ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

Facultad de Ingeniería en Electricidad y Computación

"DISEÑO DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN BASADA EN LA NORMA ISO/IEC 27002:2013 APLICADO A LOS CONTROLES DE ACCESO LÓGICOS EN LAS PLATAFORMAS DE UNA UNIDAD EDUCATIVA PARTICULAR DE GUAYAQUIL"

TRABAJO DE TITULACIÓN

PREVIO A LA OBTENCIÓN DEL TÍTULO DE

MAESTRÍA EN SEGURIDAD INFORMÁTICA

PRESENTADO POR:

ING. ANNY IVONNE CARDENAS FREIRE

ING. LISSETTE BEATRIZ MUNIZAGA SORIA

GUAYAQUIL - ECUADOR

AÑO 2024

AGRADECIMIENTO

Mi agradecimiento especial a DIOS y mis padres que han sido mi soporte para poder continuar; brindándome siempre su amor, comprensión y empuje en este importante paso de mi vida.

A mis hermanos que han sido mi ejemplo de superación, a mis amigos y compañeros dentro de este año de estudio que no faltaron al momento de compartir de sus conocimientos y estudios.

A mi esposo por ser mi compañía idónea, mi paño de lágrimas en mis momentos de tristezas, alegrías y hasta frustración. Por comprenderme y darme la calma para no abandonar mis sueños.

Lissette Beatriz Munizaga S.

AGRADECIMIENTO

Quiero agradecer a Dios por la vida y por brindarme a las personas que necesito en los momentos correctos.

Quisiera expresar mi más sincero agradecimiento a Zully Espinoza, que más que una Coordinadora en el área donde laboraba, fue una amiga y quien me dio mayor motivación y confianza para aprovechar la oportunidad que tuve.

A mi familia, por siempre estar pendiente y brindarme su apoyo, en especial a mi hermana Amyra por darse el tiempo de pasar conmigo y darme momentos compartidos durante este periodo.

A mi esposo por comprenderme y darme mi espacio cuando lo necesitaba.

Anny Ivonne Cárdenas Freire.

DEDICATORIA

Este proyecto es dedicado para los tres pilares de mi vida. Mi papito José Vicente Munizaga Arguello y mi mamita Beatriz Soria Recalde son ellos quienes de su mano me han enseñado que primero en DIOS y su tiempo perfecto lograré mis metas; que después de cada caída, habrá siempre un mejor comienzo.
Y para el ser que inspira mi vida desde el primer día de su existencia, y lo hará hasta el último día de mi vivir, mi hija Luciana Beatriz Delgado Munizaga
Su llegada a mi temprana edad, no me cambió la vida; al contrario, se convirtió en mi fuente de inspiración.

Lissette Beatriz Munizaga S.

DEDICATORIA

Este proyecto es dedicado a quienes compartieron conmigo el esfuerzo y dedicación durante el trayecto de este logro.

A los maestros que dieron también su tiempo y motivación para darnos su experiencia y sus conocimientos.

Y a mí, por no darme por vencida en momentos que creí que no podría continuar.

Anny Cárdenas Freire.

TRIBUNAL DE GRADUACIÓN

Firmado electrónicamente por:
LENIN EDUARDO FREIRE COBO

M.S.C. LENIN EDUARDO FREIRE COBO

TUTOR

Firmado electrónicamente por:
JUAN CARLOS GARCIA PLUA

M.S.C. JUAN CARLOS GARCÍA PLÚA

REVISOR

DECLARACIÓN EXPRESA

La responsabilidad del contenido de esta Tesis de Grado nos corresponde exclusivamente; y el patrimonio intelectual de la misma a la Escuela Superior Politécnica del Litoral.

ING. Anny Ivonne Cárdenas Freire

ING. Lissette Munizaga Soria

RESUMEN

El lugar objetivo es una unidad educativa particular de la ciudad de Guayaquil cuya política de calidad es brindar educación de calidad tanto en nivel básico y bachillerato.

Se establecerá la importancia de diseñar e implementar políticas que aseguren la integridad de la información a nivel lógico del plantel educativo.

Se creará un sumario que involucre los pasos para aplicar la seguridad en esta unidad educativa particular de Guayaquil, así como se realizará una auditoría para determinar las fortalezas y debilidades de la institución referente a las políticas de seguridad de Informática.

Se diseñará procesos y procedimientos de seguridad que incorporan una serie de medidas sobre los activos de información, conociendo, asumiendo y gestionando los posibles riesgos de forma documentada, estructurada, eficiente y adaptable a futuros cambios.

En el presente proyecto de titulación se pretende dar una adecuada solución de seguridad a la unidad educativa particular de Guayaquil, tomando como base estándares internacionales de seguridad de la información.

Se desea proporcionar lineamientos básicos de la seguridad de la información; gestión de riesgos y diferentes alternativas para el tratamiento de estos, basados en la implementación de la norma 27002.

Se presentará un plan de tratamiento de riesgos en donde se identificarán las acciones apropiadas, así como los responsables para minimizar los riesgos identificados para posteriormente realizar el diseño de Sistemas de Gestión de Seguridad de la Información (SGSI) en base a los controles seleccionados y finalmente obtener como resultado el manual de procedimientos y política de seguridad de la información.

Para el diseño del sistema nos basaremos única y exclusivamente en la norma de seguridad de la información ISO:27002.

Finalmente, se exponen las respectivas conclusiones y recomendaciones que fueron aplicadas al presente proyecto.

Palabras claves: Seguridad de la información, Controles, Software, Políticas, Técnicas.

ÍNDICE GENERAL

AGRADECIMIENTO 2

DEDICATORIA 4

DECLARACIÓN EXPRESA 7

RESUMEN…… 8

ÍNDICE GENERAL 10

ABREVIATURAS 13

ÍNDICE DE FIGURAS 14

ÍNDICE DE TABLAS 16

INTRODUCCIÓN 19

CAPITULO I. 20

GENERALIDADES 20

1.1. Antecedentes 20

1.2. Descripción del Problema 24

1.3. Solución Propuesta 26

1.4. Objetivos 27

1.4.1 Objetivo General 27

1.4.2 Objetivos Específicos 28

1.5. Metodología 28

CAPITULO II. 30

MARCO TEÓRICO 30

2.1 Seguridad de la Información en una Organización y de los Sistemas Informáticos 30
2.2 Definición e Implantación de las Políticas de Seguridad 32
2.2.1 Norma ISO/IEC 27001 33
2.2.2 Norma ISO/IEC 27002 36
2.3 Metodología para el Análisis de Riesgos (Metodología MAGERIT) 36
CAPÍTULO III. 47
ANÁLISIS Y SITUACIÓN ACTUAL 47
3.1 Infraestructura de red de la unidad educativa 48
3.2. Levantamiento de la información. 60
3.3 Controles de accesos lógicos y físicos 74
CAPÍTULO IV. 76
EVALUACIÓN Y TRATAMIENTO DEL RIESGO 76
4.1 Metodología De Evaluación Y Tratamiento De Riesgo 77
4.1.1 El Proceso 78
4.1.2 Identificación de las Amenazas Y Vulnerabilidades 78
4.1.3 Identificación De Los Propietarios De Riesgos 84
4.1.4 Consecuencia y Probabilidad 84
4.1.5 Nivel De Riesgo – Mapa De Calor 86
4.1.6 Criterios para la Aceptación de Riesgos 87
4.1.7 Tratamiento de los Riesgos 87
4.1.8 Plan de Tratamiento de los Riesgos 88

4.2 Cuadro de Evaluación de Riesgo 88
4.3 Identificación de Riesgos No Aceptables 100
4.4 Tratamiento del Riesgo 100
CAPÍTULO V. 124
DISEñO DE CONTROLES DE SEGURIDAD DE LA INFORMACIóN. 124
5.1 Declaración de Aplicabilidad. 124
5.1.1 Propósito, Alcance y Usuarios. 124
5.1.2 Aplicabilidad de Controles 125
5.2. Cronograma de la gestión de arranque del proyecto 157
5.3. Políticas a implementar 161
5.3.1 Política de Control de Accesos 161
5.3.2 Control de accesos 163
5.3.3 Política de Gestión de Usuarios 164
5.3.4 Política de Contraseñas 167
5.3.5 Política / Procedimiento De Acceso Al Data Center 169
5.3.6 Política de Seguridad Física 173
5.4. Implementación de controles lógicos 176

ABREVIATURAS

MAGERIT	Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información de los Administradores
EGSI	Esquema Gubernamental de Seguridad de la Información
ISO	International Organization for Standardization
SGSI	Sistema de Gestión de Seguridad de la Información
COVID-19	Coronavirus Disease 2019

ÍNDICE DE FIGURAS

FIGURA 2.1: MATRIZ DE ANÁLISIS DE RIESGOS Y CLASIFICACIÓN DE RIESGOS……..38
FIGURA 2.2: PROCESO DE GESTIÓN DE RIESGO MAGERIT 41
FIGURA 3.1: DIAGRAMA DE LA Red LAN DE LA UNIDAD EDUCATIVA....49
FIGURA 5.1: RECURSOS ADMINISTRADOS PAM360 176
FIGURA 5.2: LLAVES SSH USADA EN PAM360 177
FIGURA 5.3: AUDITORIA DE EVENTOS EN PAM360 177
FIGURA 5.4: EJEMPLO DE REPORTES GERENCIALES EN PAM 360....178
FIGURA 5.5: PANTALLA PRINCIPAL DE ADMANAGER PLUS 178
FIGURA 5.6: EJEMPLO DE REPORTE DE CAMBIOS DE CONTRASEÑA EN ADMANAGER.....179
FIGURA 5.7: EJEMPLO DE REPORTE DE COMPUTADORAS ACTIVAS EN ADMANAGER.....179
FIGURA 5.8: LISTADO DE TÉCNICOS ASIGNADOS ADMANAGER 180
FIGURA 5.9: LISTADO DE TAREAS AUTOMATIZADAS ADMANAGER ...180
FIGURA 5.10: PANTALLA PRINCIPAL LOG360.....181
FIGURA 5.11: RESUMEN DE GRÁFICAS GERENCIALES LOG360 181
FIGURA 5.12: ANÁLISIS DE COMPORTAMIENTO DE USUARIOS Y ENTIDADES LOG360 182
FIGURA 5.13: RESUMEN DE ESTADÍSTICAS DE SEGURIDAD LOG360 182

FIGURA 5.14: RESUMEN DE COMPLEMENTO DE ADMINISTRACIÓN DE ACTIVE DIRECTORY DENTRO DE LOG360 183

FIGURA 5.15: RESUMEN DE AUDITORÍA DE ACTIVE DIRECTORY DENTRO DE LOG360 183

ÍNDICE DE TABLAS

Tabla 1: Tabla de la familia de las Normas ISO 27000 33
Tabla 2: Estándares para confidencialidad 43
Tabla 3: Estándares para integridad 44
Tabla 4: Estándares para disponibilidad 45
Tabla 5: Criterios para determinar las categorías de las amenazas 45
Tabla 6: Criterios para determinar las categorías de las vulnerabilidades 46
Tabla 7: Características del servidor de Base de Datos 50
Tabla 8: Características de Laptop HP 51
Tabla 9: Módulos de la plataforma FIXED 53
Tabla 10: Inventario de Activos. 61
Tabla 11: Activos de Información - Documentos y registros. 62
Tabla 12: Activos de Información - Activos Auxiliares. 62
Tabla 13: Activos de Información - Activos Intangibles. 62
Tabla 14: Software - Sistemas Operativos. 63
Tabla 15: Software - Plataforma FIXED. 64
Tabla 16: Software - Plataforma Moodle. 65
Tabla 17: Software - Software de aplicación de oficina. 65
Tabla 18: Activos Físicos - Hardware Portátil. 65
Tabla 19: Activos Físicos - PC´s de Oficina. 66
Tabla 20: Activos Físicos - Equipos de Oficina. 66

Tabla 21: Activos Físicos - Soporte Electrónico. 67

Tabla 22: Activos Físicos - Medios de Comunicación. 67

Tabla 23: Activos Físicos – Establecimiento. 68

Tabla 24: Servicios – Establecimiento. 68

Tabla 25: Servicios – Energía. 68

Tabla 26: Servicios – Correo Electrónico. 69

Tabla 27: Servicios – Portal Externo. 69

Tabla 28: Personas/Personal. 70

Tabla 29: Roles en Sistemas de Tratamiento de Información de la Unidad Educativa……...73

Tabla 30: Matriz de Amenazas. 80

Tabla 31: Matriz de Vulnerabilidades. 83

Tabla 32: Repercusión. 84

Tabla 33: Probabilidad. 85

Tabla 34: Mapa de calor – Nivel de riesgo. 86

Tabla 35: Valoración del riesgo. 86

Tabla 36: Evaluación de riesgos. 99

Tabla 37: Totalidad de riesgos no aceptables. 100

Tabla 38: Cuadro de tratamiento de riesgos 123

Tabla 39: Controles aplicables de la normativa ISO 27001:2013 basados en la política de la seguridad de la información 126

Tabla 40: Controles aplicables de la normativa ISO 27001:2013 basados en organización de la seguridad de la información 128
Tabla 41: Controles aplicables de la normativa ISO 27001:2013 basados en la seguridad de los recursos humanos 130
Tabla 42: Controles aplicables de la normativa ISO 27001:2013 basados en la política de la seguridad de la información 134
Tabla 43: Controles aplicables de la normativa ISO 27001:2013 basados en el control de accesos 139
Tabla 44: Controles aplicables de la normativa ISO 27001:2013 basados en la seguridad de las operaciones 145
Tabla 45: Controles aplicables de la normativa ISO 27001:2013 basados en la seguridad de las comunicaciones 147
Tabla 46: Controles aplicables de la normativa ISO 27001:2013 basados en la seguridad de las comunicaciones 149
Tabla 47: Controles aplicables de la normativa ISO 27001:2013 basados en gestión de incidentes de seguridad 153
Tabla 48: Controles aplicables de la normativa ISO 27001:2013 basados en la continuidad del negocio 156
Tabla 49: Cronograma de gestión de arranque del proyecto 161
Tabla 50: Cronograma de socialización de políticas de seguridad de la Unidad Educativa 175

INTRODUCCIÓN

Para este proyecto de investigación se realizó el análisis de la norma ISO/IEC 27002:2013, con el objetivo principal de analizar la situación actual del manejo de la información para identificar los tipos de normas ISO/IEC que se utilizan para el control de seguridad de la información, con el fin de determinar políticas de seguridad utilizando la norma ISO/IEC 27002:2013 para mejorar los controles de accesos lógicos a las plataformas y sistemas utilizados en la Unidad Educativa Particular de Guayaquil. La característica principal de este proyecto es diseñar políticas de seguridad de la información para mejorar los controles de la seguridad de la información. Para hacer posible el proyecto de investigación es necesario tener muy claro cuáles son las posibles vulnerabilidades y amenazas que existen en el plantel educativo particular de Guayaquil. Y de acuerdo con el análisis se identificó que no cuenta con políticas de seguridad de la información, de acuerdo con los avances tecnológico es necesario contar con normas de seguridad para dominar posibles amenazas y ser una institución de mejor calidad.

CAPITULO I.

GENERALIDADES

1.1. Antecedentes

Para garantizar la seguridad de la información dentro de las organizaciones, es recomendable establecer un sistema de gestión de seguridad de la información (SGSI) que facilite el control y la gestión segura de la información [1]**.** La implementación de un SGSI abarca estrategias y políticas destinadas a preservar la confidencialidad, integridad y disponibilidad (CIA) de los activos de información empresarial críticos [2]**.**

Además, un SGSI permite a las organizaciones mejorar la eficacia de la gestión de sus activos de información [3]**.** Este estándar define requisitos y medidas de seguridad que pueden integrarse en un SGSI, proporcionando a las organizaciones el marco necesario para gestionar sus activos de información [4]**.** El estándar ofrece soporte para implementar, establecer, operar y mejorar el SGSI de la organización, que puede adaptarse para satisfacer necesidades organizacionales específicas [5]. Mientras que ISO/IEC 27001 proporciona una descripción general de las medidas de seguridad, ISO/IEC 27002 ofrece directrices detalladas, centrándose en medidas de seguridad técnicas y formales. No adoptar un SGSI adecuado para las operaciones y los sistemas de información puede comprometer la capacidad de garantizar la continuidad del negocio [6]. Al adherirse a estándares como la serie ISO/IEC 27000, las organizaciones pueden establecer un marco SGSI sólido. Esta serie de estándares proporciona requisitos que ayudan a salvaguardar eficazmente los activos de información de una organización [7]. La implementación de la serie ISO/IEC 27000 garantiza que la organización cuente con un SGSI adecuado. Las organizaciones deben aprovechar los estándares de seguridad de la información para implementar medidas de seguridad adecuadas [8]. Sin embargo, seleccionar e implementar un estándar SGSI apropiado puede plantear desafíos [9]. Por el contrario, las organizaciones deben demostrar su compromiso con prácticas comerciales seguras mediante la adopción de directrices autorizadas [10]. Es importante

porque los socios comerciales pueden exigir prueba de protección de activos de información. Por lo tanto, debería haber evidencia disponible que muestre medidas de protección adecuadas [11].

Además, las organizaciones adoptan principalmente estándares de seguridad de la información para garantizar y gobernar el mercado [12]. Estos estándares se consideran herramientas necesarias e influyentes hoy en día, dadas las crecientes amenazas del cibercrimen, el hacktivismo y los gobiernos extranjeros que atacan valiosos activos organizacionales [13]. En otras palabras, salvaguardar los activos de información de las organizaciones es crucial, particularmente en entornos empresariales interconectados, para mitigar el impacto de los incidentes de seguridad y garantizar la continuidad del negocio [14]. Al obtener la certificación ISO/IEC 27001, las organizaciones pueden demostrar que han alcanzado un nivel aceptable de seguridad, fomentando la confianza del cliente [15]. Además, la norma no sólo guía a las organizaciones en la implementación de un sistema de gestión, sino que también apunta a mejorar su legitimidad y credibilidad [16].

La legitimidad se puede clasificar en tres dominios: legitimidad de entrada, rendimiento y salida [17]. Para lograr la legitimidad de los resultados a través de ISO/IEC 27001, la norma debe abordar de manera efectiva la resolución colectiva de problemas [18].

Una vez recopilado diversos enfoques de la implementación de los estándares de seguridad de la información, se hablará de donde se lo implemente, pues bien la unidad educativa es un centro de educación superior ubicado en la ciudad de Guayaquil, este cuenta con más de 30 años de trayectoria, en dicho sitio también funciona las fases de educación básica y bachillerato, así como, brindando servicios de educación de tercer nivel a través de sus distintas carreras, adicionalmente existe otra división de un instituto tecnológico pero que no se lo tomara en cuenta para este trabajo, solo la unidad educativa (escuela y colegio).

En los dos últimos años a partir de la pandemia COVID-19, la unidad educativa ha tenido la necesidad de generar la implementación de sistemas tecnológicos de información que permitan realizar una mejor gestión de los procesos académicos que se llevan internamente, dando apertura a los Sistemas Académico y entornos virtuales de Aprendizaje los cuales manejan procesos académicos de forma electrónica, que antes se realizaban manualmente.

Aunque la tecnología es un elemento indispensable de cualquier organización, debe utilizarse de forma adecuada para evitar riesgos en la gestión de la información. Por tanto, es de extrema importancia que se adopten las decisiones y medidas necesarias antes de que se produzca un incidente de seguridad de la información.

En la actualidad, la unidad educativa, no cuenta con políticas y/o procedimientos de control de acceso para sus sistemas de tratamiento de información, que permitan establecer algún tipo de control sobre los usuarios, y en lo que respecta a las áreas en donde se almacena información confidencial e importantes para el plantel educativo, los controles de seguridad física son muy escasos y no se tiene una vigilancia permanente sobre estas áreas.

La norma ISO/IEC 27002 mantiene una serie de controles utilizados para establecer directrices de gestión de seguridad de la información que se detallará en el capítulo 2, y puede ser aplicada en industrias y organizaciones de todo tipo y tamaño.

La unidad educativa al no contar con los controles de seguridad adecuados mantiene el riesgo de que se presenten accesos no autorizados, modificación de información, y demás incidentes de seguridad.

1.2. Descripción del Problema

En los últimos cuatro años, Ecuador ha visto un aumento significativo en la adopción e integración de tecnologías, tanto a nivel corporativo como individual, no solo por las nuevas TIC, sino también por la situación sanitaria presentada por el COVID-19 y la forma de como drásticamente se tuvo que

adaptar a impartir clases de manera online y mejorar la seguridad de la información.

Para abordar este nuevo problema y asegurar su continuidad, las empresas más representativas de la economía ecuatoriana, como organismos financieros, empresas comerciales privadas e instituciones públicas, han automatizado o están automatizando sus servicios.

Por lo tanto, el desarrollo de esta transformación digital de las empresas genera desafíos en materia de ciberseguridad, especialmente para los bancos del Ecuador.

Por otro lado, la falta de profesionales en ciberseguridad ha obligado a las empresas existentes en Ecuador a considerar ciertas limitaciones operativas en sus servicios y no pueden ofrecer un alto nivel de sofisticación a sus clientes.

Con base en lo anterior, las empresas que luchan con problemas de seguridad cibernética necesitan una solución sostenible e innovadora. [19]**.**

En los últimos años posteriores a la pandemia, la unidad educativa ha puesto más énfasis en la necesidad de implementar sistemas de información técnica para mejorar los procesos académicos que se llevan a cabo dentro de la unidad educativa, gestionar información confidencial y, además, el departamento mantiene áreas catalogadas como sensibles al manejar información privilegiada pero no existe ninguna acción específica para ello sino

solo un control manual de vez en cuando. Debido a que estas áreas y sistemas de tecnología de la información no tienen controles para limitar el acceso lógico al nivel de seguridad de la información, la organización es vulnerable a varios tipos de incidentes, como fuga de información, uso no autorizado y ataques a la integridad, disponibilidad y la confidencialidad; y otros principios de seguridad de la información, lo que desprestigia a la unidad educativa.

Además, los roles y derechos de acceso en el sistema de procesamiento de información no están claramente definidos y no existe un proceso documentado para la salida del usuario cuando finaliza la relación contractual, durante las vacaciones, entre otros aspectos que no están reglamentados.

Finalmente, en Ecuador, donde las instituciones no han implementado los controles necesarios para protegerse efectivamente, la pérdida de información puede ser grave y la recuperación puede llevar mucho tiempo, ya que los ciberataques pueden provocar incendios, pérdida de estudiantes y certificados.

1.3. Solución Propuesta

La solución propuesta es asegurar la implementación de los controles definidos en la norma ISO/IEC 27002:2013, ya que nos proporciona las mejores prácticas para controlar el acceso a los sistemas y áreas de procesamiento de información. Definir los activos de información y los tipos de

controles de acceso que se pueden utilizar para mantener la confidencialidad, disponibilidad e integridad de esos activos de información.

Realizar evaluación de riesgos y procesamiento de activos de información con base en los principios de seguridad, así como analizar vulnerabilidades y amenazas de los activos definidos previamente.

