Artículo original/ Original article
ISSN 2953-6553

Plan de continuidad del negocio del sistema académico Fénix, en el Instituto Superior Tecnológico del Azuay, con Condición de Superior Universitario.

Business Continuity Plan of the Fenix Academic System at the Instituto Superior Tecnológico del Azuay, con Condición de Superior Universitario.

José Fabián-Chuqui Quille 0009-0005-4182-3112 , Marcelo-Monteros 0000-0002-8095-8109 , Bryam Durazno-Chumbay 0009-0002-3137-8842, Diego Cherres-Yuqilima 0009-0008-4318-8564

jose.chuqui@tecazuay.edu.ec, ruben.monteros@tecazuay.edu.ec, bryam.durazno.est@tecazuay.edu.ec, diego.cherres.est@tecazuay.edu.ec,

[a] Instituto Superior Universitario Tecnológico del Azuay, Cuenca, Ecuador

DOI 10.36500/atenas.3.005

Resumen

El artículo aborda la importancia de la información como un activo clave para mantener, en la actualidad, la competitividad y la presencia en el mercado. Se destaca la necesidad de que el Instituto implemente un plan que le permita mantenerse resiliente ante cualquier eventualidad; especialmente, ante la pérdida de información, debido a catástrofes o eventos disruptivos. El enfoque del artículo se centra en la aplicación de una metodología que garantiza la continuidad del servicio Fénix, a través de un análisis exhaustivo de riesgos. Se resalta la importancia de identificar y evaluar los posibles riesgos que podrían afectar la disponibilidad y la integridad de la información. Mediante este análisis, el Instituto puede desarrollar estrategias y medidas preventivas para mitigar o minimizar los impactos de los riesgos identificados.

La implementación de esta metodología de análisis de riesgos permite al Instituto estar preparado para hacer frente a situaciones imprevistas y asegurar la continuidad del servicio Fénix. Al adoptar un enfoque proactivo, el Instituto puede anticiparse a posibles desastres o eventos disruptivos y tomar medidas preventivas y de recuperación adecuadas para proteger y preservar la información vital para el negocio.

En resumen, el artículo destaca la importancia de la información como un activo diferenciador y propone la implementación de una metodología de análisis de riesgos a fin de garantizar la continuidad del servicio Fénix. Esta metodología permite al Instituto identificar y abordar los posibles riesgos, a través del aseguramiento de la protección de la información y la capacidad de mantenerse resiliente frente a situaciones adversas.

Abstract

The article addresses the importance of information as a key asset to maintaining competitiveness and market presence today. It highlights the need for the Institute to implement a plan to remain resilient in the face of any eventuality, especially the loss of information due to disasters or disruptive events. The article focuses on applying a methodology that ensures the continuity of the Fénix service through a comprehensive risk analysis. It emphasizes the importance of identifying and assessing potential risks that could affect the availability and integrity of the information. Through this analysis, the Institute can develop strategies and preventive measures to mitigate or minimize the impact of identified risks.

Implementing this risk analysis methodology enables the Institute to be prepared to face unforeseen situations and ensure the continuity of the Fénix service. By adopting a proactive approach, the Institute can anticipate potential disasters or disruptive events and take appropriate preventive and recovery measures to protect and preserve vital business information.

In summary, the article underscores the importance of information as a differentiating asset and proposes implementing a risk analysis methodology to ensure the continuity of the Fénix service. This methodology allows the Institute to identify and address potential risks by ensuring the protection of information and the ability to remain resilient in the face of adverse situations..

Palabras Claves – Continuidad del Negocio, ISO 22301, Plan de contingencia, sistema académico.
Keywords – Business Continuity, ISO 22301, Contingency Plan, academic system.

Recibido: 2024-03-18, Aprobado tras revisión: 2024-08-22

I. INTRODUCCIÓN

En la actualidad, la tecnología ha permeado en todos los aspectos de nuestras vidas y se ha convertido en un instrumento esencial para las organizaciones en general. Con el avance de la digitalización, las empresas han adoptado diversas herramientas informáticas que les permiten generar, almacenar y acceder a grandes cantidades de información, de manera rápida y eficiente. Sin embargo, este acceso oportuno a los datos, desde cualquier lugar del mundo, también ha dado lugar a nuevos desafíos; especialmente, en términos de seguridad. Ahora, la información tiene un valor incalculable para las organizaciones y, por lo tanto, protegerla contra los delitos informáticos se ha convertido en una prioridad absoluta (Conforme, 2018).

El Instituto Superior Universitario Tecnológico del Azuay (TEC. AZUAY) es una institución de educación superior (IES), en donde sus procesos académicos y administrativos evolucionan poco a poco, con la ayuda de las tecnologías, a través del fortalecimiento de la operatividad institucional, con la aplicación de los pilares de la seguridad de la información: confidencialidad, integridad y disponibilidad. "Estos tres elementos son críticos para proteger la información sensible o confidencial y minimizar el impacto de interrupciones o desastres en su operación diaria" (Martinez, 2020).

Con lo antes indicado, el proyecto actual tiene como objetivo identificar y evaluar los riesgos que podrían causar interrupciones en el correcto funcionamiento del sistema académico Fénix, del TEC. AZUAY. En caso de que se produzcan estas interrupciones del servicio, es imprescindible contar con sistemas de respaldo tecnológico e infraestructura que permitan mantener las operaciones. El propósito principal es garantizar la disponibilidad, confidencialidad e integridad del sistema académico, a través de la implementación de un Plan de Continuidad del Negocio (BCP). Esto, se logrará mediante la implementación de sistemas de respaldo de datos, planes de recuperación de desastres y la disponibilidad de infraestructuras alternativas, en caso de que las instalaciones principales se vean afectadas.

