A.14.2.3	Revisión técnica de las aplicaciones después de cambios en la plataforma de operación	menor	Cuando se cambian las plataformas de operación, se deben revisar las aplicaciones críticas del negocio, y someter a prueba para asegurar que no haya impacto adverso en las operaciones o seguridad de la organización.	Establecer procedimientos para cambios en las aplicaciones, web, y pruebas, con el fin de mitigar el impacto a las operaciones de la institución.	L2
A.14.2.5	Principio de Construcción de los Sistemas Seguros.	Mayor	No existe ningún principio para documentar y mantener a la construcción de sistemas seguros, y aplicarlos a cualquier actividad de implementación de sistemas de información.	Se debe documentar los principios de sistemas seguros	L0
A.14.2.7	Desarrollo contratado externamente	menor	La organización debe supervisar y hacer seguimiento de la actividad de desarrollo de sistemas contratados externamente.	Se be hacer un seguimiento a los desarrollos contratados externamente	L2
A.14.2.8	Pruebas de seguridad de sistemas	menor	Durante el desarrollo se deben llevar a cabo pruebas de funcionalidad de la seguridad.	Establecer procedimientos para las pruebas de seguridad	L2
A.14.2.9	Prueba de aceptación de sistemas	menor	Para los sistemas de información nuevos, actualizaciones y nuevas versiones, se deben establecer programas de prueba para aceptación y criterios de aceptación relacionados.	Establecer procedimientos para pruebas de nuevos sistemas	L2
A.14.3.1	Protección de datos de prueba	menor	Los datos de prueba se deben seleccionar, proteger y controlar cuidadosamente.	Establecer parámetros para la protección de datos en servicios de pruebas	L2

A15.1.1	Política de seguridad de la información para las relaciones con proveedores	menor	Los requisitos de seguridad de la información para mitigar los riesgos asociados con el acceso de proveedores a los activos de la organización se deben acordar con estos y se deben documentar.	Establecer las políticas de seguridad a los proveedores	L2
A15.1.2	Tratamiento de la seguridad dentro de los acuerdos con proveedores	menor	Se deben establecer y acordar todos los requisitos de seguridad de la información pertinentes con cada proveedor que pueda tener acceso, procesar, almacenar, comunicar o suministrar componentes de infraestructura de TI para la información de la organización.	se debe documentar los acuerdos de seguridad en a información con los proveedores	L1
A15.1.3	Cadena de suministro de tecnología de información y comunicación	menor	Los acuerdos con proveedores deben incluir requisitos para tratar los riesgos de seguridad de la información asociados con la cadena de suministro de productos y servicios de tecnología de información y comunicación.	Incorporar en los acuerdos con los proveedores los requisitos para tratar riesgos de la información	L2
A15.2.1	Seguimiento y revisión de los servicios de los proveedores	Mayor	No existe ningún seguimiento a la prestación de servicios de los proveedores.	llevar a cabo un seguimiento constante a los servicios de los proveedores	L0
A15.2.2	Gestión del cambio en los servicios de los proveedores	menor	Se deben gestionar los cambios en el suministro de servicios por parte de los proveedores, incluido el mantenimiento y las mejoras de las políticas, procedimientos y controles de seguridad de la información existentes, teniendo en cuenta la criticidad de la información, sistemas y procesos de negocio involucrados, y la revaluación de los riesgos.	se deben gestionar los cambios en los servicios de los proveedores en cuanto a la seguridad en la información	L2
A16.1.1	Responsabilidades y procedimientos	menor	Se deben establecer las responsabilidades y procedimientos de gestión para asegurar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información.	Socializar los procedimientos responsabilidades para garantizar respuestas rápida ante cualquier incidente de seguridad	L2

A16.1.2	Reporte de eventos de seguridad de la información	menor	Los eventos de seguridad de la información se deben informar a través de los canales de gestión apropiados, tan pronto como sea posible.	se debe establecer procedimientos para cualquier comunicado o evento de seguridad	L2
A16.1.4	Evaluación de eventos de seguridad de la información y decisiones sobre ellos	menor	Los eventos de seguridad de la información se deben evaluar y se debe decidir si se van a clasificar como incidentes de seguridad de la información.	evaluar los eventos de seguridad y decidir si se clasifican como incidente de seguridad	L2
A16.1.5	Respuesta a incidentes de seguridad de la información	menor	Se debe dar respuesta a los incidentes de seguridad de la información de acuerdo con procedimientos documentados.	Documentar un procedimiento	L1
A16.1.6	Aprendizaje obtenido de los incidentes de seguridad de la información	menor	El conocimiento adquirido al analizar y resolver incidentes de seguridad de la información se debe usar para reducir la posibilidad o impacto de incidentes futuros.	Socializar cualquier tipo de incidencia en cuanto a la seguridad en la información una vez se solucionen	L2
A17.1.1	Planificación de la continuidad de la seguridad de la información	menor	La organización debe determinar sus requisitos para la seguridad de la información y la continuidad de la gestión de la seguridad de la información en situaciones adversas, por ejemplo, durante una crisis o desastre.	determinar requisitos para la seguridad en la información y la continuidad ante situaciones adversas	L2
A17.1.2	Implementación de la continuidad de la seguridad de la información	menor	La organización debe establecer, documentar, implementar y mantener procesos, procedimientos y controles para asegurar el nivel de continuidad requerido para la seguridad de la información durante una situación adversa.	se debe implementar y mantener procesos actualizados	L1
A17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información	menor	La organización debe verificar a intervalos regulares los controles de continuidad de la seguridad de la información establecidos e implementados, con el fin de asegurar que son válidos y eficaces durante situaciones adversas.	implementar en la institución controles para verificar y revisar la continuidad de la seguridad en la información	L1
A17.2.1	Disponibilidad de instalaciones de procesamiento de información	menor	Las instalaciones de procesamientos de información se deben implementar con redundancia suficiente para cumplir los requisitos de disponibilidad.	establecer procedimientos de información para implementar redundancia suficiente para la disponibilidad	L2