Controlar quién tiene acceso a la información de la institución es el primer paso para protegerla. Es muy importante que decidamos quién tiene acceso a nuestra información, cómo, cuándo y con qué fines.

Este proyecto se puede utilizar para cumplir con todas las regulaciones para la unidad educativa sobre seguridad de la información o para ayudar en el proceso de certificación educativa correspondiente.

1.4. Objetivos

1.4.1 Objetivo General

Diseñar políticas y controles de acceso lógicos para los sistemas y áreas de tratamiento de información siguiendo la norma ISO/IEC 27002:2013 en una unidad educativa particular de Guayaquil para prevenir y mitigar los incidentes de seguridad de la información que alteren la integridad, confidencialidad y disponibilidad.

1.4.2 Objetivos Específicos

- Identificar y realizar levantamiento de información de los activos, plataformas y áreas donde se da el tratamiento de información junto con los roles, control de usuarios y acceso dentro de la unidad educativa.
- Generar el análisis mediante matriz de riesgo de las vulnerabilidades identificadas en los accesos lógicos a la plataforma y los activos de la unidad educativa.
- Diseñar políticas de control, monitoreo y reporte de los accesos lógicos para los sistemas y áreas de tratamiento de información.

1.5. Metodología

El enfoque de esta investigación es de tipo no experimental, con enfoque transversal de alcance descriptivo con muestreo por cuota basado en entrevistas, procediendo de la siguiente manera:

- Entrevistas al personal del departamento de Gestión Tecnológica, docentes, personal administrativo, que tienen accesos a los sistemas y equipos informáticos de la unidad educativa
- Identificar el conocimiento que poseen los entrevistados en cuanto a la seguridad de la información y la responsabilidad que conlleva.

- Realizar evaluación de riesgos existentes en las funciones, procesos, accesos, y perfiles que poseen los entrevistados
- Diseño de políticas de seguridad de la información aplicado a los controles de accesos lógicos basado en roles y perfiles; cubriendo la reducción, mitigación y tratamiento de riesgos.

CAPITULO II.

MARCO TEÓRICO

Este capítulo introduce los conceptos teóricos de diversos temas necesarios para el desarrollo de este proyecto, tales como: activos de información, seguridad de la información, pilares de seguridad, gestión de riesgos, normas ISO/IEC 27001 – 27002 y controles de seguridad de acceso lógico y de entidades.

2.1 Seguridad de la Información en una Organización y de los Sistemas Informáticos

Una organización o negocio debe ser consciente de que la información es un activo importante o esencial para la continuidad del negocio, por lo que debe

contar con medidas para asegurar su integridad, disponibilidad y confidencialidad; sin embargo, muchas empresas u organizaciones se centran únicamente en la aplicación de seguridad física, ignorando otros aspectos relacionados directamente con el procesamiento y gestión de la información, denominados “seguridad de la información”.

Cabe señalar que es casi imposible garantizar un nivel integral de protección, pero el propósito de aplicar una política de seguridad de la información es garantizar que una empresa u organización comprenda, asuma, gestione y minimice por escrito los riesgos de seguridad de la información.

En cuanto lo indicado por Gómez [20], la seguridad de sistemas informáticos puede definirse como cualquier medida implementada para evitar actividades no autorizadas en un sistema o red informática, cuyo impacto pueda amenazar su integridad, confidencialidad o autenticidad y perjudicar la seguridad de los sistemas o redes informáticas.

Además de la seguridad de un sistema informático, su funcionamiento o sistema de acceso no autorizado también está diseñado para:

- Seguir las leyes y regulaciones según el tipo de empresa u organización y el país en el que se encuentra.
- Registro de acceso al sistema informático.
- Control de acceso a los servicios del sistema informático

2.2 Definición e Implantación de las Políticas de Seguridad

Las organizaciones o empresas que quieran desarrollar e implementar reglas de seguridad de la información de acuerdo con los estándares internacionales deben desarrollar una política de seguridad de la información; este proceso se puede desarrollar con base en la norma ISO 27000 y sus series; las buenas prácticas relacionadas con la seguridad de la información pueden basarse en la norma ISO/IEC 27002.

La Organización Internacional de Normalización (ISO) y la Comisión Electrotécnica Internacional (IEC) son responsables de desarrollar normas y directrices de seguridad relacionadas.

A través de los sistemas de gestión, la estandarización permite que sean aplicados a cualquier tipo de negocio u organización a nivel internacional para facilitar el comercio global, el intercambio de información y apoyar la transferencia de tecnología tal como se lo detalla Mentor [21] ver Tabla1.

El conjunto de normas ISO/IEC 27000 reúne estándares de seguridad para proporcionar un marco de referencia para la gestión de la seguridad.

Estos estándares incluyen las mejores prácticas recomendadas en el entorno de seguridad de la información y permiten el desarrollo e implementación de políticas y sistemas de gestión de seguridad de la información.

Norma	Descripción
ISO/IEC 27000	Vocabulario estandarizado para el Sistema de Gestión de Seguridad de la Información (SGSI) y para todas las normas de la familia.
ISO/IEC 27001	Norma que puede ser certificable, a través de una auditoría, la empresa u organización debe tener implementado un SGSI.
ISO/IEC 27002	Guía de buenas prácticas a través de las cuales una organización o empresa puede mejorar la seguridad de la información.
ISO/IEC 27003	Establece las directrices para el diseño de un SGSI durante todas sus etapas.
ISO/IEC 27004	Establece una variedad de buenas prácticas para la evaluación y medición de la gestión de la seguridad de la información.
ISO/IEC 27005	Esta norma se centra en establecer las directrices y recomendaciones para la gestión de riesgos en un SGSI.
ISO/IEC 27006	Esta norma contiene la guía y directrices para la acreditación de las organizaciones encargadas de auditar los SGSI.
ISO/IEC 27007	Establece las directrices para los organismos de certificación acreditados con la finalidad de auditar un SGSI.
ISO/IEC 27799	Establece y proporciona los controles de seguridad para la protección de la información personal en los entornos relacionados a la salud.

Tabla 1: Tabla de la familia de las Normas ISO 27000

Fuente: Mentor, 2016

2.2.1 Norma ISO/IEC 27001

ISO/IEC 27001:2013 se utiliza para la certificación de sistemas de gestión de seguridad de la información.

Al utilizar este estándar, una organización puede demostrar su integridad a todos sus clientes u organizaciones con las que tiene algún tipo de relación.

Gestiona la seguridad de tu información, una característica que aumenta el valor de la disponibilidad de tu empresa.

La norma ISO 27001:2013 fue desarrollada para definir los requisitos para establecer, implementar y mantener un proceso de mejora continua para los sistemas de gestión de seguridad de la información. La implementación de un SGSI en una empresa u organización dependerá de las necesidades, objetivos, tamaño y estructura de la organización [22].

La norma ISO 27001:2013 define 10 puntos de la siguiente manera (ISO 27001):

1. Propósito y alcance: describir el propósito de la norma. Documentos normativos de referencia.
2. Términos y definiciones: Términos y definiciones de ISO/IEC 27000.
3. Entorno Organizacional: Identificar los aspectos externos e internos que afectan el sistema de gestión de seguridad de la información de la organización. Esta sección debe especificar el alcance del SGSI.
4. Liderazgo: Se refiere al compromiso y liderazgo que debe poseer la alta dirección de una organización en todos los procesos de seguridad de la información, así como el compromiso de recursos para implementarlos y operarlos.

5. Planificación: Analizar, valorar y evaluar riesgos, abordar riesgos y, además la organización debe fijar objetivos de seguridad de la información.
6. Soporte: Se refiere al documento informativo de recursos, capacidades personales e importancia que se le da a la implementación, mantenimiento y mejora continua del SGSI.
7. Operaciones: cómo se planifican y controlan las operaciones y se evalúan y gestionan los riesgos.
8. Planificación, Implementación y Control: El proceso de cumplimiento de requisitos relacionados con la seguridad de la información, evaluación y tratamiento de riesgos.
9. Evaluación del desempeño: seguimiento, medición, análisis y evaluación del SGSI; También se analiza la auditoría dentro de la organización.
10. Mejora: Se refiere a la gestión de desviaciones, acciones correctivas y mejora continua.

La segunda parte de ISO 27001:2013 contiene anexos que definen objetivos de control y controles de referencia de acuerdo con los enumerados en ISO/IEC 27002:2013.

2.2.2 Norma ISO/IEC 27002

La norma ISO/IEC 27002:2013 proporciona orientación sobre estándares de seguridad de la información para empresas y organizaciones, incluidas buenas prácticas de gestión de seguridad de la información a través de las partes de implementación y control del entorno de riesgo de seguridad de la información (Organización Internacional de Normalización) de la norma ISO/IEC 27002: Norma 2013., 2017.

La norma ISO/IEC 27002:2013 está destinada a organizaciones o empresas que pretenden en el proceso de implementación de un sistema de gestión de seguridad de la información basado en la norma ISO/IEC 27001, seleccionar elementos de control y habilitar el monitoreo de seguridad de datos.

La norma ISO 27002:2013 se divide en 14 capítulos que definen las áreas a considerar para garantizar la seguridad de la información de una organización o empresa [23]. Hay un total de 114 controles en la norma.

2.3 Metodología para el Análisis de Riesgos (Metodología MAGERIT)

El riesgo se define como la posibilidad de que una amenaza ocurra o no debido a vulnerabilidades existentes en un sistema informático o su entorno; cuyas consecuencias pueden causar daños a los servicios, equipos, proyectos, archivos, programas, materiales y otros activos informáticos de una organización o empresa.

Cuando una organización o empresa enfrenta un riesgo, pueden existir varias opciones:

- La aceptación: si un activo está dañado y no tiene valor, tiene sentido correr el riesgo.
- Tomar medidas para reducirlo o eliminarlo.
- Transferencia de riesgo (por ejemplo, compra de seguro).

Ataque: Un ataque accidental o intencional ocurre cuando se materializa una amenaza a un activo.

- **Amenazas:** Una amenaza se puede definir como un evento que puede causar daño a un sistema de información o su entorno.
- **Vulnerabilidades:** Una vulnerabilidad es una debilidad que puede ser aprovechada por una o más amenazas para causar daño a un activo u organización.

Para la evaluación de riesgo se concluye con una interpretación del mismo, utilizando la conocida Matriz de análisis, donde es posible determinar la probabilidad de riesgo versus la magnitud de daño, tomando valores respectivamente desde el 1 hasta el 4, considerando una clasificación de riesgo bajo, medio y alto versus las consecuencias [24]. Ver Figura 1.

FIGURA 2.1: MATRIZ DE ANÁLISIS **DE RIESGOS Y CLASIFICACIÓN DE RIESGOS**

Fuente: Zaragoza 2015

Metodología

La información es patrimonio de cualquier institución u organización pública o privada; la falta de información o información errónea puede conducir a fallas organizativas.

Si la información cumple con los requisitos de una empresa u organización, se puede considerar información de calidad en función de sus tres atributos:

- La integridad
- La disponibilidad
- La confidencialidad

La seguridad de la información es una disciplina que abarca la protección de los sistemas físicos, la prevención de accidentes o la prevención de actividades fraudulentas por parte de los empleados de una organización o empresa. [20].

El objetivo de la seguridad de la información se basa en tres principios que deben seguir los sistemas informáticos.

Confidencialidad

Se relaciona con la privacidad de la información almacenada y procesada en un sistema informático. Según este principio, las herramientas de seguridad deben proteger el sistema de intrusos y del acceso de personas o procesos no autorizados.

Disponibilidad

La integridad de la información se refiere a la validez y coherencia de la información almacenada; las herramientas de seguridad deben garantizar la sincronización del proceso de actualización para evitar la duplicación de información.

Integridad

La disponibilidad de la información se refiere a la continuidad del acceso a la información almacenada y procesada en un sistema informático; Según este

principio, las herramientas de seguridad deben facilitar la información que permanece en el sistema.

Metodología Magerit

MAGERIT es una metodología de análisis y gestión de riesgos que fue elaborada por la Administración Pública Española. Esta metodología está directamente relacionada con la generalización del uso de las tecnologías de la información [25], manteniendo beneficios para quien haga uso de ella. Logrando reconocer las amenazas que afecten a la corporación empresarial y las vulnerabilidades que pueden ser empleadas por dichas amenazas.

Consiguiendo así, el diseño adecuado de las medidas preventivas y correctivas más idóneas.

Magerit implementa el Proceso de Gestión de Riesgos dentro de un marco de trabajo [26] Ver Figura2, para que los entidades tomen decisiones teniendo en cuenta los riesgos derivados del uso de tecnologías de la información.

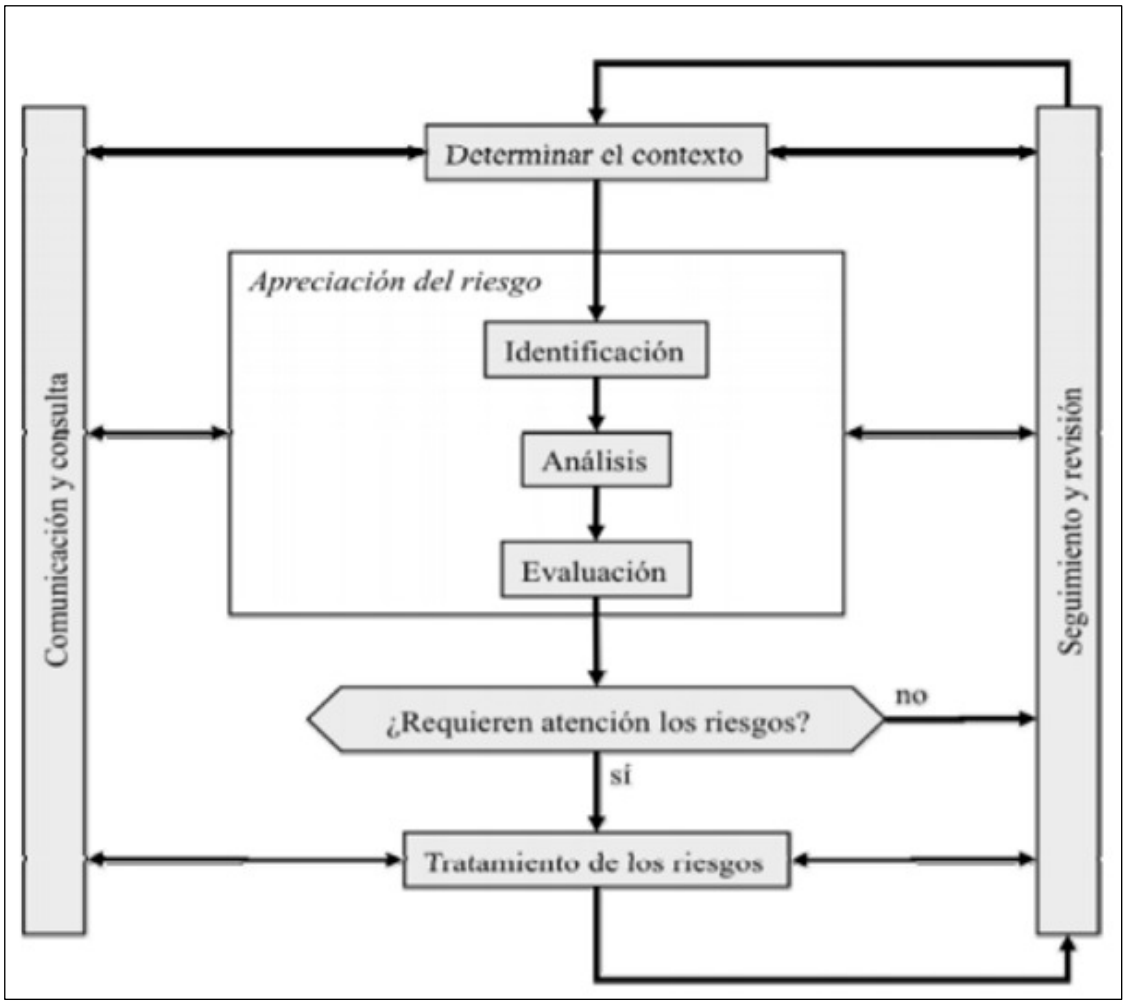

FIGURA 2.2: PROCESO DE GESTIÓN DE RIESGO MAGERIT

Fuente: Marquina 2012

Determinar los activos de la organización

El primer paso es identificar los activos de la organización. Para realizar este análisis, necesita crear una lista de activos relevantes.

Los activos deben clasificarse en una de las siguientes categorías:

Dato: Elemento que materializa información

Servicios: necesarios para la organización del sistema.

Software - Aplicaciones informáticas: Le permite gestionar y administrar sus datos.

Hardware - Elemento informático: Equipo que permite alojar datos, aplicaciones e información.

Medio de almacenamiento: dispositivo de almacenamiento

Equipo adicional: Equipo informático adicional

Red de comunicación: Red que permite el intercambio de información.

Instalación: Donde se encuentran el equipo y el personal.

Personas: Recursos Humanos

Luego, el activo se evalúa en función de su impacto en su disponibilidad, confidencialidad e integridad. La siguiente tabla es una tabla de valoración de activos; La disponibilidad, la integridad y la confidencialidad deben evaluarse individualmente, y el promedio de estos tres criterios de seguridad de la información determinará la **importancia** de un activo:

Activos de información (confidencialidad)	Clase	Descripción
1	Pública	Puede ser revelado y proporcionado a terceras partes. Si el contenido fuera revelado, hubiera pequeños efectos en las operaciones de la unidad educativa.
2	Uso Interno	Puede solo ser revelada y proporcionado en Uniplex (no disponible a terceras partes). Si el contenido fuera revelado, no hubiera mucho efecto en las operaciones de la unidad educativa
3	Secreto	Puede ser solo revelado y proporcionado a partes específicas y departamentos. Si el contenido fuera revelado, hubiera un gran efecto en las operaciones de la unidad educativa.
4	Alta confidencialidad	Puede ser solo revelado y proporcionado a partes específicas. Si el contenido fuera revelado, hubiera un efecto irrecuperable en las operaciones de la entidad educativa.

Tabla 2: Estándares para confidencialidad

Fuente: Magerit v3

Activos de información (integridad)	Clase	Descripción
1	No necesaria	Usado solo para consulta. No tiene posibles problemas
2	Necesaria	Si el contenido fuera falsificado, hubiera problemas, pero estos no afectarían mucho las operaciones de la unidad educativa
3	Importante	Si la integridad se perdiera, hubiera un efecto fatal en las operaciones de la unidad educativa

Tabla 3: Estándares para integridad

Fuente: Magerit v3

Activos de información (disponibilidad)	Clase	Descripción
1	Bajo	Si la información no llegara a estar disponible, no hubiera efectos en las operaciones de la unidad educativa
2	Mediano	Si la información no llegara a estar disponible, hubiera algún efecto en las operaciones de la unidad educativa. Sin embargo, métodos alternativos pudieran ser usados para las operaciones, o los procesos podrían ser demorados hasta que la información esté disponible

3	Alto	Si la información no estuviera disponible cuando sea necesitada en algún momento, hubiera un fatal efecto en las operaciones de la unidad educativa.

Tabla 4: Estándares para disponibilidad

Fuente: Magerit v3

La frecuencia de ocurrencia de las amenazas debe ser evaluada. A partir de la lista de amenazas, las amenazas deben ser revisadas basadas en la experiencia de operaciones y datos estadísticos que han sido ya coleccionados.

Las amenazas son típicamente divididas en tres categorías: “Baja”,”Media”,”Alta”.

Amenazas		
Probabilidad de ocurrencia	Clase	Descripción
1	Bajo	Hay una baja probabilidad. La frecuencia de ocurrencia es una vez al año o menos.
2	Medio	Hay una moderada probabilidad. La frecuencia de ocurrencia es una vez cada medio año o menos.
3	Alto	Hay una alta probabilidad. La frecuencia de ocurrencia es una vez al mes o más

Tabla 5: Criterios para determinar las categorías de las amenazas

Fuente: Magerit v3

Vulnerabilidades		
Probabilidad de ocurrencia	Clase	Descripción
1	Bajo	Se tiene controles de seguridad muy débiles o no se tiene ningún control de seguridad, de tal manera que esta vulnerabilidad es susceptible de ser explotada fácilmente
2	Medio	Hay un moderado control de seguridad
3	Alto	Si en el activo se tiene los controles de seguridad adecuados, de tal manera que sea muy difícil explotar esta vulnerabilidad

Tabla 6: Criterios para determinar las categorías de las vulnerabilidades

Fuente: Magerit v3

CAPÍTULO III.

ANÁLISIS Y SITUACIÓN ACTUAL

Este capítulo se describirá la infraestructura actual de la red de la unidad educativa de Guayaquil hasta finales de diciembre del 2023, los datos obtenidos son resultado de la información recogida en colaboración del administrador de la red de la unidad educativa, inventario realizado y revisión de las instalaciones físicas de la red.

Esta información permitirá realizar el análisis de la situación actual de la red en cuanto a seguridad para determinar el punto de partida para la implementación del Sistema de Gestión de Seguridad.

3.1 Infraestructura de red de la unidad educativa

La unidad educativa opera en la Av. Juan Tanca Marengo, ubicado en el norte de la ciudad de Guayaquil.

La unidad educativa posee cuatro edificios, los cuales tienen 4 pisos respectivamente, que son distribuidos en áreas administrativas y aulas que se encuentran separadas por las escaleras de acceso y dividido por secciones.

Con respecto a la disposición física de los servidores y equipos de la unidad educativa, estos se encuentran ubicados en una pequeña área dedicada al personal de soporte y equipos de redes que cuenta con una puerta de seguridad para su acceso. Los pisos ocupados por la Unidad educativa son de concreto, y cuentan con cableado estructurado categoría 6, lo que facilita la administración física de la red.

No cuentan con planta propia de energía eléctrica, lo que causa complicaciones en el desenvolvimiento de las funciones, ya que el 2023 ha existido cortes de energía eléctrica.