II. MARCO TEÓRICO

La ejecución del presente proyecto está basada en la norma ISO 22301, la cual establece un sistema de gestión de la continuidad del negocio (SGCN). Este sistema ayuda a las organizaciones a prepararse y responder ante situaciones de indisponibilidad del servicio, con el objetivo de minimizar el impacto negativo en la organización. La aplicación de la norma ISO 22301, se enmarca en la gestión de la continuidad del negocio, la cual proporciona un marco teórico relevante.

Recibido: 2024-03-18, Aprobado tras revisión: 2024-08-22

El SGCN implica la implementación de políticas, procedimientos, sistemas y planes de acción. También implica el diseño y desarrollo de medidas de protección, reducción y recuperación continua, en caso de interrupciones en las operaciones. Todo esto tiene como objetivo asegurar que la organización funcione de manera óptima, incluso después de un incidente grave. Por lo tanto, la gestión de la continuidad del negocio se convierte en un objetivo fundamental para cualquier organización preocupada por su supervivencia y éxito, a largo plazo.

Este sistema, se basa en el modelo Planificar-Hacer-Verificar-Actuar (PHVA). En otras palabras, implica la planificación de las medidas necesarias para garantizar la continuidad del negocio, la implementación de estas medidas, la verificación de su efectividad y la realización de ajustes y mejoras en función de los resultados obtenidos. (Bevan, 2020).

A. Alcance

El objetivo principal del plan de continuidad de servicio es establecer procedimientos y medidas de contingencia que permitan mantener las funciones críticas del sistema Fénix, en caso de interrupciones o desastres. El proceso de desarrollo del plan de continuidad de negocio involucra diversas etapas.

En primer lugar, se realiza un análisis exhaustivo de los riesgos y las amenazas potenciales que afectarían la continuidad del sistema Fénix. Esto incluye evaluar factores como fallas en el hardware o software, ataques cibernéticos, desastres naturales o incidentes humanos. Una vez identificadas las posibles amenazas, se definen los objetivos de recuperación y los plazos de tiempo aceptables para la restauración del sistema. Se determinan los recursos necesarios, tanto técnicos como humanos, para llevar a cabo la recuperación y se establecen las estrategias y procedimientos, a fin de activar el plan de continuidad de negocio.

B. Análisis situacional

El TEC. AZUAY, se consolida como una IES que sustenta sus procesos de enseñanza-aprendizaje en el ámbito técnico y tecnológico, con la más alta calidad académica y humana, con el propósito de proveer soluciones a los problemas y necesidades de la sociedad. La gestión de la información académica, actualmente, se encuentra sistematizada mediante el sistema académico Fénix, el cual es accesible mediante la instalación del mismo.

La información que se maneja dentro de este sistema es historial académico, registro de asistencia, inscripciones, matrículas, notas y cargas horarias de los estudiantes; sin embargo, también se aloja información docente, como: Plan Educativo Anual (PEA), asignación de docentes, asignación de

Recibido: 2024-03-18, Aprobado tras revisión: 2024-08-22

coordinadores de carreras, plan de clases, sílabos, reporte de avance de sílabos, reporte de notas, exámenes interciclos y finales, entre otros. En gran medida, la institución depende del sistema Fénix, para la planificación académica; y, la gestión de registro de estudiantes y docentes. Sin embargo, existe el riesgo que interrupciones en el funcionamiento puedan afectar significativamente al sistema; por ello, en la actualidad, proteger los sistemas informáticos contra accesos, usos, divulgaciones, interrupciones o destrucciones no autorizadas, se ha vuelto prioridad, como parte de la seguridad de la información.

El TEC. AZUAY no cuenta con un Plan de Continuidad del negocio que responda a la gestión de riesgo ISO 3100:2018 (ISO, 2018), seguridad de la información ISO 27001:2022 (ISO, 2023) y Continuidad del negocio ISO 22301:2022 (ISO, 2022). Estos sistemas mencionados son de suma importancia para enfrentar posibles interrupciones en el sistema, debido a desastres naturales, fallas del sistema, ciberataques y para salvaguardar de forma íntegra la información del sistema académico.

C. Planteamiento del problema

En la actualidad, la información digital es crucial y extremadamente valiosa debido a la gran cantidad de datos personales que se gestionan en internet. Sin embargo, es importante tener en cuenta que esta información corre el riesgo de ser atacada por cibercriminales, robada o empleada de manera malintencionada por parte de terceros. El phishing, malware o cracking son técnicas que se utilizan para robar esta información y, por tanto, es necesario tomar medidas de seguridad para protegerla. (L. Rosero, 2021)

En Ecuador, las universidades tienen una gran cantidad de información digital relacionada con los datos académicos de los estudiantes. Esta información se almacena en centros de datos y mediante sistemas informáticos, el personal administrativo, docentes y estudiantes, con los permisos correspondientes pueden acceder a ella de manera local o a través de internet. A menudo, este sistema se conoce como sistema académico y, lamentablemente, muchas veces no se implementan buenas prácticas de seguridad de la información para protegerlo. Como resultado, se expone a diversos riesgos, incluyendo la posibilidad de robo, destrucción, divulgación y modificación de los datos (Conforme, 2018).

Con base en lo antes mencionado, el TEC. AZUAY cuenta con -aproximadamente- 1000 estudiantes y 80 docentes, distribuidos en sus 25 carreras académicas. Sin embargo, a la seguridad de la información personal académica de profesores y alumnos no se le ha dado la suficiente importancia y no se ha implementado ninguna medida para asegurar la disponibilidad, confidencialidad e integridad de esta información, la cual es considerada sensible.

