

TECNOLÓGICO DE ESTUDIOS SUPERIORES DE COACALCO

Plan de contingencia con ISO 17799 para gestión
de seguridad de información del área informática
en el Centro de Bachillerato Tecnológico,
Industrial y de Servicios #133.

Informe Técnico de Residencias Profesionales

Para obtener el Título de
Ingeniera en Sistemas Computacionales
Con la Especialidad en
Auditoría en Seguridad Informática

Presenta:

Franco Romero Tzitzí Marisol
Matricula 201921209

Asesor:

Lic. Ovando Torres Abraham

Coacalco de Berriozábal, Méx. Marzo 2025.

AGRADECIMIENTOS

A mi familia por brindarme la oportunidad de superarme a nivel educativo y por enseñarme los valores de responsabilidad y mejora continua frente a nuevos desafíos. Su apoyo me ha sido fundamental y motivado a alcanzar los logros que hoy celebro.

También expresar mi gratitud a mis asesores y a las instituciones que me han brindado su apoyo, orientación y corrección durante este período; su acompañamiento ha sido invaluable en mi proceso de crecimiento y aprendizaje.

RESUMEN

Este proyecto tiene como objetivo implementar un Plan de Contingencia basado en la norma ISO 17799 para fortalecer la seguridad de la información en el área informática del Centro de Bachillerato Tecnológico, Industrial y de Servicios #133.

La norma ISO 17799 proporciona un marco sólido para establecer controles y procesos que salvaguarden la seguridad de la información. En el contexto del CBTIS #133, este enfoque se aplicará específicamente al ámbito informático, abordando amenazas potenciales y mitigando riesgos asociados.

El plan contempla la identificación de activos críticos de información, evaluación de vulnerabilidades, y la definición de medidas preventivas y correctivas. Se establecerán procedimientos claros para la gestión de incidentes y se desarrollarán protocolos de respuesta rápida ante posibles brechas de seguridad.

La implementación de este proyecto garantizará que el CBTIS #133 cuente con un robusto sistema de gestión de seguridad de la información, alineado con estándares internacionales, asegurando así la integridad, confidencialidad y disponibilidad de la información crítica para el adecuado funcionamiento de la institución.

CONTENIDO

CAPITULO I GENERALIDADES DEL PROYECTO.....	9
1.1 INTRODUCCIÓN.....	10
1.2 DESCRIPCIÓN DE LA EMPRESA.....	11
1.2.1 Nombre, Razón Social	11
Sector Productivo de la Empresa	12
1.2.2 Misión	12
1.2.3 Visión.....	12
1.2.4 Filosofía y/o Valores.....	12
Breve Historia de la Empresa.	13
1.4 PROBLEMA A RESOLVER.....	14
1.5 OBJETIVOS	15
1.5.1 General.....	15
1.5.2 Específicos	15
1.6 JUSTIFICACIÓN	17
CAPÍTULO II MARCO TEÓRICO	18
2.1 LA SEGURIDAD DE INFORMACIÓN	19
2.2 PLAN DE CONTINGENCIA INFORMÁTICO	19
2.3 IMPLEMENTACIÓN DE UN PLAN DE CONTINGENCIA INFORMÁTICO	20
2.4 ETAPAS PARA LA ELABORACIÓN DE UN PLAN DE CONTINGENCIA.	20
2.5 BENEFICIOS DE UN PLAN DE CONTINGENCIA	22
2.6 BUENAS PRÁCTICAS DE LA ELABORACIÓN DE UN PLAN DE CONTINGENCIA BASADO EN ISO 17799-1.....	22
2.7 DESARROLLO DE LOS LINEAMIENTOS	22

2.8 EVALUACIÓN DE LOS RIESGOS DE LA SEGURIDAD.....	23
2.9 ANÁLISIS RIESGO.....	23
2.10 DEFINICIÓN DE AMENAZA	25
2.11 DEFINICIÓN DE VIRUS Y MALWARE	25
2.12 DEFINICIÓN DE VULNERABILIDAD	25
2.13 DEFINICIÓN DE INCIDENTE DE SEGURIDAD	25
2.14 DEFINICIÓN DE EVENTO DE SEGURIDAD DE LA INFORMACIÓN.....	26
2.15 LA SEGURIDAD DE LA INFORMACIÓN	26
2.16 MATRIZ DE RIESGOS.....	26
2.17 CLASIFICACIÓN DE UNA MATRIZ DE RIESGOS	27
2.18 CONTROL DE ACCESO	28
2.19 TIPOS DE CONTROLES DE ACCESO	28
2.20 PÉRDIDA DE DATOS	30
2.21 LA IMPORTANCIA DE LA RECUPERACIÓN DE DATOS	30
2.22 DEFINICIÓN DE UN RESPALDO INFORMATICO.....	30
2.23 IMPORTANCIA DEL RESPALDO DE DATOS	31
CAPÍTULO III	33
DESARROLLO	33
3.1 ANÁLISIS DE RIESGO	34
3.1.1 Identificación de Amenazas del Plantel	34
3.1.2 Identificación de Vulnerabilidades en el Plantel	35
3.2 TABLA DE EVALUACIÓN DE RIESGOS	37
3.3 MATRIZ DE RIESGO	38
3.4 MEDIDAS PREVENTIVAS DE CONTROL DE SEGURIDAD	38
3.5 PLAN DE CONTINGENCIA	40

3.5.1 Amenazas Físicas.....	40
Caso 1. Robo de equipos.....	40
3.5.2 Amenazas Lógicas	41
Caso 1. Software Desactualizado.....	41
Caso 2. Pérdida de Datos.....	42
Caso 3. Ataques Cibernéticos.....	42
3.6 PLAN DE RECUPERACIÓN.....	44
3.6.1 Detección y Notificación	44
3.6.2 Preparación	44
3.6.3 Evaluación y Respuesta	44
3.6.4 Recuperación y Restauración.....	44
3.6.5 Comunicación y Coordinación	45
3.6.6 Evaluación Post-Incidente	45
3.7 PLAN DE CONTINUIDAD DE PRUEBAS	46
3.7.1 Pruebas por Realizar	46
Planificación de las Pruebas.....	46
Ejecución de las Pruebas	46
Análisis de los Resultados.....	47
Seguimiento y Mejora Continua.	47
3.7.2 Capacitación al Personal.....	47
3.8 POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN BASADO EN LA ISO 17799	49
3.8.1 De Hardware	49
3.8.2 De Software	50
3.8.3 De Seguridad Física	51

3.8.4 De Servicios	52
3.8.5 De Información	53
3.8.6 De Personas.....	54
3.9 MONITOREO Y ACTUALIZACIÓN CONTINUA.....	56
3.9.1 Plan de Monitoreo.....	56
3.10 REVISIÓN PERIÓDICA	58
3.11 ANÁLISIS POST-INCIDENTES	59
CAPÍTULO IV	62
RESULTADOS.....	62
4.1 INVENTARIO Y COTIZACIÓN DE ACTIVOS.....	63
4.2 IDENTIFICACIÓN DE VULNERABILIDADES Y VALOR MONETARIO.....	67
4.3 DIAGRAMA DE FLUJO DEL PLAN DE RECUPERACIÓN.....	71
4.4 DIAGRAMA DE FLUJO DEL PLAN DE PRUEBAS	72
4.5 DIAGRAMA DE FLUJO DE MONITOREO.....	73
4.6 DIAGRAMA DE FLUJO DE ACTUALIZACIÓN PERIÓDICA.....	74
4.7 DIAGRAMA DE FLUJO DEL ANÁLISIS POST-INCIDENTE	75
CONCLUSIONES.....	76
COMPETENCIAS DESARROLLADAS	77
FUENTES DE INFORMACIÓN	78
ANEXOS	79
Anexo 01. Bitácora de Laboratorio 1 y 2.....	79
Anexo 02. Carta Compromiso.	80

ÍNDICE FIGURAS

Figura 1. Organigrama de la institución.....	11
Figura 2. Proceso de análisis y gestión de riesgos de la seguridad de la información	24
Figura 3. Proceso de Administración del Riesgo.	28
Figura 4. Elaboración de documentación..	45
Figura 5. Monitoreo.....	57
Figura 6. Revisión Periódica..	58
Figura 7. Análisis de Post-incidencia..	61
Figura 8. Inventario de Equipos.	63
Figura 9. Costo de Equipos.	66
Figura 10. Porcentaje de Vulnerabilidades.	68
Figura 11. Comparación de valores monetarios.....	69
Figura 12. Priorización de Vulnerabilidades.....	70
Figura 13. Flujo de Plan de Recuperación.	71

ÍNDICE TABLAS

Tabla 1 Identificación de Amenazas del Plantel.	35
Tabla 2 Identificación de Vulnerabilidades del Plantel.	35
Tabla 3 Tabla de Evaluación de Riesgos.	37
Tabla 4 Matriz de Riesgo.	38
Tabla 5 Medidas Preventivas de Control de Seguridad.	40
Tabla 6 Tabla de Cotización de Laboratorio 1.	65
Tabla 7 Tabla de Cotización de Laboratorio 2.	66
Tabla 8 Identificación de Vulnerabilidades y Valor Monetario.....	68

CAPÍTULO I: GENERALIDADES DEL PROYECTO

1.1 INTRODUCCIÓN

El presente documento aborda la creación e implementación de un plan de contingencia informática para el Centro de Bachillerato Tecnológico, Industrial y de Servicios #133, enfocado en la gestión de la seguridad de la información. Este tema se centra en la necesidad de establecer lineamientos claros que permitan proteger los datos y activos tecnológicos de la institución ante posibles incidentes como fallas técnicas, robos de información o desastres naturales.

Uno de los problemas a resolver es el desarrollo de este plan debido a que radica la creciente vulnerabilidad informática de la institución debido a la falta de un plan de contingencia adecuado. Por lo que es de suma importancia prevenir y responder a incidentes, de los cuales se expone la institución a riesgos significativos. Proteger la continuidad operativa y garantizar la seguridad de la información es un interés académico y profesional fundamental para mantener la estabilidad institucional.

Este trabajo está pensado como una estrategia integral que incluye un análisis de riesgos para identificar vulnerabilidades, evaluar el impacto de las amenazas y definir medidas de mitigación adecuadas. La metodología empleada se basará en estándares internacionales, como la norma ISO/IEC 17799, utilizando técnicas de análisis de riesgos y evaluación de impacto, aplicadas a la infraestructura tecnológica de la institución.

Una de las limitaciones del trabajo es la constante evolución de las amenazas tecnológicas, lo que requiere actualizaciones periódicas al plan. Además, la capacitación del personal y la disponibilidad de recursos pueden ser factores que limiten su efectividad.

El documento se estructura de varios capítulos, comenzando con el capítulo I el cual nos introduce al contexto de la problemática, seguida por el capítulo III en donde se desarrolla un análisis de riesgos, plan de contingencia y los procedimientos a seguir, y finaliza en el capítulo IV con la implementación de controles basados en ISO/IEC 17799 para asegurar la confidencialidad, integridad y disponibilidad de la información crítica de la institución.

1.2 DESCRIPCIÓN DE LA EMPRESA

1.2.1 Nombre, Razón Social

Centro de Bachillerato Tecnológico, Industrial y de Servicios #133 Dr. Manuel Velasco Suárez. Ubicada en Av. Dalias No. 220, Colonia Villa de las Flores, 55710 Coacalco, Estado de México. Tiene como organización el siguiente organigrama.

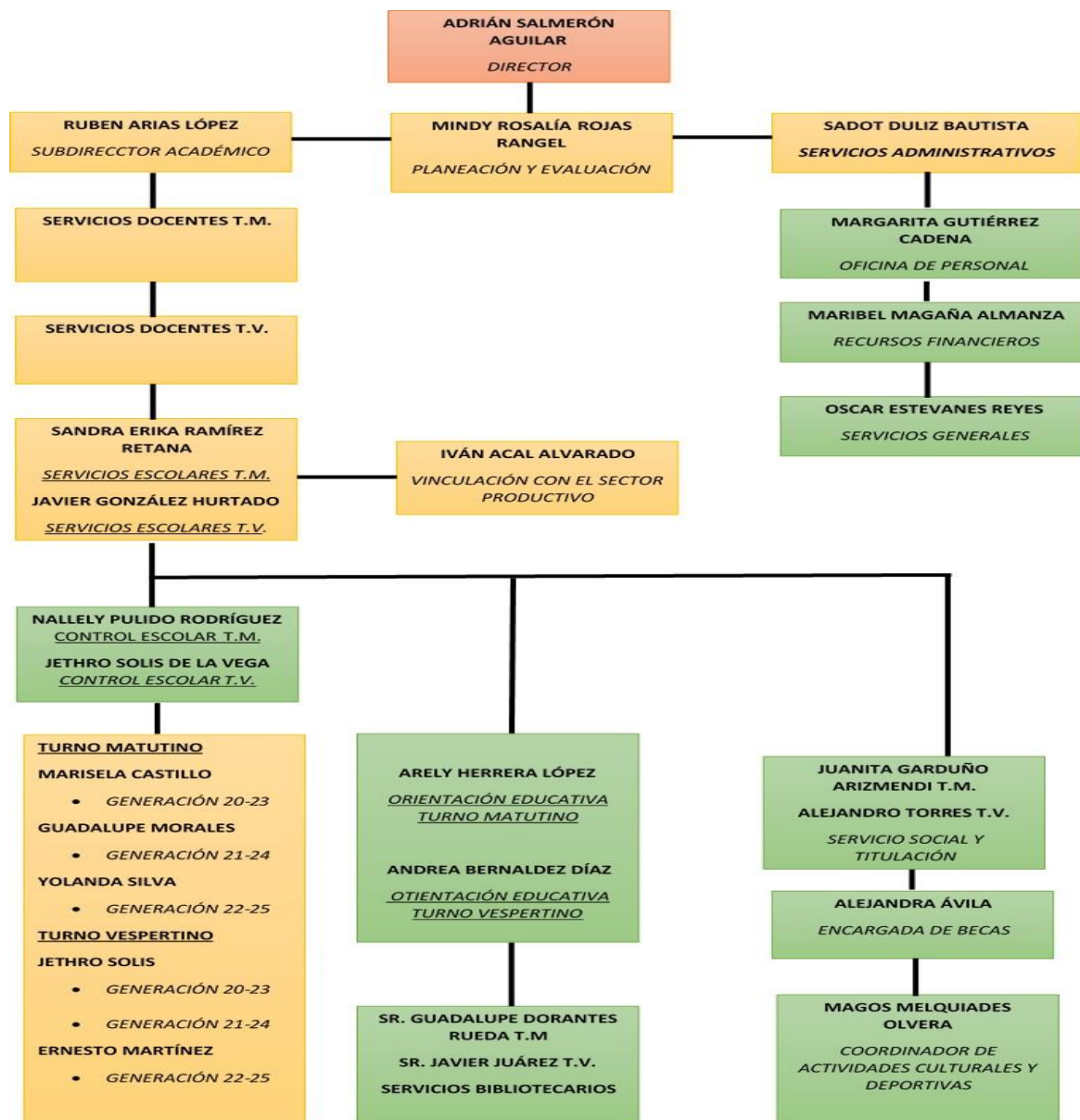


Figura 1. Organigrama de la institución, Fuente: cbtis133.edu.mx

Sector Productivo de la Empresa

Educación Media Superior Tecnológica.

1.2.2 Misión

Ofrecer una Educación Media Superior Tecnológica de calidad, que nos permita formar educandos con una amplia cultura basada en conocimientos científicos, humanistas y tecnológicos, que los comprometa a continuar sus estudios a nivel superior y al mismo tiempo les capacite para ser el eje en la conformación de un país más productivo y competitivo.