A18.1.2	Derechos propiedad intelectual (DPI)	menor	Se deben implementar procedimientos apropiados para asegurar el cumplimiento de los requisitos legislativos, de reglamentación y contractuales relacionados con los derechos de propiedad intelectual y el uso de productos de software patentados.	Implementar procedimientos apropiados para asegurar el cumplimiento de los requisitos legislativos	L2
A18.1.3	Protección de registros	menor	Los registros se deben proteger contra perdida, destrucción, falsificación, acceso no autorizado y liberación no autorizada, de acuerdo con los requisitos legislativos, de reglamentación, contractuales y de negocio.	Establecer procedimientos para proteger los registros contra perdida, destrucción o falsificación de la información	L2
A18.1.4	Privacidad y protección de información de datos personales	menor	Se deben asegurar la privacidad y la protección de la información de datos personales, como se exige e la legislación y la reglamentación pertinentes, cuando sea aplicable.	Asegurar la privacidad y protección de la información	L2
A18.1.5	Reglamentación de controles criptográficos.	menor	Se deben usar controles criptográficos, en cumplimiento de todos los acuerdos, legislación y reglamentación pertinentes.	reglamentar los controles criptográficos de acuerdo a la legislación y acuerdos pertinentes	L1
A18.2.1	Revisión independiente de la seguridad de la información	menor	El enfoque de la organización para la gestión de la seguridad de la información y su implementación (es decir los objetivos de control, los controles, las políticas, los procesos y los procedimientos para seguridad de la información), se deben revisar independientemente a intervalos planificados o cuando ocurran cambios significativos.	Revisar independientemente la seguridad en la información en todos los procedimientos objetivos, controles políticas, procesos y procedimientos	L2
A18.2.3	Revisión del cumplimiento técnico	menor	Los sistemas de información se deben revisar periódicamente para determinar el cumplimiento con las políticas y normas de seguridad de la información.	Cumplir con las revisiones periódicas para determinar el cumplimiento de las políticas y normas de seguridad	L2

6.6 Observaciones respecto a la ISO/IEC 27002:2013

Respecto al resto de controles que han obtenido en el análisis un nivel igual o mayor a L3, a continuación, se presenta una serie de observaciones que la institución deberá tener en cuenta para continuar con la mejora constante en materia de seguridad de la información.

ID	Control	TIPO DE NC	DETALLE	OPORTUNIDAD DE MEJORA	MMC
A6.1.5	Seguridad de la información en la gestión de proyectos.	Observación	La seguridad de la información se debe tratar en la gestión de proyectos, independientemente del tipo de proyecto.	se debe mantener la seguridad en cada uno de los proyectos	L3
A6.2.2	Teletrabajo	Observación	Se deben implementar una política y unas medidas de seguridad de soporte, para proteger la información a la que se tiene acceso, que es procesada o almacenada en los lugares en los que se realiza teletrabajo.	Mantener activas las políticas de seguridad para proteger la informacion en todos lugares que se realiza teletrabajo	L3
A7.1.1	Selección	Observación	Las verificaciones de los antecedentes de todos los candidatos a un empleo se deben llevar a cabo de acuerdo con las leyes, reglamentaciones y ética pertinentes y deben ser proporcionales a los requisitos de negocio, a la clasificación de la información a que se va a tener acceso y a los riesgos percibidos.	Mantener los controles de seguridad en las contrataciones nuevas, verificar antecedentes	L3
A7.1.2	Términos y condiciones del empleo	Observación	Los acuerdos contractuales con empleados y contratistas deben establecer sus responsabilidades y las de la organización en cuanto a la seguridad de la información.	Recalcar los acuerdos contractuales con cada empleado en cuanto a la responsabilidad de la informacion en la institución	L3
A7.2.1	Responsabilidades de la dirección	Observación	La dirección debe exigir a todos los empleados y contratista la aplicación de la seguridad de la información de acuerdo con las políticas y procedimientos establecidos por la organización.	La Rectoría debe impulsar por los diferentes medios la importancia de la seguridad en la informacion a toda la comunidad	L3

A7.2.2	Toma de conciencia, educación y formación en la seguridad de la información.	Observación	Todos los empleados de la organización, y en donde sea pertinente, los contratistas, deben recibir la educación y la formación en toma de conciencia apropiada, y actualizaciones regulares sobre las políticas y procedimientos de la organización pertinentes para su cargo.	se debe seguir fomentando capacitaciones para tomar conciencia de la importancia de la seguridad en la institución	L3
A7.2.3	Proceso disciplinario	Observación	Se debe contar con un proceso formal, el cual debe ser comunicado, para emprender acciones contra empleados que hayan cometido una violación a la seguridad de la información.	Social a todo el personal los reglamentos internos de trabajo, y las diferentes sanciones y proceso disciplinarios establecidos	L3
A7.3.1	Terminación o cambio de responsabilidades de empleo	Observación	Las responsabilidades y los deberes de seguridad de la información que permanecen validos después de la terminación o cambio de empleo de deben definir, comunicar al empleado o contratista y se deben hacer cumplir.	Mejorar las comunicaciones hacia los empleados en cuanto a la terminación o cambio de responsabilidades de empleo	L3
A8.1.2	Propiedad de los activos	Observación	Los activos mantenidos en el inventario deben tener un propietario.	Se debe asociar un responsable a cada activo de la institución	L3
A8.1.3	Uso aceptable de los activos	Observación	Se deben identificar, documentar e implementar reglas para el uso aceptable de información y de activos asociados con información e instalaciones de procesamiento de información.	Socializar las reglas, instructivos asociados con la información, aplicativos, activos	L3
A8.1.4	Devolución de activos	Observación	Todos los empleados y usuarios de partes externas deben devolver todos los activos de la organización que se encuentren a su cargo, al terminar su empleo, contrato o acuerdo.	Generar Paz y salvo a todo el personal para que devuelvan los activos, usuarios, unidades y todos los activos que pertenezcan a la institución	L3
A8.2.2	Etiquetado de la información	Observación	Se debe desarrollar e implementar un conjunto adecuado de procedimientos para el etiquetado de la información, de acuerdo con el esquema de clasificación de información adoptado por la organización.	verificar el etiquetado de los activos y actualizar el 100% de los activos	L3