Recibido: 2024-03-18, Aprobado tras revisión: 2024-08-22

III. METODOLOGÍA Y CÁLCULOS

En el actual proyecto, se aplicó la metodología de la norma ISO 22301 porque es recomendada por la mayoría de expertos en la materia, debido a que proporciona un marco de trabajo sistemático completo y reconocido internacionalmente para la gestión de la continuidad del negocio (ISO, 2022). Existe norma que permite a las organizaciones prepararse para eventos disruptivos potenciales que puedan afectar sus operaciones (NQA, 2020). Al seguir esta metodología, las empresas garantizan la protección de sus activos, minimizan el impacto de los incidentes y aseguran la recuperación eficiente y oportuna en caso de una interrupción en sus operaciones comerciales. Sin embargo, la (ISO 223001, 2020) propone un ciclo de mejora continua que abarca la planificación, implementación, evaluación y mejora constante del SGCN.

Para la recolección de datos en el presente estudio, se utilizaron métodos mixtos de investigación, en los cuales se aplicaron encuestas estructuradas y entrevistas semiestructuradas, las cuales permitieron obtener información detallada sobre la población objeto de estudio. Se diseñaron cuestionarios personalizados y se llevaron a cabo entrevistas con la finalidad de recolectar datos cuantitativos y cualitativos, respectivamente, lo cual permitió una aproximación integral y rigurosa al objeto de investigación. Se pueden revisar las entrevistas y encuestas realizadas en los anexos 2, 3, 4, 5 y 6.

A. Levantamiento de Equipos

El objetivo principal de este proceso fue recopilar información detallada de todos los dispositivos presentes en el centro de datos para obtener un registro completo de las especificaciones técnicas de cada uno de ellos. Para lograr esto, se realizaron visitas al centro de datos del Instituto y se recolectó información detallada sobre los diferentes activos presentes, como servidores, equipos de red, sistemas de almacenamiento, bases de datos y otros componentes fundamentales para el correcto funcionamiento del sistema académico Fénix. Una vez obtenidos todos los datos, se elaboró un inventario de los equipos, lo que permitió tener una visión clara y precisa de los recursos presentes en el data center. Cada detalle y especificación técnica fue documentado para su registro y posterior análisis de riesgo y vulnerabilidades. Se puede encontrar una lista detallada de las características y especificaciones técnicas de los equipos en el anexo 1.

B. Análisis de riesgo

Este análisis se realiza para identificar los posibles riesgos asociados y desarrollar estrategias adecuadas de mitigación para proteger la integridad, confidencialidad y disponibilidad de los activos

Recibido: 2024-03-18, Aprobado tras revisión: 2024-08-22

críticos de información que permiten la conexión al sistema académico. Es esencial realizar este análisis para garantizar un entorno seguro y confiable para el acceso y uso de la información en el sistema académico. El análisis de riesgos se basó en la tesis titulada "Análisis de las vulnerabilidades del sistema de información académica: Caso de estudio Instituto Superior Tecnológico del Azuay", realizada por los autores (Chuqui & Orellana, 2023).

En esta investigación, se identificaron y evaluaron las vulnerabilidades presentes en el sistema de información académica del Instituto. Para llevar a cabo este análisis, se utilizaron diversos materiales y metodologías específicas. En la Tabla 1, se indican los detalles completos de los materiales; y, las metodologías empleadas se pueden encontrar en la página 29 de la tesis. Esta sección proporciona una descripción exhaustiva de las herramientas y técnicas aplicadas para garantizar la precisión y efectividad del estudio.

Figura 1

Se resume las investigaciones referentes a auditorías, análisis de riesgos e implementación de Sistemas de Gestión de la Seguridad de la Información.

Lugar y Fecha de publicación	Título del documento	Vulnerabilidades encontradas	Herramientas utilizadas	Metodología
Institución Educativa Departamental Luis Carlos Galán Colombia / octubre de 2017	Auditoria de seguridad informática para la Institución Educativa Departamental Luis Carlos Galán – Municipio de Yacopí Cundinamarca	Puertos abiertos, fallos a nivel de sistemas operativos, aplicativos o servicios, vulnerabilidades tipo ransomware, alto riesgo de amenazas y vulneración en servidores web, denegaciones de un servicio, malas prácticas para la asignación de passwords.	Nmap, ping, Zenmap, Nessus y Nikto, John The Ripper.	Ethical hacking para el análisis de vulnerabilidades, Magerit V3 para el análisis de riesgos y mejora continua PHVA (planificar, hacer, verificar, actuar) como lo recomienda la norma ISO /IEC 27001.
Universidad Estatal del sur de Manabí / noviembre 2018.	Diseño de un modelo de gestión de seguridad de la información para el sistema académico de la Universidad Estatal del Sur de Manabí.	Borrado de información, limitado registro de equipos informáticos, posibilidad de infección con software de denegación de servicio.	ISO2701, ISO2702.	Metodología PDCA (Planificar – Hacer-Verificar – Actuar) en donde se establecen lineamientos de seguridad de la información en el sistema académico S@U basados en el estándar internacional ISO 27002:2017.
Universidad Nacional de Piura / julio 2019.	Diseño de un sistema de gestión de seguridad de la información para los procesos académicos de la Universidad Nacional de Piura según la NTP ISO/IEC.	Errores en backups, falta de control de acceso, falta de control de transporte o transferencia, ambiente inseguro, contraseñas inseguras, presencia de virus, falta de condiciones de seguridad, mantenimiento insuficiente.	ISO 17799. (ISO 17799,2000) ISO /IEC 27002 CNB &INDECOPI, 2008.	Investigación aplicada y no experimental con información cuantitativa y cualitativa. Las técnicas usadas fueron: entrevistas, revisión documental, observaciones de campo y cuestionarios.
Año 2020/Corporación Universitaria Rafael Nuñez / julio 2020.	Diseño de un sistema de gestión de seguridad de la información para el proceso de gestión de la infraestructura tecnológica de instituciones académicas basado en la herramienta de gestión de riesgo Magerit.	Importancia de los activos en la institución, su relevancia para la organización por su impacto en los procesos administrativos y académicos. Activos críticos son servidores, los archivos de respaldo y seguridad, y los mecanismos de acceso al sistema.	MAGERIT, MOVA	Cuantitativa, con diseño no experimental transeccional descriptivo. Aplicación de un sistema de gestión adecuado a sus políticas, mediante el enfoque de la norma ISO 27001 y la metodología MAGERIT. Caracterización y ponderación de los activos, amenazas y salvaguardas. Mecanismos de control y políticas de seguridad.