1.2.3 Visión

Ser una organización abierta a la comunidad y brindar un servicio de calidad, que garantice una educación tecnológica de excelencia, orientada a la formación de ciudadanos con valores cívicos y éticos, capaces de trascender en el campo profesional y laboral, desarrollando conocimientos con una alta pertinencia, capacidad creativa y equidad, que cuenten con identidad estatal y nacional.

1.2.4 Filosofía y/o Valores

La institución se compromete con una visión integral que promueve el bien común, la integridad y la honradez como pilares fundamentales de nuestra acción. Buscamos cultivar una cultura organizacional basada en la imparcialidad, la justicia y la transparencia, donde cada individuo sea responsable y rinda cuentas por sus acciones.

Nos comprometemos a preservar y promover un entorno cultural y ecológico sostenible, reconociendo nuestra responsabilidad hacia las generaciones futuras. Practicamos la generosidad y promovemos la igualdad, el respeto y el liderazgo ético en todas nuestras interacciones.

Creemos en el poder transformador del diálogo y la colaboración, fomentando la participación de todos los miembros de nuestra comunidad. Nuestra filosofía se basa en la creencia de que juntos podemos construir un mundo más justo, equitativo y sostenible para todos.

Breve Historia de la Empresa.

El Centro de Bachillerato Tecnológico Industrial y de Servicios No.133 es una institución educativa mexicana con una historia marcada por el compromiso con la formación técnica y profesional de los jóvenes. El CBTIS 133 ha sido un pilar en la comunidad local, proporcionando educación de calidad en áreas como tecnología, industria y servicios.

A lo largo de los años, el CBTIS 133 ha evolucionado para adaptarse a los avances tecnológicos y las demandas cambiantes del mercado laboral, ofreciendo programas educativos actualizados que preparan a los estudiantes para enfrentar los desafíos del mundo moderno. Con un enfoque en la excelencia académica y el desarrollo integral de los alumnos, la institución ha forjado una sólida reputación por su dedicación a la enseñanza y el aprendizaje.

El CBTIS 133 ha sido un semillero de talento y una fuente de orgullo para la comunidad, graduando a generaciones de profesionales capacitados que han contribuido al desarrollo económico y social de la región. Su legado perdura a través de la trayectoria exitosa de sus egresados y su continua labor en la formación de nuevas generaciones de líderes en el ámbito tecnológico e industrial. (CBTIS 133, s.f.)

1.4 PROBLEMA A RESOLVER

El Centro de Bachillerato Tecnológico, Industrial y de Servicios #133 se enfrenta a diversos retos en cuanto a la seguridad de la información, dado el creciente uso de la tecnología y la digitalización de procesos académicos y administrativos. Como en otras instituciones educativas, el CBTIS #133 está expuesto a amenazas y vulnerabilidades que podrían afectar la integridad, confidencialidad y disponibilidad de su información sensible.

Ante esta situación, la institución carece de un plan de contingencia para gestionar la seguridad informática, lo que la vuelve vulnerable a incidentes como brechas de datos y accesos no autorizados. La ausencia de procedimientos claros para la respuesta ante incidentes y la falta de formación y concienciación del personal sobre seguridad informática agravan esta problemática.

Dado el contexto de constante evolución tecnológica y la falta de actualización en las medidas de seguridad, es importante adoptar acciones preventivas y correctivas que mitiguen estos riesgos. La necesidad de cumplir con estándares internacionales, como la norma ISO 17799, resulta fundamental para garantizar la calidad y seguridad en la gestión de la información.

De no implementarse el "Plan de Contingencia con ISO 17799 para la Gestión de Seguridad de la Información", la institución quedaría expuesta a incidentes graves que podrían comprometer sus activos críticos. Por lo tanto, la adopción de este plan es una respuesta estratégica para fortalecer la postura de seguridad informática del CBTIS #133 y salvaguardar la información clave de la institución.

1.5 OBJETIVOS

1.5.1 General

Establecer un marco integral y eficiente que asegure la confidencialidad, integridad y disponibilidad de la información en el área informática del CBTIS 133, mediante la adopción de buenas prácticas de seguridad de la información según la norma ISO/IEC 17799, garantizando así la continuidad operativa y minimizar el impacto de eventos adversos logrando la protección de los activos de información.

1.5.2 Específicos

- Identificar las amenazas potenciales y evaluar su impacto en el área informática del CBTIS #133, para garantizar la protección de los sistemas y datos sensibles.
- Establecer una serie de pasos específicos a seguir en caso de un incidente, incluyendo la notificación de personas clave, la activación de equipos de respuesta y la implementación de medidas de seguridad, con el fin de asegurar una reacción rápida y eficaz.
- Desarrollar políticas de respaldo de datos críticos y garantizar la ubicación segura de estos respaldos, basadas en los lineamientos de la ISO/IEC 17799, para proteger la información ante posibles incidentes.
- Definir estrategias de recuperación de sistemas y datos, que permitan restaurar la operatividad después de un incidente, asegurando la continuidad de los servicios informáticos.
- Establecer protocolos de comunicación interna y externa, que involucren a directivos, profesores y personal clave, para coordinar de manera eficiente la respuesta a un incidente.
- Asegurar que el personal esté capacitado para seguir los procedimientos de contingencia y asignar roles y responsabilidades claras durante un incidente, con el objetivo de minimizar los tiempos de respuesta y mitigación.

- Programar simulacros y pruebas regulares para evaluar la eficacia del plan de contingencia y revisar periódicamente el plan para adaptarlo a los cambios en la infraestructura y las nuevas amenazas emergentes, garantizando su vigencia y efectividad

1.6 JUSTIFICACIÓN

El interés por mejorar la seguridad de la información en el Centro de Bachillerato Tecnológico, Industrial y de Servicios #133 surge por una serie de factores clave que afectan directamente la integridad, confidencialidad y disponibilidad de los datos que son esenciales para el funcionamiento de la institución.

Uno de los motivos principales es la creciente complejidad de las amenazas a las que la institución está expuesta. Actualmente, la falta de un plan de contingencia adecuado deja al CBTIS #133 vulnerable a incidentes como accesos no autorizados o ataques informáticos más graves, lo que puede comprometer su estabilidad operativa e incluso su reputación.

Además, la ausencia de procedimientos claros para responder ante incidentes aumenta los riesgos. Sin una guía establecida, la institución corre el peligro de enfrentar filtraciones de datos, accesos indebidos o incluso robos de equipos, sin poder reaccionar de manera rápida y efectiva. Esta falta de preparación no solo alarga los tiempos de recuperación, sino que también intensifica el impacto de las posibles brechas de seguridad.

Por otro lado, la motivación surge de adoptar estándares internacionales, como la norma ISO 17799, es fundamental no solo para proteger la información, sino también para garantizar que docentes y alumnos puedan trabajar en un entorno seguro. Cumplir con estos estándares mejoraría la capacidad del CBTIS #133 para prevenir, detectar y responder a las amenazas emergentes, brindando mayor confianza a la comunidad educativa.

CAPÍTULO II: MARCO TEÓRICO

2.1 LA SEGURIDAD DE INFORMACIÓN

La seguridad es un aspecto de mayor importancia en la correcta administración informática ya que las medidas de seguridad están basadas en la definición de controles físicos, funciones, procedimientos y programas que conlleven no sólo a la protección de la integridad de los datos, sino también a la seguridad física de los equipos y de los ambientes en que éstos se encuentren. Con relación a la seguridad de la información, existen medidas para evitar la pérdida o modificación de los datos, información o software por personas no autorizadas, para lo cual se deben tomar en cuenta una serie de medidas para la identificación y contraseñas a los usuarios. (Palacios Pacheco & Quiroz Carranza, 2013)

2.2 PLAN DE CONTINGENCIA INFORMÁTICO

Un plan de contingencia es un instrumento de gestión que contiene las medidas que garanticen la continuidad del negocio protegiendo el sistema de información de los peligros que lo amenazan o recuperándolo tras un impacto. (Aguilera López, 2010)

El plan de contingencia consta de tres planes independientes:

- Plan de respaldo.

Ante una amenaza, se aplican medidas preventivas para evitar que se produzca un daño. (Aguilera López, 2010)

- Plan de emergencia.

Contempla qué medidas tomar cuando se está materializando una amenaza o cuando acaba de producirse. (Aguilera López, 2010)

- Plan de recuperación.

Indica las medidas que se aplicaran cuando se ha producido un desastre. El objetivo es evaluar el impacto y regresar lo antes posible a un estado normal de funcionamiento del sistema y de la organización. (Aguilera López, 2010)

2.3 IMPLEMENTACIÓN DE UN PLAN DE CONTINGENCIA INFORMÁTICO

Toda organización debe planear y desarrollar un Plan de Contingencia cuando todavía no es necesario, es decir, antes de que los eventos ocurran. La planificación aumenta la habilidad y capacidad de la organización para “sobrevivir” y mantener las operaciones en caso de incidentes o desastres, sirviendo como punto de partida y aportando una guía de acciones que se deben ejecutar para una adecuada respuesta en caso de emergencia. (Espinoza Asto, 2014)

2.4 ETAPAS PARA LA ELABORACIÓN DE UN PLAN DE CONTINGENCIA.

Las etapas básicas para elaborar el Plan de Contingencia informática de una organización según Espinoza Asto, son:

- Análisis y valoración de riesgo.

Se debe realizar un análisis del impacto en donde se identifican riesgos a los procesos críticos y las consecuencias que se presentan en caso de no estar en funcionamiento. (Espinoza Asto, 2014)

Así mismo, es recomendable determinar el costo que representa para la organización experimentar estos incidentes debido a que ayuda a:

- Determinar la relación costo/beneficio y tener argumentos para decidir entre aceptar la pérdida de información o invertir en implementar sistemas de contingencia. (Espinoza Asto, 2014)
- Clasificar los componentes de la plataforma tecnológica en términos de riesgo (alto, medio, bajo) e identificar aquellos que representen mayor riesgo. (Espinoza Asto, 2014)
- Cuantificar el impacto en el caso de suspensión del servicio. (Espinoza Asto, 2014)
- Determinar la información que pueda representar pérdidas considerables para la organización o que impida una adecuada toma de decisiones. (Espinoza Asto, 2014)

Este análisis de posibles riesgos permitirá identificar las fortalezas, oportunidades, debilidades y amenazas, y profundizar en las medidas que se deben tomar para gestionarlas, de manera que en caso de incidentes se pueda recuperar la operatividad en el menor tiempo posible. (Espinoza Asto, 2014)

Un plan de contingencia debe incluir una lista de los sistemas, aplicaciones y prioridades, así como la identificación de elementos informáticos tales como hardware, software base, software de aplicaciones, telecomunicaciones para que puedan ser críticos ante cualquier incidente o desastre, jerarquizándolos de acuerdo con el orden de importancia dentro de la organización. (Tamayo Arias & A., 1999).

De la misma manera deberá existir el establecimiento de requerimientos de recuperación por lo cual en esta etapa se deberá determinar qué hacer para lograr una óptima solución. Para ello se debe profundizar la definición del problema, analizar áreas o componentes problema, comunicaciones y sus flujos, formulación de medidas de seguridad necesarias dependiendo del nivel de seguridad requerido, justificación del costo de implantar las medidas de seguridad, análisis y evaluación del plan de contingencia actual, así como también determinar los recursos humanos, técnicos y económicos necesarios para desarrollar el plan, hasta definir un tiempo viable para lograr entrar en operación el dicho plan de contingencia. (Tamayo Arias & A., 1999).

Una vez finalizado el plan, se elaborará un informe final con los resultados de su ejecución. En esta etapa se debe tener presente que el plan de contingencia no busca resolver la causa del problema, sino asegurar la continuidad de las tareas críticas de la institución.

Es necesario definir y generar simulaciones que permitan poner a prueba el plan de contingencia, el personal y los recursos necesarios para su realización. Por lo que se deberá hacer una evaluación analizando si el resultado varió por un problema en el ambiente de pruebas del plan o si el plan tiene vacíos o carencias en su definición. (Tamayo Arias & A., 1999).

Es indispensable la capacitación y participación del equipo de contingencia para detectar y evidenciar posibles carencias del plan.

Con el plan aprobado y documentado, surge la necesidad de su difusión y capacitación entre las personas encargadas de llevarlo a cabo (Tamayo Arias & A., 1999).

2.5 BENEFICIOS DE UN PLAN DE CONTINGENCIA

El plan de contingencia determinará la puesta en marcha de copias de seguridad, para evitar cualquier pérdida de datos producida por una incidencia informática. El plan de contingencia debe estar listo en la fase de planificación del proyecto, mucho antes del proyecto entrar en la fase de ejecución. Este plan ayudará a planificar y coordinar las acciones adecuadas de respuesta en tiempo. Mármol García, A. J. (2019)

Los planes de recuperación ante desastres describen cómo restaurar el funcionamiento de los sistemas de información afectados por un incidente no deseado. (Areitio Bertolin, 2008)

2.6 BUENAS PRÁCTICAS DE LA ELABORACIÓN DE UN PLAN DE CONTINGENCIA BASADO EN ISO 17799-1

La Norma ISO17799-1 en el capítulo 11 “Gestión de continuidad del negocio (plan de contingencia)” añade las buenas prácticas, las cuales son:

- Proceso de gestión de la continuidad del negocio. (ISO17799-1)
- Continuidad del negocio y análisis de impactos. (ISO17799-1)
- Redacción e implantación de planes de continuidad. (ISO17799-1)
- Marco de planificación para continuidad del negocio. (ISO17799-1)
- Prueba, mantenimiento y reevaluación de planes de continuidad. (ISO17799-1)

2.7 DESARROLLO DE LOS LINEAMIENTOS

Como se establece en la Norma ISO17799-1 se deberán desarrollar los propios lineamientos en la institución con este código de prácticas. No todos los controles y lineamientos en este código de práctica pueden ser aplicables. Es más, se pueden requerir controles y lineamientos adicionales no incluidos en este estándar. Cuando los documentos son desarrollados conteniendo lineamientos o controles adicionales, cuando sea aplicable podría ser útil incluir referencias cruzadas con las cláusulas en este estándar para facilitar el chequeo de conformidad realizado por los auditores y socios comerciales. (ISO17799-1)

2.8 EVALUACIÓN DE LOS RIESGOS DE LA SEGURIDAD

Así mismo, la Norma ISO17799-1 en la cláusula 4.1 “Evaluando los riesgos de la seguridad” describe los requerimientos de seguridad se identifican mediante una evaluación metódica de los riesgos de seguridad. El gasto en controles debiera ser equilibrado con el daño comercial probable resultado de fallas en la seguridad. Los resultados de la evaluación del riesgo ayudarán a guiar y determinar la acción de gestión apropiada y las prioridades para manejar los riesgos de seguridad de la información, e implementar los controles seleccionados para protegerse contra esos riesgos. La evaluación del riesgo se debiera repetir periódicamente para tratar cualquier cambio que podría influir en los resultados de la evaluación del riesgo. (ISO17799-1)

2.9 ANÁLISIS RIESGO

Bertolin define el análisis de riesgo como una parte clave de la gestión consistente en identificar los peligros que afectan la seguridad, identificar las áreas que necesitan salvaguardas. Es por ello, que es importante aplicar un análisis de riesgos ya que es una técnica que permite:

- Identificar los activos y controles de seguridad. (Areitio Bertolin, 2008)
- Gestionar las alertas de los riesgos próximos. (Areitio Bertolin, 2008)
- Proporcionar una guía de cara a los gastos de recursos. (Areitio Bertolin, 2008)
- Relacionar el programa de control con la misión de la organización. (Areitio Bertolin, 2008)
- Proporcionar criterios para diseñar y evaluar planes de contingencia. (Areitio Bertolin, 2008)
- Mejorar la conciencia global sobre la seguridad. (Areitio Bertolin, 2008)

En esta figura se muestra un mapa en el cual se dividen los submodelos del análisis y gestión de riesgos de seguridad, con el objetivo de gestionar la seguridad de información.