Debido a la confidencialidad, se nos ha permitido un bosquejo estratégico de la estructura de la red de datos; la cual se adjunta a continuación:

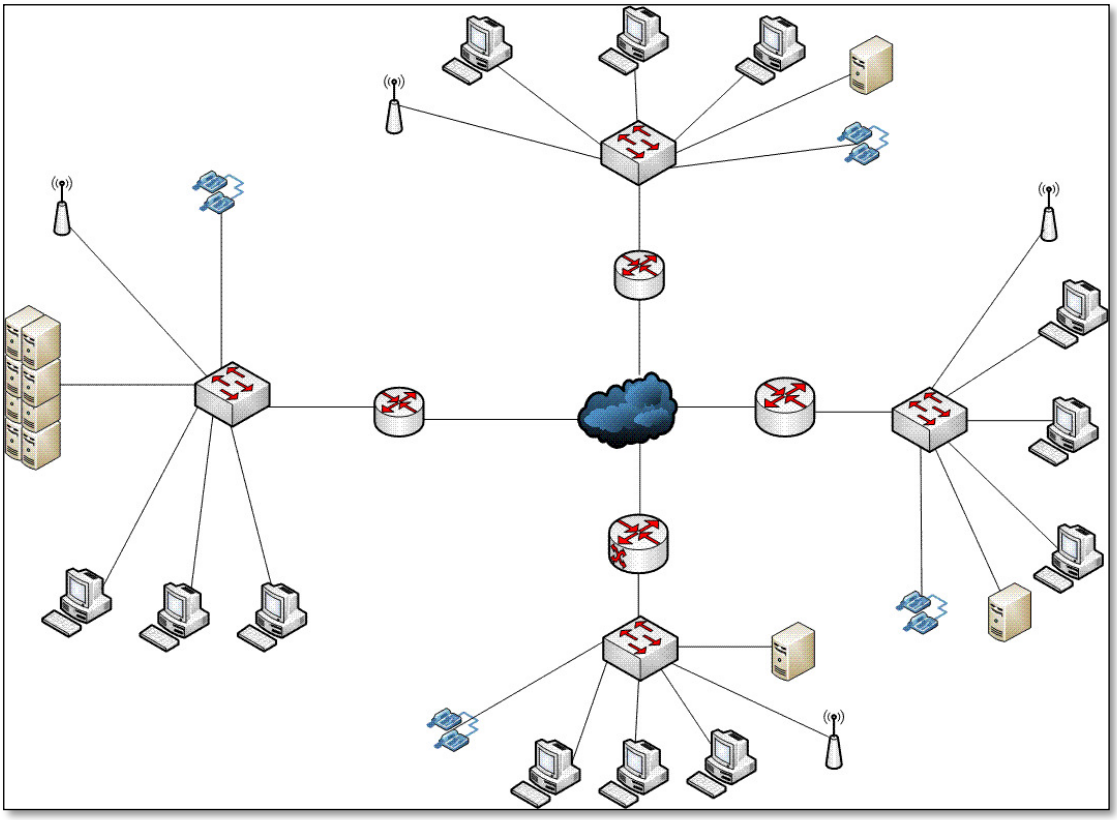

FIGURA 3.1: DIAGRAMA DE LA RED LAN DE LA UNIDAD EDUCATIVA

Fuente: Anny Cárdenas y Lissette Munizaga

La red LAN cuenta con dos servidores, y las estaciones de trabajo están divididas de acuerdo con la necesidad de distribución de red actual de la unidad educativa, el cual se encuentra alejado de las aulas donde la mayoría son desktop y unas pocas portátiles que se encuentran en el edificio principal, y se distribuyen por departamentos como se muestra en la figura 3.

En el pequeño cuarto de servidores se tiene:

- 8 Switch HP de 24 puertos, para la interconexión a la red hacia los equipos de acceso.
- 1 Firewall Fortinet puesto por el proveedor de Internet, el mismo que cuenta con varios puertos disponibles para la conexión de red interna y para la cual se mantiene aplicadas políticas de filtrado de paquetes de acuerdo con las necesidades de la institución educativa.

Datos de los Servidores

La unidad educativa particular de Guayaquil cuenta con dos servidores; los cuales se detallan a continuación:

Base de Datos: Se utiliza como base de datos SQL, con las siguientes características del hardware:

Base de Datos: SQL	
Aplicación	FIXED y MOODLE
Procesador	Intel Xeon E-2224G - 3.5Ghz
Modelo	DELL
Disco Duro-SATA	1 TB
Memoria UDIMM	16GB
Sistema operativo	Windows Server

Tabla 7: Características del servidor de Base de Datos

Fuente: Anny Cárdenas y Lissette Munizaga

Correo Electrónico y Sistema de Aplicaciones: Se utiliza la opción Microsoft 365 en nube y también para los sistemas contables se utiliza un desarrollo llamado FIXED

Datos De Las Estaciones De Trabajo

Las estaciones de trabajo tienen instalado el antivirus básico, así como Microsoft Office 365 y, utilizan como navegador web Firefox y Chrome ya que no hay una política al respecto, así como en ciertas maquinas el acceso a otras aplicaciones como Acrobat Reader, impresoras dependiendo del usuario.

A continuación, se detallan las características de los equipos:

LAPTOP DELL	
Modelo	CLON
Procesador	Intel Core i3
Disco Duro	250 GB
Memoria	8 GB
Sistema Operativo	Windows

Tabla 8: Características de Laptop HP

Fuente: Anny Cárdenas y Lissette Munizaga

Además, en la red LAN se encuentran conectadas 10 impresoras de las cuales son de la marca EPSON.

Actualmente en la red interna no se encuentra implementado ningún sistema de gestión que permita una administración de la red. Es decir, no cuenta con ninguna herramienta de Software, Hardware que permita el monitoreo de la red y el análisis de vulnerabilidades.

Estructura De La Red WAN De La Unidad Educativa

La unidad educativa cuenta con un enlace para acceso a Internet, de la que los equipos que brindan el servicio son administrados por el proveedor.

Cuenta con un router y un firewall que es propiedad del proveedor del servicio de Internet, para proveer y gestionar el servicio de Internet restricciones a la red interna.

Seguridad De La Información Implementada Actualmente En La Unidad Educativa

Para proporcionar una visión de la situación actual de la seguridad en la unidad educativa, se realizó un análisis para determinar el grado de seguridad y saber cómo se ha venido salvaguardando las ventajas competitivas.

Seguridad De Las Comunicaciones de la plataforma FIXED

Plataforma FIXED: esta plataforma posee dos módulos, uno administrativo y uno académico.

Los cuales se distribuyen de la siguiente manera:

Módulo	
Administrativo	Departamento Financiero
	RRHH
	Colecturía
Académico	Docentes
	Secretaría
	Colecturía

Tabla 9: Módulos de la plataforma FIXED

Fuente: Anny Cárdenas y Lissette Munizaga

Contraseñas nuevas y cambio de contraseña: la contraseña que se almacena en la base de datos es encriptada.

- El usuario no posee la opción de “olvidé la contraseña” para poder generar él mismo el cambio/reseteo de la misma
- Si el usuario se olvida de la contraseña, proceden con la notificación vía correo electrónico y en ciertas ocasiones vía WhatsApp, a los administradores de sistemas para que este realice el cambio. Luego el administrador de sistema desde su perfil administrador habilita el

proceso de reseteo de contraseña donde la contraseña por defecto será 1234.

- No cuenta con políticas de contraseña, es decir no valida tipo o cantidad de caracteres ingresados para la clave.
- No cuenta con solicitud de cambio periódico o expiración de contraseña.
- No cuenta con un registro historial de los cambios solicitados y realizados en las contraseñas de los usuarios.

Seguridad De Las Comunicaciones PLATAFORMA MOODLE

- Utilizada por docentes y estudiantes, asociada a la cuenta de office 365. En esta aplicación, los docentes comparten información, actividades sincrónicas y asincrónicas; la cual podríamos decir que se asimila a TEAMS.
- Los usuarios no cuentan con permisos para realizar cambio de contraseña, de ser necesario realizarse en la plataforma (Office 365). El docente o estudiante debe dirigirse al área técnica mediante WhatsApp para que le proporcionará una contraseña temporal, y se le habilita al usuario el cambio para que este ingrese su nueva contraseña. En el caso de los estudiantes, la solicitud la realizan por medio de inspectoría o los envían al departamento de sistemas para que le generen contraseña temporal (que suelen dar el nombre del estudiante y un número).

- Entre la característica de esta contraseña se solicita que sea mínimo de ocho caracteres y que incluya letras y números) no considera mayúsculas y minúsculas).
- De forma reiterada el administrador de sistemas ha brindado la misma contraseña temporal al docente o estudiante.
- Una vez registrado o ingresado la contraseña proporcionada por el administrador en la plataforma Moodle, lo direcciona al correo de Office 365 donde obliga al usuario a actualizarla. El usuario no puede mantener la contraseña proporcionada por el administrador.
- La contraseña normalmente se la brinda al inicio de año lectivo de los estudiantes.
- Estudiantes y docentes utilizan autoguardado (olvidan contraseña), y los estudiantes comparten contraseñas.
- No cuenta con logs automáticos de contraseñas, ni registros manuales de los usuarios que han solicitado cambio de esta.

Control de Acceso a los Equipos Administrativos

Mediante directorio activo, el administrador puede acceder a los equipos informáticos del personal administrativo (actualizaciones, antivirus).

- Cada usuario posee usuario y contraseña a las máquinas asignada.
- El usuario no puede realizar instalaciones de ningún tipo.

- El acceso a páginas es controlado mediante el equipo FW (FORTINET) del proveedor de internet.
- No posee control de dispositivos periféricos.

Control de Acceso a los Servidores

Poseen un solo servidor con una máquina virtual de AZURE, a esta se accede con un único usuario y el acceso se lo realiza mediante escritorio remoto.

El Usuario de acceso, únicamente lo conocen dos personas del departamento de sistemas.

Control de Acceso a Base de Datos

Poseen usuario “administrador”, lo manejan únicamente dos personas.

Se realiza respaldo de información regularmente 3 veces por semana, el mismo que está conectado a otro servidor (disco en la nube).

Control de Acceso a Correos Electrónicos de la Unidad Educativa

- No utilizan plataforma de Zimbra.
- El correo es manejado mediante plataforma office 365 (Outlook).
- No poseen servidor de correo electrónico. Todo el personal se maneja mediante correo de office 365.
- Personal administrativo tiene acceso a este correo.
- Políticas de contraseña de correo es manejado mediante las políticas del Office365.

Administración Del Centro De Computo

Responsabilidad del equipo de sistemas

No hay responsabilidades puntuales asignadas a cada empleado, tampoco hay un encargado de la seguridad. Existe un responsable general del área de Tecnologías de Información y Comunicaciones, que es el Encargado de TIC (Networking). Él es el que planifica y junto con el jefe de software delega las tareas a los demás empleados del área de sistemas/redes, generalmente una vez por semana haciéndolo responsable de sus propios tiempos.

El administrador es el encargado de reportar a los jefes de área sobre las actividades en el área de TIC. Estos reportes generalmente se realizan a modo de auto evaluación ya que no son un pedido de ningún directivo.

Mantenimiento

- Solicitud de mantenimiento: cada vez que los usuarios necesitan asesoramiento o servicios del área de tecnologías, se comunican telefónicamente con el Ing. de soporte explicando su situación. Cada requerimiento no se registra en un documento.
- Mantenimiento preventivo: Este trabajo es realizado por el personal del área de TI previamente planificado.
- Clasificación de datos y hardware: los equipos de la empresa no han sido clasificados formalmente según su prioridad, aunque se

puede identificar que las máquinas que están en el sector de administración tienen mayor prioridad que el resto. En la escala siguen las de gerencia, y por último el resto de las PC´s, en cuanto al orden de solución de problemas.

- Rótulos: Actualmente existe un inventario detallado de las características de los equipos de computación.

Instaladores

Los instaladores de las aplicaciones utilizadas en la unidad educativa se encuentran en sus CD´s originales almacenados en un armario del centro de cómputos, y no disponen de instaladores en disquetes.

Licencias

Están actualmente licenciados equipos con Windows X, y equipos con Windows Server.

Backups

- Backups de datos en los servidores: Cuando se hace un cambio en la configuración del servidor, no se guardan copias de las configuraciones anterior y posterior al cambio, ni se documentan los cambios que se realizan ni la fecha de estas modificaciones.

- No hay ningún procedimiento formal para la realización ni la recuperación de los backups. Además, no se realizan chequeos para comprobar que el funcionamiento sea el correcto.
- Backups de datos en las PC's: Los usuarios deben realizar sus propios backups de los datos almacenados en sus máquinas, ya que estos datos son propiedad de los empleados.

  Si hacen un backup deberían hacerlo en sus propias máquinas o en elementos de almacenamiento.

Documentación

En el centro de cómputo existe documentación sobre:

- Licencias del software, y en qué máquinas está instalado.
- Números IP de las máquinas y de los equipos de comunicación.
- Gráficos de la ubicación física de los equipos de las distintas áreas.

No hay backups de ninguno de estos datos, ya que son documentos impresos que se van modificando manualmente.

Existe un plan de contingencia elaborado por la empresa desarrolladora del software, pero no se ha realizado la implementación de este.

3.2. Levantamiento de la información.

Para la identificación de los activos se utilizaron los datos proporcionados por el administrador de la red, y los activos se dividieron en 3 categorías:

• **Aplicación de Software**: Programas necesarios para la gestión de la información en la unidad educativa.

• **Equipo**: hardware utilizado para gestionar la información y la comunicación.

• **Instalación**: donde se ubican los sistemas de información. El responsable de los activos es la persona que gestiona los activos de información.

Para lo cual se va a resumir el compendio de activos ligados a la aplicabilidad de este documento:

ID	Categoría	Nombre
1	Aplicación de SW	Sistema “FIXED”
2	Aplicación de SW	Sistema “MOODLE”
3	Aplicación de SW	Office 365
4	Equipo informático	Router Proveedor
5	Equipo informático	Firewall Proveedor
6	Equipo informático	Switches

7	Equipo informático	Access Point
8	Equipo informático	Biométrico
9	Instalaciones	Data Center
10	Instalaciones	Oficina Rectorado / Vicerrectorado
11	Instalaciones	Dpto. Secretaría
12	Instalaciones	Dpto. Administración Financiera
13	Instalaciones	Dpto. Pasantías y vinculación
14	Instalaciones	Dpto. Biblioteca
15	Equipo Informático	Servidores
16	Equipo Informático	Desktop / Laptop

Tabla 10: Inventario de Activos.

Fuente: Anny Cárdenas y Lissette Munizaga

Activos De Información

Documentos y Registros	
Descripción	Soporte estático no electrónico que contiene datos.
Activos	Actas Documentación de procesos (POA: Plan Operativo Anual) Contratos con los clientes

	Contratos con los proveedores de servicio médico Facturas Memos Oficios Reglamento del SRI Papel Tarjetas de Afiliación

Tabla 11: Activos de Información - Documentos y registros.

Fuente: Anny Cárdenas y Lissette Munizaga

Activos Auxiliares	
Descripción	Otros dispositivos que ayudan al funcionamiento de la organización
Activos	Suministros de oficina

Tabla 12: Activos de Información - Activos Auxiliares.

Fuente: Anny Cárdenas y Lissette Munizaga

Activos Intangibles	
Descripción	Activos que representan el buen nombre de la empresa y la imagen que los clientes tienen de ella.
Activos	Imagen y Reputación de la empresa

Tabla 13: Activos de Información - Activos Intangibles.

Fuente: Anny Cárdenas y Lissette Munizaga

Software

Sistemas Operativos	
Descripción	Esta denominación comprende todos los programas de una computadora que constituyen la base operativa sobre la cual se ejecutarán todos los otros programas (servicios o aplicaciones). Incluye un núcleo y funciones o servicios básicos. Dependiendo de su arquitectura, un sistema operativo puede ser monolítico o puede estar formado por un micronúcleo y un conjunto de módulos del sistema. El sistema operativo abarca principalmente todos los servicios de gestión del hardware (CPU, memoria, discos, periféricos e interfaces redes), los servicios de gestión de tareas o procesos y los servicios de gestión de usuarios y de sus derechos.
Activos	Laptops y PC's que las utilizan

Tabla 14: Software - Sistemas Operativos.

Fuente: Anny Cárdenas y Lissette Munizaga

Como se puede apreciar en el inventario realizado, existen varias áreas y sistemas de tratamiento de información sobre las cuales es de mucha importancia poder establecer controles de acceso ya que así podemos mitigar posibles incidentes de seguridad de la información que se puedan presentar dentro de la unidad educativa.

PLATAFORMA FIXED	
Descripción	Plataforma que utiliza personal administrativo (FIXED – Administrado por la unidad educativo. (Sistema comprado)). La plataforma FIXED no es con la cuenta de office 365 son usuarios locales de los sistemas - Usuarios son registrados en la base de datos - No se maneja a nivel perfiles, sino a nivel permisos. Ejemplo: Usuario de secretaría se le activan las opciones del sistema que requiere y los reporte que puede visualizar. Pero no hay un perfil que se llame Secretaría. Permisos se brindan y otorgan desde el usuario administrador del FIXED (realizado por Juan del área técnica) Permisos de docente: Registra calificaciones, comportamiento Permisos de secretaria: Matriculación, datos de estudiantes (información personal y académica) Permisos de colecturía: Registros de pagos matriculas, pensiones, expresos, etc. Permisos de financiero y contable: Registro a ingresos y egresos de la unidad educativa, pago a proveedores (compra de nuevos equipos, mantenimiento, etc., comprobantes electrónicos)
Activos	Manejado por el proveedor y es accesado por la nube

Tabla 15: Software - Plataforma FIXED.

Fuente: Anny Cárdenas y Lissette Munizaga

Plataforma Moodle	
Descripción	Moodle es una plataforma de aprendizaje diseñada para proporcionarle a educadores, administradores y estudiantes un sistema integrado único, robusto y seguro para crear ambientes de aprendizaje personalizados. Utilizada por docentes y estudiantes conectada a la cuenta de office 365. Docentes comparten información, actividades sincrónicas y asincrónicas (se asimila a TEAMS)
Activos	Servidor físico de la institución.

Tabla 16: Software - Plataforma Moodle.

Fuente: Anny Cárdenas y Lissette Munizaga

Software de aplicación de oficina	
Descripción	Datos y servicios informáticos compartidos y privados, que utilizan los protocolos y tecnologías de comunicación (por ejemplo, tecnología de Internet).
Activos	Antivirus, Software de impresión

Tabla 17: Software - Software de aplicación de oficina.

Fuente: Anny Cárdenas y Lissette Munizaga

Activos Físicos

Hardware Portátil	
Descripción	Hardware informático diseñado para poder ser transportado manualmente con el fin de utilizarlo en lugares diferentes.
Activos	Portátil

Tabla 18: Activos Físicos - Hardware Portátil.

Fuente: Anny Cárdenas y Lissette Munizaga

PC´s de oficina	
Descripción	Hardware informático que pertenece al organismo o que es utilizado en los locales del organismo.
Activos	Estaciones de trabajo.

Tabla 19: Activos Físicos - PC´s de Oficina.

Fuente: Anny Cárdenas y Lissette Munizaga

Equipos de Oficina	
Descripción	Hardware informático que pertenece al organismo o que es utilizado en los locales del organismo.
Activos	Estaciones de trabajo.
Servidores	
Descripción	Hardware informático que pertenece al organismo y maneja información importante de la empresa y clientes.
Activos	Describir

Tabla 20: Activos Físicos - Equipos de Oficina.

Fuente: Anny Cárdenas y Lissette Munizaga

Soporte Electrónico	
Descripción	Soporte informático conectado a una computadora o a una red informática para el almacenamiento de datos. Susceptible de almacenar un gran volumen de datos sin modificar su pequeño tamaño. Se utiliza a partir de equipo informático estándar.
Activos	USB y Discos externos

Tabla 21: Activos Físicos - Soporte Electrónico.

Fuente: Anny Cárdenas y Lissette Munizaga

Medios de comunicación	
Descripción	Los medios o soportes de comunicación y telecomunicación pueden caracterizarse principalmente por las características físicas y técnicas del soporte (punto a punto, difusión) y por los protocolos de comunicación (enlace o red – capas 2 y 3 del modelo OSI de 7 capas).
Activos	Red de datos, correo electrónico

Tabla 22: Activos Físicos - Medios de Comunicación.

Fuente: Anny Cárdenas y Lissette Munizaga

Establecimiento	
Descripción	El tipo establecimiento está formado por el conjunto de lugares que contienen todo o parte del sistema y los medios físicos necesarios para su funcionamiento.
Activos	Describir

Tabla 23: Activos Físicos – Establecimiento.

Fuente: Anny Cárdenas y Lissette Munizaga

Servicios

Comunicación	
Descripción	Servicios y equipo de telecomunicaciones propiedad del proveedor
Activos	Describir

Tabla 24: Servicios – Establecimiento.

Fuente: Anny Cárdenas y Lissette Munizaga

Energía	
Descripción	Servicios y medios (fuentes de energía y cableado) necesarios para a alimentación eléctrica del hardware y los periféricos.
Activos	Entrada de la red eléctrica.

Tabla 25: Servicios – Energía.

Fuente: Anny Cárdenas y Lissette Munizaga

Correo Electrónico	
Descripción	Dispositivo que permite, a los usuarios habilitados, el ingreso, la consulta diferida y la transmisión de documentos informáticos o de mensajes electrónicos, a partir de computadoras conectadas en red.
Activos	Office 365

Tabla 26: Servicios – Correo Electrónico.

Fuente: Anny Cárdenas y Lissette Munizaga

Portal Externo	
Descripción	Un portal externo es un punto de acceso que encontrará o utilizará un usuario cuando busque información o un servicio del organismo. Los portales brindan un gran abanico de recursos y de servicios.
Activos	Portal de información (Página Web de la empresa)

Tabla 27: Servicios – Portal Externo.

Fuente: Anny Cárdenas y Lissette Munizaga

Personas

Personas	
Descripción	Es el personal que manipula elementos delicados en el marco de su actividad y que tiene una responsabilidad particular en ese tema. Puede disponer de privilegios particulares de acceso al sistema de información para cumplir con sus tareas cotidianas.
Activos	Describir las áreas de la organización.

Tabla 28: Personas/Personal.

Fuente: Anny Cárdenas y Lissette Munizaga

Dentro del presente proyecto es sumamente importante generar una correcta definición de roles y derechos de acceso en los sistemas de información, ya que así se podrá delimitar las funciones y tareas que realizará cada usuario y a su vez establecer controles en los privilegios que se tendrán dependiendo de sus necesidades.

La unidad educativa no cuenta con una administración de seguridad de información ya que esta se encuentra distribuida principalmente entre los departamentos que se tienen en cuenta y solo puede ser accesible por las

jefaturas o las gestiones principales que manejen dichas áreas. Las funciones de desarrollo y mantenimiento de políticas y roles de seguridad no están definidas dentro de los roles de la Institución tecnológica superior.

Dado la cantidad de estudiantes y las distintas operaciones que se manejan a lo largo de cada periodo académico la información es considerada de alta prioridad para el tiempo de vida estudiantil de los jóvenes, considerando lo que antecede es un requisito indispensable contar con roles y políticas que permitan reducir el riesgo de pérdida de información ya que una incorrecta asignación de privilegios sobre los sistemas puede afectar a la confidencialidad, integridad y disponibilidad de la información que se gestiona sobre ellos.

Para realizar el siguiente trabajo deberemos contar con un levantamiento de información para identificar las áreas que necesiten vincular de forma más efectiva al personal de alto nivel que estará dentro de los roles pertenecientes a cada departamento. Con el fin de garantizar desde un principio de la planeación de roles y políticas un punto de partida de éxito con la implementación.

Se realizó el respectivo levantamiento de información con el equipo de administradores de los distintos sistemas de información, los cuales se encargan de tomar las medidas necesarias para planear, implementar y hacer seguimiento a todas las actividades necesarias para mantener un modelo de

seguridad de la información al interior de la entidad así como planear las actividades necesarias para una adecuada administración y sostenibilidad del mismo, de la misma forma hemos empleado un concepto de: “Todo está prohibido, a no ser que permita expresamente”.