A8.2.3	Manejo de activos	Observación	Se deben desarrollar e implementar procedimientos para el manejo de activos, de acuerdo con el esquema de clasificación de información adoptado por la organización.	Socializar los procedimientos para el manejo de los activos a cada uno de los responsables	L3
A8.3.2	Disposición de los medios	Observación	Se debe disponer en forma segura de los medios cuando ya no se requieran, utilizando procedimientos formales.	actualizar formatos y procedimientos para el manejo de los medios	L3
A9.1.2	Acceso a redes y a servicios en red	Oportunidad de Mejora	Solo se debe permitir acceso de los usuarios a la red y a los servicios de red para los que hayan sido autorizados específicamente.	se ha implementado este control pero pueden mejorar con un procedimiento	L4
A9.2.1	Registro y cancelación del registro de usuarios	Observación	Se debe implementar un proceso formal de registro y de cancelación de registro de usuarios, para posibilitar la asignación de los derechos de acceso.	Verificar el proceso para el registro o cancelación de usuarios	L3
A9.2.2	Suministro de acceso de usuarios	Observación	Se debe implementar un proceso de suministro de acceso formal de usuarios para asignar o revocar los derechos de acceso para todo tipo de usuarios para todos los sistemas y servicios.	Actualizar el procedimiento para el suministro de todos los usuarios de la institución al personal nuevo	L3
A9.2.3	Gestión de derechos de acceso privilegiado	Observación	Se debe restringir y controlar la asignación y uso de derechos de acceso privilegiado	Verificar y actualizar los controles de acceso privilegiados	L3
A9.2.4	Gestión de información de autenticación secreta de usuarios	Oportunidad de Mejora	La asignación de información de autenticación secreta se debe controlar por medio de un proceso de gestión formal.	Este procedimiento se lleva acabo pero se debe mejorar la entrega oportuna de los usuarios	L4
A9.2.5	Revisión de los derechos de acceso de usuarios	Observación	Los propietarios de los activos deben revisar los derechos de acceso de los usuarios, a intervalos regulares.	Se debe verificar los accesos a los usuarios con frecuencia	L3
A9.2.6	Retiro o ajuste de los derechos de acceso	Oportunidad de Mejora	Los derechos de acceso de todos los empleados y de usuarios externos a la información y a las instalaciones de procesamiento de información se deben retirar al terminar su empleo, contrato o acuerdo, o se deben ajustar cuando se hagan cambios.	Este procedimiento se lleva a cabo, pero se debe hacer en un menor tiempo	L4
A9.4.1	Restricción de acceso a la información	Oportunidad de Mejora	El acceso a la información y a las funciones de los sistemas de las aplicaciones se debe restringir de	Se considera revisar con frecuencia la	L4

			acuerdo con la política de control de acceso.	política de control de acceso	
A9.4.2	Procedimiento de ingreso seguro	Oportunidad de Mejora	Cuando lo requiere la política de control de acceso, el acceso a sistemas y aplicaciones se debe controlar mediante un proceso de ingreso seguro.	se cuenta con este procedimiento, se pone mejora de acceso para los visitantes	L4
A9.4.5	Control de acceso a códigos fuente de programas	Oportunidad de Mejora	Se debe restringir el acceso a los códigos fuente de los programas.	se proponer documentar todos los procedimientos al códigos seguros	L4
A11.1.2	Controles de acceso físicos	Observación	Las áreas seguras deben estar protegidas con controles de acceso apropiados para asegurar que sólo se permite el acceso a personal autorizado.	Verificar los accesos a las áreas seguras, restringir y demarcar el acceso para el personal autorizado	L3
A11.1.6	Áreas de carga, despacho y acceso público	Observación	Se deben controlar los puntos de acceso tales como las áreas de despacho y carga y otros puntos por donde pueden entrar personas no autorizadas y, si es posible, aislarlos de las instalaciones de procesamiento de información para evitar el acceso no autorizado.	Controlar las áreas de carga y despacho en la institución y accesos público	L3
A11.2.1	Ubicación y protección de los equipos	Observación	Los equipos deben de estar ubicados y protegidos para reducir los riesgos de amenazas y peligros del entorno, y las posibilidades de acceso no autorizado.	Se sugiere que se verifiquen todos los equipos y se tomen medidas de protección en cuanto a amenazas, peligros de entorno y acceso no autorizado	L3
A11.2.2	Servicios de suministro	Observación	Los equipos se deben proteger contra fallas de energía y otras interrupciones causadas por fallas en los servicios de suministro.	Verificar el estado de las UPS, plantas y protección ante bajas en el suministro Eléctrico	L3
A11.2.3	Seguridad en el cableado.	Oportunidad de Mejora	El cableado de energía eléctrica y de telecomunicaciones que porta datos o brinda soporte a los servicios de información se debe proteger contra interceptación, interferencia o daño.	como oportunidad de mejora se propone hacer mantenimiento, revisión de todo el cableado para evitar futuras interferencias o daños	L5