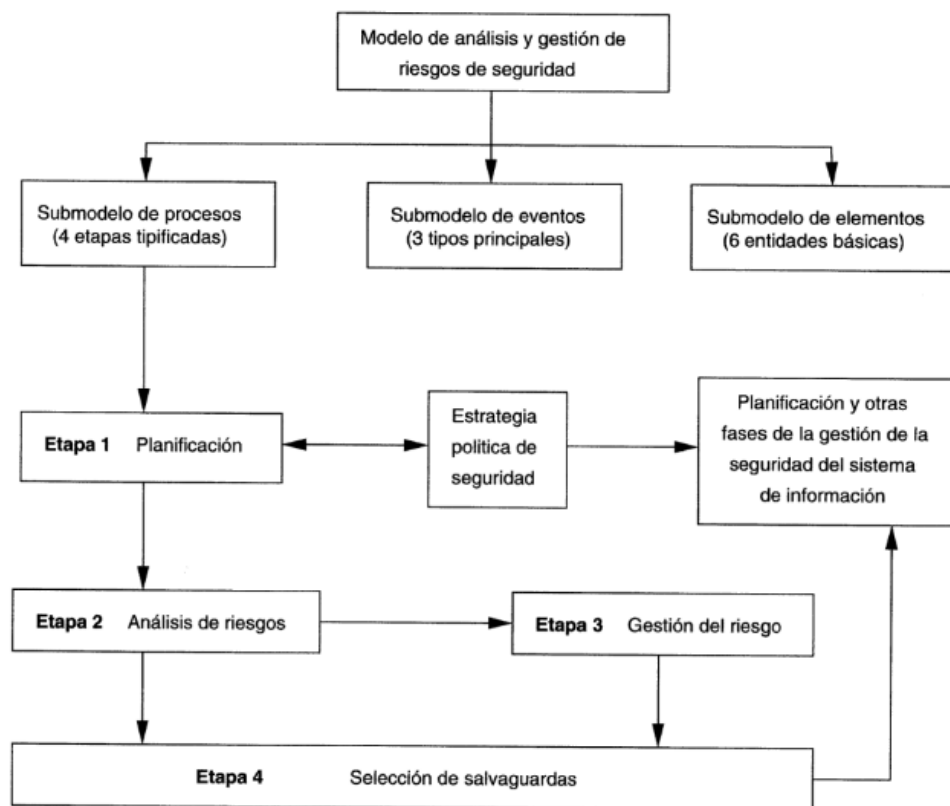


Figura 2. Proceso de análisis y gestión de riesgos de la seguridad de la información.

Fuente: Seguridad de la información. Redes, informática y sistemas de información. por Areditio Bertolín, J. (2008). Ediciones Paraninfo, SA.

2.10 DEFINICIÓN DE AMENAZA

La norma UNE-ISO/IEC 27000 dice que una amenaza es una causa potencial de un incidente no-deseado, el cual puede resultar en daño a un sistema u organización. (UNE-ISO/IEC 27000, 2014)

2.11 DEFINICIÓN DE VIRUS Y MALWARE

Ciccariello describe a un virus informático como un programa con un código malicioso que infecta la computadora con el objetivo de alterar el correcto funcionamiento de un equipo, cosa que logra contagiando los archivos mediante un código maligno. Se caracteriza porque necesita de la intervención del usuario para ser ejecutado; luego, hace copias de sí mismo y, de esta forma, se propaga a través de la red, el correo electrónico, los pendrives y todo elemento que pueda contener o enviar código. El objetivo principal de un virus es afectar una computadora y su rendimiento, destruir archivos y tomar el control a nivel remoto del equipo. (Ciccariello, 2022)

Por otro lado, el malware es un programa que ejecuta comandos con diferentes propósitos malintencionados, como invadir un sistema, eliminar información, robar contraseñas y tomar el control de servicios vitales del sistema. (Ciccariello, 2022)

2.12 DEFINICIÓN DE VULNERABILIDAD

Conforme a la norma UNE-ISO/IEC 27000, una vulnerabilidad es la debilidad de un activo o grupo de activos que puede ser explotada por una o más amenazas. (UNE-ISO/IEC 27000, 2014),

2.13 DEFINICIÓN DE INCIDENTE DE SEGURIDAD

Haciendo referencia a la norma UNE-ISO/IEC 27000 Un incidente de seguridad de la información es indicado por un solo evento o una serie de eventos inesperados de seguridad de la información que tienen una probabilidad significativa de comprometer las operaciones comerciales y amenazar la seguridad de la información. (UNE-ISO/IEC 27000, 2014)

2.14 DEFINICIÓN DE EVENTO DE SEGURIDAD DE LA INFORMACIÓN

Se plantea en la norma UNE-ISO/IEC 27000 que cualquier evento de seguridad de la información es una ocurrencia identificada del estado de un sistema, servicio o red indicando una posible falla en la política de seguridad de la información o falla en las salvaguardas, o una situación desconocida que puede ser relevante para la seguridad. (UNE-ISO/IEC 27000, 2014)

2.15 LA SEGURIDAD DE LA INFORMACIÓN

Se considera en ISO 17799 la preservación de confidencialidad, integración y disponibilidad de la información; además también puede involucrar otras propiedades como autenticidad, responsabilidad no-repudiación y confiabilidad. (ISO 17799)

2.16 MATRIZ DE RIESGOS

Una matriz es un proceso sistemático y analítico para evaluar, gestionar y comunicar los riesgos para mitigarlos o eliminarlos, si es posible. Se realiza para entender la naturaleza de las consecuencias negativas de las amenazas. (Naveiro Flores & David, 2022)

Así mismo, una matriz de riesgo es una herramienta de análisis de riesgos que sirve para evaluar la probabilidad y la gravedad del riesgo durante el proceso de planificación del proyecto. (Team de Asana, 2024)

Una vez que se haya evaluado la probabilidad y la gravedad de cada riesgo, se puede ubicar en la matriz para calcular la calificación del impacto de cada riesgo. (Team de Asana, 2024)

Estas calificaciones ayudarán a determinar que prioridad asignar a los riesgos del proyecto y a gestionarlos de manera efectiva. (Team de Asana, 2024)

2.17 CLASIFICACIÓN DE UNA MATRIZ DE RIESGOS

Una matriz de riesgos se clasifica como:

- Evaluación de riesgos.

Se centra en la obtención de información sobre la verosimilitud y los impactos asociados a las amenazas que potencialmente afectan a un sistema, cuando se materialicen. (Team de Asana, 2024)

- Gestión de riesgos.

Comprende las actividades realizadas para controlar las amenazas, en el sentido de reducir la probabilidad de que se materialicen y/o reducir su impacto, en caso de que lo hagan. (Team de Asana, 2024)

- Comunicación de riesgos.

Se refiere al intercambio de opiniones e información relativa a los riesgos y a sus factores asociados, entre los evaluadores, los gestores y cualquier otra parte involucrada en el problema. (Team de Asana, 2024)

En la Figura 3 se muestra un proceso de la elaboración de una matriz de riesgo que parte de la identificación de riesgos y culmina en la aceptación o rechazo del riesgo residual de una matriz.

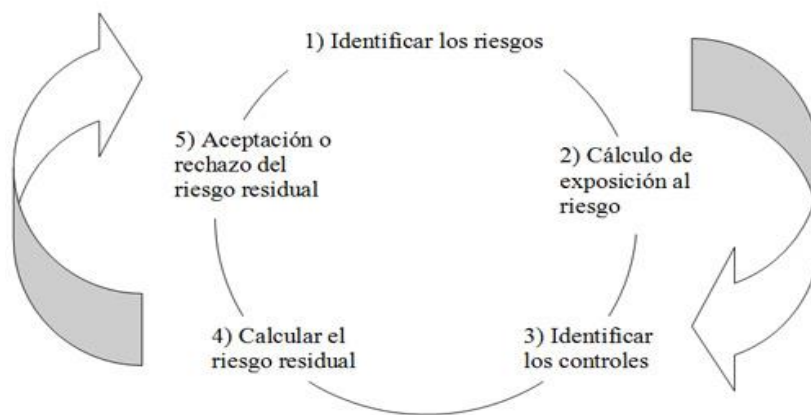


Figura 3. Proceso de Administración del Riesgo. Fuente: Proceso de Administración del Riesgo, por Salvador Zamora, 2009.

2.18 CONTROL DE ACCESO

Aguilera define el control de acceso como un espacio donde se encuentra el sistema de información (locales y edificios), los cuales tienen mecanismos de seguridad física. Los dispositivos-tipos, categorías o número-que se utilicen para controlar la entrada de personas a un edificio o a algunas de sus áreas dependerán del nivel de seguridad que requiera un sistema de información y de la cuantificación del impacto de una amenaza sobre sus activos. (Aguilera López, 2010)

2.19 TIPOS DE CONTROLES DE ACCESO

Existe una variedad de tipos de control de acceso, tal como lo menciona Enrique en el cual consiste en establecer contraseñas seguras, autenticación de dos factores y solicitar permisos de acceso según el rol de la persona. (Enrique, 2023)

De acuerdo con las practicas recomendadas y las obligaciones organizativas o normativas, como las establecidas por la NIST e ISO 27000, es necesario implementar

metodologías de control, como la profundidad en defensa. Además, es importante evaluar y utilizar indicadores de cumplimiento para gestionar la seguridad física de las infraestructuras tecnológicas. (ISO 27000)

A continuación, se detalla la importancia de los indicadores de cumplimiento desde el punto de vista de la ISO 27000:

- Evaluación de la conformidad.

Los indicadores de cumplimiento permiten evaluar si las medidas de seguridad física implementadas cumplen con los estándares y requisitos establecidos por ISO 27000. Esto ayuda a identificar posibles brechas o deficiencias en la protección de la infraestructura física y tomar las medidas correctivas necesarias. (ISO 27000)

- Verificación del grado de protección.

Los indicadores de cumplimiento permiten verificar el grado de protección de la infraestructura tecnológica. Esto ayuda a identificar posibles brechas o deficiencias en la protección de la infraestructura física y tomar medidas correctivas necesarias. (ISO 27000)

- Monitoreo continuo.

Esto permite detectar cualquier cambio o desviación en tiempo real y tomar medidas preventivas o correctivas de manera oportuna. (ISO 27000)

- Identificación de áreas de mejora.

Analizar los indicadores, se pueden identificar patrones, tendencias o áreas problemáticas específicas que requieran atención adicional y mejoras en los controles de seguridad física. (ISO 27000)

- Cumplimiento normativo.

Estos indicadores demostraron evidencia objetiva de que se han implementado las medidas de seguridad física necesarias para proteger la infraestructura tecnológica. (ISO 27000)

- Toma de decisiones informada.

Proporciona información clave para la toma de decisiones informada en la gestión de la seguridad física. Al tener datos cuantitativos y cualitativos sobre el cumplimiento de los estándares y requisitos, se pueden tomar decisiones basadas en evidencia para mejorar la seguridad física de las infraestructuras tecnológicas. (ISO 27000)

2.20 PÉRDIDA DE DATOS

Una pérdida de datos es aquella situación en la que no se puede acceder a datos importantes almacenados en un sistema informático. Esta situación se puede producir por cualquier causa, tanto una avería, un error humano, un borrado accidental o provocado, desastres naturales, incendios, golpes, reparar disco duro, etc. Las pérdidas de datos tienen un origen, sin embargo, el más frecuente es el de averías físicas, seguido del error humano. (Recovery Labs, 2024)

2.21 IMPORTANCIA DE RECUPERACIÓN DE DATOS

La recuperación de datos es una forma de proteger la información personal o laboral de los usuarios almacenada en dispositivos, evitando la pérdida de datos cuando falla algún dispositivo. De igual manera es importante tener una estrategia adecuada de copia de seguridad y restauración, así la información personal y laboral de un usuario puede recuperarse rápidamente, lo que favorece la continuidad del trabajo y aumenta la productividad. (Buenning, 2024)

2.22 DEFINICIÓN DE UN RESPALDO INFORMATICO

Un respaldo de información es la copia de los datos importantes de un dispositivo primario en uno o en varios dispositivos secundarios para que en caso de que el primer dispositivo sufra una vería electromecánica o un error en su estructura lógica, sea posible contar con la mayor parte de la información necesaria para continuar con las actividades rutinarias y evitar perdida generalizada de datos. (Multicomp Soluciones de seguridad en TI, 2019)

2.23 IMPORTANCIA DEL RESPALDO DE DATOS

La importancia de tener un respaldo radica en que todos los dispositivos de almacenamiento masivo de información tienen la posibilidad de fallar, por lo tanto, es necesario que se cuente con una copia de seguridad de información importante, ya que la probabilidad de que dos dispositivos fallen de manera simultánea es menos probable. (Multicomp Soluciones de seguridad en TI, 2019)

Sin embargo, en (Amazon Web Services, Inc., s.f.) se describen tres estrategias principales de copia de seguridad de datos, que detallamos a continuación.

- Copia de seguridad completa

Cuando el software de copia de seguridad realiza una copia de seguridad completa, copia todo el conjunto de datos, independientemente de si se han realizado cambios en dichos datos. Por lo general, este tipo de copia de seguridad se realiza con menos frecuencia por motivos prácticos. Por ejemplo, puede llevar mucho tiempo y también ocupar una gran cantidad de espacio de almacenamiento. Las alternativas a las copias de seguridad completas de datos incluyen las copias de seguridad diferenciales o incrementales. (Amazon Web Services, Inc., s.f.)

- Copia de seguridad incremental

Una copia de seguridad incremental solo copia los datos modificados desde la última copia de seguridad. Por ejemplo, si realizó una copia de seguridad completa el domingo, la copia de seguridad incremental del lunes solo copiará los cambios realizados desde la copia de seguridad del domingo. El martes, solo copiaría los cambios del archivo de imagen de copia de seguridad desde la copia de seguridad del lunes. (Amazon Web Services, Inc., s.f.)

- Respaldo diferencial

Una estrategia de copia de seguridad diferencial copia solo los datos recién agregados y modificados desde la última copia de seguridad completa. Si la última copia de seguridad completa se realizó el domingo, una copia de seguridad del lunes copiará todos los cambios

realizados desde el domingo. Si hubieras realizado otra copia de seguridad el martes, también copiaría todos los cambios realizados desde el domingo. El tamaño del archivo de copia de seguridad aumentaría progresivamente hasta la próxima copia de seguridad completa. (Amazon Web Services, Inc., s.f.)

CAPÍTULO III: DESARROLLO

3.1 ANÁLISIS DE RIESGO

El primer paso para la realización del plan de contingencia informático consiste en analizar el espacio donde se trabajará para identificar amenazas y vulnerabilidades dentro del plantel, esto con el objetivo de implementar los controles de seguridad como se explica en el Estándar Internacional ISO/IEC 17799, capítulo 4 “Evaluación y tratamiento del riesgo” pág. 17. Donde se relata que se deberá identificar, cuantificar y priorizar el ciclo de control de impacto de los riesgos para determinar la gestión de la seguridad de la información.

3.1.1 Identificación de Amenazas del Plantel

En esta tabla se muestra las amenazas identificadas del plantel con la finalidad de que la institución priorice los riesgos para poder mitigarlos de acuerdo con la probabilidad.