Nota. Gráfico de las herramientas utilizadas 2024

C. Identificación y clasificación de activos de información

En este punto, se recopilaron datos y se desarrolló una matriz que permitió una clasificación y valoración sistemática de los activos identificados, teniendo en cuenta su importancia y su impacto potencial en el funcionamiento del sistema. En la tabla 2, se puede observar un listado de los activos identificados que se utilizan en el sistema académico Fénix para garantizar la disponibilidad y la integridad de la información, en caso de posibles fallos o pérdidas.

Recibido: 2024-03-18, Aprobado tras revisión: 2024-08-22

Tabla 1.

Activos para el funcionamiento del sistema académico Fénix

Categoría	Activo	Cantidad	Marca
Equipos de Red	Router	1	ZTE
	Switch	1	Mikro Tik
		1	Tp Link
	Server	1	HP
	Access Point	6	Ubiquiti
		1	
	PoE	2	
		5	
Otros Equipos	UPS	1	FIRMSESA Comp. Power
		1	FIRMESA Dataline
	Aire acondicionado	1	SANKEY
	Rack eléctrico	1	Ducati Sistemi
Información digital del Instituto	Calificaciones	-	Digital
	Matrículas	-	
	Información de los estudiantes, docente y personal administrativo	-	
	Credenciales	Usuarios/Contraseñas	Digitales
	Registro de asistencia estudiantil	-	Digital

Nota. Equipos y servicios 2024.

D. Valoración de activos de información

Después de identificar y clasificar los activos de información, se valoró su impacto en la utilidad del servicio. El criterio utilizado fue el costo asociado a la pérdida de confidencialidad, integridad y disponibilidad. Por medio de la elaboración de una matriz de riesgos, se identificó que todos los activos se encuentran en un estado crítico de inseguridad y carecen de planes de contingencia efectivos, lo que crea una situación preocupante y deja a la institución vulnerable a graves riesgos. Es esencial establecer controles de seguridad apropiados, analizar los riesgos y fallas potenciales, establecer protocolos de respuesta a incidentes, educar al personal sobre los procedimientos de seguridad y probar regularmente

Recibido: 2024-03-18, Aprobado tras revisión: 2024-08-22

los planes de contingencia. En la tabla 3, se observa la valoración de los activos de información con su respectiva dependencia dentro del sistema académico.

Tabla 2.

Valoración de los activos de la información.

Activo	Dependiente	Integridad/confidencialidad/ disponibilidad
Servidor Fénix	Todos los activos dependen del servidor.	Si se compromete afectaría totalmente sistema académico.
Switch Mikro Tik	Todos los activos dependen del equipo para realizar la comunicación entre equipos.	Si se compromete afectaría la comunicación entre equipos y el sistema académico.
Firewall	Todos los activos dependen para la protección de los sistemas y equipos	Si se compromete afectaría totalmente sistema académico.
Cableado de red	Es importante para la trasmisión de información de una manera fluida rápida	
UPS	Todos los activos dependen del UPS para tener un respaldo de energía mínima	
Aire acondicionado	Todos los activos dependen para mantener el ambiente adecuado para los equipos	
Usuarios /contraseñas	Información necesaria para el acceso al sistema Fénix	Si se compromete afectaría totalmente a la información del sistema académico.
Información del sistema académico	Información necesaria que maneja el sistema Fénix	
Copia de seguridad del servidor	Importante para restaurar información desde un punto de partida	Si se compromete afectaría totalmente la información que se ha respaldado, perdiendo la información que maneja el sistema académico.

Nota. Valoración de activos de información 2024.

E. Identificación de amenazas y vulnerabilidades

Una vez identificados los activos y el sistema Fénix es esencial tener en cuenta la existencia de vulnerabilidades y amenazas, que pueden causar daño, a través de la explotación de las mismas. En el proceso se analizaron diversas fuentes de amenazas y vulnerabilidades, tanto externas como internas, que

Recibido: 2024-03-18, Aprobado tras revisión: 2024-08-22

incluyen ataques cibernéticos, malware, phishing, acceso no autorizado o mal uso de privilegios, entre otros. Identificar estas vulnerabilidades es fundamental para entender cómo las amenazas podrían comprometer la seguridad de los activos. Después de identificar las amenazas y vulnerabilidades, se estableció una base sólida para desarrollar estrategias de mitigación y protección. En la tabla 4, se muestra detalladamente la identificación de las amenazas y vulnerabilidades del sistema académico.