A11.2.4	Mantenimiento de los equipos.	Oportunidad de Mejora	Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.	se propone documentar todo el mantenimiento de los equipos, para llevar el control y detectar la vida útil de los equipos	L4
A11.2.5	Retiro de activos	Oportunidad de Mejora	Los equipos, información o software no se deben retirar de su sitio sin autorización previa	mejora el proceso de salida y entrada de equipos	L4
A11.2.6	Seguridad de equipos y activos fuera de las instalaciones	Observación	Se deben aplicar medidas de seguridad a los activos que se encuentran fuera de las instalaciones de la organización, teniendo en cuenta los diferentes riesgos de trabajar fuera de dichas instalaciones.	se debe mantener segura la información de los equipos fuera en las instalaciones	L3
A11.2.8	Equipos de usuario desatendido	Observación	Los usuarios deben asegurarse de que a los equipos desatendidos se les da protección apropiada.	se debe mantener seguros los equipos que no estén todo el tiempo en funcionamiento	L3
A12.1.1	Procedimientos de operación documentados	Observación	Los procedimientos de operación se deben documentar y poner a disposición de todos los usuarios que los necesitan.	Socializar los procedimientos de operación en el sistema de gestión de calidad	L3
A12.1.2	Gestión de cambios	Observación	Se deben controlar los cambios en la organización, en los procesos de negocio, en las instalaciones y en los sistemas de procesamiento de información que afectan la seguridad de la información.	Mantener todos los controles en los cambios a procedimientos que afecten los sistemas de información	L3
A12.4.2	Protección de la información de registro	Observación	Las instalaciones y la información de registro se deben proteger contra alteración y acceso no autorizado.	se debe proteger las instalaciones y la información ante cualquier alteración y acceso no autorizado	L3
A12.4.3	Registros del administrador y del operador	Observación	Las actividades del administrador y del operador del sistema se deben registrar, y los registros se deben proteger y revisar con regularidad.	se debe mantener un registro del administrador y del operador de los sistemas de información	L3
A12.5.1	Instalación de software en sistemas operativos	Observación	Se deben implementar procedimientos para controlar la instalación de software en sistemas operativos.	Se deben establecer en los procedimientos los controles y restricciones para	L3

				instalación de sistemas operativos	
A12.6.2	Restricciones sobre la instalación de software	Observación	Se deben establecer e implementar las reglas para la instalación de software por parte de los usuarios.	Socializar las reglas al personal en cuanto a la instalación de cualquier tipo de software	L3
A13.1.2	Seguridad de los servicios de red	Observación	Se deben identificar los mecanismos de seguridad, los niveles de servicio y los requisitos de gestión de todos los servicios de red, e incluirlos en los acuerdos de servicio de red, ya sea que los servicios se presten internamente o se contraten externamente.	se deben verificar las clausulas con los proveedores externos en cuanto a los servicios de red	L3
A13.2.4	Acuerdos de confidencialidad o de no divulgación	Observación	Se deben identificar, revisar regularmente y documentar los requisitos para los acuerdos de confidencialidad o no divulgación que reflejen las necesidades de la organización para la protección de la información.	Todos los acuerdo de confidencialidad y divulgación se deben identificar, revisar y documentar	L3
A.14.1.3	Protección de transacciones de los servicios de las aplicaciones.	Observación	La información involucrada en las transacciones de los servicios de las aplicaciones se debe proteger para evitar la transmisión incompleta, el enrutamiento errado, la alteración no autorizada de mensajes, la divulgación no autorizada, y la duplicación o reproducción de mensajes no autorizada.	Se debe proteger las transacciones de servicios y aplicaciones	L3
A.14.2.1	Política de desarrollo seguro	Observación	Se debe establecer y aplicar reglas para el desarrollo de software y de sistemas, a los desarrollos dentro de la organización.	Verificar las políticas de desarrollo en los sistemas de la Institución	L3
A.14.2.4	Restricciones en los cambios a los paquetes de software	Observación	Se deben desalentar las modificaciones a los paquetes de software, los cuales se deben limitar a los cambios necesarios, y todos los cambios se deben controlar estrictamente.	Tener un control estricto en los cambios u actualizaciones de software	L3

A.14.2.6	Ambiente de desarrollo seguro	Observación	Las organizaciones deben establecer y proteger adecuadamente los ambientes de desarrollo seguros para las actividades de desarrollo e integración de sistemas que comprendan todo el ciclo de vida de desarrollo de sistemas.	verificar y proteger el ambiente de desarrollo seguro, que este	L3
A16.1.3	Reporte de debilidades de seguridad de la información	Observación	Se debe exigir a todos los empleados y contratistas que usan los servicios y sistemas de información de la organización, que observen y reporten cualquier debilidad de seguridad de la información observada o sospechada en los sistemas o servicios.	Comunicar frecuentemente los contactos para reportar cualquier novedad que se presente en cuanto a la seguridad de la información	L3
A16.1.7	Recolección de evidencia	Observación	La organización debe definir y aplicar procedimientos para la identificación, recolección, adquisición y preservación de información que pueda servir como evidencia.	Se debe definir los procedimientos para la recolección de evidencias	L3
A18.1.1	Identificación de la legislación aplicable.	Observación	Todos los requisitos estatutarios, reglamentarios y contractuales pertinentes y el enfoque de la organización para cumplirlos, se deben identificar y documentar explícitamente y mantenerlos actualizados para cada sistema de información y para la organización.	Los reglamentos, estatutos se deben actualizar para cada sistema y para la organización	L3
A18.2.2	Cumplimiento con las políticas y normas de seguridad	Observación	Los directores deben revisar con regularidad el cumplimiento del procesamiento de información dentro de su área de responsabilidad, con las políticas y normas de seguridad apropiadas, y cualquier otro requisito de seguridad.	Todos los directores deben conocer los procedimientos de información en su área de responsabilidad y los requisitos de seguridad	L3

6.7 Presentación de resultados

En este apartado se mostraran los resultados obtenidos de la realización de la auditoria a la Fundación Universitaria San Mateo, teniendo en cuenta la norma ISO/IEC 27001:2013