Amenazas	Posibilidad
De área	100%
Possible acceso de personas no autorizadas al laboratorio.	45%
Riesgo de robo o pérdida de equipos y datos sensibles.	45%
Vandalismo en el área informática.	10%
De software.	100%
Riesgo de infección de sistemas y dispositivos con software malicioso.	85%
Posible pérdida de datos o interrupción de servicios.	10%
Filtración de datos.	5%
De hardware.	100%
Posible riesgo de inundación.	45%
Riesgo de derrumbe en caso de terremotos y/o sismos de alto impacto.	50%
Incendios en el laboratorio de cómputo.	5%

De personal.	100%
Configuración incorrecta de sistemas y dispositivos.	95%
Eliminación de datos importantes.	5%

Tabla 1 Identificación de Amenazas del Plantel. Fuente: propia.

3.1.2 Identificación de Vulnerabilidades en el Plantel

En esta tabla se muestran las vulnerabilidades clasificadas de software, hardware con la finalidad de organizar, priorizar y calificar las vulnerabilidades y el nivel de probabilidad de que estas ocurran.

Vulnerabilidades	Posibilidad
De software.	100%
Falta de actualizaciones de Software.	85%
Sistemas infectados y propagación de virus por medio de phishing.	15%
De hardware.	100%
Daño de equipos de cómputo.	35%
Posibles descargas eléctricas.	50%
Fallo de cableado.	15%
De personal.	100%
Mal control de activos.	35%
Nulo establecimiento de políticas de seguridad.	50%
Probable daño en las instalaciones debido a la mala adaptación del laboratorio.	15%

Tabla 2 Identificación de Vulnerabilidades del Plantel. Fuente: propia.

3.2 TABLA DE EVALUACIÓN DE RIESGOS

En segundo lugar, se evaluarán los riesgos que ponen en juego la seguridad de la institución, por lo cual se medirá la probabilidad (alta, media o baja) de cada riesgo identificado. Esto nos sirve para poder priorizar cada una de las amenazas anteriormente evaluadas.

Tipo de incidente	Incidente	Posibilidad
De software:	Código malicioso en los equipos de cómputo.	Alta.
	Posible pérdida de datos.	Baja.
	Software desactualizado.	Alto.
	Filtración de datos.	Baja.
	Phishing.	Medio.
De hardware:	Daño en los monitores del área informática.	Medio.
	Posibles descargas eléctricas.	Medio.
	Derrame de líquidos.	Medio.
	Daño en los puertos del equipo de cómputo.	Medio.
	Fallo en el cableado.	Medio.
Del área:	Accesos no autorizados.	Medio.
	Robo de equipos.	Medio.
	Vandalismo en el área informática.	Medio.
	Incendios.	Bajo.
	Inundaciones.	Medio.
	Terremotos/sismos.	Medio.
Del personal:	Mala configuración de las instalaciones.	Alta.
	Eliminación de aplicaciones accidentalmente.	Alta.
	Mal control de activos	Medio.
	Nulo establecimiento de políticas de seguridad.	Medio.
	Contraseñas mal administradas.	Medio.

Tabla 3 Tabla de Evaluación de Riesgos. Fuente: propia.

3.3 MATRIZ DE RIESGO

En tercer lugar, se desarrollará una matriz de riesgo la cual permite determinar los riesgos relevantes para la seguridad de la institución, basado en el anterior análisis de riesgo que donde se analizó los diferentes tipos de riesgo, vulnerabilidades y amenazas que ponen en prueba la seguridad e integridad física y lógica del laboratorio del Centro de Bachillerato Tecnológico, Industrial y de Servicios #133.

	Insignificante	Menor	Moderado	Mayor	Catastrófico
Casi seguro			-Accesos no autorizados.	-Software desactualizado.	-Código malicioso.
Muy probable		-Inundaciones.	-Fallo en el cableado.	-Robo de equipos.	-Mala configuración de las instalaciones. -Eliminación de aplicaciones.
Possible			-Terremoto/sismos. -Daño en los puertos.	-Inundaciones. -Descargas eléctricas.	-Nulo establecimiento de políticas de seguridad.
Poco probable		- Incendios. -Filtración de datos.	-Phishing.	-Vandalismo -Derrame de líquidos. .	-Mal control de activos.
Raro		-Pérdida de datos.	-Contraseñas mal administradas.	-Daño en los monitores.	

Tabla 4 Matriz de Riesgo. Fuente: propia.

3.4 MEDIDAS PREVENTIVAS DE CONTROL DE SEGURIDAD

Con base en la evaluación de riesgos, se pueden definir medidas de control para mitigar los riesgos identificados. Por ejemplo:

- Implementación de seguridad física en el área informática, con el objetivo de evitar el acceso físico no autorizado, daño e interferencia con equipos de cómputo.
- Uso de software antivirus y firewall para proteger los sistemas contra malware y virus.
- Proporcionar medios de respaldos para hacer una copia de seguridad periódica de la información para mitigar el riesgo de pérdida de datos por fallos en la infraestructura o

errores humanos. Esto se tendrá que almacenar en un lugar apartado, a la distancia de cualquier daño.

- Establecimiento de políticas de seguridad para promover buenas prácticas de seguridad y responder de manera efectiva ante incidentes y mantenimiento de la información en toda la institución.
- Prevenir el área informática de incendios, utilizando extinguidores y señales de evacuación para evitar perdida en los activos y la interrupción de las actividades en la institución. Se deberá monitorear y documentar periódicamente las condiciones ambientales para un mayor control de seguridad en el área.

A continuación, se desarrolló un formato para documentar de manera eficaz las inspecciones del área en caso de algún desastre natural.

Nombre del evaluador Técnico:			
Profesión:			
Fecha:	No. Ticket:		
1. Ubicación del edificio:			
Dirección:			
Colonia:			
CP:	Referencias:		
Coordenadas geográficas:			
Personal contactado:	Teléfono:		
Uso del inmueble:			
Casa	Departamentos	Educación	Industrias
Oficinas	Comercios	Bodegas	Centro de reunión
Otro:			
Numero de edificios:			
Número de salones:			

Numero de personal:		
Tipo de inspección:	Exterior	Interior
	Ambas	
Estado de la edificación:	Sí	No
a. Derrumbe total		
b. Derrumbe parcial		
c. Edificación separada de su cimentación		
d. Asentamiento diferencial o hundimiento		
e. Inclinación notoria		
f. Daños a elementos estructurales		
g. Daños en elementos no estructurales		
h. Daños en instalaciones eléctricas		

Tabla 5 Medidas Preventivas de Control de Seguridad. Fuente: propia.

3.5 PLAN DE CONTINGENCIA

De acuerdo con el Estándar Internacional ISO/IEC 17799, capítulo 14.1.4 “Marco Referencial de la planeación de la continuidad del negocio” pág. 149. Hace referencia a que cada plan deberá especificar el plan de intensificación y las condiciones para la activación.

En este caso, se han priorizado las amenazas para la activación del plan de contingencia en caso de una emergencia por alguna incidencia presentada.

3.5.1 Amenazas Físicas

Caso 1. Robo de Equipos.

Una de las amenazas físicas más alarmantes es el robo de los activos, por lo cual es importante seguir un plan de acción establecido para minimizar las pérdidas y recuperar la

situación lo antes posible. A continuación, se describirán los pasos que se deberá seguir como respuesta a la amenaza presentada.

- Llamar a las autoridades: Se deberá notificar a las autoridades locales para que inicien una investigación sobre el robo y ayuden a recuperar los equipos robados.
- Asegurar el área: Asegurar el área afectada para preservar cualquier evidencia que pueda ser útil para la investigación policial. Evitar manipular o alterar cualquier elemento que pueda ayudar a identificar al ladrón o a recuperar los equipos robados.
- Evaluar el alcance del robo: Realizar un inventario detallado de los equipos y dispositivos robados para determinar el alcance total de las pérdidas.
- Notificar a la administración y al personal: Informar a la administración y al personal del laboratorio sobre el robo y proporcionar detalles sobre los equipos robados.
- Revisar las medidas de seguridad: Evaluar las medidas de seguridad existentes en el laboratorio y determinar si se requieren mejoras o ajustes para evitar futuros robos.
- Registrar el incidente: Mantener un registro detallado del incidente, incluyendo la fecha, hora, descripción de los equipos robados y cualquier otra información relevante.

3.5.2 Amenazas Lógicas

Caso 1. Software Desactualizado.

- Identificación de la vulnerabilidad: Se realizará un análisis de evaluación para determinar el alcance de vulnerabilidad del software desactualizado.
- Evaluación del impacto: Se determinará el impacto de la vulnerabilidad en la seguridad y operación.
- Priorización de acciones: Establecer prioridad para abordar la vulnerabilidad.
- Actualización del software: Actualizar el software desactualizado para corregir la vulnerabilidad. Acciones correctivas: instalar parches de seguridad o actualizar a versiones más recientes que incluyan las correcciones necesarias.
- Implementación de medidas temporales: Se realizará la configuración de firewalls o la desactivación de funciones vulnerables.

- Monitorización y seguimiento: Se tendrá que dar seguimiento a los registros de seguridad y realización de pruebas de seguridad adicionales.
- Planificación de medidas preventivas: Planificar y elaborar medidas preventivas a largo plazo para evitar futuras vulnerabilidades similares con ello se podrá incluir políticas de gestión de parches, implementación de sistemas de detección de vulnerabilidades.

Caso 2. Pérdida de Datos.

- Evaluación de la situación: Se realizará un análisis de la situación, implicando qué datos se han perdido, cuál es su importancia y cuánto tiempo ha transcurrido desde la pérdida.
- Notificación de la pérdida de datos: Informar de inmediato a los responsables del laboratorio y a las autoridades pertinentes sobre la pérdida de datos.
- Recuperación de datos: Recuperar los datos perdidos utilizando copias de seguridad, si están disponibles.
- Investigación de la causa: Determinar la causa raíz de la pérdida de datos para prevenir incidentes similares en el futuro.
- Comunicación con los afectados: Informar a las personas afectadas por la pérdida de datos, como usuarios o empleados, sobre lo ocurrido y las medidas que se están tomando para mitigar el impacto.
- Implementación de medidas correctivas: Tomar medidas correctivas para evitar futuras pérdidas de datos.
- Evaluación del impacto: Realizar una evaluación sobre el impacto de la pérdida de datos en el laboratorio. Determinando qué valor, disponibilidad y sensibilidad tenía la información perdida.

Caso 3. Ataques Cibernéticos.

- Identificación y desconexión de los equipos infectados: Identificar equipos infectados y aislarlos de la red para evitar la propagación del virus a otros sistemas. Es decir, si los equipos comparten una red de datos se tendrán que desconectar los equipos de la red y desactivar cualquier conexión inalámbrica.

- Contención: Detener la actividad maliciosa del virus y evitar que cause más daño en los equipos infectados.
- Escaneo y limpieza: Realizar un escaneo exhaustivo en busca de virus en todos los equipos del laboratorio utilizando herramientas de seguridad actualizadas. Eliminar cualquier amenaza detectada y restaurar los archivos afectados desde copias de seguridad limpias.
- Actualización de seguridad: Aplicar parches de seguridad y actualizaciones de software en todos los equipos para cerrar las vulnerabilidades.
- Recuperación de datos: Restaurar los datos perdidos o dañados debido al ataque de virus utilizando copias de seguridad recientes.

3.6 PLAN DE RECUPERACIÓN

Conforme al Estándar Internacional ISO/IEC 17799 capítulo 14.1.3 “Desarrollar e implementar los planes de continuidad incluyendo la seguridad de la información” pág. 147 describe el proceso de planeación de continuidad para restaurar las operaciones y asegurar la disponibilidad de la información. Tales como:

3.6.1 Detección y Notificación

- Implementación de sistemas de detección de intrusiones y monitoreo de seguridad en los sistemas del laboratorio.
- Establecimiento de alertas automáticas para detectar posibles incidentes de seguridad, como anomalías en el tráfico de red o comportamientos sospechosos.
- Notificación inmediata a los responsables del área en caso de detección de una incidencia.

3.6.2 Preparación

- Designación de un equipo de respuesta a incidentes compuesto por personal técnico y de seguridad de la información.
- Desarrollo de un registro de contactos de emergencia que incluya a proveedores de servicios, autoridades de la institución y otros contactos clave.
- Creación de un inventario detallado de los activos en estado crítico, incluyendo sistemas, datos y aplicaciones.

3.6.3 Evaluación y Respuesta

- Análisis detallado de la incidencia para determinar su origen, el alcance de la afectación y las acciones requeridas para mitigarla.
- Recopilación de evidencia para facilitar la investigación y el análisis posterior del incidente.

3.6.4 Recuperación y Restauración

- Restauración de los sistemas afectados utilizando copias de seguridad.
- Implementación de parches de seguridad y actualizaciones de software para corregir las vulnerabilidades explotadas por la incidencia.

3.6.5 Comunicación y Coordinación

- Comunicación regular con el personal del laboratorio, los responsables del área y otras partes interesadas sobre el progreso de la recuperación.
- Coordinación con proveedores de servicios externos y autoridades pertinentes para garantizar una respuesta efectiva y coordinada.

3.6.6 Evaluación Post-Incidente

- Análisis detallado del incidente para identificar las causas y las lecciones aprendidas.
- Evaluación de los procedimientos de respuesta a incidentes.
- Implementación de medidas correctivas y preventivas.

En esta figura se muestran de manera resumida los pasos del seguimiento de un incidente presentado con la finalidad de que se cumpla el proceso y documentación adecuada para llevar un orden del seguimiento.



Figura 4. Elaboración de documentación. Fuente: propia.

3.7 PLAN DE CONTINUIDAD DE PRUEBAS

Con base al Estándar Internacional ISO /IEC 17799, capítulo 14.1.5 “Prueba, mantenimiento y reevaluación de los planes de continuidad del negocio” pág. 150, menciona que el programa de continuidad deberá indicar cómo, cuándo se deberá probar cada elemento con regularidad.

3.7.1 Pruebas por Realizar

- De funcionalidad: Verificar que todas las funciones y características de los sistemas y aplicaciones funcionen según lo previsto.
- De rendimiento: Evaluar el rendimiento de los sistemas y aplicaciones bajo diferentes cargas de trabajo y condiciones de uso.
- De seguridad: Validar la efectividad de los controles de seguridad implementados para proteger los sistemas y datos del laboratorio contra posibles amenazas y ataques.
- De recuperación anti-desastres: Evaluar la capacidad de los sistemas y aplicaciones para recuperarse de fallos y desastres, incluyendo la restauración de datos desde copias de seguridad.

Planificación de las Pruebas

- Identificar escenarios de uso y situaciones de prueba que cubran todos los aspectos críticos de los sistemas y aplicaciones.
- Designar un equipo de pruebas responsable de ejecutar las pruebas y recopilar los resultados.
- Establecer un calendario de pruebas que incluya fechas de inicio y finalización, así como los recursos necesarios para llevar a cabo las pruebas.
- Configurar un entorno de pruebas separado y aislado del entorno de producción para realizar pruebas sin afectar la operación normal del laboratorio.

Ejecución de Pruebas

- Realizar pruebas siguiendo los casos de prueba definidos y documentando los resultados obtenidos.
- Supervisar el progreso de las pruebas y resolver cualquier problema o inconveniente que pueda surgir durante la ejecución.
- Registrar detalladamente los resultados de las pruebas, incluyendo cualquier anomalía o hallazgo relevante observado durante las pruebas.

Análisis de los Resultados

- Analizar los resultados de las pruebas para identificar áreas de mejora y posibles problemas que requieran atención.
- Establecer prioridades para abordar los problemas identificados y definir un plan de acción para resolverlos.
- Elaborar un informe detallado que resuma los resultados de las pruebas, las conclusiones obtenidas y las recomendaciones para mejorar la calidad y seguridad del laboratorio de computación.

Seguimiento y Mejora Continua.

- Tomar medidas para abordar los problemas identificados durante las pruebas y mejorar la calidad y seguridad del laboratorio.
- Realizar revisiones periódicas del plan de pruebas y actualizarlo según sea necesario para adaptarse a cambios en los sistemas, aplicaciones o requisitos del laboratorio.
- Proporcionar capacitación al personal del laboratorio sobre la ejecución de pruebas y la interpretación de resultados para fomentar una cultura de calidad y seguridad en el laboratorio.