Tabla 3.

Identificación de amenazas y vulnerabilidades.

Identificación de amenazas y vulnerabilidades			**Afecta confidencialidad, integridad, disponibilidad**.
Activos	**Amenazas**	**Vulnerabilidades**	
Servidor Fénix	Ataques cibernéticos	Falta de actualizaciones en el sistema operativo	X
		Configuración errónea de software	X
	Indisponibilidades del servidor	Falta de mantenimiento en el servidor	X
Switch mikro Tik	Acceso a la red por personas no autorizadas.	Falta de políticas de contraseñas seguras	X
	Ataques cibernéticos	Configuración errónea de switch.	X
Firewall	Ataques cibernéticos	Firewall desactualizado /módulo ataques DDOS	X
Cableado de red	Interceptación de datos	Falta de control de acceso físico al gabinete de telecomunicaciones	X
	Acceso físico no autorizado a los gabinetes de telecomunicación	Control de accesos ineficientes	X
UPS	Indisponibilidad del servicio por falla eléctrica	Falta de mantenimiento en los equipos	X
Aire acondicionado	Indisponibilidades del servicio por sobrecalentamiento	Falta de mantenimiento en los equipos	X
Usuarios /contraseñas	Accesos no aterrizados	Sin políticas de contraseñas seguras, expuestos a ataques de cibernéticos	X
Información del sistema académico	Accesos no aterrizados	Falta de política de control de accesos	X

Recibido: 2024-03-18, Aprobado tras revisión: 2024-08-22

Copia de seguridad del servidor	Pérdida de datos del servidor fénix	Tiempo de backups muy extenso	X

Nota. Equipos y vulnerabilidades 2024.

Es importante destacar que, a pesar de la investigación realizada, no se encontraron indicios de ninguna propuesta o implementación de controles destinados a mitigar las amenazas identificadas. Esta ausencia de medidas preventivas puede tener implicaciones significativas en términos de seguridad y protección de los activos involucrados.

F. Evaluación de riesgo

El análisis de amenazas y vulnerabilidades implica la evaluación de la probabilidad y gravedad de eventos adversos, al explotar dicha vulnerabilidad, mediante el análisis respectivo. Para ello, se utiliza un sistema de valoración en el que se asocian diferentes valores a la probabilidad e impacto. La probabilidad puede ser baja, media o alta y se asignan valores de 1 a 3. El riesgo se calcula multiplicando la probabilidad de ocurrencia por el impacto, lo que proporciona una medida cuantitativa de la magnitud del riesgo y una base sólida para la gestión de riesgos.

$$\boldsymbol{RIESGO} = PROBABILIDAD\ DE\ OCURRENCIA\ \boldsymbol{x}\ IMPACTO$$

Es importante destacar que, este cálculo no es un proceso estático; este debe ser revisado periódicamente, a fin de asegurar que la evaluación del riesgo esté siempre actualizada. Las tablas 5 y 6 presentan los criterios elaborados para la evaluación de riesgos teniendo en cuenta la gravedad del daño y la probabilidad de ocurrencia de la amenaza.

Tabla 4.

Probabilidad de ocurrencia.

Probabilidad de que ocurra la amenaza		
Clasificación	**Descripción**	**Valor**
Baja	La probabilidad de que la amenaza permita explotar la vulnerabilidad es extremadamente baja.	1
Media	La probabilidad ocasional de que la amenaza permita explotar vulnerabilidades.	2
Alta	Probabilidad frecuente de que la amenaza permita explotar vulnerabilidades.	3

Nota. Clasificación de la probabilidad 2024.

Recibido: 2024-03-18, Aprobado tras revisión: 2024-08-22

Tabla 5.

Impacto si se materializa la amenaza

Impacto		
Clasificación	**Descripción**	**Valor**
Baja	El daño causado por la amenaza no tiene repercusiones significativas para la institución.	1
Media	El daño ocasionado por la amenaza tiene consecuencias significativas para la institución	2
Alta	El daño resultante de la amenaza tiene consecuencias graves para la institución.	3

Nota. Clasificación del impacto 2024.

G. Estimación del Riesgo

En la tabla 7, se indica que, a través del uso de la fórmula mencionada anteriormente es posible determinar la escala de valores asignados para la estimación del riesgo. A continuación, se presenta en la siguiente tabla un resumen del cálculo realizado.

Tabla 6.

Valoración de impacto

		Impacto		
		Bajo	Medio	Alto
Probabilidad de Ocurrencia	Baja	1 a 3 es Bajo	1 a 3 es Bajo	4 a 8 es Medio
	Medio	1 a 3 es Bajo	4 a 8 es Medio	9 a 27 es Alto
	Alto	4 a 8 es Medio	9 a 27 es Alto	28 más es Alto

Nota. Escala de valores asignados para la estimación del riesgo 2024.

H. Riesgos sobre los activos de información

Este proceso incluye la agrupación de los activos; todo esto se resume en la matriz de riesgos que se desarrolla para identificar el nivel de riesgo al que se encuentran expuestos los activos y permitir una mejor comprensión de los posibles impactos y toma de decisiones informadas para su gestión y protección

Recibido: 2024-03-18, Aprobado tras revisión: 2024-08-22

adecuada. Esta matriz es una herramienta visual que facilita la identificación y priorización de medidas de control y mitigación necesarias. En la tabla 8 presentada, se muestra la evaluación de riesgos y se determina de manera clara y efectiva el nivel de exposición de cada activo y establece estrategias de seguridad apropiadas para reducir los riesgos a niveles aceptables.

Tabla 7.