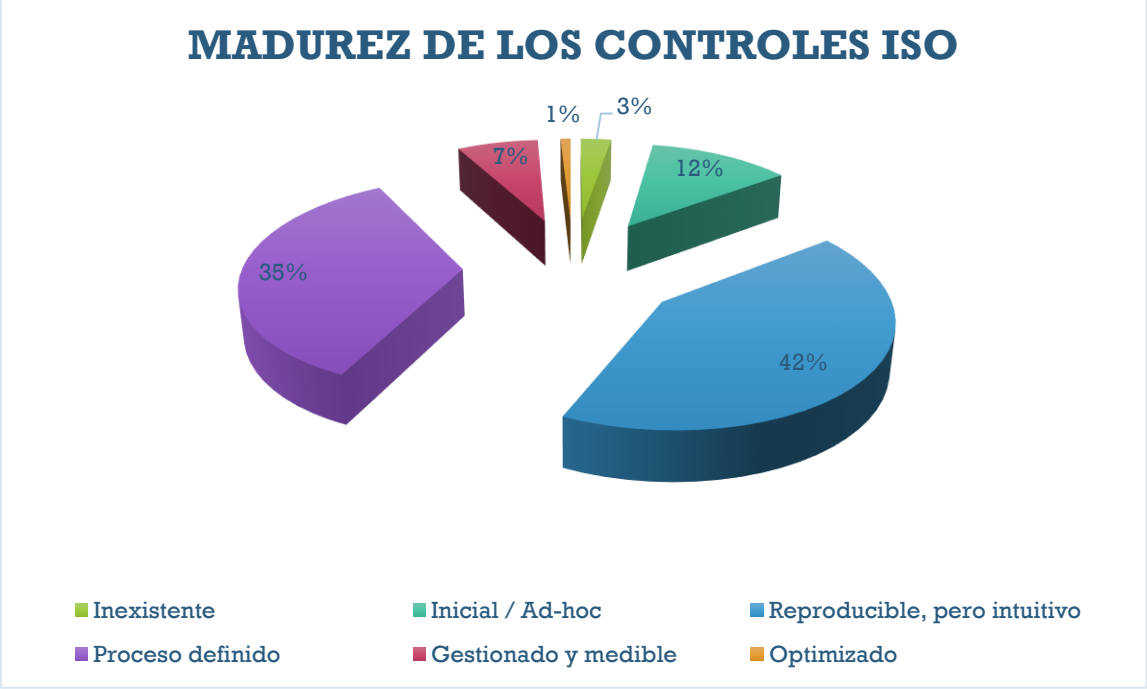
A continuación se muestra el nivel de madurez adquirido durante la implementación respecto al GAP inicial

Tabla 26 Porcentajes requisitos norma ISO 27001:2013

ítem	Aspectos Requeridos del SGSI	Inicial	Final
4	Contexto de la Organización	20%	80%
5	Liderazgo	40%	100%
6	Política	0%	50%
7	Soporte	50%	75%
8	Operación	0%	45%
9	Evaluación de Desempeño	0%	50%
10	Mejora	0%	50%
Promedio Total		**16%**	**64%**

Los resultados del diagnóstico muestran que el nivel de cumplimiento promedio del SGSI con base a los requerimientos mínimos de la norma ISO/IEC 27001:2013 (numerales 4 al 10) es del 64%, lo cual se cumple parcialmente.

Ilustración 18 Grado de Madurez MMC



En la ilustración anterior se puede observar el nivel de madurez de la Fundación Universitaria san mateo, en el cual se identifica que hay que realizar una trabajo fuerte en algunos de los controles.

En la siguiente tabla se muestra el porcentaje de madurez de los Dominios de la ISO/IEC 27002:2013

Para mayor ilustración podemos ver el Documento Anexo Evaluación de Madurez respecto a los controles definidos en la ISO 27002

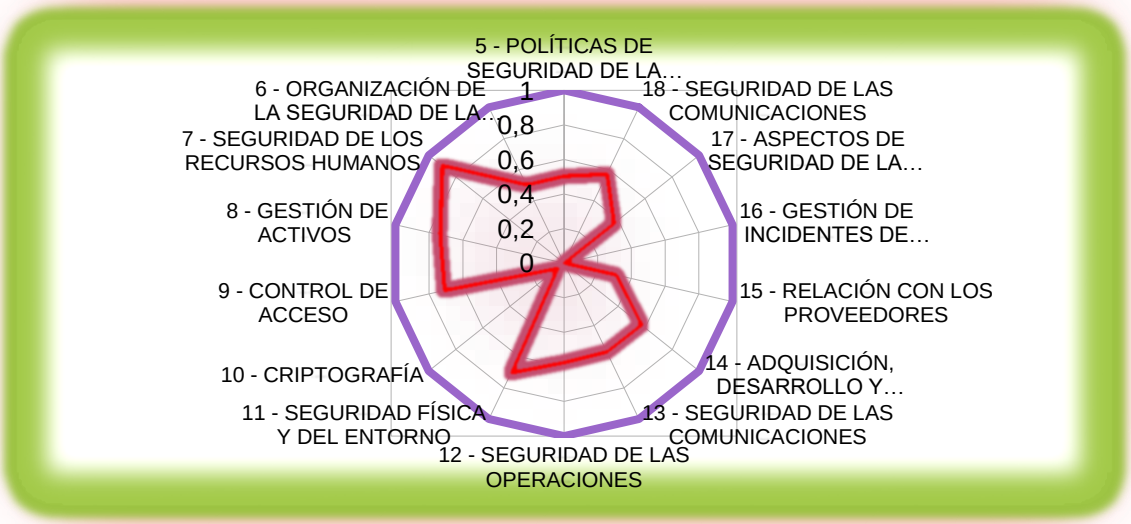
Tabla 27 Porcentaje de madurez de los dominios ISO 27002

Dominio	% de Efectividad
5 - POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN	50%
6 - ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	50%
7 - SEGURIDAD DE LOS RECURSOS HUMANOS	90%
8 - GESTIÓN DE ACTIVOS	73%
9 - CONTROL DE ACCESO	71%
10 - CRIPTOGRAFÍA	5%
11 - SEGURIDAD FÍSICA Y DEL ENTORNO	70%
12 - SEGURIDAD DE LAS OPERACIONES	57%
13 - SEGURIDAD DE LAS COMUNICACIONES	57%
14 - ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	57%
15 - RELACIÓN CON LOS PROVEEDORES	31%
16 - GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	0%
17 - ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTION DE CONTINUIDAD DE NEGOCIO	37%
18 - SEGURIDAD DE LAS COMUNICACIONES	57%

Como se puede observar, hay varios dominios que tiene un margen de mejora amplio, y se debe trabajar con prioridad los dominios 10 y 16.