3.7.2 Capacitación al Personal

Con el fin de tener un buen funcionamiento sobre el plan de contingencia, se deberá adoptar nuevas costumbres para realizar constantes capacitaciones al personal de la institución, esto con la finalidad de asegurar la continuidad de las medidas de seguridad implantadas y desarrolladas para un buen funcionamiento del área.

Los procesos de capacitación se abordarán a través de juntas donde se expondrán los documentos que se abordan a lo largo del documento, logrando así una continuidad alrededor de seis meses cada año para poder actualizarse constantemente debido a nuevas amenazas que pudiesen presentarse.

Los temas por ver deberán ser los siguientes:

- Importancia del plan de contingencia.
- Elementos del plan de contingencia.
- Asignación de roles.
- Ejemplos de incidencias.
- Planes de pruebas realizadas.
- Ejecución del plan de contingencia.
- Actualización del plan de contingencia.

3.8 POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN BASADO EN LA ISO 17799

Con el objetivo de establecer y mantener un sistema de gestión de seguridad de la información para proteger los recursos del laboratorio, se realizaron políticas de seguridad basadas en el Estándar Internacional ISO / IEC 17799 capítulo 5 “Política de seguridad”, pág. 19.

3.8.1 De Hardware

1. El docente encargado se dará a la tarea de realizar la asignación de equipos de cómputo a cada uno de los alumnos del grupo en curso. El uso de los medios electrónicos será únicamente utilizado por el alumno que se encuentre en el laboratorio y cumpliendo su hora de clase. En ningún momento podrán acceder alumnos no correspondientes a la clase y hacer uso de las maquinas.
2. El alumnado y el docente deberán comprometerse a cuidar y hacer buen uso de los laboratorios y equipos de cómputo dentro de las horas que tengan asignadas en su materia; manteniendo dicho elemento en su lugar correspondiente. No deberán mover o quitar los elementos (teclado, ratón, gabinete, etc.) que componen el ordenador. En caso de que algún componente falte, se deberá notificar de inmediato al profesor el cual dará aviso al personal encargado de los laboratorios para que haga una revisión de los grupos ingresados anteriormente. En el caso de que no se halle el elemento faltante, se tomará en cuenta una sanción al profesor asignado de laboratorio.
3. La instalación desde el ensamblado y conexión de los elementos. Así también como la configuración del equipo de cómputo será realizada únicamente por el encargado del laboratorio, contando con ayuda de personas capacitadas y supervisadas por el mismo. Ninguna persona terciaria y sin conocimiento previo hará manipulación de dichos componentes.
4. El mantenimiento y limpieza de los equipos de cómputos será realizado por medio de los encargados de los laboratorios contando con las medidas de precaución y artículos correspondientes (brochas, aire comprimido, paños de microfibra, etc.) a cada componente de la computadora. No se permite que personal del área de limpieza realice alguna actividad a los equipos de cómputo, únicamente pisos y mesas para limpiar.

5. Queda prohibido el consumo de alimentos y bebidas en los laboratorios. Por lo cual, los alumnos y docentes no deberán ingresar con comida o bebidas. Se podrá colocar un área en donde los alumnos podrán dejar sus mochilas y bebidas antes de ingresar al laboratorio para evitar derrames de líquidos y residuos de comida sobre el hardware.
6. Por medio del encargado de laboratorios se llevará a cabo un sistema de registro donde se enumerarán los equipos y se colocarán un estampado con dicho número. Tal registro se plasmará dentro de una bitácora en donde se coloca el nombre, marca y numero asignado del elemento para llevar el seguimiento de los equipos utilizados en el área y evitar robos o extravíos de los equipos.

3.8.2 De Software

7. Toda adquisición de Licencia de software será revisada por los encargados de laboratorios para la aprobación de la instalación en los equipos de cómputo. Por lo que se prohíbe a los alumnos descargar e instalar algún tipo de software comercial, shareware o freeware que ponga en riesgo la seguridad de los archivos o infecte la máquina con virus.
8. Los encargados de laboratorios deberán de instalar y llevar a cabo las actualizaciones correspondientes de los antivirus y sistema operativo de las maquinas. Esto para proteger el sistema y garantizar un rendimiento optimo en el uso del sistema.
9. El alumnado deberá hacer uso adecuado del software únicamente de las tareas asignadas en su hora de clase. No deberá descargar o ejecutar programas / sitios web para su uso personal.
10. El encargado de laboratorio deberá realizar copias de seguridad y recuperación de datos periódicamente para evitar pérdidas de datos debido a fallas en el software o errores del personal. Así como también limpieza de los equipos (congelamiento de sistema operativo) para evitar que estas se saturen.
11. Para registro de alumnos en plataformas como Teams, el área de TI deberá ser los únicos en manipular el sistema. Por lo que queda estrictamente prohibido la filtración de personas ajenas en el sistema para una mayor seguridad y confidencialidad en los datos de los alumnos y docentes.

12. Para acceder al sistema se deberá realizar por medio de autenticación en la que pedirá matrícula y contraseña para la identificación de los alumnos y docentes que accedan para ver o modificar (en caso de ser profesores) las calificaciones que se suban al sistema.

3.8.3 De Seguridad Física

13. Para mayor seguridad de los equipos de cómputos se deberá contar con una bitácora con fecha, nombre o matrícula, número de la computadora que usa, hora de entrada y salida ante el acceso del alumnado. Así como también el profesor tendrá que firmar y colocar su nombre para comprometerse que será el encargado en sus horas asignadas y cualquier daño o robo será canalizado por medio del profesor y la bitácora existente de los alumnos.
14. Se asignarán áreas para guardar información confidencial (documentos, archivos, medios de almacenamiento, etc.) así como también componentes o refacciones de los equipos de cómputo deberán ser resguardados y monitoreados, utilizando sistemas de detección de intrusos o alarmas en todo momento. Así como también el acceso será únicamente al personal autorizado.
15. En caso de visitantes, el acceso a las instalaciones deberá ser supervisado y acompañado en todo momento. Así como también se tendrá que contar con una identificación oficial de la persona externa en las instalaciones.
16. Los materiales peligrosos como combustibles o residuos tóxicos que hagan daño tanto al personal como a los equipos o documentación física se deberán resguardar a una distancia considerada para prevenir daños a las instalaciones o a la salud del personal. Se recomienda un área restringida en donde no haya demasiada circulación de personas, es decir, a fuera de las instalaciones o cualquier edificio cerca.
17. En caso del cableado se deberá proteger utilizando tubos y materiales aislantes para evitar algún corto o daño en las instalaciones. Así como también se deberán de clasificar las instalaciones de cable las cuales deben de cumplir las normativas y los estándares, es la única forma de asegurar que sobre ellas se podrán comunicar los sistemas con la velocidad, seguridad y disponibilidad deseada. La red de cableado está formada por cableado horizontal que es el que va del puesto de trabajo hasta el rack de

telecomunicaciones y de cableado vertical que es el que proporciona interconexiones entre cuartos o armarios de telecomunicaciones. Una distancia de punto de cable no deberá superar los 90 metros y se podrán utilizar cables de UTP o fibra óptica según el presupuesto de la institución. Es recomendado que este cableado sea realizado por medio de una empresa certificada en redes para poder asegurar la calidad y requerimientos del cableado y evitar daños a equipos de cómputo.

18. En caso de que un equipo de cómputo o documento oficial tenga que salir de las instalaciones, se deberá notificar al encargado de laboratorio para llevar un registro en el cual se anotará el nombre, modelo, marca y número asignado. Si es para reparación se anotará el daño y lugar donde se mandó a arreglar. En caso de que sea a fines de documentación por medio de otro empleado se tendrán que tomar los datos del profesor como nombre, firma que es el responsable y que deberá regresar el equipo sin daños.

3.8.4 De Servicios

19. El acceso a Internet en las instalaciones escolares se limitará exclusivamente a actividades y tareas institucionales. Esto significa que tanto docentes como alumnos solo podrán utilizar Internet para propósitos relacionados con la educación y el trabajo escolar. Para garantizar el uso adecuado del servicio, se llevará a cabo un monitoreo y análisis del tráfico de datos de la red. Esto permitirá detectar cualquier uso inapropiado de Internet dentro de las instalaciones.
20. El encargado del laboratorio de computación o de TI deberá restringir el acceso a sitios web que no sean necesarios para las actividades académicas de la institución. Esto incluye redes sociales u otros sitios web que puedan poner en riesgo la seguridad y la privacidad de la institución al permitir la divulgación de información confidencial. El objetivo es garantizar que los recursos de Internet se utilicen de manera responsable y segura.
21. Tanto los alumnos como los docentes deberán contar con una cuenta de correo electrónico institucional. Esta cuenta será utilizada para comunicarse y llevar a cabo actividades relacionadas con las materias y la institución. El área de Tecnologías de la Información será responsable de proporcionar este servicio y asegurarse de que

funcione correctamente. El correo institucional facilitará la comunicación y la organización en el entorno educativo.

22. El alumnado recibirá capacitación por parte del área de Tecnologías de la Información sobre las políticas de privacidad relacionadas con los servicios de Internet, el acceso remoto y la configuración. El objetivo es asegurarse de que los estudiantes estén familiarizados con las reglas y regulaciones en cuanto a los riesgos de seguridad en línea. Esta capacitación ayudará a los alumnos a tomar decisiones informadas y a utilizar Internet de manera responsable y segura.
23. Cualquier actualización de documentos, equipos o software se realizará únicamente por parte del personal designado en las respectivas áreas. Se prohíbe estrictamente que el personal externo a estas áreas manipule, distribuya, configure o modifique la información y los recursos tecnológicos de la institución. Esta medida garantizará la integridad y la seguridad de los sistemas y la información de la institución.

3.8.5 De Información

24. Cualquier información de la escuela en general deberá ser salvaguardada para garantizar la disponibilidad, confidencialidad y respaldo de esta por medio del personal docente encargado y alumnos que hagan uso de dicha información.
25. En caso de que existan carpetas compartidas en los equipos de cómputo para la disponibilidad de información dentro de las instalaciones, se deben tomar las siguientes medidas:
 - Establecer un límite de tiempo para el recurso compartido, es decir, definir cuánto tiempo estará disponible para su acceso.
 - Si la información es confidencial, se deben encriptar las carpetas y compartirlas únicamente con el personal autorizado que necesite acceder a dicha información en ese momento.
 - Después de utilizar la carpeta compartida, se debe eliminar cualquier rastro de esta para asegurar que la información confidencial no quede expuesta.

26. Las copias de seguridad de la información son fundamentales para garantizar su disponibilidad en caso de pérdida o daño. En este sentido:
- Deben realizarse copias de seguridad periódicamente, asegurando que se respalde toda la información relevante para el trabajo de los docentes y alumnos.
 - Se debe mantener un registro de las personas encargadas de realizar las copias de seguridad, incluyendo la hora y la fecha en que se llevaron a cabo.
 - Las copias de seguridad deben ser resguardadas en un lugar aparte y seguro, lejos de las instalaciones principales, para evitar que se dañen o se pierdan junto con la información original.
27. El equipo de TI tiene la responsabilidad de monitorear y prevenir el uso indebido de los equipos tecnológicos, así como salvaguardar la información de la institución. Esto para reducir los riesgos de difusión de archivos confidenciales, tanto para docentes como para alumno.
28. Cada responsable de área debe contar con una contraseña privada para proteger los archivos y datos relacionados con su área de trabajo. Esto garantiza un acceso seguro y evita que personas no autorizadas puedan acceder a información sensible.
29. Se deben establecer procedimientos claros para detectar incidentes de seguridad, como brechas de datos o ataques cibernéticos, y definir las medidas de seguridad correspondientes en el área de TI. Esto garantiza la protección de la información tanto para docentes como para alumnos, y ayuda a prevenir y gestionar posibles riesgos de seguridad cibernética que puedan afectar el entorno educativo.

3.8.6 De Personas

30. Para los docentes y alumnos, esto significa que, si necesitan realizar cambios en sus cuentas de usuario, como modificar sus datos personales, crear una nueva cuenta o eliminar una cuenta existente, deberán comunicarse con el encargado de TI. Este encargado será responsable de procesar estas solicitudes y llevar a cabo las acciones necesarias en los sistemas informáticos.

31. Tanto para docentes como para alumnos, esto implica que el equipo de TI estará supervisando y ajustando la configuración de la red de manera regular para garantizar que tanto el personal como los usuarios no utilicen los servicios de manera inapropiada o indebida. Esto se hace para mantener un entorno seguro y eficiente en el uso de los recursos informáticos.
32. En el caso de los docentes y alumnos, esto significa que, si un usuario finaliza su relación laboral o educativa con la organización, el equipo de TI y el encargado serán responsables de desactivar y eliminar su cuenta de usuario de los sistemas. Esto implica que la base de datos se actualizará regularmente para reflejar los cambios y se tomarán las medidas adecuadas para garantizar la seguridad de la información y realizar copias de seguridad necesarias.
33. Cada usuario es responsable de cerrar su sesión en los equipos de cómputo después de usarlos. Si un usuario deja su cuenta abierta y alguien externo hace un uso indebido de esa sesión, el equipo de TI no será responsable de los problemas o incidentes que puedan surgir. Por lo tanto, es importante que los usuarios cierren su sesión para proteger su información y evitar accesos no autorizados.
34. La información relacionada con la organización ya sea documentos, comunicaciones o cualquier otro tipo de datos, deberá ser manejada exclusivamente a través de los correos internos o institucionales proporcionados por la organización. Se recomienda no utilizar cuentas personales o externas para tratar asuntos relacionados con la escuela, a fin de garantizar la seguridad y la confidencialidad de los datos.
35. Queda prohibido eliminar información confidencial de la institución de forma intencional. Además, no se permite imprimir o divulgar archivos que sean propiedad exclusiva del instituto. Esto se aplica tanto a documentos en formato digital como físico. Los docentes y alumnos deben asegurarse de respetar la privacidad y confidencialidad de la información de la escuela, evitando cualquier acción que pueda comprometerla.

3.9 MONITOREO Y ACTUALIZACIÓN CONTINUA

De acuerdo con el Estándar Internacional ISO / IEC 17799, capítulo 10.2.2 “Monitoreo y revisión de los servicios de terceros” pág. 67. Consiste en asegurar que se cumplan los términos y condiciones de seguridad, y que se manejen apropiadamente los incidentes y problemas de seguridad de la información.

3.9.1 Plan de Monitoreo.

Objetivo. Implementar un sistema continuo de monitoreo de seguridad para identificar nuevas amenazas y evaluar la eficacia de las medidas de mitigación.

Este plan de monitoreo proporciona una estructura sólida para detectar, responder y mitigar incidentes de seguridad en un laboratorio. Se requiere revisar y actualizar regularmente este plan para adaptarse a cambios continuos en el entorno de amenazas y garantizar su efectividad

- Objetivos del monitoreo de incidencias:

Detectar y responder rápidamente a posibles incidentes de seguridad en el laboratorio. Minimizar el impacto de los incidentes en la operación del laboratorio y en la seguridad de la información.

- Implementación de herramientas de monitoreo:

Sistemas de detección de intrusiones y prevención de intrusiones en la red del laboratorio para monitorear el tráfico y detectar actividades sospechosas.

Configuración de sistemas de registro en los equipos del laboratorio para registrar eventos de seguridad, como intentos de acceso no autorizado y cambios en la configuración del sistema.

- Monitoreo continuo:

Monitoreo constante de los sistemas y redes del laboratorio en busca de actividad sospechosa o comportamientos anómalos.