A continuación, identificamos todos los roles presentes en los sistemas de tratamiento de información, con su respectiva descripción.

ROL	DESCRIPCIÓN
Administrador	Control total de la plataforma Moodle y FIXED. Este rol es asignado al administrador del sistema que a su vez es el propietario del activo.
Docente	Acceso a los módulos de Moodle y contenido de las actividades educativas.
Estudiante	Acceso a los módulos necesarios Moodle para su gestión como estudiante. No tendrá acceso a los módulos de configuración de la plataforma Moodle.

Secretaria	Acceso a los módulos de Moodle y Fixed, Validación de documentos solicitados en proceso de matriculación de estudiantes.
Colecturía	Registros de pagos matriculas, pensiones, expresos, etc.
Financiero y Contable	Registro a ingresos y egresos de la unidad educativa, pago a proveedores (compra de nuevos equipos, mantenimiento, etc., comprobantes electrónicos)
Unidad de servicios de Biblioteca	Carga de libras en formato digital, correspondientes a las diversas materias que contienen las carreras de la unidad educativa.
Centro de Idiomas	Acceso a los módulos de Ingles y contenido de las actividades educativas que se imparte en la unidad educativa.

Tabla 29: Roles en Sistemas de Tratamiento de Información de la Unidad Educativa

Fuente: Anny Cárdenas y Lissette Munizaga

Todos estos roles identificados, deben ser definidos en cada sistema y realizado en conjunto con la persona que es designada como administrador del sistema de información, con el fin de poder realizar la labor de manera más eficiente.

3.3 Controles de accesos lógicos y físicos

En la actualidad dentro de la Unidad Educativa se encuentran ya aplicados ciertos controles de seguridad que corresponde a los accesos tanto lógicos como físicos, que se han venido implementando dada las exigencias solicitadas por el Ministerio de Educación. Sin embargo, esto no es llevado de forma general, más bien es realizado de forma individual de quienes conforman cada departamento de la Unidad Educativa.

Otro punto que se encontró dentro de este proceso levantamiento de información es que los controles de seguridad de accesos que se encuentran aplicados no han sido familiarizados con los colaboradores de la institución (estudiantes, docentes, personal administrativo, personal seguridad física) esto es únicamente realizado por cada administrador de sistemas y por temas de cumplimientos ya antes mencionado.

Entre los controles de seguridad de acceso tomando como base la ISO/IEC 27002:2013 que hemos validado que se encuentran implementados son:

- Identificadores únicos para cada usuario en cada uno de los sistemas de información a los que tiene acceso.
- Requerimientos mínimos de complejidad en las contraseñas.
- Registro de intentos fallidos y exitosos en los sistemas.
- Circuito cerrado de televisión
- Acceso biométrico a Data Center

- Bitácora de acceso a Data Center

Así como existen estos controles aplicados, podemos detallar controles que no han sido tomados en consideración y son de gran importancia:

- Política de control de accesos.
- Procedimientos formales de autorización de acceso a la red de la institución.
- Inhabilitación o eliminación de usuarios al personal que deja la unidad educativa.
- Mantener un registro central de accesos otorgados.
- Revisión periódica de los derechos de acceso concedidos.
- Responsabilidades del usuario sobre el uso de sus accesos.
- Proteger contra intentos de fuerza bruta de inicio de sesión.

Como se indicó anteriormente, a pesar de que se tienen ya aplicados ciertos controles que se encuentran alineados a la ISO/IEC 27002:2013, no se cubre en su totalidad todos los controles que se hacen referencia en el control A.9 ya que en él se abarcan muchos más temas de seguridad lo cual ayudará a la unidad educativa a mejorar su postura de seguridad.

CAPÍTULO IV.

EVALUACIÓN Y TRATAMIENTO DEL RIESGO

Este capítulo se centra en la continuación natural del desarrollo del trabajo, la propuesta se centra en la evaluación de riesgos de seguridad de la información de los sistemas y áreas (activos) de procesamiento de información especificados en el Capítulo 3.

La evaluación de riesgos es uno de los procesos más importantes en educación, ya que permite comprender el alcance de diversas amenazas y vulnerabilidades que enfrentan los activos de información que son esenciales para la gestión de los procesos académicos y administrativos.

Actualmente, pocas organizaciones creen que sus activos están seguros y que no son vulnerables a las amenazas. Esto se debe a la falta de comprensión o el escaso respeto de los directivos por la seguridad informática, por lo que optan por no aplicar controles que ayudarían a mitigar los riesgos que pueda ocurrir. Este trabajo permite a instituciones de nivel técnico superior identificar amenazas y vulnerabilidades que enfrentan los activos de información esenciales para la gestión de procesos académicos y administrativos.

4.1 Metodología De Evaluación Y Tratamiento De Riesgo

El propósito de la evaluación y tratamiento de riesgos para la Unidad Educativa es obtener información precisa, comprender las amenazas y sus fuentes, identificar las medidas de control preventivo necesarias y su planificación, establecer prioridades adecuadas y comprender posibles daños a los activos de la institución.

La metodología desarrollada fue presentada por nosotros los desarrolladores del documento y aprobada por las autoridades que rigen en la institución, a través de una reunión que se llevó a cabo en las instalaciones de la entidad.

La metodología realizada consta de:

4.1.1 El Proceso

La evaluación de riesgos se implementa a través de la tabla de evaluación de riesgos. El proceso de evaluación de riesgos es coordinado por el personal de soporte de la Unidad Educativa, la identificación de amenazas y vulnerabilidades la realizan los compañeros de soporte juntamente con los propietarios de los activos, y la evaluación de consecuencias y probabilidad es realizada por los nuevos nombrados propietarios de los riesgos.

4.1.2 Identificación de las Amenazas Y Vulnerabilidades

El próximo paso natural es identificar todas las amenazas y vulnerabilidades relacionadas con cada uno de los activos.

Las amenazas y vulnerabilidades se identifican utilizando la matriz de amenazas y vulnerabilidades que se muestra a continuación:

ORIGEN	AMENAZA
Desastre Natural	Fuego
	Daño por agua
	Fenómeno climático
	Fenómeno sísmico

	Fenómeno de origen volcánico
	Fenómeno meteorológico
De origen industrial	Fuego
	Polvo
	Contaminación mecánica
	Corte del suministro eléctrico
	Variaciones de voltaje
	Fallas en la climatización
Errores y fallos no intencionados	Error de uso por parte de usuarios
	Error de uso por parte del administrador
	Errores de monitorización
	Deficiencias de la organización
	Alteración accidental de la información
	Saturación del sistema informático
	Indisponibilidad del personal
Ataques intencionados	Manipulación de los registros de actividad
	Manipulación de la configuración

	Suplantación de la identidad del usuario
	Abuso de privilegios de acceso
	Difusión de software dañino
	Acceso no autorizado
	Modificación deliberada de la información
	Destrucción de información
	Divulgación de información
	Manipulación de los equipos
	Instalación no autorizada de software
	Denegación de servicios
	Robo
	Vandalismo
	Ingeniería social

Tabla 30: Matriz de Amenazas.

Fuente: Magerit v3

VULNERABILIDADES
Sesiones activas después del horario laboral
Colocación de cables
Interfaz de usuario complicada
Claves criptográficas accesibles a personas no autorizadas
Eliminación de soportes de almacenamiento sin borrado de datos
Poderes de gran alcance
Inadecuada capacidad de gestión
Inadecuado control de cambios
Inadecuado nivel de conocimiento y/o concienciación de empleados
Mantenimiento inadecuado
Inadecuada gestión de redes
Inadecuada separación de tareas
Inadecuada supervisión de proveedores externos
Inadecuada supervisión del trabajo de los empleados
Inadecuados derechos de usuario
Información disponible para personas no autorizadas
Falta de evidencia en envío o recepción de mensajes
Falta de control en datos de entrada y salida
Inadecuada o falta de implementación de auditoría interna
Falta de validación de datos procesados

Ubicación susceptible a desastres naturales
Ubicación susceptible a pérdidas de agua
Equipamiento móvil proclive para robar
Redes accesibles a personas no autorizadas
Falta de desactivación de cuentas de usuario luego de finalizado el empleo
Falta de separación de entornos de prueba y operativos
Bases de datos con protección desactualizada contra códigos maliciosos
Sobre dependencia en un dispositivo o sistema
Elección inadecuada de datos de prueba
Susceptibilidad del equipamiento a la humedad y a la contaminación
Susceptibilidad del equipamiento a la temperatura
Susceptibilidad del equipamiento a alteraciones en el voltaje
Única copia, sólo una copia de la información
Cuentas de usuario generadas por sistema en las que las contraseñas permanecen sin modificación
Sistemas desprotegidos ante acceso no autorizado
Acceso no autorizado a instalaciones
Nivel de confidencialidad no definido con claridad
Reglas criptográficas no definidas con claridad

Reglas organizacionales no definidas con claridad
Requisitos para desarrollo de software no definidos con claridad
Reglas para control de acceso no definidos con claridad
Reglas para trabajo afuera de las instalaciones no definidas con claridad
Copiado sin control
Descargas de Internet sin control
Uso no controlado de sistemas de información
Software no documentado
Empleados desmotivados o disconformes
Conexiones de red pública sin protección
Uso de equipamiento obsoleto
Contraseñas inseguras
Malas condiciones higiénicas

Tabla 31: Matriz de Vulnerabilidades.

Fuente: Magerit v3

Como esto es un evento en cadena cada uno de los activos puede estar relacionado a varias amenazas, y cada amenaza puede estar vinculada a varias vulnerabilidades.

4.1.3 Identificación De Los Propietarios De Riesgos

Para cada uno de los riesgos es necesario identificar un dueño: ya sea la persona o unidad organizativa responsable de cada uno de los mismos. Esta persona puede o no ser la misma que el propietario del activo.

4.1.4 Consecuencia y Probabilidad

Es necesario evaluar también las repercusiones para cada combinación de amenazas y vulnerabilidades de un activo específico en caso de que ello se pueda producir:

Baja	1	La pérdida de confidencialidad, disponibilidad o integridad no afecta las finanzas, las operaciones, las obligaciones legales o contractuales o el prestigio de la organización.
Moderada	2	La pérdida de confidencialidad, disponibilidad o integridad causa gastos y tiene consecuencias bajas o moderadas sobre obligaciones legales o contractuales o sobre el prestigio de la organización.
Alta	3	La pérdida de confidencialidad, disponibilidad o integridad tiene consecuencias importantes y/o inmediatas sobre las finanzas, las operaciones, las obligaciones legales o contractuales o el prestigio de la organización.

Tabla 32: Repercusión.

Fuente: Magerit V3

Luego de la evaluación de las repercusiones es necesario evaluar la probabilidad de que se materialice ese riesgo; es decir, la probabilidad de que una amenaza se aproveche de la vulnerabilidad del activo en cuestión.

Baja	1	En el futuro inmediato no se esperan incidentes nuevos (menor o igual a 1 cada 2 años).
Moderada	2	Es poco probable, pero puede pasar la ocurrencia de nuevos incidentes, (menor o igual a 1 vez al año).
Alta	3	Existe una elevada probabilidad de que haya incidentes en el futuro. (más de 1 vez cada trimestre)

Tabla 33: Probabilidad.

Fuente: Magerit V3

El nivel de riesgo potencial se calcula automáticamente multiplicando el valor de la consecuencia y probabilidad.

Riesgo potencial = Consecuencia * Probabilidad

4.1.5 Nivel De Riesgo – Mapa De Calor

		Consecuencia		
		Baja (1)	Moderada (2)	Alta (3)
Probabilidad	Baja (1)	1	2	3
	Moderada (2)	2	4	6
	Alta (3)	3	6	9

Tabla 34: Mapa de calor – Nivel de riesgo.

Fuente: Magerit v3

La valoración del riesgo es la que se muestra a continuación.

VALORACIÓN DEL RIESGO	
NIVEL RIESGO	**CALIFICACIÓN**
ALTO	**6 a 9**
MODERADO	**3 a 4**
BAJO	**1 a 2**

Tabla 35: Valoración del riesgo.

Fuente: Magerit v3

4.1.6 Criterios para la Aceptación de Riesgos

Los valores 1 y 2 son riesgos aceptables por la Unidad Educativa, los valores entre 3 y 9 son riesgos no aceptables que requieren tener un tratamiento.

4.1.7 Tratamiento de los Riesgos

El tratamiento de riesgos se implementa mediante el Cuadro de tratamiento de riesgos, copiando desde el Cuadro de evaluación de riesgos todos los riesgos identificados como no aceptables. El tratamiento de riesgos es realizado por los maestrantes para el presente trabajo.

Para los riesgos que se encuentren entre 3 y 9 se deben seleccionar una o más soluciones de tratamiento.

1. **Mitigar el riesgo:** Disminuir el riesgo hasta un nivel de riesgo aceptable mediante la elección/aplicación de controles de seguridad. Estos controles pueden ser los controles de la ISO 27002:2013.
2. **Aceptar el riesgo:** Se reconoce la existencia del riesgo, la acción a generar es monitorearlo para que se mantenga en aceptable.
3. **Transferir el riesgo:** Compartir el riesgo, asociación con alguien. Por ejemplo, Compartir el riesgo con socios o transferirlo mediante cobertura de seguros, acuerdos contractuales u otros medios.
4. **Evitar el riesgo:** Eliminación de actividades que pueden ser la causa de afectar negativamente los activos de información.

La elección de opciones se implementa a través del Cuadro de tratamiento de los riesgos. En el caso de la primera elección (escoger controles de seguridad), es necesario evaluar el nuevo valor de consecuencia y probabilidad en el Cuadro de tratamiento de riesgos, para evaluar la efectividad de los controles planificados.

Esto se conoce como riesgo residual.

Riesgo Residual: Consecuencia * Probabilidad

4.1.8 Plan de Tratamiento de los Riesgos

En nombre de los propietarios de riesgos, el Rectorado, Vicerrectorado, Gestión Académica y administrativo financiero aceptará el Plan de tratamiento de riesgos en el que se planificará la implementación de los controles seleccionados.

4.2 Cuadro de Evaluación de Riesgo

En la tabla a continuación se muestra el resumen de la evaluación del riesgo sobre los activos que se identificaron en el capítulo 3, en donde por medio de entrevistas se pudo identificar las amenazas, vulnerabilidades y el valor cuantitativo de consecuencia y probabilidad.

No	Nombre del activo	Amenaza	Vulnerabilidad	C	P	Riesgo inherente
1	Sistema "FIXED"	Acceso no autorizado	Contraseñas inseguras	2	2	4
			Sesiones activas después del horario laboral	2	1	2
			Falta de desactivación de cuentas de usuario luego de finalizado el empleo	3	3	9
			Reglas para control de acceso no definidos con claridad	3	3	9
			Sistemas desprotegidos ante acceso no autorizado	2	3	6
		Divulgación de información	Empleados desmotivados o disconformes	3	1	3
		Abuso de privilegios de acceso	Inadecuados derechos de usuario	3	2	6
		Manipulación de los	Inadecuados derechos de usuario	3	1	3

		registros de actividad				
		Error de uso por parte del administrador	Inadecuada capacidad de gestión	2	1	2
2	Sistema "MOODLE"	Acceso no autorizado	Contraseñas inseguras	2	3	6
			Sesiones activas después del horario laboral	2	1	2
			Falta de desactivación de cuentas de usuario luego de finalizado el empleo	3	3	9
			Reglas para control de acceso no definidos con claridad	3	3	9
			Sistemas desprotegidos ante acceso no autorizado	2	3	6
		Divulgación de información	Empleados desmotivados o disconformes	3	1	3
		Abuso de privilegios de acceso	Inadecuados derechos de usuario	3	2	6

		Manipulación de los registros de actividad	Inadecuados derechos de usuario	3	1	3
		Error de uso por parte del administrador	Inadecuada capacidad de gestión	2	1	2
3	Office 365	Error de uso por parte de usuarios	Interfaz de usuario complicada	2	1	2
			Inadecuado nivel de conocimiento y/o concienciación de empleados	2	2	4
		Error de uso por parte del administrador	Inadecuada capacidad de gestión	1	1	1
		Abuso de privilegios de acceso	Empleados desmotivados o disconformes	2	2	4
			Inadecuados derechos de usuario	3	2	6
		Acceso no autorizado	Falta de desactivación de cuentas de usuario luego de finalizado el empleo	3	3	9
			Sesiones activas después del horario laboral	2	3	6

			Falta de controles/políticas de seguridad de accesos	3	3	9
			Sistemas desprotegidos ante acceso no autorizado	3	3	9
			Reglas para control de acceso no definidos con claridad	2	3	6
4	Router Proveedor	Polvo	Mantenimiento inadecuado	1	1	1
		Daño por agua	Susceptibilidad del equipamiento a la humedad y a la contaminación	2	1	2
		Robo	Acceso no autorizado a instalaciones	3	2	6
			Falta de controles de seguridad física	3	3	9
		Manipulación de los registros de actividad	Inadecuados derechos de usuario	2	2	4

		Manipulación de la configuración	Empleados desmotivados o disconformes	2	2	4
		Manipulación de los equipos	Falta de controles de seguridad física	3	2	6
5	Firewall Proveedor	Polvo	Mantenimiento inadecuado	1	1	1
		Daño por agua	Susceptibilidad del equipamiento a la humedad y a la contaminación	2	1	2
		Robo	Acceso no autorizado a instalaciones	3	2	6
			Falta de controles de seguridad física	3	3	9
		Manipulación de los registros de actividad	Inadecuados derechos de usuario	2	2	4
		Manipulación de la configuración	Empleados desmotivados o disconformes	2	2	4
		Manipulación de los equipos	Falta de controles de seguridad física	3	2	6
			Inadecuados derechos de usuario	3	2	6

		Abuso de privilegios de acceso	Empleados desmotivados o disconformes	2	2	4
6	Switches	Fallas en los equipos	Susceptibilidad del equipamiento a alteraciones en el voltaje	3	2	6
			Susceptibilidad del equipamiento a la humedad y a la contaminación	3	2	6
		Polvo	Mantenimiento inadecuado	1	1	1
		Error de uso por parte del administrador	Inadecuada capacidad de gestión	2	1	2
		Manipulación de la configuración	Inadecuados derechos de usuario	2	2	4
		Acceso no autorizado	Reglas para control de acceso no definidos con claridad	2	2	4
			Sistemas desprotegidos ante acceso no autorizado	3	2	6
			Falta de controles/políticas	3	3	9

			de seguridad de accesos			
7	Access Point	Robo	Acceso no autorizado a instalaciones	3	2	6
			Falta de controles de seguridad física	3	2	6
		Polvo	Mantenimiento inadecuado	1	1	1
		Manipulación de la configuración	Empleados desmotivados o disconformes	2	2	4
			Inadecuados derechos de usuario	2	2	4
8	Biométrico	Polvo	Mantenimiento inadecuado	1	1	1
		Robo	Acceso no autorizado a instalaciones	3	2	6
			Falta de controles de seguridad física	3	2	6
		Manipulación de los registros de actividad	Inadecuados derechos de usuario	2	2	4
		Manipulación de la configuración	Empleados desmotivados o disconformes	2	2	4

			Inadecuados derechos de usuario	2	2	4
9	Data Center	Fuego	Susceptibilidad del área a alteraciones en el voltaje	3	1	3
		Fenómeno sísmico	Ubicación susceptible a desastres naturales	3	1	3
		Acceso no autorizado	Falta de controles de seguridad física	3	3	9
10	Oficina Rectorado / Vicerrectorado	Fuego	Susceptibilidad del área a alteraciones en el voltaje	3	1	3
		Fenómeno sísmico	Ubicación susceptible a desastres naturales	3	1	3
		Acceso no autorizado	Falta de controles de seguridad física	3	3	9
11	Dpto. Secretaría	Fuego	Susceptibilidad del área a alteraciones en el voltaje	3	1	3
		Fenómeno sísmico	Ubicación susceptible a desastres naturales	3	1	3
		Acceso no autorizado	Falta de controles de seguridad física	3	3	9

12	Dpto. Administrativo Financiero	Fuego	Susceptibilidad del área a alteraciones en el voltaje	3	1	3
		Fenómeno sísmico	Ubicación susceptible a desastres naturales	3	1	3
		Acceso no autorizado	Falta de controles de seguridad física	3	3	9
13	Dpto. Pasantías y Vinculación	Fuego	Susceptibilidad del área a alteraciones en el voltaje	3	1	3
		Fenómeno sísmico	Ubicación susceptible a desastres naturales	3	1	3
		Acceso no autorizado	Falta de controles de seguridad física	3	3	9
14	Dpto. Biblioteca	Fuego	Susceptibilidad del área a alteraciones en el voltaje	3	1	3
		Fenómeno sísmico	Ubicación susceptible a desastres naturales	3	1	3
		Acceso no autorizado	Falta de controles de seguridad física	3	3	9
15	Servidores	Polvo	Mantenimiento inadecuado	1	1	1
		Daño por agua	Susceptibilidad del equipamiento a la	2	1	2

			humedad y a la contaminación			
		Robo	Acceso no autorizado a instalaciones	3	2	6
			Falta de controles de seguridad física	3	3	9
		Manipulación de los registros de actividad	Inadecuados derechos de usuario	2	2	4
		Manipulación de la configuración	Empleados desmotivados o disconformes	2	2	4
		Manipulación de los equipos	Falta de controles de seguridad física	3	2	6
		Abuso de privilegios de acceso	Inadecuados derechos de usuario	3	2	6
			Empleados desmotivados o disconformes	2	2	4
16	Desktop/Laptop	Polvo	Mantenimiento inadecuado	1	1	1
		Daño por agua	Susceptibilidad del equipamiento a la humedad y a la contaminación	2	1	2

		Robo	Acceso no autorizado a instalaciones	3	2	6
			Falta de controles de seguridad física	3	3	9
		Manipulación de los registros de actividad	Inadecuados derechos de usuario	2	2	4
		Manipulación de la configuración	Empleados desmotivados o disconformes	2	2	4
		Manipulación de los equipos	Falta de controles de seguridad física	3	2	6
		Abuso de privilegios de acceso	Inadecuados derechos de usuario	3	2	6
			Empleados desmotivados o disconformes	2	2	4

Tabla 36: Evaluación de riesgos.

Fuente: Anny Cárdenas y Lissette Munizaga

4.3 Identificación de Riesgos No Aceptables

Posterior a la obtención del riesgo inherente, podemos indicar que mantenemos 92 riesgos que nos son aceptables.

RIESGOS NO ACETABLES	
MODERADO	**45**
ALTO	**57**

Tabla 37: Totalidad de riesgos no aceptables.

Fuente: Anny Cárdenas y Lissette Munizaga

4.4 Tratamiento del Riesgo

Los 102 riesgos inherentes no aceptables por la Unidad Educativa requieren de un tratamiento para poder disminuir su criticidad y que estos se mantengan dentro de un nivel aceptable.

A continuación, se muestra el cuadro de tratamiento de riesgo donde se ha seleccionado los controles de la ISO 27002:2013 que ayudaran a poder disminuir la valoración del riesgo, dando un riesgo residual aceptable.