Una visión más detallada es la que se presenta como 'diagrama de radar' que mostraría el nivel de cumplimiento de cada uno de los dominios de la Norma ISO/IEC 2700:2013, podemos identificar el estado actual respecto al estado deseado.

Ilustración 19 Porcentaje de madurez medido en la auditoría



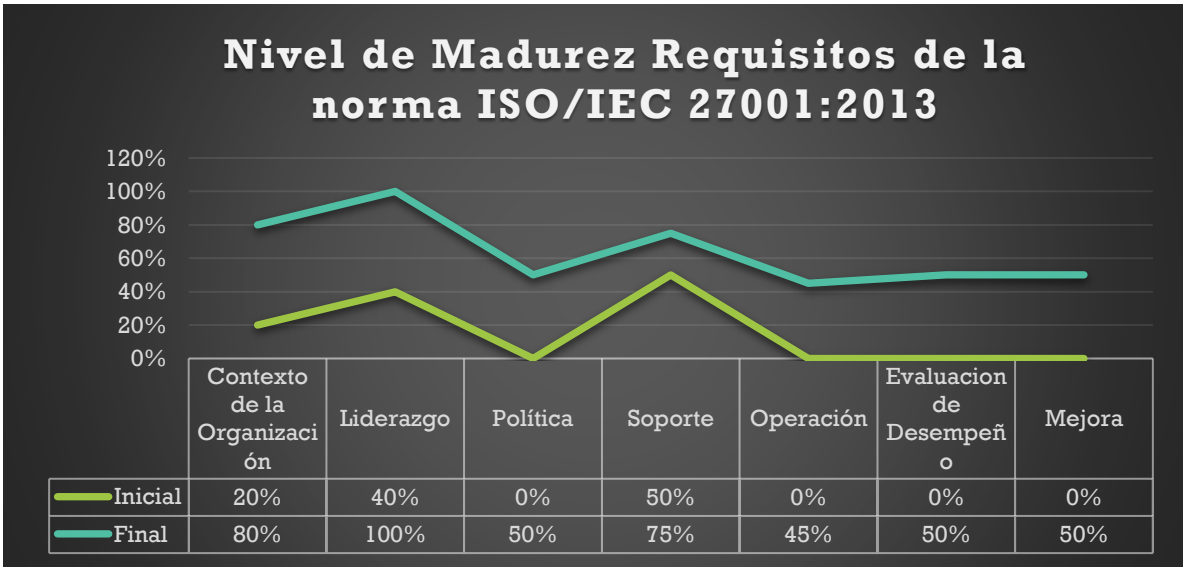
---------- **Estado actual**

---------- **Estado deseado**

Teniendo en cuenta la ilustración anterior podemos ver que la mayoría de los dominios se deben verificar, trabajar para mejorar la madurez en la Seguridad de la información en la institución

6.8 Resultados

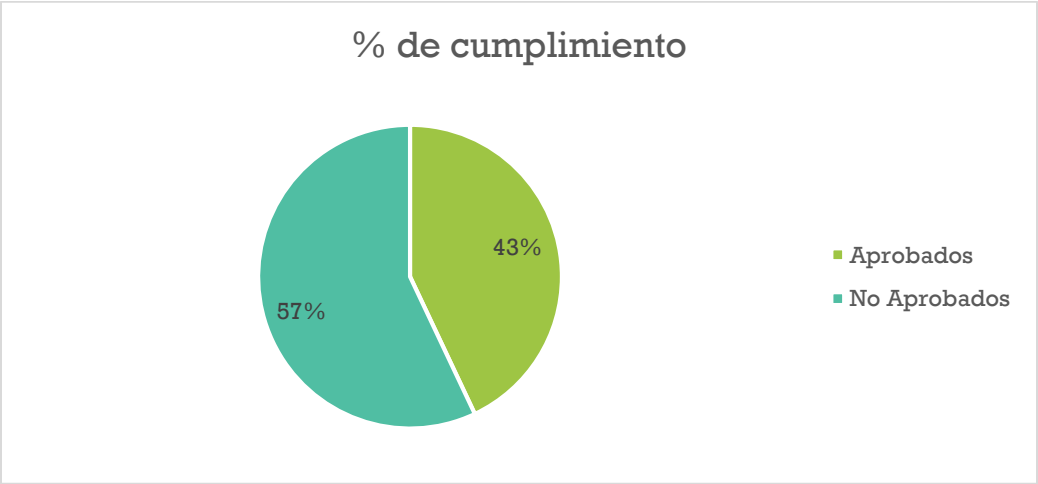
Ilustración 20 Porcentaje de cumplimiento de la Norma ISO 27001



	Contexto de la Organización	Liderazgo	Política	Soporte	Operación	Evaluacion de Desempeño	Mejora
Inicial	20%	40%	0%	50%	0%	0%	0%
Final	80%	100%	50%	75%	45%	50%	50%

Una vez completada esta fase se tendrá una visión del cumplimiento de los diferentes dominios de la ISO/IEC 27002:2013 – y de su incumplimiento

Ilustración 21 Porcentaje de cumplimiento de la Norma ISO 27002-.



En la ilustración anterior podemos identificar que un 57% de los controles no se están cumpliendo respecto a la Norma ISO/IEC 27002:2013, Estos controles están un % de efectividad por debajo del 50%, y un 43% está entre 90% y 100% de efectividad en los controles.