Revisión regular de los registros de eventos y alertas de seguridad para identificar posibles incidentes de seguridad y responder a ellos de manera oportuna.

Esta figura muestra de manera resumida el proceso de monitoreo para la detección de incidencias presentadas en el plantel.



Figura 5. Monitoreo. Fuente: propia.

3.10 REVISIÓN PERIÓDICA

De acuerdo con el Estándar Internacional ISO / IEC 17799, capítulo 14.1.5 “Prueba, mantenimiento y reevaluación de los planes de continuidad del negocio” pág. 150.

Objetivo. Realizar evaluaciones periódicas del análisis de riesgos para adaptarse a cambios en la infraestructura, amenazas emergentes o nuevas vulnerabilidades.

- Evaluación y mejora continua:

Revisión regular del rendimiento del sistema de monitoreo de incidencias para identificar áreas de mejora y optimización.

Evaluación de la efectividad de las alertas y umbrales establecidos, así como de los procedimientos de respuesta a incidentes.

Implementación de medidas correctivas y actualizaciones en el sistema de monitoreo para fortalecer la detección y respuesta a incidentes en el laboratorio.

En esta figura se representa el proceso de una revisión periódica con la finalidad de prevenir al sistema de futuros incidentes y tomar medidas correctivas en caso de que se presente alguna vulnerabilidad.

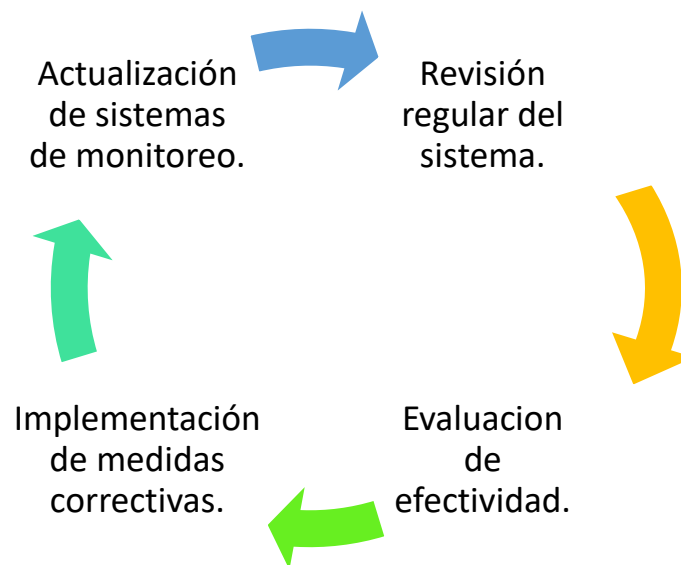


Figura 6. Revisión Periódica. Fuente: propia.

3.11 ANÁLISIS POST-INCIDENTES

El análisis post-incidente es una parte del proceso de gestión de incidentes de seguridad de la información. Después de que se ha resuelto un incidente, es importante llevar a cabo un análisis para comprender lo que sucedió, identificar las causas y tomar medidas correctivas para prevenir incidentes futuros.

Es importante tomarse el tiempo necesario para llevar a cabo un análisis y desarrollar medidas correctivas efectivas.

- Recopilación de datos.

Revisión de todos los registros, alertas, registros de actividad y otra información relevante relacionada con el incidente.

Entrevistas con el personal involucrado en la detección, respuesta y mitigación del incidente para obtener una comprensión completa de lo que sucedió.

- Identificación de las causas raíz.

Identificar los fallos en los controles de seguridad, las vulnerabilidades del sistema y los errores humanos.

Analizar el origen el incidente, cómo se propagó y cómo se detectó y respondió.

- Evaluación del impacto.

Evaluar el impacto del incidente en la organización, incluyendo la pérdida de datos, la interrupción de servicios, el costo financiero y el daño a la reputación.

Determinar qué activos de información se vieron afectados y qué datos se vieron comprometidos.

- Identificación de lecciones aprendidas.

Identificar las lecciones aprendidas del incidente, incluyendo áreas de mejora en los controles de seguridad, procedimientos de respuesta a incidentes y capacitación del personal.

Considerar cómo se podrían haber evitado o mitigado los efectos del incidente.

- Desarrollo de medidas correctivas.

Desarrollar medidas correctivas específicas para abordar las causas raíz identificadas y prevenir incidentes similares en el futuro.

Esto puede incluir la actualización de políticas y procedimientos, y la mejora de la capacitación del personal.

- Implementación de mejoras.

Implementar las medidas correctivas identificadas de manera oportuna y efectiva.

Asegurarse de que se comuniquen adecuadamente las lecciones aprendidas y las mejoras implementadas a todo el personal relevante.

- Revisión y actualización de políticas y procedimientos.

Revisar y actualizar las políticas y procedimientos de seguridad de la información en base a las lecciones aprendidas y las mejoras implementadas.

Asegurarse de que todos los procedimientos de respuesta a incidentes estén actualizados y alineados con las mejores prácticas de seguridad.

- Seguimiento y revisión periódica.

Realizar un seguimiento regular del estado de las medidas correctivas implementadas y revisar periódicamente la efectividad de las mejoras realizadas.

Ajustar las políticas, procedimientos y controles de seguridad según sea necesario para mantener la resiliencia del sistema de seguridad de la información.

En esta figura se muestra de manera resumida el proceso de un análisis después de una incidencia con la finalidad de cumplir y actualizar procesos ante una incidencia presentada.

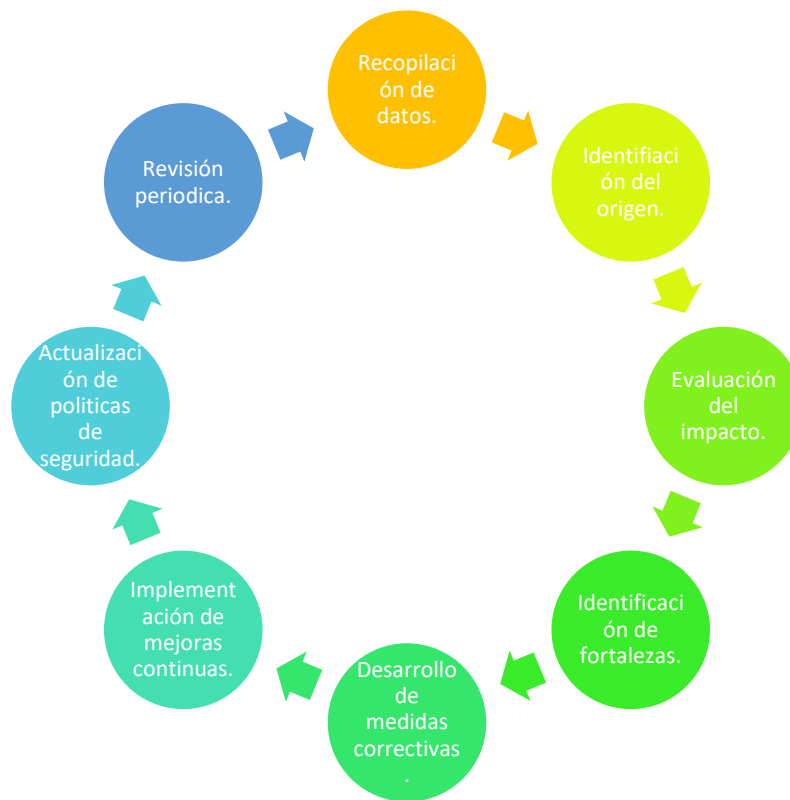


Figura 7. Análisis de Post-incidencia. Fuente: propia.

CAPÍTULO IV: RESULTADOS

4.1 INVENTARIO Y COTIZACIÓN DE ACTIVOS

Al realizar un inventario de los activos se pudo detectar la existencia de un total aproximado de 115 equipos de cómputo, divididos entre el Laboratorio 1 (45 equipos), laboratorio 2 (55 equipos) y equipos de respaldo (15 equipos).

En esta figura se muestra gráficamente el total de los equipos que se encuentran en los laboratorios del plantel.



Figura 8. Inventario de Equipos. Fuente: propia.

Al encuestar al personal encargado del laboratorio del Centro de Bachillerato Tecnológico, Industrial y de Servicios #133, se ha obtenido la información de que existen diferentes tipos de máquinas, las cuales se identificaron con los siguientes elementos:

En esta tabla se muestra la cotización de los equipos identificados en el Laboratorio 1 que cuenta la institución.

Ubicación: Laboratorio 1.		
Número de equipo: Equipo 1.		
HARDWARE:		
Procesador:	Intel® core™ i5-10400 CPU@ 2.9 GHz 2.90Ghz	\$6,599
Tipo de RAM:	8.00 GB (7.83 usable)	
Disco duro:	240GB SSD, SATA III	
Adaptador de video:	1 x HDMI, 1 x VGA	
Adaptador de sonido:	Frontal Salida de Audio, Micrófono, posterior Realtek 7.1 Surround Sound High Definition Audio CODEC*	
Adaptador de RED:	Realtek 1Gb Ethernet	
Puertos:	1.- Botón de encendido. 2.- Puertos USB 3.0 3.- Ranura de tarjeta SD 4.- Ranura de tarjeta microSD 5.- Entrada de audio de 3.5 mm. 6.- Salida de audio de 3.5 mm	
Marca y modelo del teclado:	Vorago / KM-107	\$289
Marca y modelo del mouse:	Vorago / KM-107	
Marca y modelo del monitor:	Vorago / LED-W19-205	\$1,357
Observaciones:	N/A	TOTAL: \$8,245
SISTEMA OPERATIVO:		
Programas instalados.	¿Dispone de licencia?	\$
AutoCAD 2012 – Spanish.	NO	GRATUITO
Cisco Packet Tracer 8.2.1	NO	GARTUITO
Dev-C++	NO	GRATUITO
Foxit PDF Reader.	NO	GARTUITO
Google Chrome.	NO	GRATUITO

Microsoft Office Personal Plus 2019	SI	\$2,599
TeamViewer.	NO	GARUITO
WinRAR 6.24	NO	GRATUITO

Tabla 6 Tabla de Cotización de Laboratorio 1. Fuente: propia.

En esta tabla se muestra la cotización de los equipos identificados en el Laboratorio 2 que cuenta la institución.

Ubicación: Laboratorio 2.		
Número de equipo: Equipo 1.		
HARDWARE:		
Procesador:	Intel® core™ i5-9400F	\$10,829
Tipo de RAM:	8.00 GB	
Disco duro:	1TB HDD	
Adaptador de video:	1 x HDMI, 1 x VGA	
Adaptador de sonido:	Frontal Salida de Audio, Micrófono, posterior Realtek 7.1 Surround Sound High Definition Audio CODEC*	
Adaptador de RED:	Realtek REL8111H	
Puertos:	Channel Audio (3 ports), 2x PS2, 1x Kensington lock, 2x USB2.0, 2x USB 3.1 Gen 1, 1x RS232 (COM Port)	
Marca y modelo del teclado:	Vorago / KM-107	\$289
Marca y modelo del mouse:	Vorago / KM-107	
Marca y modelo del monitor:	HP / P204 LCD 19.5" NEGRO 100V/240V	\$2,450
Observaciones:	N/A	TOTAL: \$13,568
SISTEMA OPERATIVO:		

Programas instalados.	¿Dispone de licencia?	\$
AutoCAD 2012 – Spanish.	NO	GRATUITO
Cisco Packet Tracer 8.2.1	NO	GARTUITO
Dev-C++	NO	GRATUITO
Foxit PDF Reader.	NO	GARTUITO
Google Chrome.	NO	GRATUITO
Microsoft Office Personal Plus 2019	SI	\$2,599
TeamViewer.	NO	GARUITO
WinRAR 6.24	NO	GRATUITO

Tabla 7 Tabla de Cotización de Laboratorio 2. Fuente: propia.

Así mismo, se ha realizado la cotización aproximada de equipos de cómputo, logrando así una suma de \$1,240,940.

En esta figura se muestra de forma gráfica el costo aproximado de los equipos cada laboratorio, así como también los equipos de respaldo.

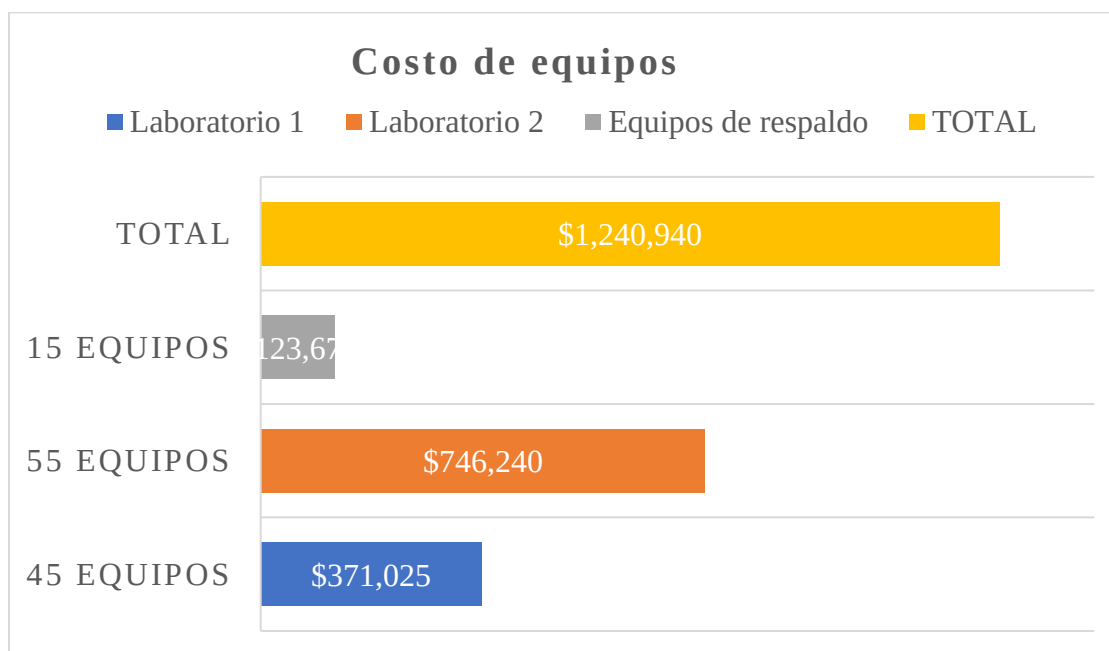


Figura 9. Costo de Equipos. Fuente: propia.

4.2 IDENTIFICACIÓN DE VULNERABILIDADES Y VALOR MONETARIO

La siguiente tabla fue elaborada como parte de un análisis de riesgos, teniendo en cuenta las posibles vulnerabilidades que podrían afectar la seguridad de la información en el entorno del laboratorio. Cada fila de la tabla representa una vulnerabilidad identificada, y se han asignado valores aproximados en términos monetarios para evaluar el impacto financiero potencial asociado a cada una.

Además de los valores monetarios, la tabla incluye el porcentaje correspondiente al personal encargado del laboratorio, lo que permite comprender mejor la responsabilidad y la participación del personal en la gestión de riesgos.

Para evaluar de manera más precisa el impacto financiero esperado, se ha calculado el Valor Monetario Esperado (EMV), que representa el costo monetario promedio que se espera en caso de que ocurra cada vulnerabilidad.

Este cálculo se obtiene multiplicando el valor monetario asociado a la vulnerabilidad por la probabilidad de ocurrencia de esta. El EMV proporciona una medida útil para priorizar las acciones de mitigación de riesgos y asignar recursos de manera eficiente, esto para la toma de decisiones informadas y estratégicas para proteger los activos y minimizar el riesgo de pérdidas económicas.