Evaluación de riesgos

Evaluación de riesgos				
Clasificación de activos	Tipo de activo	Nombre de Activo	Amenazas	Nivel de Riesgo
Infraestructura TIC	Servidor	Base de datos	Ataques cibernéticos	Alto
Información del sistema Fénix	Información	Información del Instituto	Falta de políticas de control de accesos	Alto
Equipos físicos	Equipos físicos	Firewall	Ataques cibernéticos	Alto

Nota. Nivel de riesgo al que se encuentran expuestos los activos 2024.

La evaluación determinó que todos los activos presentan un riesgo alto, lo cual puede afectar su disponibilidad, confiabilidad e integridad. Por lo que es crucial tomar medidas inmediatas para reducir y controlar estos riesgos, ya que esto indica una alta probabilidad de eventos adversos que tendrían consecuencias graves.

I. Plan de recuperación ante desastres.

RPO: El RPO (Objetivo del Punto de Recuperación) es la cantidad de datos que una empresa puede perder sin que afecte negativamente a su trabajo normal después de un desastre. Por lo tanto, se refiere a la antigüedad de los archivos recuperados y establece el tiempo máximo que una empresa puede permitirse perder sin afectar su flujo de trabajo (Crocetti, 2021).

RTO: El RTO (Objetivo de tiempo de recuperación) es el tiempo máximo que una empresa puede permitirse estar sin sus sistemas de tecnología después de un desastre o interrupción, sin graves consecuencias. En términos sencillos, es el tiempo que tarda una empresa en recuperarse después de un desastre para continuar con su trabajo normal (Mañas, 2022).

MTPD: El MTPD (Período máximo tolerable de interrupción) es el tiempo máximo en el que una empresa puede permitirse estar sin su sistema de tecnología, después de un desastre, sin que

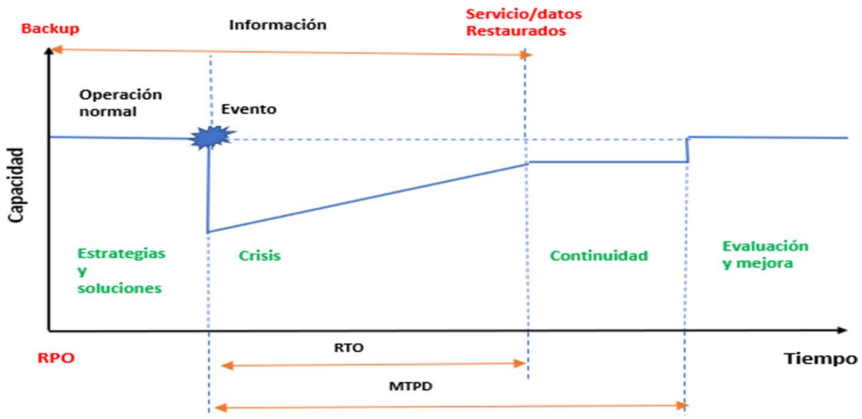
Recibido: 2024-03-18, Aprobado tras revisión: 2024-08-22

afecte gravemente su negocio.

En la Figura 2, se explica con exactitud los procesos de RPO, RTO y MTPD.

Figura 2

Procesos de RPO, RTO y MTPD.



Nota. Período máximo tolerable de interrupción. 2024

La identificación del RTO es crucial para garantizar una planificación y gestión adecuadas de los recursos y procesos relacionados con la recuperación del sistema académico Fénix, a fin de lograr una rápida y efectiva recuperación ante un evento disruptivo. En el anexo 6, se detalla el RTO, RTO y MTPD de este proyecto.

J. Impactos

Los impactos en un BCP son las consecuencias negativas que ocurren cuando se produce una interrupción no planificada en las operaciones de una empresa. Algunos de estos impactos pueden ser la pérdida de ingresos, el aumento de costos, el daño a la reputación de la empresa y la relación con los clientes; por ello, es importante considerar las medidas respectivas para minimizar estos impactos y garantizar que el negocio funcione sin problemas.

Una vez que se ha establecido el RTO y el RPO en el marco de una recuperación ante desastres del sistema académico, se evalúan los impactos asociados con las interrupciones imprevistas o ataques cibernéticos. Este análisis permitió desarrollar medidas específicas para garantizar la continuidad del negocio, minimizando los niveles de daño posibles y asegurando la estabilidad del TEC. AZUAY.

Recibido: 2024-03-18, Aprobado tras revisión: 2024-08-22

En las tablas 9 y 10, se presentan las áreas y valoración de los riesgos identificados que, de acuerdo a los niveles de impacto son los siguientes:

Tabla 8.

Nivel de impacto

Impacto	
Crítico	3
Moderado	2
Insignificante	1

Nota. Impactos asociados con las interrupciones imprevistas o ataques cibernéticos 2024.

Tabla 9.

Ponderación de impacto, con base en sus respectivas áreas:

Impactos	8 horas	1 día	3 días	5 días	1 semana	15 días	1 mes
Área de impacto							
Confidencialidad	1	1	2	3	3	3	3
Integridad	1	1	2	3	3	3	3
Disponibilidad	1	2	2	3	3	3	3
Legal	1	1	2	3	3	3	3
Imagen institucional	1	1	2	3	3	3	3
Total, impacto	1	1,2	2	3	3	3	3

Nota. Riesgos identificados, de acuerdo a los niveles de impacto 2024.

IV. RESULTADOS Y DISCUSIÓN

En esta sección, se ha propuesto una serie de políticas y controles de seguridad orientadas a garantizar una adecuada continuidad del negocio, reducir el riesgo de interrupción del servicio y proteger la integridad, disponibilidad y confidencialidad de la información contenida en el sistema.