Nombre del activo	Amenaza	Vulnerabilidad	RI	Control	C	P	Riesgo Resi-dual
Sistema "FIXED"	Acceso no autorizado	Contraseñas inseguras	4	Control A.9.4.3 Sistema de Gestión de claves	**1**	**1**	**1**
		Falta de desac-tivación de cuentas de usuario luego de finalizado el empleo	9	Control A.9.2.1 Re-gistro y baja de usuarios	**2**	**1**	**2**
		Reglas para control de ac-ceso no defini-dos con clari-dad	9	Control A.9.1.1 Po-lítica de control de acceso	**2**	**1**	**2**

		Sistemas desprotegidos ante acceso no autorizado	6	Control A.9.4.2 Procedimientos seguros de inicio de sesión	**1**	**2**	**2**
	Divulgación de información	Empleados desmotivados o disconformes	3	Establecer evaluaciones perennes con el personal humano que confirma la unidad educativa	**2**	**1**	**2**
	Abuso de privilegios de acceso	Inadecuados derechos de usuario	6	Control A.9.2.5 Revisión de los derechos de acceso del usuario	2	1	2

	Manipulación de los registros de actividad	Inadecuados derechos de usuario	3	Control A.9.2.5 Revisión de los derechos de acceso del usuario	**2**	**1**	**2**
Sistema "MOODLE"	Acceso no autorizado	Contraseñas inseguras	6	Control A.9.4.3 Sistema de Gestión de claves	1	1	**1**
		Falta de desactivación de cuentas de usuario luego de finalizado el empleo	9	Control A.9.2.1 Resgistro y baja de usuarios	2	1	**2**
		Reglas para control de acceso no definidos con claridad	9	Control A.9.1.1 Política de control de acceso	2	1	**2**

		Sistemas desprotegidos ante acceso no autorizado	6	Control A.9.4.2 Procedimientos seguros de inicio de sesión	1	2	**2**
	Divulgación de información	Empleados desmotivados o disconformes	3	Establecer evaluaciones perennes con el personal humano que confirma la Unidad Educativa	2	1	**2**
	Abuso de privilegios de acceso	Inadecuados derechos de usuario	6	Control A.9.2.5 Revisión de los derechos de acceso del usuario	2	1	2

	Manipulación de los registros de actividad	Inadecuados derechos de usuario	3	Control A.9.2.5 Revisión de los derechos de acceso del usuario	2	1	**2**
Office 365	Error de uso por parte de usuarios	Inadecuado nivel de conocimiento y/o concienciación de empleados	4	Capacitaciones sobre el uso de las plataformas	1	1	1
	Abuso de privilegios de acceso	Empleados desmotivados o disconformes	4	Establecer evaluaciones perennes con el personal humano que confirma la Unidad Educativa	1	1	1

		Inadecuados derechos de usuario	6	Control A.9.2.5 Revisión de los derechos de acceso del usuario	2	1	2
	Acceso no autorizado	Falta de desactivación de cuentas de usuario luego de finalizado el empleo	9	Control A.9.2.1 Registro y baja de usuarios	2	1	2
		Sesiones activas después del horario laboral	6	Control A.9.4.2 Procedimientos seguros de inicio de sesión	1	1	**1**

		Falta de controles/políticas de seguridad de accesos	9	Control A.9.1.1 Política de control de acceso	1	1	**1**
		Sistemas desprotegidos ante acceso no autorizado	9	Control A.9.4.2 Procedimientos seguros de inicio de sesión	1	2	**2**
		Reglas para control de acceso no definidos con claridad	6	Control A.9.1.1 Política de control de acceso	1	2	**2**
Router Proveedor	Robo	Acceso no autorizado a instalaciones	6	Control A.11.1.2 Controles físicos de entrada	2	1	**2**

		Falta de controles de seguridad física	9	Control A.11.1.2 Controles físicos de entrada	1	1	**1**
	Manipulación de los registros de actividad	Inadecuados derechos de usuario	4	Control A.9.2.5 Revisión de los derechos de acceso del usuario	1	1	**1**
	Manipulación de la configuración	Empleados desmotivados o disconformes	4	Establecer evaluaciones perennes con el personal humano que confirma la Unidad Educativa	1	1	**1**

	Manipulación de los equipos	Falta de controles de seguridad física	6	Control A.11.1.2 Controles físicos de entrada	1	1	**1**
Firewall Proveedor	Robo	Acceso no autorizado a instalaciones	6	Control A.11.1.2 Controles físicos de entrada	2	1	**2**
		Falta de controles de seguridad física	9	Control A.11.1.2 Controles físicos de entrada	1	1	**1**
	Manipulación de los registros de actividad	Inadecuados derechos de usuario	4	Control A.9.2.5 Revisión de los derechos de acceso del usuario	1	1	**1**

	Manipulación de la configuración	Empleados desmotivados o disconformes	4	Establecer evaluaciones perennes con el personal humano que confirma la Unidad Educativa	1	1	**1**
	Manipulación de los equipos	Falta de controles de seguridad física	6	Control A.11.1.2 Controles físicos de entrada	1	1	**1**
	Abuso de privilegios de acceso	Inadecuados derechos de usuario	6	Control A.9.2.5 Revisión de los derechos de acceso del usuario	2	1	2

		Empleados desmotivados o disconformes	4	Establecer evaluaciones perennes con el personal humano que confirma la Unidad Educativa	1	1	**1**
Switches	Fallas en los equipos	Susceptibilidad del equipamiento a alteraciones en el voltaje	6	Adquirir reguladores de voltaje para los equipos	2	1	**2**
		Susceptibilidad del equipamiento a la humedad y a la contaminación	6	Validar otras marcas de equipos que no sean susceptibles a la humedad	1	1	**1**

	Manipulación de la configuración	Inadecuados derechos de usuario	4	Control A.9.2.5 Revisión de los derechos de acceso del usuario	1	1	1
	Acceso no autorizado	Reglas para control de acceso no definidos con claridad	4	Control A.9.1.1 Política de control de acceso	1	1	**1**
		Sistemas desprotegidos ante acceso no autorizado	6	Control A.9.4.2 Procedimientos seguros de inicio de sesión	1	2	**2**
		Falta de controles/políticas de seguridad de accesos	9	Control A.9.1.1 Política de control de acceso	1	1	**1**

Access Point	Robo	Acceso no autorizado a instalaciones	6	Control A.11.1.2 Controles físicos de entrada	2	1	**2**
		Falta de controles de seguridad física	6	Control A.11.1.2 Controles físicos de entrada	1	1	**1**
	Manipulación de la configuración	Empleados desmotivados o disconformes	4	Establecer evaluaciones perennes con el personal humano que confirma la Unidad Educativa	1	1	**1**
		Inadecuados derechos de usuario	4	Control A.9.2.5 Revisión de los derechos de	1	1	**1**

				acceso del usuario			
Biométrico ZKteco K30 (Data Center)	Robo	Acceso no autorizado a instalaciones	6	Control A.11.1.2 Controles físicos de entrada	2	1	**2**
		Falta de controles de seguridad física	6	Control A.11.1.2 Controles físicos de entrada	1	1	**1**
	Manipulación de los registros de actividad	Inadecuados derechos de usuario	4	Control A.9.2.5 Revisión de los derechos de acceso del usuario	1	1	**1**

	Manipulación de la configuración	Empleados desmotivados o disconformes	4	Establecer evaluaciones perennes con el personal humano que confirma la Unidad Educativa	1	1	**1**
		Inadecuados derechos de usuario	4	Control A.9.2.5 Revisión de los derechos de acceso del usuario	1	1	**1**
Data Center	Fuego	Susceptibilidad del área a alteraciones en el voltaje	3	Control A.11.1.4 Protección contras las amenazas externas y ambientales	2	1	2
	Fenómeno sísmico	Ubicación susceptible a	3	Control A.11.1.4 Protección	2	1	2

		desastres naturales		contras las amenazas externas y ambientales			
	Acceso no autorizado	Falta de controles de seguridad física	9	Control A.11.1.2 Controles físicos de entrada	1	1	**1**
Oficina Rectorado / Vicerectorado	Fuego	Susceptibilidad del área a alteraciones en el voltaje	3	Control A.11.1.4 Protección contras las amenazas externas y ambientales	2	1	2
	Fenómeno sísmico	Ubicación susceptible a desastres naturales	3	Control A.11.1.4 Protección contras las amenazas externas y ambientales	2	1	2

	Acceso no autorizado	Falta de controles de seguridad física	9	Control A.11.1.2 Controles físicos de entrada	1	1	1
Dpto. Secretaría	Fuego	Susceptibilidad del área a alteraciones en el voltaje	3	Control A.11.1.4 Protección contras las amenazas externas y ambientales	2	1	2
	Fenómeno sísmico	Ubicación susceptible a desastres naturales	3	Control A.11.1.4 Protección contras las amenazas externas y ambientales	2	1	2
	Acceso no autorizado	Falta de controles de seguridad física	9	Control A.11.1.2 Controles físicos de entrada	1	1	1

Dpto. Administrativo Financiero	Fuego	Susceptibilidad del área a alteraciones en el voltaje	3	Control A.11.1.4 Protección contras las amenazas externas y ambientales	2	1	2
	Fenómeno sísmico	Ubicación susceptible a desastres naturales	3	Control A.11.1.4 Protección contras las amenazas externas y ambientales	2	1	2
	Acceso no autorizado	Falta de controles de seguridad física	9	Control A.11.1.2 Controles físicos de entrada	1	1	1
Dpto. Pasantías y Vinculación	Fuego	Susceptibilidad del área a alteraciones en el voltaje	3	Control A.11.1.4 Protección contras las amenazas externas y ambientales	2	1	2

	Fenómeno sísmico	Ubicación susceptible a desastres naturales	3	Control A.11.1.4 Protección contras las amenazas externas y ambientales	2	1	2
	Acceso no autorizado	Falta de controles de seguridad física	9	Control A.11.1.2 Controles físicos de entrada	1	1	1
Dpto. Biblioteca	Fuego	Susceptibilidad del área a alteraciones en el voltaje	3	Control A.11.1.4 Protección contras las amenazas externas y ambientales	2	1	2
	Fenómeno sísmico	Ubicación susceptible a desastres naturales	3	Control A.11.1.4 Protección contras las amenazas externas y ambientales	2	1	2

	Acceso no autorizado	Falta de controles de seguridad física	9	Control A.11.1.2 Controles físicos de entrada	1	1	**1**
Servidores	Robo	Acceso no autorizado a instalaciones	6	Control A.11.1.2 Controles físicos de entrada	2	1	**2**
		Falta de controles de seguridad física	9	Control A.11.1.2 Controles físicos de entrada	1	1	**1**
	Manipulación de los registros de actividad	Inadecuados derechos de usuario	4	Control A.9.2.5 Revisión de los derechos de acceso del usuario	1	1	**1**
	Manipulación de la configuración	Empleados desmotivados o disconformes	4	Establecer evaluaciones perennes con el personal humano que	1	1	**1**

				confirma la Unidad Educativa			
	Manipulación de los equipos	Falta de controles de seguridad física	6	Control A.11.1.2 Controles físicos de entrada	1	1	**1**
	Abuso de privilegios de acceso	Inadecuados derechos de usuario	6	Control A.9.2.5 Revisión de los derechos de acceso del usuario	2	1	2
		Empleados desmotivados o disconformes	4	Establecer evaluaciones perennes con el personal humano que confirma la Unidad Educativa	1	1	**1**

Desktop/Laptop	Robo	Acceso no autorizado a instalaciones	6	Control A.11.1.2 Controles físicos de entrada	2	1	**2**
		Falta de controles de seguridad física	9	Control A.11.1.2 Controles físicos de entrada	1	1	**1**
	Manipulación de los registros de actividad	Inadecuados derechos de usuario	4	Control A.9.2.5 Revisión de los derechos de acceso del usuario	1	1	**1**
	Manipulación de la configuración	Empleados desmotivados o disconformes	4	Establecer evaluaciones perennes con el personal humano que confirma la Unidad Educativa	1	1	**1**

	Manipulación de los equipos	Falta de controles de seguridad física	6	Control A.11.1.2 Controles físicos de entrada	1	1	**1**
		Inadecuados derechos de usuario	6	Control A.9.2.5 Revisión de los derechos de acceso del usuario	2	1	2
	Abuso de privilegios de acceso	Empleados desmotivados o disconformes	4	Establecer evaluaciones perennes con el personal humano que confirma la Unidad Educativa	1	1	**1**

Tabla 38: Cuadro de tratamiento de riesgos

Fuente: Anny Cárdenas y Lissette Munizaga

CAPÍTULO V.

DISEÑO DE CONTROLES DE SEGURIDAD DE LA INFORMACIÓN.

5.1 Declaración de Aplicabilidad.

5.1.1 Propósito, Alcance y Usuarios.

En esta sección de la propuesta, se debe definir la forma en cómo se implementarán algunos de los controles más idóneos a implementarse en la Unidad Educativa, así mismo, se incluyen los objetivos propuestos para dichos controles y la forma de implementación de estos. Los elementos que componen esta sección se corresponden a los controles aplicables de la normativa ISO/IEC 27001:2013 en base a la implementación de un SGSI.

5.1.2 Aplicabilidad de Controles

El principal objetivo de esta sección es definir cuáles de las medidas de seguridad incluidos en el estándar ISO 27001:2013 son los que pueden aplicarse. A continuación, se muestran estos: Controles aplicables de la normativa ISO 27001:2013 a la Unidad Educativa, en base a los hallazgos realizados en las secciones precedentes.

CONTROL_ID	CONTROL	APLICABLE	IMPLEMENTACIÓN
A.5	**POLÍTICAS DE LA SEGURIDAD DE LA INFORMACIÓN**		
A.5.1	***Orientación de la dirección para la gestión de la seguridad de la información***		
A.5.1.1	Políticas para la seguridad de la información	**SI**	Se redactarán y documentarán las políticas de seguridad de la información acordes a los objetivos de seguridad acordados y niveles de riesgo tolerables. Este documento se pone a disposición de los empleados y público en general.

A.5.1.2	Revisión de las políticas para la seguridad de la información	**SI**	Las políticas de seguridad de la información se revisarán y evaluarán periódicamente y/o cuando sea necesario. La revisión es llevada a cabo por el Líder del Proceso de Desarrollo Tecnológico, el Jefe de Seguridad de la Información y la Dirección Estratégica. Se documentan los cambios y las justificaciones de estos.

Tabla 39: Controles aplicables de la normativa ISO 27001:2013 basados en la política de la seguridad de la información

Fuente: Anny Cárdenas y Lissette Munizaga

CONTROL_ID	CONTROL	APLICABLE	IMPLEMENTACIÓN
A.6	**ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN**		
A.6.1	***Organización Interna***		
	Roles y responsabilidades		Los roles y responsabilidades de la

A.6.1.1	para la seguridad de la información	**SI**	seguridad de la información estarán definidas.
A.6.1.2	Separación de deberes	**SI**	El personal estará separado por áreas y se les otorga acceso sólo a los activos y/o información estrictamente necesaria para la realización de su trabajo.
A.6.1.3	Contacto con las autoridades	**SI**	El Líder del Proceso de Desarrollo Tecnológico y el Jefe de Seguridad mantiene los contactos actualizados para incidentes de seguridad
A.6.1.4	Contacto con grupos de interés especial	**SI**	El Líder del Proceso de Desarrollo Tecnológico y el Jefe de Seguridad (por contratar o asignar) mantendrán contactos con autoridades nacionales para los incidentes de seguridad para informes en tiempo real y soluciones a implementar.

A.6.1.5	Seguridad de la información en la gestión de proyectos	**SI**	El Jefe de Seguridad (por contratar o asignar) es el encargado de velar por la aplicación de una metodología de análisis y evaluación de riesgos en los proyectos de TI.
A.6.2	***Dispositivos móviles y trabajo a distancia***		
A.6.2.1	Políticas para dispositivos móviles	**SI**	Se documentará una política de seguridad apropiada para los móviles. Los dispositivos móviles son configurados bajo las condiciones de seguridad aplicables antes de realizar cualquier conexión a la red institucional.
A.6.2.2	Trabajo a distancia	**NO**	**NA**

Tabla 40: Controles aplicables de la normativa ISO 27001:2013 basados en organización de la seguridad de la información

Fuente: Anny Cárdenas y Lissette Munizaga

CONTROL_ID	CONTROL	APLICABLE	IMPLEMENTACIÓN
A.7	**SEGURIDAD DE LOS RECURSOS HUMANOS**		
A.7.1	***Antes de asumir el empleo***		
A.7.1.1	Selección	**SI**	El personal es seleccionado cuidadosamente en base a su perfil y la idoneidad del trabajo a realizar.
A.7.1.2	Términos y condiciones del empleo	**SI**	Los acuerdos contractuales actualmente incluyen las responsabilidades asignadas relativas a la seguridad de la información.
A.7.2	***Durante la ejecución del empleo***		
A.7.2.1	Responsabilidades de la dirección	**SI**	La dirección comprende la importancia de la seguridad de la información y soporta el diseño del SGSI.
A.7.2.2	Toma de conciencia, educación y formación en la	**SI**	El Líder del Proceso de Desarrollo Tecnológico y el Jefe de Seguridad (por contratar o asignar)

	seguridad de la información		realizaran campañas y talleres de formación y educación en la seguridad de la información de forma periódica al personal administrativo
A.7.2.3	Proceso disciplinario	**SI**	Los funcionarios son sometidos a procesos disciplinarios en caso de incumplimiento con las políticas de seguridad de la información de forma deliberada.
A.7.3	***Terminación y cambio de empleo***		
A.7.3.1	Terminación o cambio de responsabilidades de empleo	**SI**	El Jefe de Seguridad (por contratar o asignar) vela que el funcionario que termine contrato o cambie de responsabilidades, se le sean reasignados los permisos y condiciones de seguridad de la información.

Tabla 41: Controles aplicables de la normativa ISO 27001:2013 basados en la seguridad de los recursos humanos

Fuente: Anny Cárdenas y Lissette Munizaga

CONTROL_ID	CONTROL	APLICABLE	IMPLEMENTACIÓN
A.8	**GESTIÓN DE ACTIVOS**		
A.8.1	***Responsabilidad por los activos***		
A.8.1.1	Inventario de activos	**SI**	El Líder del Proceso de Desarrollo Tecnológico y el Jefe de Seguridad (por contratar o asignar) junto a los funcionarios, realizan el inventario de activos y se documentan con su clasificación y responsable.
A.8.1.2	Propiedad de los activos	**SI**	Los activos inventariados tienen asignados los funcionarios responsables.
A.8.1.3	Uso aceptable de los activos	**SI**	Los funcionarios se comprometen a utilizar los activos de forma aceptable

			teniendo en cuenta las políticas de seguridad de información generales.
A.8.1.4	Devolución de activos	**SI**	Se mantienen registros de la devolución de los activos entregados a los empleados. Necesarios para firmar paz y salvo con la organización.
A.8.2	***Clasificación de la información***		
A.8.2.1	Clasificación de la información	**SI**	Cada uno de los activos inventariados contiene la clasificación de la información asociada de acuerdo con los niveles de seguridad establecidos
A.8.2.2	Etiquetado de la información	**SI**	Cada uno de los activos inventariados están etiquetados

			con la clasificación de la información asociada.
A.8.2.3	Manejo de activos	**SI**	El Líder del Proceso de Desarrollo Tecnológico y el Jefe de Seguridad junto a los funcionarios realizan y documentan los procedimientos para el manejo de los activos de acuerdo a la clasificación de cada uno.
A.8.3	***Manejo de medios***		
A.8.3.1	Gestión de medios removibles	**SI**	Existe una política para la gestión de los medios removibles y se clasifican y protegen de acuerdo con su tipo.
A.8.3.2	Disposición de los medios	**SI**	Los medios removibles son dispuestos en lugares seguros y

			su información es almacenada en medios seguros.
A.8.3.3	Transferencia de medios físicos	**NO**	**NA**

Tabla 42: Controles aplicables de la normativa ISO 27001:2013 basados en la política de la seguridad de la información

Fuente: Anny Cárdenas y Lissette Munizaga

CONTROL_ID	CONTROL	APLICABLE	IMPLEMENTACIÓN
A.9	**CONTROL DE ACCESO**		
A.9.1	***Requisitos del negocio para control de acceso***		
A.9.1.1	Política de control de acceso	**SI**	La política de control de acceso estará documentada en las Políticas de la Seguridad de Información.

A.9.1.2	Acceso a redes y a servicios en red	**SI**	Las redes estarán segmentadas en VLAN y el acceso a ella está protegido a personas no autorizadas. Los estudiantes, docentes y administrativos contienen una VLAN separada y que permite el acceso a ella sólo a aquellos que son debidamente autenticados.
A.9.2	***Gestión de acceso de usuarios***		
A.9.2.1	Registro y cancelación de registro de usuarios	**SI**	A través de la herramienta AD Manager
A.9.2.2	Suministro de acceso de usuarios	**Si**	A través de la herramienta AD Manager

A.9.2.3	Gestión de derechos de acceso privilegiado	**SI**	A los funcionarios se les otorgan los privilegios fijos o variables con un PAM a los sistemas de acuerdo con las necesidades mínimas de trabajo. Estos privilegios son documentados y los funcionarios son agrupados bajo Perfiles de Usuario.
A.9.2.4	Gestión de información de autenticación secreta de usuarios	**SI**	La entrega de claves de acceso de los sistemas se realiza de forma personal y se fuerza a que sea cambiada inmediatamente en su primer acceso.
A.9.2.5	Revisión de los derechos de acceso de usuarios	**SI**	El Jefe de Seguridad (por contratar o asignar) junto a los funcionarios encargados verifican que los permisos y derechos de acceso de los usuarios son los que en realidad tienen asignados. Esta verificación se realiza de forma periódica y cualquier anormalidad es debidamente documentada.

A.9.2.6	Retiro o ajuste de los derechos de acceso	**SI**	El Líder del Proceso de Desarrollo Tecnológico y el Jefe de Seguridad (por contratar o asignar) verifican y eliminan los permisos asignados al personal que sea retirado.
A.9.3	***Responsabilidades de los usuarios***		
A.9.3.1	Uso de información de autenticación secreta	**SI**	La información de autenticación del empleado en los sistemas y acceso a información es confidencial.
A.9.4	***Control de acceso a sistemas y aplicaciones***		
A.9.4.1	Restricción de acceso a la información	**SI**	Los derechos de acceso a los sistemas e información son controlados de acuerdo con rol y responsabilidad del empleado en la organización.

A.9.4.2	Procedimiento de ingreso seguro	**SI**	Los sistemas están protegidos mediante un mecanismo de inicio de sesión seguro. Se emplean mecanismos seguros de cifrado de información.
A.9.4.3	Sistema de gestión de contraseñas	**SI**	Se implementan mecanismos de recuperación de contraseñas de forma automática y se garantiza que la nueva contraseña del funcionario cumpla con los requisitos de seguridad expuestos en la Política de Seguridad de contraseñas
A.9.4.4	Uso de programas utilitarios privilegiados	**SI**	El Líder del Proceso de Desarrollo Tecnológico verifica que los sistemas y activos críticos sólo se les instalan los programas estrictamente necesarios y licenciados. Se realiza una verificación de forma aleatoria.
	Control de acceso a		El Jefe de Seguridad verifica que los códigos fuentes de los

A.9.4.5	códigos fuente de programas	**SI**	programas permanecen de forma confidencial.