En esta tabla se calcula aproximadamente el valor de cada vulnerabilidad

Vulnerabilidad	%	Valor monetario aproximado	Cálculo de emv	Valor monetario aprox. De la vulnerabilidad
1. Falta de actualización de software.	43%	\$18,975	$0.43 * 18,975$	\$8,159.25
2. Falta de políticas de seguridad.	20%	\$20,000	$0.20 * 20,000$	\$4,000
3. Instalaciones incorrectas en el área.	14%	\$120,000	$0.14 * 120,000$	\$16,800

4. Acceso no autorizado.	70%	\$10,000	$0.70 * 10,000$	\$7,000
5. Pérdida de activos por desastres naturales.	89%	\$200,000	$0.89 * 200,000$	\$178,000
6. Eliminación de datos accidentalmente.	60%	\$2,599	$0.60 * 2,599$	\$1,599.4
7. Malware o virus.	80%	\$80,385	$0.80 * 80,385$	\$64,308

Tabla 8 Identificación de Vulnerabilidades y Valor Monetario. Fuente: propia.

La siguiente gráfica proporciona una herramienta visual útil para comprender cómo puede influir en la probabilidad de ocurrencia de vulnerabilidades.

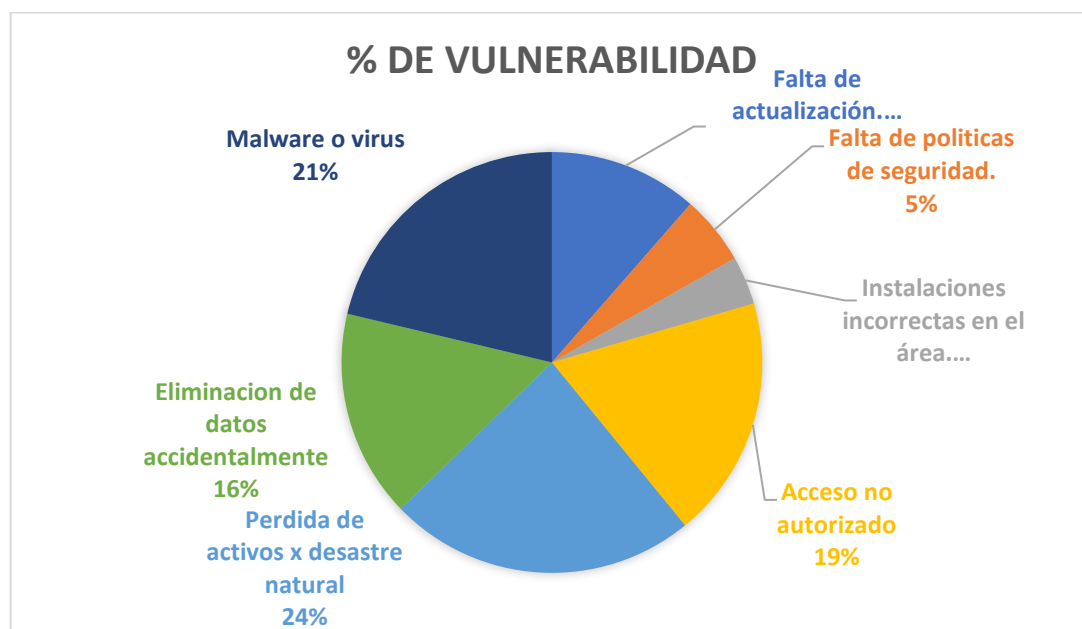


Figura 10. Porcentaje de Vulnerabilidades. Fuente: propia.

Así mismo, se presenta un gráfico en el cual se destaca la línea azul, que representa el valor monetario aproximado, mientras que una línea naranja muestra el valor monetario aproximado de la vulnerabilidad.

Estas líneas proporcionan una representación visual entre el valor monetario y la vulnerabilidad identificada. La línea azul muestra una tendencia general del valor monetario, brindando una visión de conjunto de los costos asociados con las distintas vulnerabilidades. Por otro lado, la línea naranja resalta el valor monetario relacionado con las vulnerabilidades, lo que permite una evaluación más detallada de su impacto financiero.

Esta gráfica facilita la identificación de las vulnerabilidades que pueden tener un mayor impacto económico, lo que ayuda a priorizar las acciones de mitigación de riesgos.

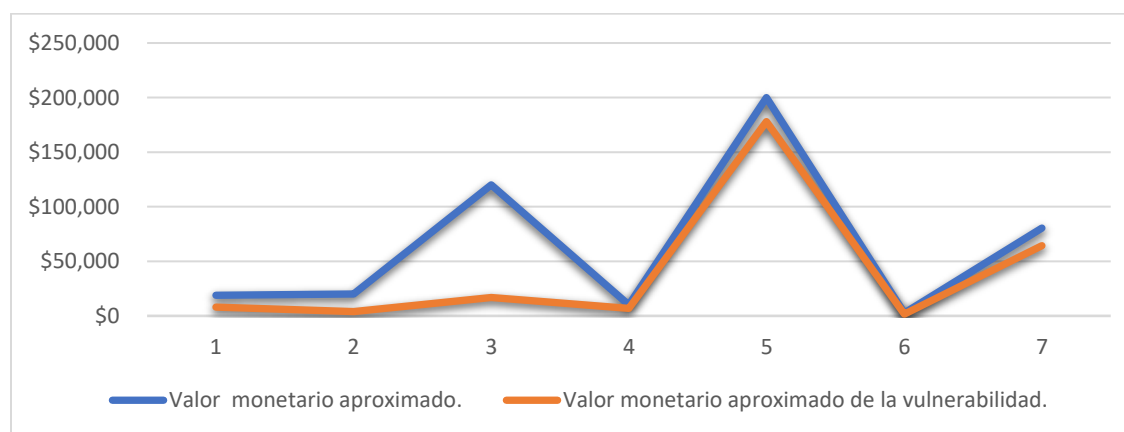


Figura 11. Comparación de valores monetarios. Fuente: propia.

Tras analizar los resultados, se destaca que la vulnerabilidad con el impacto más significativo es la relacionada con desastres naturales. Por lo tanto, se sugiere dar prioridad a esta área en caso de una emergencia de este tipo, dado que su impacto económico es de mayor estimación.

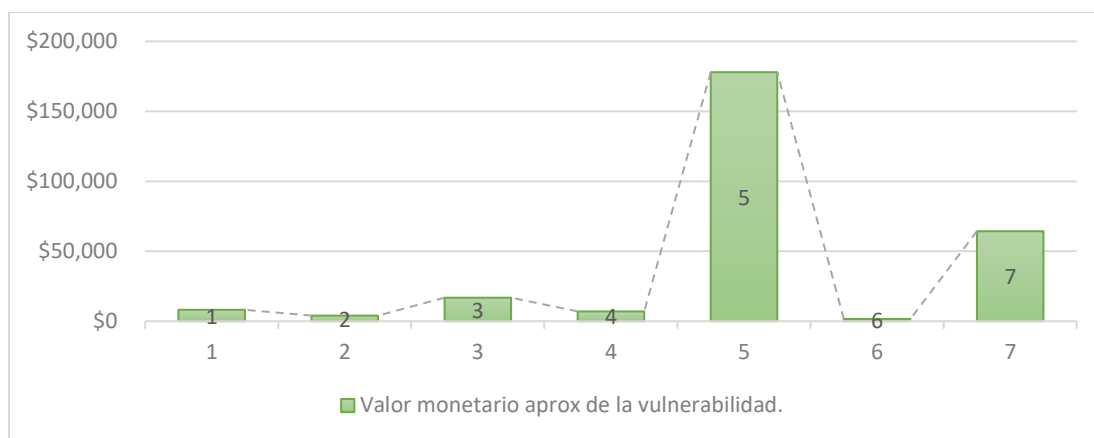


Figura 12. Priorización de Vulnerabilidades. Fuente: propia.

4.3 DIAGRAMA DE FLUJO DEL PLAN DE RECUPERACIÓN

Conforme al Estándar Internacional ISO/IEC 17799 capítulo 14.1.3 “Desarrollar e implementar los planes de continuidad incluyendo la seguridad de la información” pág. 147 se desarrolló un diagrama con el proceso de planeación de continuidad para restaurar las operaciones y asegurar la disponibilidad de la información.

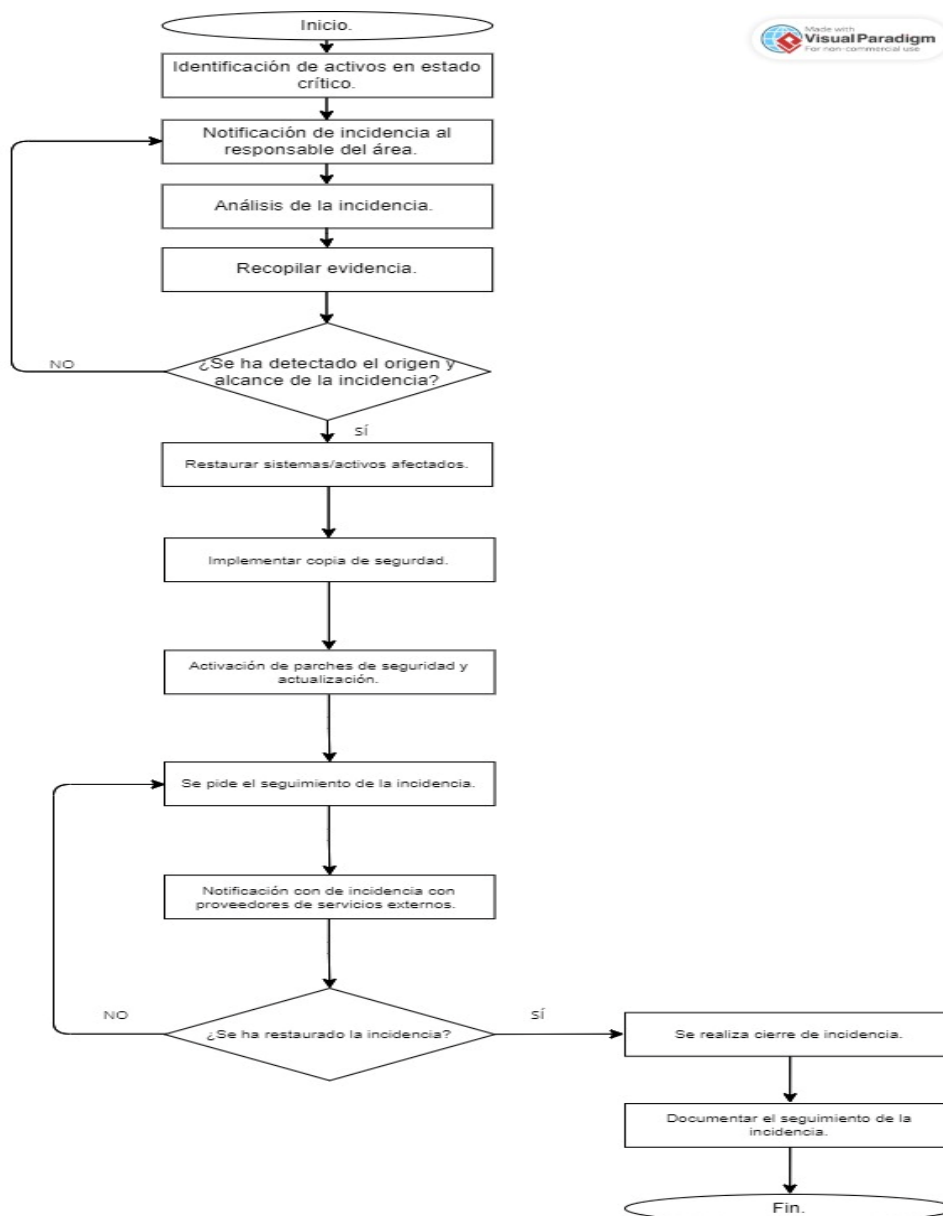


Figura 13. Flujo de Plan de Recuperación. Fuente: propia.

4.4 DIAGRAMA DE FLUJO DEL PLAN DE PRUEBAS

Con base al Estándar Internacional ISO /IEC 17799, capítulo 14.1.5 “Prueba, mantenimiento y reevaluación de los planes de continuidad del negocio” pág. 150, se desarrolló un diagrama el cual menciona el programa de continuidad para ejecución del desarrollo del plan de pruebas.

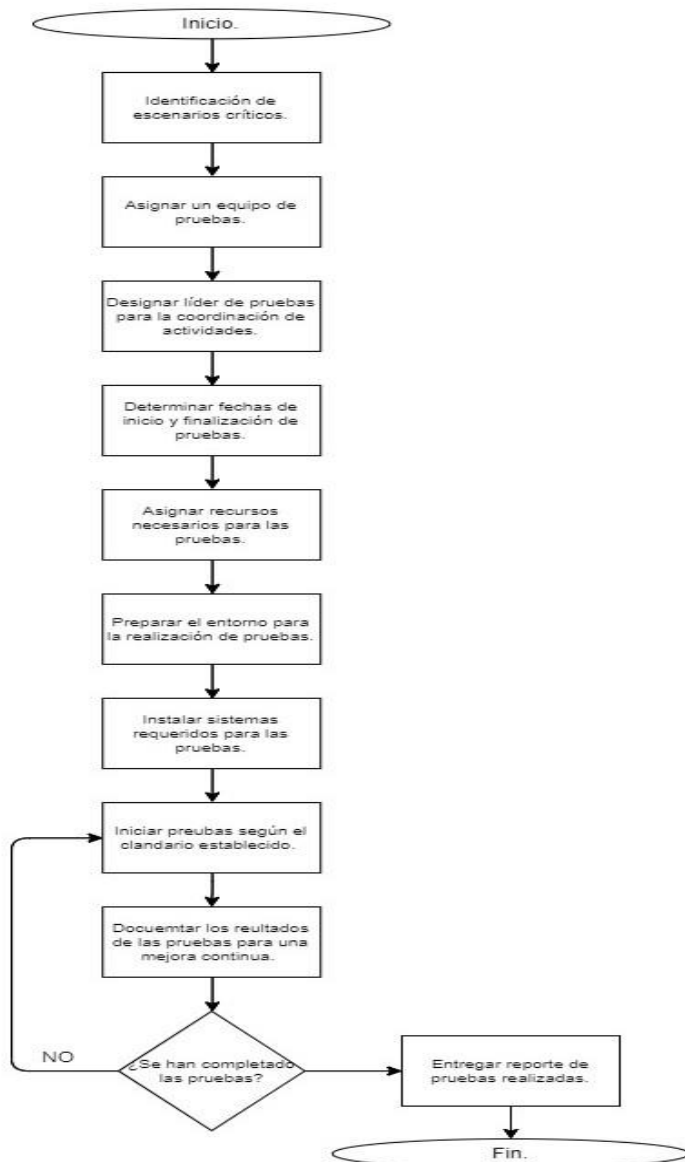


Figura 14. Flujo de Plan de Pruebas. Fuente: propia.

4.5 DIAGRAMA DE FLUJO DE MONITOREO

De acuerdo con el Estándar Internacional ISO / IEC 17799, capítulo 10.2.2 “Monitoreo y revisión de los servicios de terceros” pág. 67. Se desarrolló un diagrama de flujo para comprobar que se cumplan los términos y condiciones de seguridad, y que se manejen apropiadamente los incidentes y problemas de seguridad de la información.