Marco de políticas de seguridad de la información y continuidad del negocio

Recibido: 2024-03-18, Aprobado tras revisión: 2024-08-22

Tomando en cuenta la norma ISO 27002:2022, se presenta una propuesta para implementar un marco de políticas de seguridad de la información con el objetivo de mejorarla y asegurar la continuidad del sistema académico Fénix. Las mismas se describen a continuación en la tabla 10.

Tabla 10.

Marco de políticas de seguridad de información y continuidad del negocio.

Marco de políticas de seguridad de la información y continuidad del negocio

Referencia control	Política ISO 27002:2022	Detalle de la política a implementar
8.19	Instalación de software en sistemas operativos	**Política de instalación y actualización de sistemas** Mantener los sistemas operativos actualizados y parchados hasta su última actualización.
8.8	Gestión de las vulnerabilidades técnicas	**Política de configuración adecuada** Especificar, controlar y modificar la configuración por defecto de los sistemas informáticos.
8.9	Gestión de configuración.	
8.20	Seguridad de las redes	**Política de controles de seguridad** Solo los administradores podrán acceder a la configuración de equipos de red.
8.21	Seguridad de los servicios de red	
8.9	Información de autentificación	**Política para la autentificación** Implantar un control de acceso basado en un doble factor de autenticación en todos los sistemas que sean de gestión del TEC. AZUAY. **Política de contraseñas seguras** Las contraseñas deben tener una longitud mínima de 8 caracteres y es obligatorio incluir mayúsculas, minúsculas, caracteres especiales. Además, deben ser cambiadas con frecuencia.
7.13	Mantenimiento de los equipos	**Política de mantenimiento de equipos y software** Al inicio de año se deberá establecer un cronograma de mantenimientos preventivos para todos los equipos, los cuales deben ser planificados fuera de horario. **Política para mantenimiento correctivo** Implementar un SLA (Service Level Agreement) para el mantenimiento correctivo de todos los equipos; este SLA debe ser menor a 3 días.
8.7	Protección contra el malware	**Política de protección antimalware** Especificar, controlar y configurar herramientas de detección de malware.
8.13	Información de respaldo.	**Política para copias de seguridad** Los backups deben ser realizados en la fecha establecida y deben ser realizadas fuera de horario.
7.1	Perímetro de seguridad física	**Política de la seguridad física en las instalaciones** Contar con sistemas biométricos para el acceso de Data center.
7.2	Entrada Física	

Recibido: 2024-03-18, Aprobado tras revisión: 2024-08-22

6.3	Sensibilización, educación y formación en materia de seguridad de la información	**Política de capacitación y concientización de usuarios** Planificar las campañas de capacitación e información a los usuarios de forma trimestral para crear conciencia sobre la protección y preservación de la información institucional.
5.31	Requisitos legales, reglamentarios y contractuales	
5.33	Protección de los registros	**Política de privacidad y protección de la información** Implementar la política de protección de datos.
5.34	Privacidad y protección de la información personal	
5.29	Seguridad de la información durante la interrupción	**Política de seguridad durante una interrupción** Establecer un plan de continuidad de negocio para situaciones de emergencia y desastres.
5.30	Preparación de las TIC para la continuidad de la actividad	

Nota. Propuesta para implementar un marco de políticas de seguridad de la información. 2024.

Marco de controles de seguridad.

A continuación, se presenta una propuesta de controles que permiten asegurar el cumplimiento de las políticas, procesos y procedimientos definidos para la gestión de riesgos, lo que a su vez permite mantener la continuidad del negocio, en caso de incidentes o desastres.

Tabla 11.

Marco de controles para el cumplimiento de políticas.

Subprocesos	Activo	Amenazas	Vulnerabilidades	Controles
Infraestructura TIC	Servidor Fénix	Ataques cibernéticos	Falta de actualizaciones en el sistema operativo	Implementación de actualizaciones de software de manera automática o manualmente.
			Configuración errónea de software	Realizar pruebas de seguridad de la configuración del software.
		Indisponibilidad del servidor	Falta de mantenimiento en el servidor	Programar mantenimientos a los gabinetes de telecomunicación.
	Switch mikro Tik	Ataques cibernéticos	Configuración errónea de switch	Implementar políticas de contraseñas seguras en los equipos.
	Firewall	Ataques cibernéticos	Firewall desactualizado Módulo ataques DoS	Realizar pruebas de seguridad de la configuración del software Implementar un ambiente de pruebas para la verificación de la configuración del software

Recibido: 2024-03-18, Aprobado tras revisión: 2024-08-22

Información del sistema fénix	Cableado de red	Interceptación de datos	Falta de control de acceso físico al gabinete de telecomunicaciones	Implementación de actualizaciones de software manera automáticamente o manualmente
		Acceso físico no autorizado a los gabinetes de telecomunicación	Control de accesos ineficientes	Implementar controles de acceso físico a los gabinetes de telecomunicación.
	UPS	Indisponibilidad del servicio por falla eléctrica	Falta de mantenimiento en los equipos	
	Aire acondicionado	Indisponibilidad del servicio por sobrecalentamiento	Falta de mantenimiento en los equipos	Programar mantenimientos al centro de telecomunicación
	Usuarios y contraseñas	Accesos no autorizados	Sin políticas de contraseñas seguras, expuestos a ataques de cibernéticos	
	Información del sistema académico	Accesos no autorizados	Falta de políticas de control de accesos	Implementar políticas de contraseñas seguras para el sistema Fénix
	Copia de seguridad del servidor	Pérdida de datos del servidor fénix	Tiempo de backups muy extenso	
	Usuarios y contraseñas	Accesos no autorizados	Sin políticas de contraseñas seguras, expuestos a ataques de cibernéticos	Monitoreo y optimización continua de los backups

Nota. Controles que permiten asegurar el cumplimiento de las políticas 2024.