FASE 6 7. Presentación de Resultados y Entrega de Informes

7.1 Introducción

En este apartado se recopila la información relevante del Plan Directora de Seguridad en la Fundación Universitaria San Mateo.

7.2 Objetivos

El objetivo genérico de esta fase es la generación de la documentación, que deberá incluir como mínimo los siguientes aspectos

- Resumen ejecutivo: breve descripción en que se incluya la motivación, enfoque del proyecto y principales conclusiones extraídas.
- Memoria descriptiva: donde se incluirá un detalle del proceso, incluyendo como mínimo la descripción de la empresa en estudio, el análisis de riesgos realizado, el nivel de cumplimiento de la empresa actualmente, un plan de acción para mejorar la seguridad, la cuantificación de la mejora que supondrá el plan y los aspectos organizativos que conviene abordar para hacer viable el plan.
- Una presentación a la dirección planteada para un tiempo de 1h en que se expongan los principales resultados del estudio, se plantee el plan de acción y los aspectos organizativos relevantes.

7.3 Entregables

La documentación que se entrega en este apartado es la que sigue:

- Resumen ejecutivo con las principales conclusiones del plan Director
- Presentación Power point con resumen de las distintas fases del Plan Director de Seguridad
- Memorias de Proyectos, Anexos
- Resultados de análisis de Riesgos
- Nivel de cumplimiento de la ISO basado en el análisis de los 114 controles planteados por la norma.
- Proyectos planteados a la dirección, detallando el coste económico de los mismos, su planificación temporal y su impacto sobre el cumplimiento normativo de la ISO/IEC 27002:2013 en los diferentes dominios.
- Video de la defensa del Plan director de Seguridad

8. Conclusiones

8.1 Introducción

Tras haber realizado con éxito todas las fases anteriores, se puede concluir que se han cumplido los objetivos propuestos al inicio de este proyecto, es decir mejora la seguridad de la información de la Fundación Universitaria San Mateo gracias a la implementación de un plan de seguridad.

8.2 Objetivos Específicos

- Se ha establecido el estado inicial de la seguridad de la información de la Fundación Universitaria San Mateo, así como alcanzar los objetivos tras la implantación el SGSI.
- Se ha definido y desarrollado el esquema documental necesario para el cumplimiento normativo ISO/IEC 27001:2013
- Se realizó el análisis de riesgos de la Institución del que se ha obtenido la lista de todos los activos, las amenazas posibles a las que está expuesta la institución, así como el impacto y el riesgo de todos los activos para verificar la prioridad en cuanto a seguridad de información.
- Se implementaron una serie de proyectos con el fin de mitigar los riesgos obtenidos en el análisis de riesgos realizado a la Fundación Universitaria San Mateo.
- Se evaluó el nivel de madurez de la seguridad de la información con respecto a la norma ISO/IEC 27002:2013
- Se ha conseguido reducir el riesgo de los activos de la organización

8.3 Recomendaciones

- Se deben implantar las mejoras propuestas en la fase de auditoria de cumplimiento
- Una vez ejecutados los proyectos se deberán intentar conseguir la certificación ISO/IEC 27001:2013.
- Se debe seguir trabajando en las recomendaciones y hacer revisiones constantes a los sistemas de información más débiles.
- Se deben realizar auditorías más frecuentes para detectar debilidades y realizar mejoras en tiempos cortos.

8. Términos y Definiciones

- **Análisis de riesgos**: Proceso sistemático para estimar la magnitud de los riesgos a los que está expuesta la Organización

- **Activos de Información**: Información y recursos asociados, que tienen valor para la organización

- **Amenaza:** causa potencial de un incidente no deseado, el cual puede causar el daño a un sistema o la organización.

- **Aplicaciones:** Es todo el software que se utiliza para la gestión de la información

- **Acción Correctiva:** Acción tomada para eliminar la causa de una no conformidad detectada u otra situación indeseable para evitar que vuelva a ocurrir

- **Acción Preventiva:** Acción tomada para eliminar la causa de una no conformidad potencial u otra situación potencialmente indeseable, para evitar que ocurra.
-
- **Auditor:** Persona encargada de verificar, de manera independiente, la calidad e integridad del trabajo que se ha realizado en un área particular.

- **Auditoria:** Proceso planificado y sistemático en el cual un auditor obtiene evidencias objetivas que le permitan emitir un juicio informado sobre el estado y efectividad del SGSI de una organización

- **Confidencialidad:** Propiedad que determina que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados.

- **Control**: Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido.

- **Corrección:** Acción emprendida para eliminar una no conformidad.

- **Datos**: Son todos aquellos elementos básicos de la información (en cualquier formato) que se generan, Recogen, gestionan, transmiten y destruyen

- **Disponibilidad:** Propiedad de que la información se accesible y utilizable por solicitud de una entidad autorizada.

- **Eficiencia:** Capacidad de disponer de alguien o de algo para conseguir un efecto determinado

- **Eficacia:** Capacidad de lograr el efecto que se desea o se espera

- **Gestión de riesgos:** Proceso de identificación, control y minimización o eliminación, a un coste aceptable, de los riesgos que afecten a la información de la organización. Incluye la valoración de riesgos y el tratamiento de riesgos.

- **Incidente de Seguridad de la Información**: Un evento o serie de eventos de seguridad de la información no deseada o inesperada, que tienen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.

- **Impacto:** Es la evaluación del efecto o consecuencia de la materialización del riesgo. Generalmente, la implicación del riesgo se mide en aspectos económicos, legales imagen

de la empresa, disminución de capacidad de respuesta y competitividad, interrupción de operaciones, entre otros.

- **Integridad:** Propiedad de salvaguardar la exactitud y estado completo de los activos.

- **No conformidad**: Incumplimiento de un requisito. Puede ser no conformidad de los servicios, de los procesos o del Sistema de Gestión de Seguridad de la Información.