Tabla 43: Controles aplicables de la normativa ISO 27001:2013 basados en el control de accesos

Fuente: Anny Cárdenas y Lissette Munizaga

CONTROL_ID	CONTROL	APLICABLE	IMPLEMENTACIÓN
A.12	**SEGURIDAD DE LAS OPERACIONES**		
A.12.1	***Procedimientos operacionales y responsabilidades***		
A.12.1.1	Procedimientos de operación documentados	**SI**	El Líder del Proceso de Desarrollo Tecnológico, el Jefe de Seguridad (por contratar o asignar) y los funcionarios documentan los procedimientos de las operaciones relativas a la

			seguridad de la información de cada uno de los activos.
A.12.1.2	Gestión de cambios	**SI**	El Jefe de Seguridad verifica que los cambios en los equipos que afectan la seguridad de la información son controlados y debidamente planeados y probados.
A.12.1.3	Gestión de capacidad	**SI**	El Líder del Proceso de Desarrollo Tecnológico y los funcionarios realizan un monitoreo continuo a los recursos y la adquisición de los nuevos y se proyecta de acuerdo a las necesidades críticas de la organización.
	Separación de los ambientes		El Jefe de Seguridad asegura que los ambientes de

A.12.1.4	de desarrollo, pruebas y operación	**SI**	desarrollo, pruebas y operación están debidamente separados y no ponen en riesgo la información.
A.12.2	***Protección contra códigos maliciosos***		
A.12.2.1	Controles contra códigos maliciosos	**SI**	Existe un plan de capacitación y campaña de concienciación a los funcionarios sobre la seguridad de la información y los riesgos a los que están expuestos los activos, especialmente sobre el *software* de código malicioso. El Jefe de Seguridad y los funcionarios verifican que el *software* está protegido con antivirus y existe una política documentada de actualización

			de todo el *software* utilizado, antivirus y sistema operativo.
A.12.3	***Copias de respaldo***		
A.12.3.1	Respaldo de la información	**SI**	El Jefe de Seguridad y funcionarios pertinentes realizan las copias de seguridad de toda la información a intervalos programados y de acuerdo a las políticas de seguridad. El procedimiento es documentado y se realizan pruebas de recuperación a intervalos programados.
A.12.4	***Registro y seguimiento***		
A.12.4.1	Registro de eventos	**SI**	El Jefe de Seguridad y funcionarios pertinentes revisan periódicamente los registros de los usuarios y las actividades relativas a la seguridad de la información. El proceso es auditado y documentado.

A.12.4.2	Protección de la información de registro	**SI**	Se implementan controles de seguridad que garanticen la protección de la información de los registros.
A.12.4.3	Registros del administrador y del operador	**SI**	Las acciones y registros de los administradores también son almacenados y protegidos de cualquier modificación.
A.12.4.4	Sincronización de relojes	**SI**	El Líder del Proceso de Desarrollo Tecnológico asegura que todos los sistemas están acordes y ajustados en una referencia de tiempo única y sincronizada.
A.12.5	***Control de software operacional***		
A.12.5.1	Instalación de *software* en los sistemas operativos	**SI**	Existe una documentación sobre el procedimiento de instalación de los sistemas operativos y *software*, que cumpla con las políticas de seguridad de la información.

A.12.6	***Gestión de la vulnerabilidad técnica***		
A.12.6.1	Gestión de las vulnerabilidades técnicas	**SI**	Existe una metodología de análisis y evaluación de riesgos sistemática y documentada.
A.12.6.2	Restricciones sobre la instalación de *software*	**SI**	La instalación de *software* es realizada sólo por el personal autorizado y con *software* probado y licenciado, además de otorgar el principio del menor privilegio. El procedimiento de instalación es documentado.
A.12.7	***Consideraciones sobre auditorías de sistemas de información***		
A.12.7.1	Controles de auditorías de	**SI**	El Líder del Proceso de Desarrollo Tecnológico, el Jefe de Seguridad y los funcionarios pertinentes acuerdan sobre las

	sistemas de información		fechas de auditorías internas para los sistemas de información. El procedimiento es documentado.

Tabla 44: Controles aplicables de la normativa ISO 27001:2013 basados en la seguridad de las operaciones

Fuente: Anny Cárdenas y Lissette Munizaga

CONTROL_ID	CONTROL	APLICABLE	IMPLEMENTACIÓN
A.13	**SEGURIDAD DE LAS COMUNICACIONES**		
A.13.1	***Gestión de la seguridad de las redes***		
A.13.1.1	Controles de redes	**SI**	El Jefe de Seguridad y el Administrador de Redes implementan una Infraestructura de Llave Pública (PKI) mediante algoritmos fuertes de cifrado que garanticen la confidencialidad e integridad de la información que

			se transmite a través de las redes.
A.13.1.2	Seguridad de los servicios de red	**SI**	El acceso a la red de los proveedores de servicio de red es monitoreado y controlado.
A.13.1.3	Separación en las redes	**SI**	Las redes están segmentadas en VLAN y el acceso a ella está protegido a personas no autorizadas. Los estudiantes, docentes y administrativos contienen una VLAN separada y que permite el acceso a ella sólo a aquellos que son debidamente autenticados.
A.13.2	***Transferencia de información***		
A.13.2.1	Políticas y procedimientos de transferencia de información	**SI**	Las políticas y procedimientos para la transferencia de la información están debidamente documentados y se aplican los mecanismos de seguridad necesarios para garantizar la confidencialidad e integridad de la información.

A.13.2.2	Acuerdos sobre transferencia de información	**SI**	Existen documentos y acuerdos sobre los algoritmos de cifrado a utilizar para la transferencia de información que garanticen su confidencialidad e integridad.
A.13.2.3	Mensajería electrónica	**SI**	El Jefe de Seguridad y el Administrador de Redes implementan una Infraestructura de Llave Pública (PKI) mediante algoritmos fuertes de cifrado que garanticen la confidencialidad e integridad de la información que se transmite a través de las redes.
A.13.2.4	Acuerdos de confidencialidad o de no divulgación	**SI**	En los documentos y acuerdos contractuales de los empleados se estipula el compromiso con la confidencialidad de la información.

Tabla 45: Controles aplicables de la normativa ISO 27001:2013 basados en la seguridad de las comunicaciones

Fuente: Anny Cárdenas y Lissette Munizaga

CONTROL_ID	CONTROL	APLICABLE	IMPLEMENTACIÓN
A.15	**RELACIONES CON LOS PROVEEDORES**		
A.15.1	***Seguridad de la información en las relaciones con los proveedores***		
A.15.1.1	Política de seguridad de la información para las relaciones con proveedores	**SI**	Existe una política de seguridad de la información relacionada con los proveedores.
A.15.1.2	Tratamiento de la seguridad dentro de los acuerdos con proveedores	**SI**	Existen los acuerdos documentados con cada uno de los proveedores para el tratamiento de la seguridad de la información y los riesgos asociados.
A.15.1.3	Cadena de suministro de tecnología de	**SI**	Existen los acuerdos documentados con cada uno de los proveedores para el tratamiento de la seguridad

	información y comunicación		de la información y los riesgos asociados.
A.15.2	***Gestión de la prestación de servicios de proveedores***		
A.15.2.1	Seguimiento y revisión de los servicios de los proveedores	**SI**	Existen los acuerdos documentados con cada uno de los proveedores para el tratamiento de la seguridad de la información y los riesgos asociados.
A.15.2.2	Gestión de cambios en los servicios de los proveedores	**SI**	Existen los acuerdos documentados con cada uno de los proveedores para el tratamiento de la seguridad de la información y los riesgos asociados.

Tabla 46: Controles aplicables de la normativa ISO 27001:2013 basados en la seguridad de las comunicaciones

Fuente: Anny Cárdenas y Lissette Munizaga

CONTROL_ID	CONTROL	APLICABLE	IMPLEMENTACIÓN
A.16	**GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN**		
A.16.1	***Gestión de incidentes y mejoras de la seguridad de la información***		
A.16.1.1	Responsabilidades y procedimientos	**SI**	El Líder del Proceso de Desarrollo Tecnológico, el Jefe de Seguridad y los funcionarios pertinentes tienen documentado los procesos y procedimientos para los incidentes de la seguridad de la información. Se tiene documentado el Plan de Continuidad del Negocio donde están identificados claramente los responsables de su ejecución.
	Reporte de eventos de		Los funcionarios están alertados de los eventos e

A.16.1.2	seguridad de la información	**SI**	incidentes correspondientes relativos a la seguridad de la información. Los incidentes son reportados, evaluados y documentados. Se establecen los procedimientos a seguir.
A.16.1.3	Reporte de debilidades de seguridad de la información	**SI**	Existen los formatos documentados disponibles para que los funcionarios reporten las debilidades de la seguridad de la información. Estas notificaciones son evaluadas de forma inmediata por el Jefe de Seguridad.
	Evaluación de eventos de		Existen los formatos documentados disponibles

A.16.1.4	seguridad de la información y decisiones sobre ellos	**SI**	para que los funcionarios reporten las debilidades de la seguridad de la información. Estas notificaciones son evaluadas de forma inmediata por el Jefe de Seguridad.
A.16.1.5	Respuesta a incidentes de seguridad de la información	**SI**	El Líder del Proceso de Desarrollo Tecnológico, el Jefe de Seguridad y los funcionarios pertinentes tienen documentado los procesos y procedimientos para los incidentes de la seguridad de la información. Se tiene documentado el Plan de Continuidad del Negocio donde están

			identificados claramente los responsables de su ejecución.
A.16.1.6	Aprendizaje obtenido de los incidentes de seguridad de la información	**SI**	Los incidentes de la seguridad de la información son documentados especificando las vulnerabilidades, amenazas, riesgos y los posibles controles de seguridad a implementar constituyendo así una base de conocimiento.
A.16.1.7	Recolección de evidencia	**SI**	Existen formatos y documentos para recolectar la evidencia y emitirlos a las autoridades competentes.

Tabla 47: Controles aplicables de la normativa ISO 27001:2013 basados en gestión de incidentes de seguridad

Fuente: Anny Cárdenas y Lissette Munizaga

CONTROL_ID	CONTROL	APLICABLE	IMPLEMENTACIÓN
A.17	**ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO**		
A.17.1	***Continuidad de seguridad de la información***		
A.17.1.1	Planificación de la continuidad de la seguridad de la información	**SI**	El Líder del Proceso de Desarrollo Tecnológico, el Jefe de Seguridad y los funcionarios pertinentes tienen documentado los procesos y procedimientos para los incidentes de la seguridad de la información. Se tiene documentado el Plan de Continuidad del Negocio donde están identificados claramente los responsables de su ejecución.

A.17.1.2	Implementación de la continuidad de la seguridad de la información	**SI**	El Líder del Proceso de Desarrollo Tecnológico, el Jefe de Seguridad y los funcionarios pertinentes tienen documentado los procesos y procedimientos para los incidentes de la seguridad de la información. Se tiene documentado el Plan de Continuidad del Negocio donde están identificados claramente los responsables de su ejecución.
A.17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información	**SI**	El Líder del Proceso de Desarrollo Tecnológico, el Jefe de Seguridad y los funcionarios pertinentes tienen documentado los procesos y procedimientos

			para los incidentes de la seguridad de la información. Se tiene documentado el Plan de Continuidad del Negocio donde están identificados claramente los responsables de su ejecución.
A.17.2	***Redundancias***		
A.17.2.1	Disponibilidad de instalaciones de procesamiento de información	**SI**	En el Plan de Continuidad del Negocio se establece la instalación e infraestructura disponible para el procesamiento de información.

Tabla 48: Controles aplicables de la normativa ISO 27001:2013 basados en la continuidad del negocio

Fuente: Anny Cárdenas y Lissette Munizaga

5.2. Cronograma de la gestión de arranque del proyecto

Id	Nombre de la tarea	Duración	Comienzo	Fin	Recursos
1	Creación de políticas y procedimientos de control de accesos	27 días	29/04/2024	04/06/2024	Directivos, Técnicos, Ing. Lissette Munizaga, Ing. Anny. Cárdenas
2	Reunión con técnicos y directiva	1 día	29/04/2024	29/04/2024	Directivos, Técnicos, Ing. Lissette Munizaga, Ing. Anny. Cárdenas
3	FASE 1	5 días	30/04/2024	04/05/2024	Directivos, Técnicos, Ing. Lissette Munizaga, Ing. Anny. Cárdenas
4	Creación de políticas de control de accesos	4 días	30/04/2024	03/05/2024	Directivos, Técnicos, Ing. Lissette

					Munizaga, Ing. Anny. Cárdenas
5	revisión y aprobación	1 día	04/05/2024	04/05/2024	Directivos, Técnicos, Ing. Lissette Munizaga, Ing. Anny. Cárdenas
6	FASE 2	5 días	06/05/2024	10/05/2024	Directivos, Técnicos, Ing. Lissette Munizaga, Ing. Anny. Cárdenas
7	Creación de políticas de gestión de usuarios	4 días	06/05/2024	09/05/2024	Directivos, Técnicos, Ing. Lissette Munizaga, Ing. Anny. Cárdenas
8	Revisión y aprobación	1 día	10/05/2024	10/05/2024	Directivos, Técnicos, Ing. Lissette Munizaga, Ing. Anny. Cárdenas

9	FASE 3	5 días	13/05/2024	17/05/2024	Directivos, Técnicos, Ing. Lissette Munizaga, Ing. Anny. Cárdenas
10	Creación de políticas de contraseñas	4 días	13/05/2024	16/05/2024	Directivos, Técnicos, Ing. Lissette Munizaga, Ing. Anny. Cárdenas
11	Revisión y aprobación	1 día	17/05/2024	17/05/2024	Directivos, Técnicos, Ing. Lissette Munizaga, Ing. Anny. Cárdenas
12	FASE 4	5 días	20/05/2024	24/05/2024	Directivos, Técnicos, Ing. Lissette Munizaga, Ing. Anny. Cárdenas
13	Creación de políticas,	4 días	20/05/2024	23/05/2024	Directivos, Técnicos, Ing.

	procedimientos de acceso al Data Center				Lissette Munizaga, Ing. Anny. Cárdenas
14	Revisión y aprobación	1 día	24/05/2024	24/05/2024	Directivos, Técnicos, Ing. Lissette Munizaga, Ing. Anny. Cárdenas
15	FASE 5	9 días	27/05/2024	06/06/2024	Directivos, Técnicos, Ing. Lissette Munizaga, Ing. Anny. Cárdenas
16	Reunión con el área administrativa	1 día	27/05/2024	27/05/2024	Directivos, Técnicos, Ing. Lissette Munizaga, Ing. Anny. Cárdenas
17	Implementación de versión de prueba Manage Engine Ad Manager y PAM	4 días	28/05/2024	31/05/2024	Directivos, Técnicos, Ing. Lissette

					Munizaga, Ing. Anny. Cárdenas
18	Implementación de versión de prueba Manage Engine Log 360	3 días	03/06/2024	05/06/2024	Directivos, Técnicos, Ing. Lissette Munizaga, Ing. Anny. Cárdenas
19	Revisión y aprobación	1 día	06/06/2024	06/06/2024	Directivos, Técnicos, Ing. Lissette Munizaga, Ing. Anny. Cárdenas

Tabla 49: Cronograma de gestión de arranque del proyecto

Fuente: Anny Cárdenas y Lissette Munizaga

5.3. Políticas a implementar

5.3.1 Política de Control de Accesos

Objetivo

Definir las reglas de acceso para los diversos sistemas, equipos, instalaciones e información en base a los niveles de autorización para el uso apropiado de los mismos, brindando a la Institución educativa una fácil organización y un

control a los bienes y recursos a determinadas áreas o departamentos dentro de las instalaciones.

Alcance

Esta política aplica a todos los sistemas, equipos, instalaciones utilizadas dentro de la unidad educativa particular.

Documentos de referencia:

Norma ISO/IEC 27002/2013, capítulos A.9.1.1, A.9.1.2, A.9.2.1, A.9.2.2, A.9.2.3, A.9.2.4, A.9.2.5, A.9.2.6, A.9.3.1, A.9.4.1, A.9.4.3

Lineamientos generales:

- El principio básico es que el acceso a todos los sistemas, redes, servicios e información está prohibido salvo que sea expresamente permitido a usuarios individuales o a grupo de usuarios.
- Los administradores de los sistemas de tratamiento de información son los encargados de crear y proporcionar las credenciales de acceso a los colaboradores de la institución educativa.
- Los administradores de los sistemas de tratamiento de información son los responsables de la asignación de permisos y privilegios de los usuarios que se solicite la creación.
- El área de Recursos humanos debe informar al área de TICs la desvinculación del personal administrativo/Docente para proceder a des

habilitación de usuarios de acceso a las plataformas, sistemas y sectores físicos de la organización según se requiera.

- Los accesos deben ser revisados a intervalos planificados por el administrador de plataforma, sistema.
- Todo acceso nuevo que se vaya a otorgar debe responder a: “La necesidad de conocer” y “La necesidad de usar”.

5.3.2 Control de accesos

Acceso a las redes y a los servicios de red

- El acceso a las redes estará basado en la premisa “todo está restringido, a menos que esté expresamente permitido”
- Los colaboradores de la unidad educativa tendrán acceso a las redes y servicios de red únicamente necesarias y autorizadas para la ejecución de sus gestiones.
- El método de autenticación para las redes y servicios de red se dará mediante usuarios creados localmente en los ordenadores del personal docente/administrativos, plataformas y sistemas.
- Si se requiere un acceso adicional o temporal, este debe ser autorizado por la gestión de TICs y rectorado/vicerrectorado.

Control de conexión a las redes

- Las estaciones de trabajo para acceder a las redes de la organización se deben conectar a red inalámbrica perteneciente a su área de trabajo.

Conexiones de diagnóstico

- Los colaboradores deberán permitir la toma de control de sus equipos, por el personal del área de TICs, en mantenimiento de equipo, revisión de incidentes, escenarios de soporte.
- Tener en cuenta que no deben tener a la vista archivos con información sensible, y no dejar el equipo desatendido mientras se mantenga la revisión.
- El personal de TICs cuenta con un plazo de 24 horas para poder generar un resultado del diagnóstico de los equipos que se mantengan en revisión.

5.3.3 Política de Gestión de Usuarios

Objetivo:

El objetivo de la presente política es definir lineamientos para garantizar la gestión y utilización segura de usuarios y contraseñas.

Alcance:

Esta política aplica a todos los usuarios de los sistemas, equipos, instalaciones utilizadas dentro de la institución educativa.

Documentos de referencia:

- Norma ISO/IEC 27002:2013, capítulos A.9.2.1, A.9.2.2, A.9.2.3, A.9.2.4, A.9.2.5, A.9.2.6, A.9.3.1, A.9.4.2, A.9.4.

Administración de usuarios:

Dentro de la institución educativa se seguirán los siguientes lineamientos generales respecto a la gestión/administración de cuentas de usuario:

- La creación de los usuarios se lo realizará con el ingreso del personal.
- El uso de la cuenta de usuario es responsabilidad de la persona a la que se encuentre asignada.
- La cuenta de usuario es de uso personal e intransferible
- Toda cuenta de usuario debe mantener una contraseña, que debe cumplir con los requisitos de seguridad indicados en el apartado 3.3.1 del presente documento
- La cuenta de usuario no debe ser compartida a otras personas, incluyendo a su jefe inmediato o superiores.

Gestión de usuarios y accesos:

- Cada usuario para crear debe cumplir el requerimiento de ser único, es decir, en un mismo sistema no debe existir dos usuarios similares.
- La eliminación o inhabilitación de usuarios y/o accesos se darán en los siguientes escenarios:
  - **Salida de la organización:**
    - Para personal administrativo con accesos a los sistemas o áreas de tratamiento de información, se procederá a inhabilitar de forma inmediata todos los usuarios y/o accesos que mantenían.

- La eliminación de los usuarios y/o accesos sea de área administrativa u docencia que se han inhabilitado, se lo generará en un plazo máximo de 24 horas después de la desactivación del usuario.

- **Cambio de área:**
  - Si en la nueva área requerirá los mismos usuarios solo se generará el cambio de accesos y privilegios (de ser necesario).
  - Los accesos a los sistemas de la unidad educativa deben estar autorizados por la coordinación o gestor del área a la que corresponde la persona.
  - Para los accesos a los sistemas y áreas de tratamiento de información considerados como sensibles o críticos (sea de área administrativa o docencia), estos deben ser autorizados por la coordinación o gestor del área de quien solicita, y revisado por el área de TICs.
  - El administrador del sistema de tratamiento de información debe verificar el nivel de acceso otorgado a los usuarios.
  - El área de TICs, debe mantener un registro de los usuarios creados a los diversos sistemas de la institución.

Gestión de usuarios privilegiados

- Los usuarios privilegiados deben de ser únicos para cada sistema de información.
- Todo usuario privilegiado por defecto en los sistemas que se manejan en la institución educativa debe ser eliminado. De no ser posible la eliminación del usuario por temas operativos, este debe ser deshabilitado y modificar su contraseña, cumpliendo con los requisitos de seguridad establecidos anteriormente en el presente documento. El área de TICs será el custodio de este usuario.
- Los usuarios de acceso privilegiado deben ser utilizados específicamente para actividades relacionadas para administración y gestión de los sistemas de información.
- Los cambios realizados en cuentas privilegiadas deben ser registradas y autorizadas.

5.3.4 Política de Contraseñas

Objetivos

El objetivo de la presente política es definir lineamientos para garantizar la seguridad de las cuentas de usuarios por medio de la generación de contraseñas seguras.

Alcance

Esta política aplica a todos los sistemas utilizados por la unidad educativa.

Seguridad en la generación de contraseñas

Para garantizar la seguridad en los sistemas se debe tener en cuenta los siguientes lineamientos en la generación de contraseñas:

- Longitud mínima de 8 caracteres.
- Debe contener letras mayúsculas y minúsculas.
- Debe contener dígitos numéricos.
- Debe contener caracteres especiales como: ”, #, $, %, &, /, (,), =, ?,etc.
- No debe contener información sensible como: número de CI, fecha de nacimiento, etc.

Gestión segura de la contraseña

- No se debe utilizar la misma contraseña para acceder a los distintos servicios y/o sistemas de la Institución educativa.
- La contraseña debe ser tratada con carácter confidencial.
- No dejar las contraseñas escritas en un papel o en post-it de su puesto de trabajo.
- Se debe evitar en la medida de lo posible, teclear contraseñas en frente de otros colaboradores.
- No se debe revelar la contraseña a otras personas, incluyendo a su jefe inmediato o superiores.
- No debe revelar contraseñas en reportes, formularios, etc.