V. CONCLUSIONES

En conclusión, la implementación de un plan de continuidad de negocios para el sistema académico Fénix es fundamental para garantizar la disponibilidad, confidencialidad e integridad del sistema. A través de la realización de una evaluación de riesgos exhaustiva, se han identificado las posibles amenazas y vulnerabilidades que podrían afectar la continuidad del sistema, lo que ha permitido la adopción de estrategias y medidas de mitigación adecuadas para proteger la información.

Mediante el PHVA (Planificar-Hacer-Verificar-Actuar), se han identificado las áreas críticas y vulnerables de la institución, lo que ha facilitado el desarrollo de medidas específicas para mitigar los riesgos y fortalecer la seguridad del sistema académico Fénix. La evaluación de diferentes áreas de interrupción ha sido crucial para identificar la capacidad de recuperación del sistema, determinar los tiempos de recuperación necesarios y comprender los posibles impactos en la pérdida de información.

La definición de procedimientos y protocolos para la gestión de incidentes y emergencias deben implementarse para una respuesta eficiente ante cualquier situación que afecte el funcionamiento del

Recibido: 2024-03-18, Aprobado tras revisión: 2024-08-22

sistema académico Fénix. Además, la designación de responsabilidades claras y la comunicación efectiva con el personal académico han sido elementos clave en la elaboración exitosa del plan de continuidad.

El uso de las normas ISO 27001 y 22301 ha sido fundamental para definir la política y el alcance del plan de contingencia, proporcionando un marco de referencia reconocido internacionalmente y asegurando la adopción de las mejores prácticas en seguridad de la información. Esto ha demostrado un compromiso con la calidad y la excelencia en la protección de la información en el sistema académico Fénix.

VI. REFERENCIAS BIBLIOGRÁFICAS

Angulo, N., Encalada, J., & Bolaños, F. (febrero de 2020). *editorialibkn.* Obtenido de LA continuidad de negocio en las instituciones de educación: https://editorialibkn.com/index.php/yachasun/article/download/39/98/

bevan, t. (16 de octubre de 2020). *nqa.com.* obtenido de guía de implantación de la continuidad de negocio: https://www.nqa.com/medialibraries/nqa/nqa-media-library/pdfs/spanish%20qrfs%20and%20pdfs/nqa-iso-22301-guia-de-implantacion.pdf

chuqui, f., & orellana, d. (2023). análisis de las vulnerabilidades del sistema de información académica: caso de estudio instituto superior tecnológico del azuay. 140.

rosero, l., (2021). ataque que intenta robar su dinero o su identidad, haciendo que divulgue información persona. https://dspace.ups.edu.ec/bitstream/123456789/21699/4/ups-gt003573.pdf

conforme, c. (20 de noviembre de 2018). *repositorio.uisek.* obtenido de https://repositorio.uisek.edu.ec/bitstream/123456789/3222/1/proyecto-tesiscarlosconforme-act%20%281%29.pdf

crocetti, p. (28 de julio de 2021). *computerweekly.com.* obtenido de plan de recuperación de desastres o drp: https://www.computerweekly.com/es/definicion/plan-de-recuperacion-de-desastres-o-drp?_gl=1*19cjbpm*_ga*mtk2mjq3ntm2lje2odc4odq3mzu.*_ga_tqke4gs5p9*mty4nzg4ndcznc4xljeumty4nzg4ntazmy4wljauma..&_ga=2.268727286.625102833.1687884735-196247536.1687884735

ISO. (2018). *orestales.ujed.mx.* Obtenido de NORMA INTERNACIONAL ISO 3100: http://forestales.ujed.mx/succi/recursos/documento_29.pdf

Recibido: 2024-03-18, Aprobado tras revisión: 2024-08-22

ISO. (2022). *nqa.com.* Obtenido de NORMA INTERNACIONAL ISO 27001: https://www.nqa.com/getmedia/d6e32642-2bc6-4fe8-a7b8-e27054b3083c/Final-27001-Gap-Guide-ES.pdf

ISO. (24 de abril de 2023). *NORMA ISO 27001.* Obtenido de ISO 27001 SEGURIDAD DE LA INFORMACIÓN: https://normaiso27001.es/

ISO 223001. (2020). *nqa.com.* Obtenido de GUÍA IMPLEMENTACIÓN ISO 22301: https://www.nqa.com/es-es/certification/standards/iso-22301/implementation

Mañas, J. (abril de 2022). *PILAR – Continuidad del negocio.* Obtenido de https://www.ar-tools.com/doc/manual_bcm_es_20221.pdf

Martinez, C. (18 de junio de 2020). *linkedin.* Obtenido de Confidencialidad, integridad y disponibilidad: https://www.linkedin.com/pulse/confidencialidad-integridad-y-disponibilidad-martinez-ramirez/?originalSubdomain=es

NQA. (2020). *nqa.Organismos de Certificacion Global.* Obtenido de GUÍA IMPLEMENTACIÓN ISO 22301: https://www.nqa.com/es-ca/certification/standards/iso-22301/implementation

TEC. AZUAY. (s.f.). *tecazuay.edu.ec.* Obtenido de Mision Tec Azuay: https://www.tecazuay.edu.ec/main/instituto.php#mision

Recibido: 2024-03-18, Aprobado tras revisión: 2024-08-22