- **Personal:** Es todo el personal subcontratado por la Fundación Universitaria San Mateo, Administrativos, Docentes, Estudiantes y los clientes, usuarios y en general y todos aquellos que tengan acceso de una manera u otra a los activos de información

- **Riesgo**: Estimación del grado de exposición a que una amenaza se materialice sobre uno o más activos causando daños o perjuicios a la Organización

- **Servicios:** Son tanto los servicios internos, aquellos que una parte de la Institución suministra a otra, como los externos, aquellos que la Institución suministra a clientes y usuarios

- **SGSI**: Sistema de Gestión de Seguridad de la Información, parte del sistema de gestión global, basada en un enfoque hacia los riesgos globales de un negocio, cuyo fin es establecer, implementar operar hacer seguimiento, revisar, mantener y mejorar la seguridad de la información.

9. Anexos

Anexo A Autodiagnóstico

Anexo B Políticas de Seguridad en La Información

Anexo C Procedimiento Auditoria Interna

Anexo D Gestión de Indicadores

Anexo E Procedimiento Revisión por la Dirección

Anexo F Gestión de Roles y Responsabilidades

Anexo G Metodología de Análisis de Riesgos

Anexo H Declaración de la Aplicabilidad

Anexo I Evaluación de Madurez respecto a los controles definidos en la ISO 27002

ANEXO J Declaración de Aplicabilidad San Mateo

ANEXO K Resumen de Análisis de nivel de Riesgo

ANEXO L Informe de Auditoria Interna

ANEXO M Inventario San Mateo

Anexo N Resultado de evaluación de Madurez

Anexo Ñ Resultado de Evaluación de Madurez2

Bibliografía

Ciclo PDCA (Planificar, Hacer, Verificar y Actuar): El círculo de Deming de mejora continua | PDCA Home. (n.d.). Retrieved April 28, 2018, from https://www.pdcahome.com/5202/ciclo-pdca/

Director de Seguridad de Ícaro Luis Rodríguez Conde Página, P. S., Luis Rodríguez Conde Dirección Antonio José Segovia Henares, A., & Rodríguez Conde Página, L. (2700). Trabajo Fin de Master (MISTIC) Máster Interuniversitario en Seguridad de las Tecnologías de la Información y la Comunicación (MISTIC). Retrieved from http://openaccess.uoc.edu/webapps/o2/bitstream/10609/64545/1/liziyoTFM0617-Resumen Ejecutivo-Memoria.pdf

Documentación requerida por la ISO 27001. (n.d.). Retrieved June 6, 2018, from https://www.pmg-ssi.com/2016/05/documentacion-requerida-por-la-iso-27001/

famila iso 27001 - Buscar con Google. (n.d.). Retrieved June 6, 2018, from https://www.google.com.co/search?ei=a8AXW_25CMyfzwKGiLXYBw&q=famila+iso+2700

1&oq=famila+iso+27001&gs_l=psy-ab.3...773.2126.0.2438.6.6.0.0.0.0.0.0..0.0....0...1c.1.64.psy-ab..6.0.0....0.jAJBOCiEyo4

Fundacion San Mateo. (2018). Fundacion San Mateo. Retrieved from http://www.sanmateo.edu.co/

FUNDACIÓN SAN MATEO. (2014). Retrieved from www.sanmateo.edu.co

ISO. (2016). ISO - International Organization for Standardization. Retrieved April 28, 2018, from https://www.iso.org/home.html

ISO 27001: La implementación de un Sistema de Gestión de Seguridad de la Información. (n.d.). Retrieved April 28, 2018, from https://www.pmg-ssi.com/2015/01/iso-27001-la-implementacion-de-un-sistema-de-gestion-de-seguridad-de-la-informacion/

Larrahondo Nuñez, A., & Alexander Larrahondo Página, T. N. (n.d.). Master Interuniversitario en Seguridad de las TIC (MISTIC) Trabajo Final de Máster Plan Director de Seguridad de la Información. Retrieved from http://openaccess.uoc.edu/webapps/o2/bitstream/10609/23383/6/alarrahondoTFM0613memoria.pdf

Marco, I., & Poblano, A. P. (n.d.). ISO/IEC 27001 Gestión de la seguridad de la información. Retrieved from http://www.ema.org.mx/sectorsalud/descargas/dia2/Aplicaciones_informaticas_para_la_consulta.pdf

Norma ISO 27002: El dominio política de seguridad. (n.d.-a). Retrieved June 6, 2018, from https://www.pmg-ssi.com/2017/08/norma-iso-27002-politica-seguridad/

Norma ISO 27002: El dominio política de seguridad. (n.d.-b). Retrieved March 25, 2018, from https://www.pmg-ssi.com/2017/08/norma-iso-27002-politica-seguridad/

Oberta De Catalunya Autor, U., & Rojas Valduciel, H. (2014). Universidad Oberta de Catalunya. Retrieved from http://openaccess.uoc.edu/webapps/o2/bitstream/10609/40297/1/hrojasvTFM1214.pdf

organigrama.png (2846×1722). (n.d.). Retrieved June 6, 2018, from http://www.sanmateo.edu.co/img/organigrama.png

PCS. (2017). Políticas de Seguridad de la Información. Retrieved from http://jacevedo.imprenta.gov.co/documents/10280/2763839/E4+-+GSI-DC-1+-

+Politicas+Seguridad+Informacion+-+V.4+-+20170421.pdf/29c4e197-dbf2-4ba3-9bef-c944e2ee91d8

- POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN. (n.d.). Retrieved from https://www.invima.gov.co/images/stories/formatotramite/GDIDIEPL010version2.pdf

San Mateo. (n.d.). San Mateo/ Educación Superior. Retrieved May 17, 2018, from http://sanmateo.edu.co/sanmateo.html

TFM_SGSI_CASTPEC1.).