- Si detecta o existen indicios de que su contraseña pueda estar en riesgo, comprometida o siendo utilizada por un tercero, debe reportarlo con la coordinación de TICs.
- Los sistemas de información deben solicitar de forma automática (de ser posible) el cambio de contraseña en los usuarios cada 90 días.
- Los sistemas de información deben mantener configurado (de ser posible) el bloqueo de la cuenta de usuario tras tres intentos fallidos de ingreso de contraseña.
- Los sistemas de información deben mantener configurado (de ser posible) un historial de contraseñas de 3.
- Se debe habilitar el cambio de contraseña (de ser posible) en los sistemas de información en el que el Administrador ha asignado una clave de acceso temporal.
- La contraseña debe ser proporcionada a los usuarios de manera exclusiva y segura. Por ejemplo: Correo electrónico protegido (texto cifrado) – Sobre cerrado.

5.3.5 Política / Procedimiento De Acceso Al Data Center

Objetivo

Establecer los criterios necesarios para permitir el acceso al Data Center

Alcance

Esta política aplica a todo el personal que ingrese al Data Center.

Generalidades

- Todo acceso de personal externo debe ser previamente programado y autorizado y registrado en bitácora
- Ningún equipo del Data Center podrá salir sin la debida autorización escrita por el área administrativa y área de TICs.
- Se ha definido al interior del Data Center áreas de alta sensibilidad denominados pasillos calientes.
- Se prohíbe el ingreso de alimentos, bebidas, materiales, combustibles.
- Se prohíbe el ingreso de dispositivos de almacenamiento que no se encuentren debidamente autorizados.

De control de accesos

- Todos los ingresos al Data Center deben ser registrados en la bitácora de ingresos y es obligatorio el llenado el formulario.
- Es obligatorio llenar el registro de salida del Data Center.
- El departamento que recibe una visita será responsable del personal que ingresará al Data Center hasta la finalización de esta, de igual forma, es responsable por los equipos que se ingresen a esta área.

Procedimiento de ingreso al Data Center

Ingreso al Data Center del personal de TICs

- Dpto. Sistemas - Personal Autorizado de Sistemas.
    1. Tome el formulario de Acceso situado en la puerta de Acceso al Data Center.
    2. Registre los siguientes datos del formulario “Registro de Entrada”:
        a. Fecha.
        b. Nombre Completos.
        c. Hora de Entrada.
        d. Descripción del Trabajo.
    3. Coloque el formulario de Acceso en su lugar.
    4. Colocar su huella (Previamente Autorizada).
    5. Ingrese al Data Center.
    6. Cierre la Puerta de Ingreso al Data Center.
    7. Fin.

Salida del Data Center del personal de TICs

1. Presione botón de salida para salir del Data Center.
2. Salga del Data Center.
3. Tome el formulario de Acceso situado en la puerta de Acceso al Data Center.

4. Registre la Hora de Salida.
5. Firme el registro.
6. Coloque el formulario en su lugar.
7. Fin.

Ingreso al Data Center del personal externo

1. Tome el formulario de Acceso situado en la puerta de Acceso al Data Center.
2. Entregue Formulario al personal externo para que sea llenado.
3. Indique al Personal Externo los campos que debe de llenar:
    a. Fecha.
    b. Nombre Completos,
    c. Hora de Entrada.
    d. Descripción del Trabajo.
4. Coloque su huella en el biométrico (Previamente Autorizada).
5. Ingrese al Data Center.
6. Verifique que la Puerta de Ingreso al Data Center este cerrada.
7. Fin.

Salida de la data center del personal externo.

1. Presione el botón de salida para salir del Data Center.
2. Salga el Data Center.
3. Tome el formulario de Acceso situado en la puerta de Acceso al Data Center.

4. Registre la Hora de Salida.
5. Firme el registro.
6. Coloque el formulario en su lugar.

5.3.6 Política de Seguridad Física

Objetivo

Establecer los lineamientos a cumplir para asegurar los accesos a áreas sensibles únicamente al personal autorizado.

Alcance

Esta política aplica a todo el personal de la unidad educativa que ingrese a las instalaciones y al personal encargado de la seguridad física.

Generalidades:

- Se cuenta con guardianía las 24 horas del día, los 7días de la semana, los 365 días del año.
- Se cuenta con un circuito cerrado de televisión, el cual se encuentra ubicado estratégicamente.
- Vigilancia con video en toda la instalación y su perímetro.
- Los accesos que son dados mediante biométrico deben ser revisado de forma trimestral.
- Se prohíbe el ingreso a personal externo sin autorización formal.

- Todo el personal que sea parte de la institución educativa o externo debe portar su identificación en un lugar visible.
- El único acceso considerado como autorizado a las áreas catalogadas como sensibles es el del responsable del área.
- Toda incidencia relacionada con un evento de seguridad física debe ser notificada a las autoridades de la institución educativa y estos a su vez a las autoridades competentes.

Personal Externo

- Todos los visitantes deben mostrar identificación y dejarla bajo custodia del personal de seguridad física, mientras dura su visita, al final esta será devuelta.
- No se permitirá el acceso a personas que no sean plenamente identificables y que no se encuentran autorizadas por el departamento que espera su visita.
- El personal de seguridad física debe registrar en su bitácora la fecha, la hora de entrada y salida de las instalaciones de la institución educativa, de todo personal externo.

Socialización de Políticas

La difusión de las políticas creadas se la realiza en coordinación entre los maestrantes con el personal del departamento de TICs mediante el departamento de comunicación de la institución educativa.

El canal de comunicación por el cual se generará a difusión será a través del correo institucional, del departamento de talento humano

Cronograma de socialización de políticas de seguridad de la Unidad Educativa

Difusión de Política de Control de Accesos	10/07/2024
Difusión de Política de Gestión de usuarios	13/07/2024
Difusión de Política de Contraseñas	15/07/2024
Difusión de Política/Procedimiento acceso al Data Center	17/07/2024
Difusión de Política y Controles físicos de entrada a la unidad educativa	20/07/2024
Reunión de presentación de las políticas de seguridad de accesos para el personal docente/administrativo.	22/07/2024
Socialización de las políticas de seguridad por parte de los docentes a los cursos de la unidad educativa	24/07/2024 – 28/07/2024

Tabla 50: Cronograma de socialización de políticas de seguridad de la Unidad Educativa

Fuente: Anny Cárdenas y Lissette Munizaga

5.4. Implementación de controles lógicos

Una vez socializadas las políticas se procede con la implementación de los controles lógicas mediante software de Manage Engine ya que posee versión de prueba de 30 días gratis con todas las bondades.

Para la implementación de este software solo se requiere un espacio virtualizado para ello.

A continuación, se muestra evidencia de los controles aplicados dentro de los sistemas:

IDENTIFY ACCESS MANAGEMENT PARA ACCESOS TEMPORALES

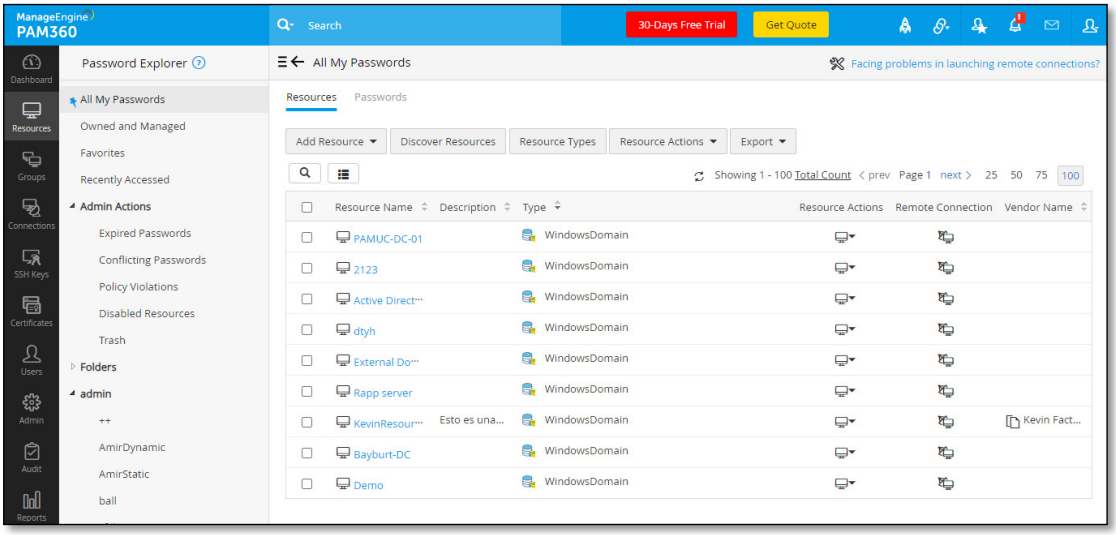

FIGURA 5.1: RECURSOS ADMINISTRADOS PAM360

Fuente: Anny Cárdenas y Lissette Munizaga

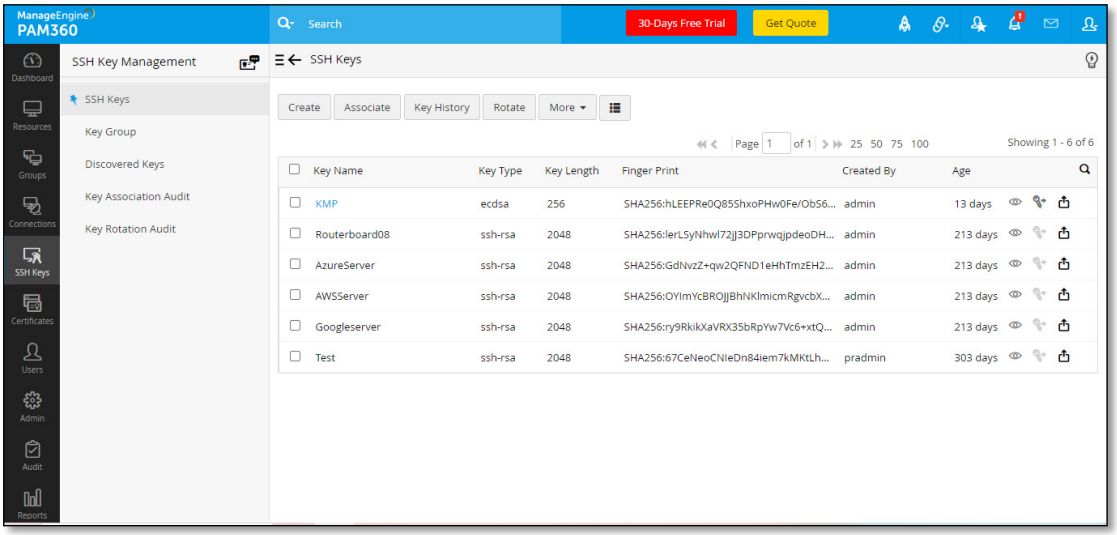

FIGURA 5.2: LLAVES SSH USADA EN PAM360

Fuente: Anny Cárdenas y Lissette Munizaga

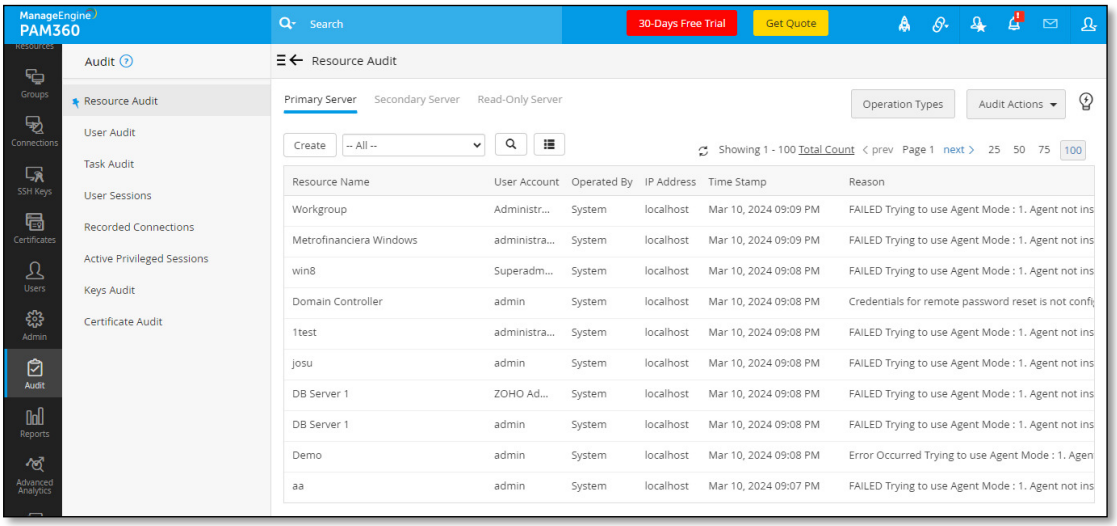

FIGURA 5.3: AUDITORIA DE EVENTOS EN PAM360

Fuente: Anny Cárdenas y Lissette Munizaga

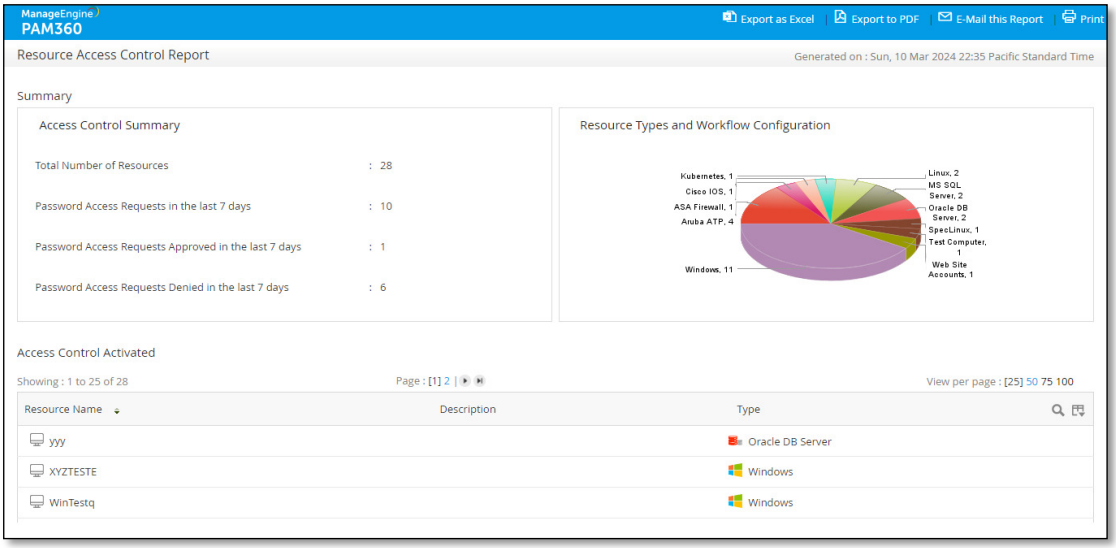

FIGURA 5.4: EJEMPLO DE REPORTES GERENCIALES EN PAM 360

Fuente: Anny Cárdenas y Lissette Munizaga

CONTROL DE ACCESO DE DIRECTORIO ACTIVO

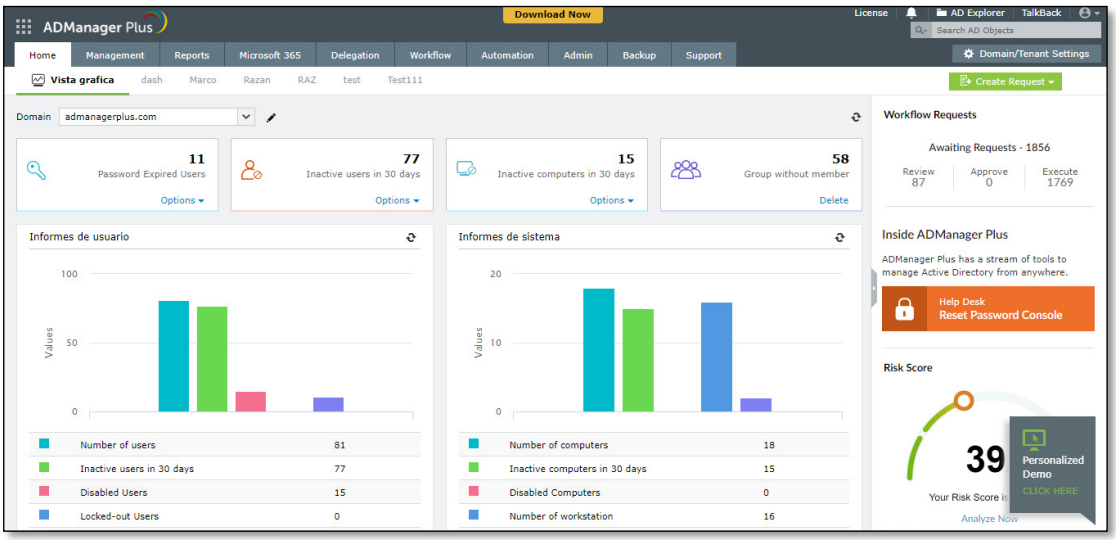

FIGURA 5.5: PANTALLA PRINCIPAL DE ADMANAGER PLUS

Fuente: Anny Cárdenas y Lissette Munizaga

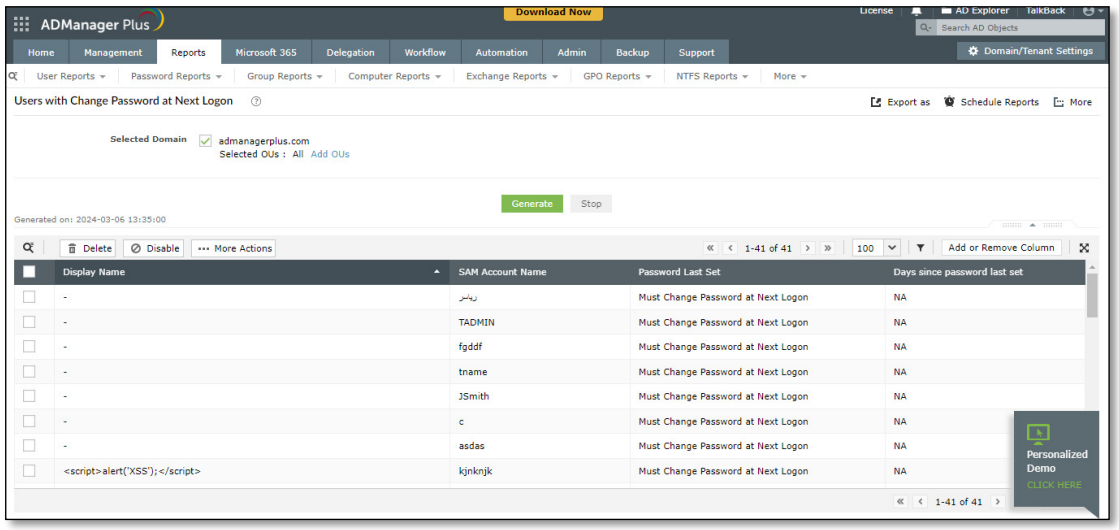

FIGURA 5.6: EJEMPLO DE REPORTE DE CAMBIOS DE CONTRASEÑA EN ADMANAGER

Fuente: Anny Cárdenas y Lissette Munizaga

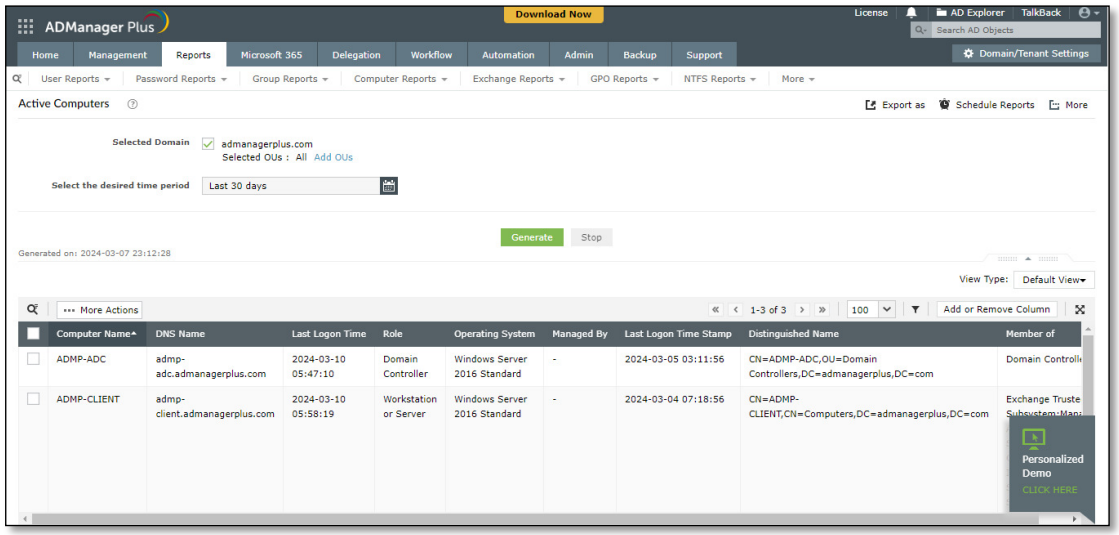

FIGURA 5.7: EJEMPLO DE REPORTE DE COMPUTADORAS ACTIVAS EN ADMANAGER

Fuente: Anny Cárdenas y Lissette Munizaga

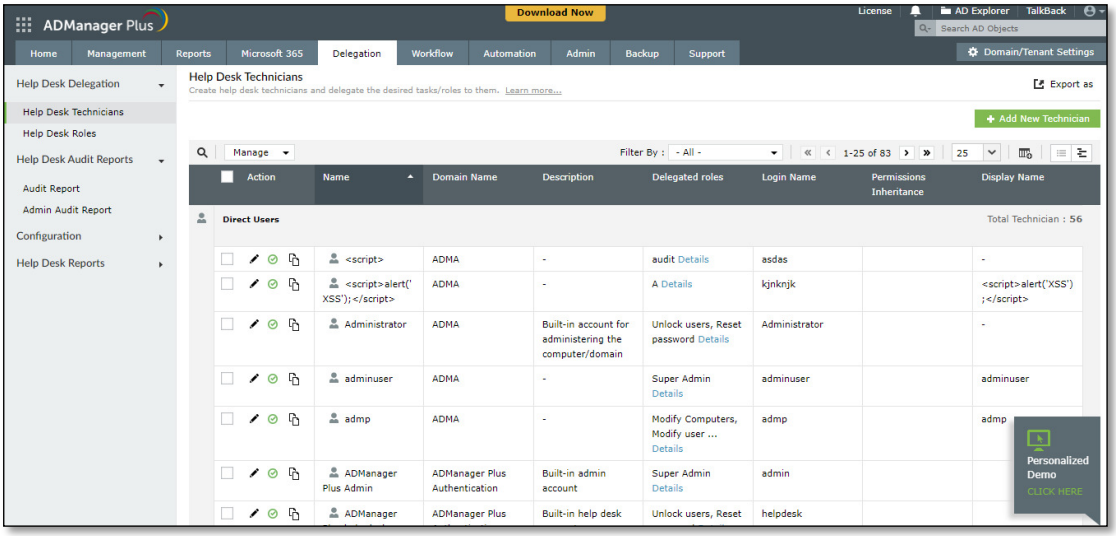

FIGURA 5.8: LISTADO DE TÉCNICOS ASIGNADOS ADMANAGER

Fuente: Anny Cárdenas y Lissette Munizaga

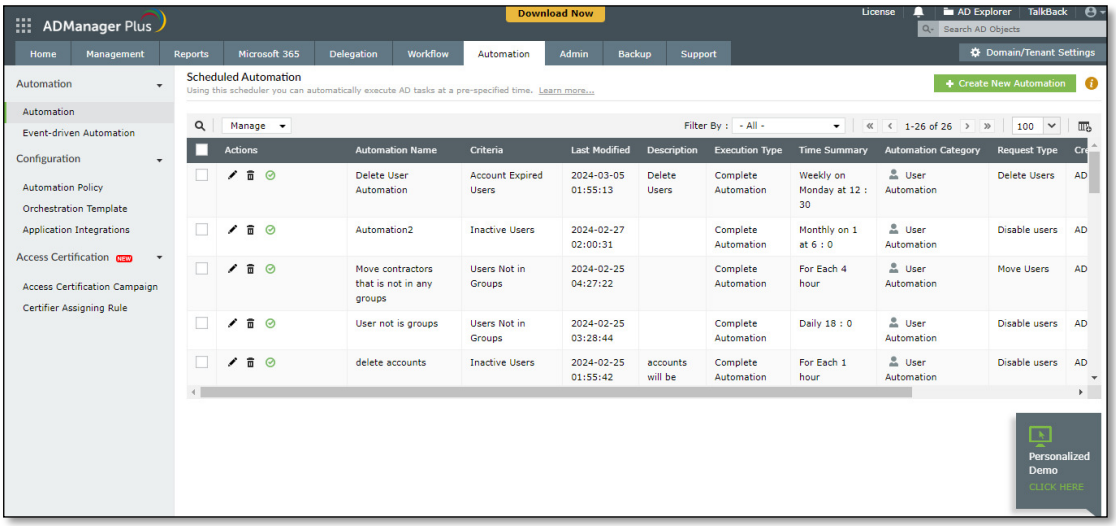

FIGURA 5.9: LISTADO DE TAREAS AUTOMATIZADAS ADMANAGER

Fuente: Anny Cárdenas y Lissette Munizaga

SIEM (SECURITY INFORMATION AND EVEN MANAGEMENT) PARA SEGURIDAD AUTOMATIZADA

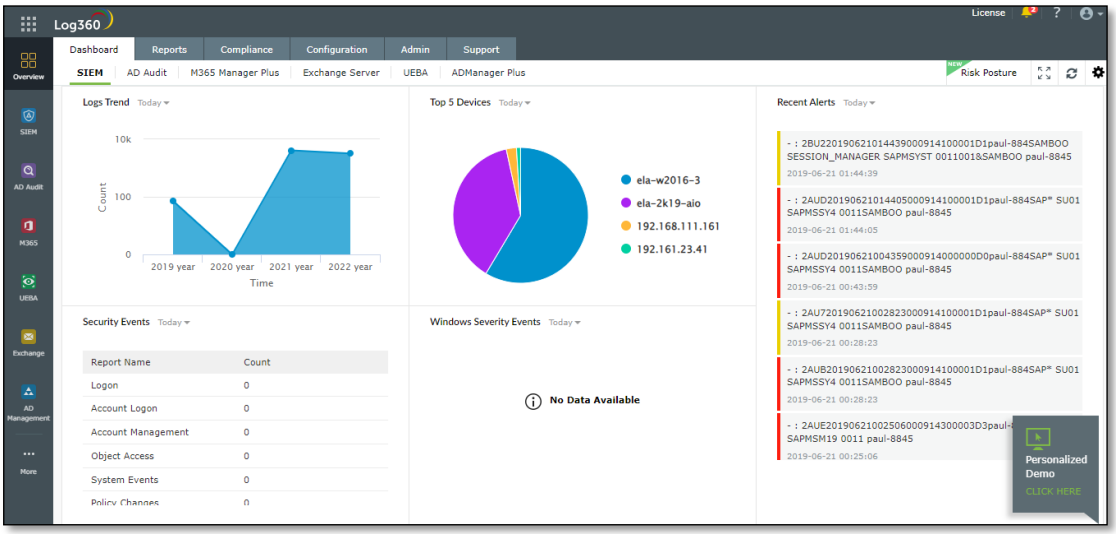

FIGURA 5.10: PANTALLA PRINCIPAL LOG360

Fuente: Anny Cárdenas y Lissette Munizaga

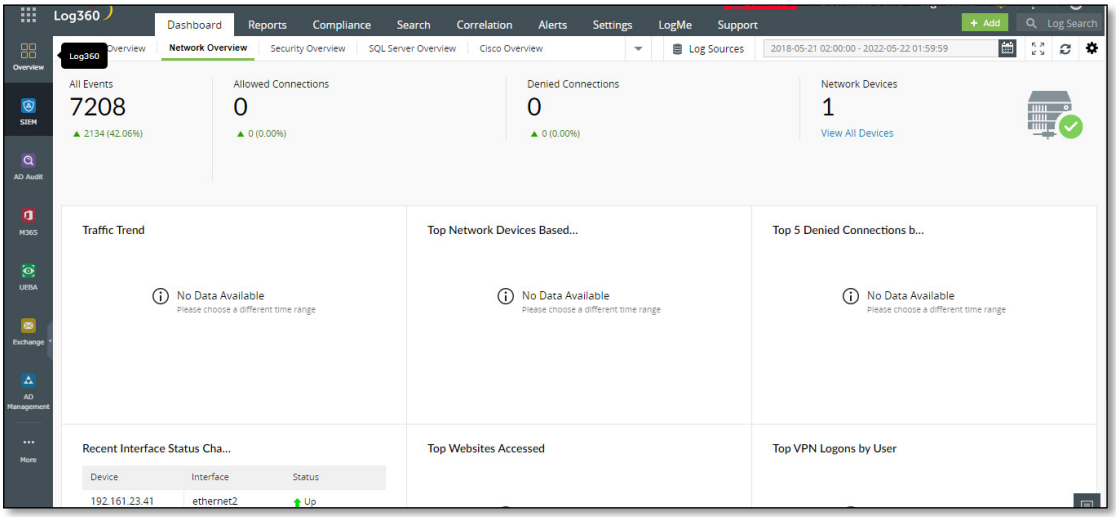

FIGURA 5.11: RESUMEN DE GRÁFICAS GERENCIALES LOG360

Fuente: Anny Cárdenas y Lissette Munizaga

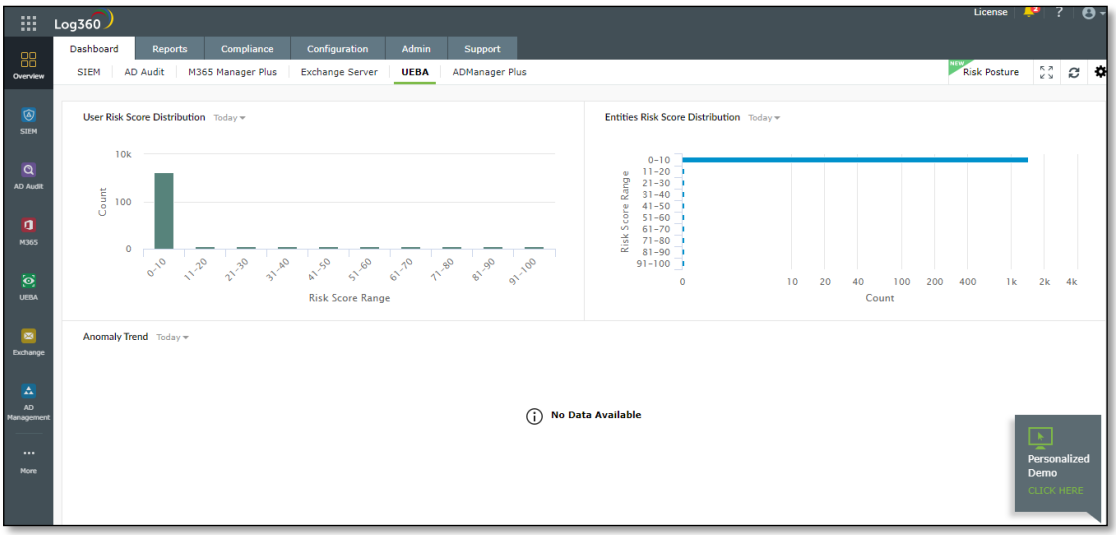

FIGURA 5.12: ANÁLISIS DE COMPORTAMIENTO DE USUARIOS Y ENTIDADES LOG360

Fuente: Anny Cárdenas y Lissette Munizaga

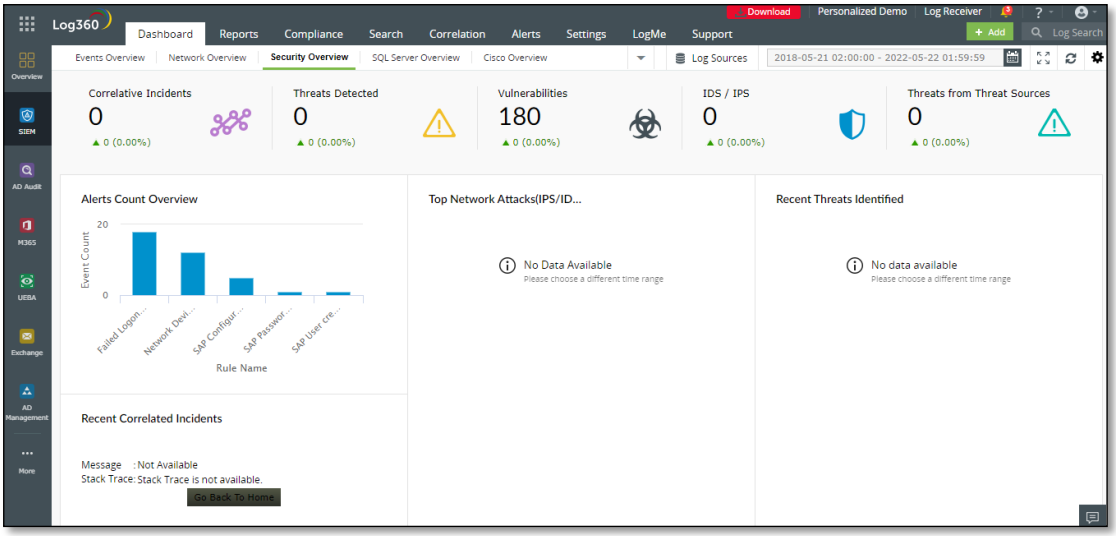

FIGURA 5.13: RESUMEN DE ESTADÍSTICAS DE SEGURIDAD LOG360

Fuente: Anny Cárdenas y Lissette Munizaga

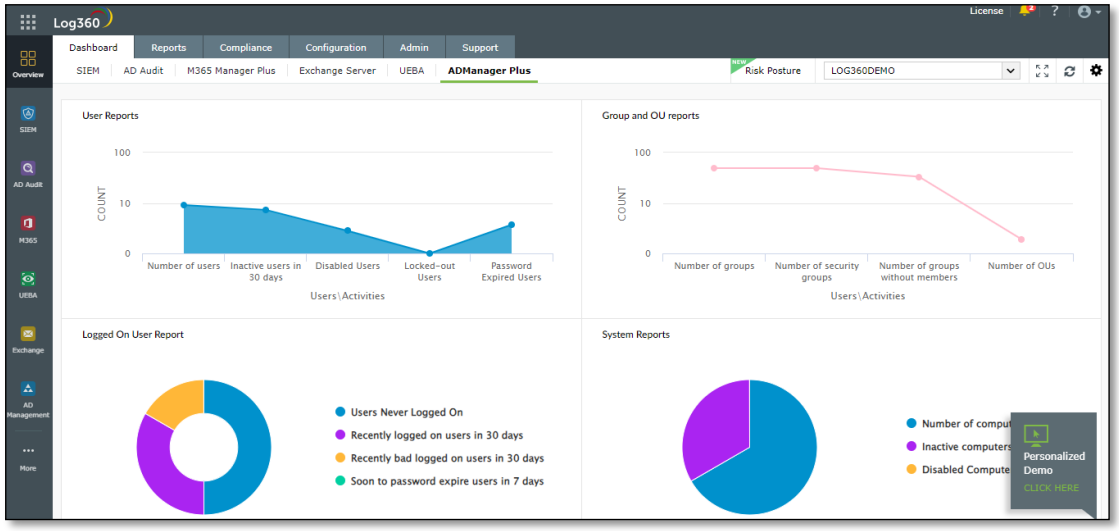

FIGURA 5.14: RESUMEN DE COMPLEMENTO DE ADMINISTRACIÓN DE ACTIVE DIRECTORY DENTRO DE LOG360

Fuente: Anny Cárdenas y Lissette Munizaga

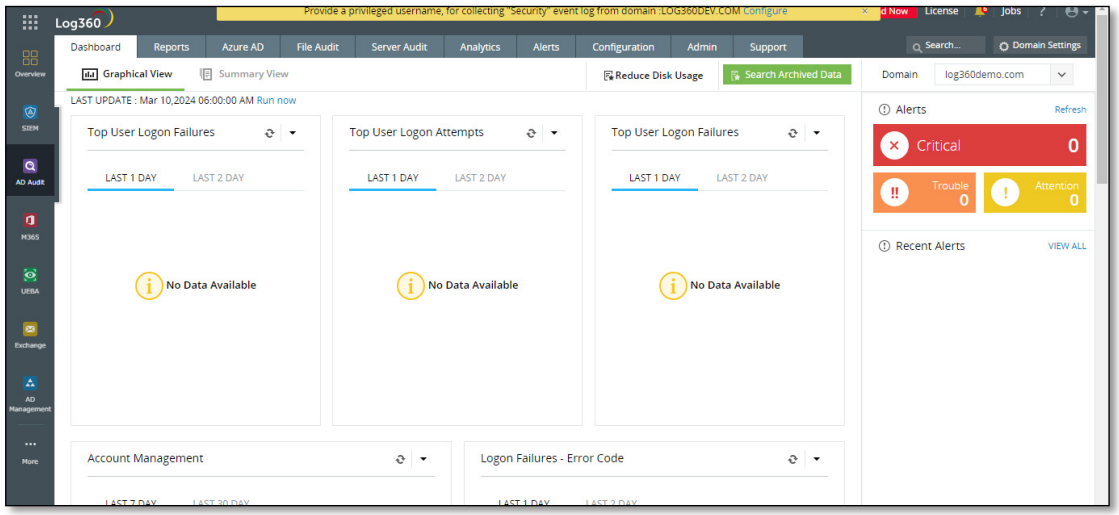

FIGURA 5.15: RESUMEN DE AUDITORÍA DE ACTIVE DIRECTORY DENTRO DE LOG360

Fuente: Anny Cárdenas y Lissette Munizaga

CONCLUSIONES

1. Tras haber generado la identificación de los sistemas y áreas de tratamiento de información, se pudo evidenciar que estos carecen de seguridad lógica y física en sus accesos, a su vez que los roles definidos en los sistemas no estaban acorde a las funciones de quienes pueden acceder a la información, teniendo mayores o menores privilegios de los que necesitaban para sus funciones.

2. Gracias a la metodología de evaluación y tratamiento de riesgos desarrollada, el personal responsable de los activos de información

pudo identificar las amenazas y vulnerabilidades a los cuales se encuentran expuestos, permitiendo obtener la valoración del riesgo para cada uno de ellos y a su vez establecer los controles de la norma ISO/IEC 27002:2013 que permiten tratar el riesgo para que este sea aceptable por la unidad educativa.

3. La unidad educativa no contaba con controles de accesos que permitiesen mantener la seguridad sobre sus activos tanto físicas como lógicas, causando así una serie de incidentes, entre estos la perdida de información y accesos no autorizados. Con la elaboración e implementación de políticas de seguridad de accesos se logra mitigar los incidentes antes mencionados, y establecer un mayor control sobre sobre sus activos en el transcurso de los periodos académicos, dando camino a la implantación de un SGSI.

4. A través de las distintas actividades llevadas a cabo en el presente proyecto, se concluye que se ha alcanzado el establecimiento de una postura de seguridad de la información en la unidad educativa, logrando así preservar los tres pilares fundamentales (integridad, confidencialidad y disponibilidad) sobre sus activos de información.

RECOMENDACIONES

1. Identificar a los demás activos de información (tecnológicos, humanos, infraestructura) que posee la unidad educativa para que estos puedan ser evaluados acorde a la metodología de evaluación y tratamiento de riesgos establecidas en el presente proyecto, y así se logre identificar las amenazas y vulnerabilidades que se mantienen y se encuentran imperceptibles, para que en los posterior se pueda generar la implementación de controles de seguridad que sean necesarios.

2. Se recomienda adicionar al departamento de TICS funciones relacionadas con seguridad de la información y este a su vez pueda realizar auditorías de forma periódica y planificada del cumplimiento de las políticas y controles de seguridad de accesos que fueron creados.

3. Capacitar a todos los funcionarios (docente, administrativo, estudiantil) de la unidad educativa en temas de seguridad de la información, con especial énfasis en usuarios, contraseñas y su correcto uso basado en las buenas prácticas de seguridad de la información.

BIBLIOGRAFÍA

[1] E. Morales-Osorio y M. López-Trujillo, «Sistemas de gestión de seguridad de la información para empresas KPO: una aproximación», *Ventana Informática*, n.º 37, 2017.

[2] O. A. Fonseca-Herrera, A. E. Rojas, y H. Florez, «A model of an information security management system based on NTC-ISO/IEC 27001 standard», *IAENG Int. J. Comput. Sci*, vol. 48, n.º 2, pp. 213-222, 2021.

[3] J. D. Shaw, J. Zhu, M. K. Duffy, K. L. Scott, H.-A. Shih, y E. Susanto, «A contingency model of conflict and team effectiveness.», *Journal of applied psychology*, vol. 96, n.º 2, p. 391, 2011.

[4] S. Al-Dhahri, M. Al-Sarti, y A. Abdul, «Information security management system», *International Journal of Computer Applications*, vol. 158, n.º 7, pp. 29-33, 2017.

[5] S. Hadzhikoleva, D. Orozova, N. Andonov, y E. Hadzhikolev, «Generalized net model of a system for quality assurance in higher education», en *AIP Conference Proceedings*, AIP Publishing, 2019.

[6] M. Poongodi, V. Vijayakumar, F. Al-Turjman, M. Hamdi, y M. Ma, «Intrusion prevention system for DDoS attack on VANET with reCAPTCHA controller using information based metrics», *IEEE Access*, vol. 7, pp. 158481-158491, 2019.

[7] M. Poongodi, V. Vijayakumar, F. Al-Turjman, M. Hamdi, y M. Ma, «Intrusion prevention system for DDoS attack on VANET with

reCAPTCHA controller using information based metrics», *IEEE Access*, vol. 7, pp. 158481-158491, 2019.

[8] Y. Kamil, S. Lund, y M. S. Islam, «Information security objectives and the output legitimacy of ISO/IEC 27001: stakeholders' perspective on expectations in private organizations in Sweden», *Information Systems and e-Business Management*, vol. 21, n.º 3, pp. 699-722, 2023.

[9] H. Susanto y M. N. Almunawar, *Information Security Management Systems: A Novel Framework and Software as a Tool for Compliance with Information Security Standards*. 2020. doi: 10.1201/9781315232355.

[10] M. Siponen y R. Willison, «Information security management standards: Problems and solutions», *Information & management*, vol. 46, n.º 5, pp. 267-270, 2009.

[11] R. von Solms, «Information security management: why standards are important», *Inf. Manag. Comput. Secur.*, vol. 7, pp. 50-58, 1999.

[12] B. Shojaie, H. Federrath, y I. Saberi, «Evaluating the Effectiveness of ISO 27001: 2013 Based on Annex A», en *Proceedings - 9th International onference on Availability, Reliability and Security, ARES 2014*, sep. 2014, pp. 259-264. doi: 10.1109/ARES.2014.41.

[13] A. Andersson, F. Karlsson, y K. Hedström, «Consensus versus warfare–unveiling discourses in de jure information security standard development», *computers & security*, vol. 99, p. 102035, 2020.

[14] D. Proença y J. Borbinha, «Information Security Management Systems - A Maturity Model Based on ISO/IEC 27001», 2018, pp. 102-114. doi: 10.1007/978-3-319-93931-5_8.

[15] G. Disterer, «ISO/IEC 27000, 27001 and 27002 for Information Security Management», *Journal of Information Security*, vol. 04, pp. 92-100, ene. 2013, doi: 10.4236/jis.2013.42011.

[16] P. Douvreleur, «Challenges Faced by Legal Counsels in Big Data and Cybersecurity Activity», *Int'l. In-House Counsel J.*, vol. 12, p. 1, 2019.

[17] V. A. Schmidt, «Democracy and legitimacy in the European Union revisited: Input, output and 'throughput'», *Political studies*, vol. 61, n.º 1, pp. 2-22, 2013.

[18] R. Werle y E. J. Iversen, «Promoting legitimacy in technical standardization», *Science, Technology & Innovation Studies*, vol. 2, n.º 1, pp. 19-39, 2006.

[19] K. Arias Marín, P. Carrillo Maldonado, y J. Torres Olmedo, «Análisis del sector informal y discusiones sobre la regulación del trabajo en plataformas digitales en el Ecuador», 2020.

[20] M. C. A. Garrido, A. L. C. León, J. G. Gómez, J. L. L. Olivencia, y J. A. G. Ruiz, *Fundamentos de Informática*. en Manuales (Universidad de Málaga). Servicio de Publicaciones e Intercambio Científico de la Universidad de Málaga, 2009. [En línea]. Disponible en: https://books.google.com.ec/books?id=ZS2_cQAACAAJ

[21] A. Mentor, «Normas ISO sobre gestión de seguridad de la información». España: Ministerio Educación, Cultura y Deporte. Obtenido de: http …, 2016.

[22] A. L. Neira y J. R. Spohr, «El portal de ISO 27001 en Español», *línea]. Available: http://www. iso27000. es/iso27000. html.[Último acceso: 05 07 2015]*, 2016.

[23] I. Tools, «ISO Tools excellence», *Obtenido de https://www. isotools. org/2015/08/02/normas-iso-mas-empleadas-anivel-mundial*, 2017.

[24] M. L. Hurtado Cruz, «Gestión de riesgo, metodologías Octave y Magerit», B.S. thesis, Universidad Piloto de Colombia, 2018.

[25] A. E. de N. y Certificación, *Metodología de análisis y gestión de riesgos para los sistemas de información*. AENOR, 2008. [En línea]. Disponible en: https://books.google.com.ec/books?id=on5QzwEACAAJ

[26] M. L. E. Geovanny, *Análisis Y Gestión de Riesgos Implementando la Metodología Magerit*. Editorial Academica Espanola, 2012. [En línea]. Disponible en: https://books.google.com.ec/books?id=L-htLwEACAAJ