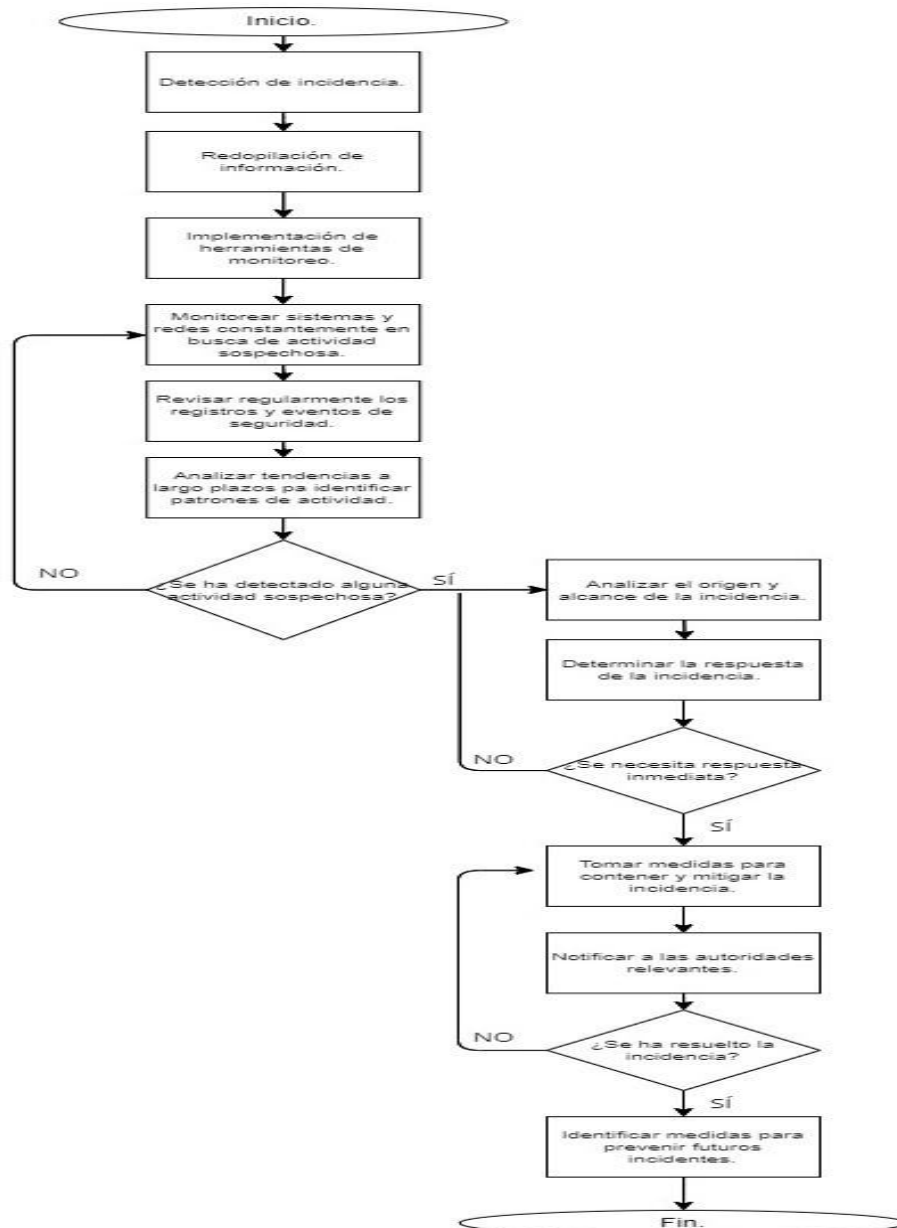


Figura 15. Flujo de Monitoreo. Fuente: propia.

4.6 DIAGRAMA DE FLUJO DE ACTUALIZACIÓN PERIÓDICA

De acuerdo con el Estándar Internacional ISO / IEC 17799, capítulo 14.1.5 “Prueba, mantenimiento y reevaluación de los planes de continuidad del negocio” pág. 150.

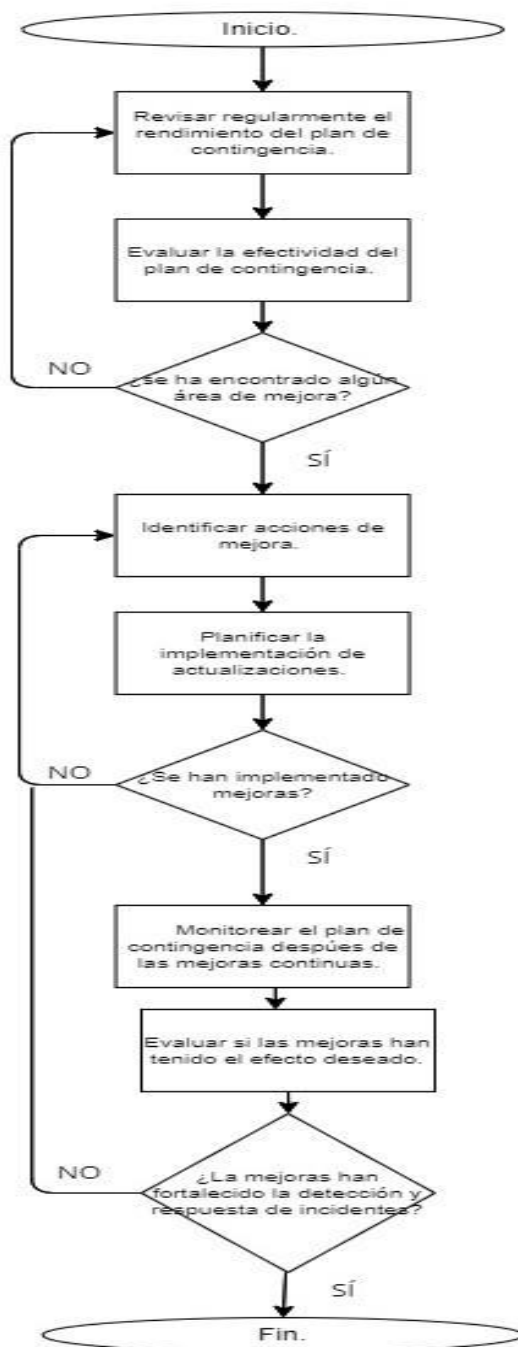


Figura 16. Flujo de Actualización Periódica. Fuente: propia.

4.7 DIAGRAMA DE FLUJO DEL ANÁLISIS POST-INCIDENTE

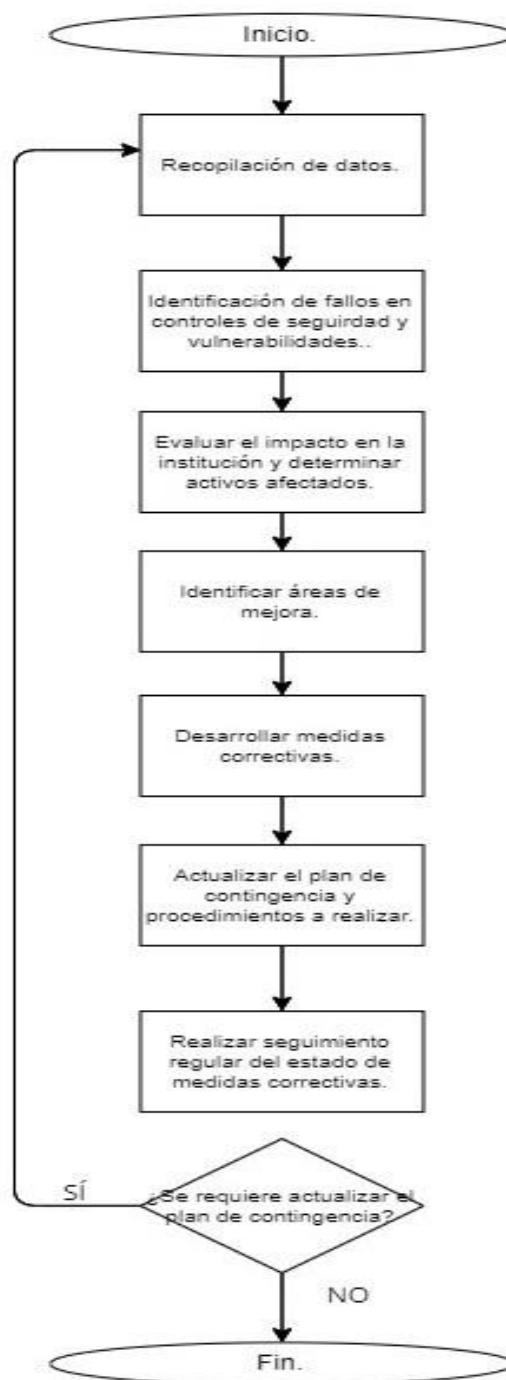


Figura 17. Flujo de Análisis de Post-incidencias. Fuente: propia.

CONCLUSIONES

En este proyecto, la seguridad de la información surge como tema principal, dado a que se presentan datos sensibles del alumnado de la institución. Una mejora continua en este ámbito puede ser implementada a través de un control de activos, que incluya un inventario detallado de los equipos de cómputo almacenados, así como de los dispositivos de respaldo disponibles para casos de incidencia.

En el plano lógico, se recomienda establecer un protocolo para la creación regular de copias de seguridad de los datos más críticos, las cuales deben ser almacenadas en ubicaciones accesibles únicamente para el personal autorizado, incluyendo directivos y personal con los permisos correspondientes.

Además, para mitigar el riesgo de infección por virus en los equipos de cómputo del laboratorio, se sugiere la implementación de un software de congelamiento de sistema. Esta medida garantizará que ningún archivo malicioso pueda ser almacenado permanentemente en los equipos, minimizando así la amenaza y fortaleciendo el plan de contingencia ante posibles incidentes de seguridad. Además, se recomienda llevar a cabo una capacitación continua para el personal sobre las mejores prácticas de seguridad informática, con el objetivo de fomentar una cultura de seguridad cibernética dentro de la institución y garantizar una protección integral de los datos y sistemas.

Para finalizar, el uso de políticas de seguridad se presenta como un elemento para garantizar la protección de la información y la integridad de los sistemas. Estas políticas deben ser comunicadas de manera efectiva a todo el personal y alumnado involucrado en la institución, asegurándose de que comprendan sus responsabilidades en cuanto a la seguridad de la información. Además, es importante establecer mecanismos de monitoreo y cumplimiento para garantizar la efectividad de estas. Es importante revisar periódicamente las políticas establecidas y actualizarlas según sea necesario para adaptarse a los cambios en el entorno de seguridad y a las nuevas amenazas que puedan surgir ya que ayudará a fortalecer la postura de seguridad general de la institución.

COMPETENCIAS DESARROLLADAS

Concluyendo el proyecto, se tiene que las siguientes competencias fueron desarrolladas:

- Diseña, implementa y administra bases de datos optimizando los recursos disponibles, conforme a las normas vigentes de manejo y seguridad de la información.
- Evalúa tecnologías de hardware para soportar aplicaciones de manera efectiva
- Detecta áreas de oportunidad empleando una visión empresarial para crear proyectos aplicando las Tecnologías de la Información y Comunicación

Así mismo, se destacan los siguientes tributos para la realización del proyecto:

- Calidad para razonar, analizar, sintetizar y establecer estrategias argumentadas para la solución de problemas complejos de cómputo.
- Establece y gestiona conforme a normas vigentes de conectividad y seguridad, sistemas informáticos para el sector empresarial, industrial y de servicios.
- Aptitud para establecer comunicación crítica y objetiva frente a auditorios interculturales.
- Preserva y cultiva una conducta ética y profesional, considerando el impacto de las soluciones de ingeniería en el ámbito global, económico, ambiental y social.
- Atiende una estrategia para la formación e instrucción permanente, necesaria para actualizar la habilidad de situar, evaluar, integrar y aplicar conocimiento afín a las tecnologías de la información y comunicaciones.

FUENTES DE INFORMACIÓN

- Amazon Web Services, Inc. (s.f.). *Explicación de la copia de seguridad de datos: AWS*. (s. f.). .
Obtenido de <https://aws.amazon.com/es/what-is/data-backup/>
- Aguilera López, P. (2010). *Seguridad informática*. España: Editex.
- Areitio Bertolin, J. (2008). *Seguridad de la información. Redes, informática y sistemas de información*. Ediciones Paraninfo, S.A.
- Buenning, M. (25 de Marzo de 2024). *La importancia de la recuperación de datos*. Obtenido de <https://www.ninjaone.com/es/blog/recuperacion-de-datos-para-endpoints/>
- Ciccariello, P. (10 de Marzo de 2022). *MALWARE COMO ENFRENTARLOS*. Obtenido de <https://www.redusers.com/noticias/publicaciones/malware-como-enfrentarlos/>
- Enrique, M. G. (2023). *Seguridad de Equipos Informáticos*. Ra-Ma Editorial, 2023.
- Espinoza Asto, S. (2014). *Diseño de un plan de contingencia de sistemas informáticos para la Universidad Peruana los Andes*.
- Multicomp Soluciones de seguridad en TI. (27 de Mayo de 2019). *Respaldo de información (Backup)*. Obtenido de <https://multicomp.com.mx/seguridad-informatica/respaldo-de-informacion/>
- Naveiro Flores, R., & David, R. I. (2022). *¿Qué sabemos de analisis de riesgos?* España: Los Libros de la Catarata; Primera edición (8 abril 2022).
- Palacios Pacheco, R. A., & Quiroz Carranza, J. (2013). *Plan de contingencia de los equipos y sistemas informáticos en el gobierno autónomo descentralizado municipal del cantón Junín*. Calceta: Espam: Bachelor's thesis.
- Recovery Labs. (02 de Septiembre de 2024). Obtenido de Principales factores que causan una pérdida de información: <https://www.recoverylabs.com/ayuda-y-soporte/data-recovery-white-papers/informes/principales-factores-que-causan-una-perdida-de-informacion/#:~:text=Una%20p%C3%A9rdida%20de%20datos%20es,%C2%BFNecesitas%20m%C3%A1s%20informaci%C3%B3n?>
- Tamayo Arias, J., & A., T. A. (1999). *Aprender a Investigar. Módulo 5 El proyecto de investigación*. Santa fe de Bogotá: ARFO EDITORES LTDA.
- Team de Asana. (25 de Febrero de 2024). *Matriz de riesgos: cómo evaluar los riesgos para lograr el éxito del proyecto (incluye ejemplos)*. Obtenido de <https://asana.com/es/resources/risk-matrix-template>
- (2014). *UNE-ISO/IEC 27000*. España.

Anexo 02. Carta Compromiso.

A quien corresponda,

Por medio de la presente, yo, **Franco Romero Tzitz Marisol** identificado con la matrícula: 201921209, manifiesto mi compromiso y cumplimiento en el manejo adecuado y responsable de los datos e información proporcionados en el presente documento.

Declaro y acepto los siguientes términos:

1. Compromiso de Uso Responsable de los Datos

Me comprometo a emplear la información entregada exclusivamente para los fines autorizados y dentro del ámbito de mis funciones en la institución. En ningún caso haré uso de la información para fines distintos a los expresamente autorizados, ni la divulgaré sin el consentimiento formal y por escrito de la Institución.

2. Compromiso de No Compromiso Legal para la Institución

Declaro y acepto que la información proporcionada en el presente documento no compromete legalmente a la Institución, debido a que los datos utilizados son aproximados y de carácter general. La información no incluye datos confidenciales ni detalles específicos que puedan comprometer la seguridad o integridad de la Institución.

3. Confidencialidad y Seguridad de los Datos

Me comprometo a mantener la confidencialidad y seguridad de la información proporcionada, y a protegerla conforme a las políticas y normativas vigentes, así como a los principios éticos de la Institución.

4. Exclusión de Responsabilidad de la Institución

Reconozco que toda responsabilidad por el uso de los datos recae exclusivamente en mi persona, y que la Institución no asume ninguna obligación o responsabilidad legal en relación con la utilización o el destino de la información proporcionada en el marco de mis funciones.

5. Cumplimiento de Normativas

Acepto cumplir con todas las normativas legales, regulaciones y políticas internas aplicables a la protección y manejo de datos, asumiendo cualquier consecuencia derivada del incumplimiento de los términos de esta carta compromiso.

Atentamente,



Franco Romero Tzitz Marisol