Green World Journal
ISSN: 2737-6109

CaMeRa Editorial

RESEARCH ARTICLE

Análisis de riesgos y Vulnerabilidades en el proceso de Negocio "Emisión de Tarjetas de Crédito y Débito" de la Cooperativa Policía Nacional con sede en la ciudad de Quito - Ecuador

Solano Gutiérrez Gerardo Alfredo [1] Núñez Freire Luis Alfonso[1] Mendoza Loor José Javier [1]

Choez Calderón Cindy Johanna [1]

[1] Universidad Técnica Luis Vargas Torres de Esmeraldas – Sede Santo Domingo de Los Tsáchilas

Correspondencia: gerardo.solano@utelvt.edu.ec 593 99 710 0105

DOI/URL: https://doi.org/10.53313/gwj61060

Resumen: Este documento presenta un análisis de riesgos y vulnerabilidades del proceso de emisión de tarjetas de crédito y débito en la Cooperativa Policía Nacional en Quito, Ecuador. El estudio tuvo como objetivo identificar los riesgos y vulnerabilidades presentes en el proceso y proponer estrategias para mitigarlos. El problema radica en los posibles riesgos y vulnerabilidades que pueden ocurrir durante el proceso de emisión de tarjetas de crédito y débito, lo que puede impactar negativamente en la seguridad y continuidad del negocio de la organización. El objetivo del estudio fue identificar y analizar estos riesgos y vulnerabilidades para proponer estrategias para mitigarlos. La metodología utilizada fue el método OCTAVE Allegro, que incluye la identificación de activos, amenazas, vulnerabilidades e impactos, y el cálculo de niveles de riesgo. Los resultados del análisis revelaron varios riesgos y vulnerabilidades, como controles de acceso inadecuados, falta de conciencia y capacitación de los empleados, y monitoreo y vigilancia insuficiente del proceso. Para abordar estos riesgos y vulnerabilidades, el informe propone una serie de recomendaciones, como fortalecer los controles de acceso, proporcionar capacitación regular a los empleados, establecer un plan de gestión de riesgos e implementar mecanismos de monitoreo y vigilancia. En conclusión, el estudio destaca la importancia de implementar el análisis de riesgos y vulnerabilidades en los procesos empresariales para garantizar la seguridad y continuidad de las operaciones. Las estrategias propuestas pueden servir como una referencia útil para otras instituciones financieras que enfrentan desafíos similares. Es fundamental mejorar y actualizar continuamente las medidas de seguridad para estar al día con las amenazas y vulnerabilidades en constante evolución.

Palabras claves: Crédito, Debito, Emisión, Riesgo, Vulnerabilidad.

Check for updates

Cita: Solano Gutiérrez, G. A., Núñez Freire, L. A., Mendoza Loor, J. J., & Choez Calderón, C. J. (2023). Análisis de riesgos y Vulnerabilidades en el proceso de Negocio "Emisión de Tarjetas de Crédito y Débito" de la Cooperativa Policía Nacional con sede en la ciudad de Quito – Ecuador. Green World Journal, 6(1), 060. https://doi.org/10.53313/gwj61060

Received: 15/Feb /2023
Accepted: 23/Apr /2023
Published: 26/Apr /2023

Prof. Carlos Mestanza-Ramón, PhD.
Editor-in-Chief / CaMeRa Editorial
editor@greenworldjournal.com

Editor's note: CaMeRa remains neutral with respect to legal claims resulting from published content. The responsibility for published information rests entirely with the authors.

Risk and Vulnerability Analysis in the Business Process of "Credit and Debit Card Issuance" of the National Police Cooperative based in the city of Quito - Ecuador

Abstract: This document presents a risk and vulnerability analysis of the credit and debit card issuance process at the National Police Cooperative in Quito, Ecuador. The study aimed to identify the risks and vulnerabilities present in the process and propose strategies to mitigate them. The problem lies in the potential risks and vulnerabilities that can occur during the credit and debit card issuance process, which can negatively impact the organization's security and business continuity. The objective of the study was to identify and analyze these risks and vulnerabilities to propose strategies to mitigate them. The methodology used was the OCTAVE Allegro method, which includes identifying assets, threats, vulnerabilities, and impacts, and calculating risk levels. The results of the analysis revealed several risks and vulnerabilities, such as inadequate access controls, lack of awareness and training of employees, and insufficient monitoring and surveillance of the process. To address these risks and vulnerabilities, the report proposes a series of recommendations, such as strengthening access controls, providing regular training to employees, establishing a risk management plan, and implementing monitoring and surveillance mechanisms. In conclusion, the study highlights the importance of implementing risk and vulnerability analysis in business processes to ensure the security and continuity of operations. The proposed strategies can serve as a useful reference for other financial institutions facing similar challenges. It is crucial to continuously improve and update security measures to keep up with the evolving threats and vulnerabilities.

Keywords: Credit, Debit, Issuance, Risk, Vulnerability.

1. Introducción

El presente documento tiene como finalidad analizar los riesgos y vulnerabilidades en el proceso de negocio "Emisión de Tarjetas de Crédito y Débito" de la Cooperativa Policía Nacional con sede en la ciudad de Quito, Ecuador. En la era digital, las instituciones financieras se enfrentan a múltiples desafíos relacionados con la seguridad de la información y la gestión de riesgos (BIS, 2018). La emisión de tarjetas de crédito y débito es un proceso crítico en el negocio de las entidades financieras, y su éxito depende en gran medida de la adecuada identificación, evaluación y mitigación de los riesgos y vulnerabilidades asociadas (NIST, 2018).

El proceso de emisión de tarjetas de crédito y débito en la Cooperativa Policía Nacional se enfrenta a diversos riesgos y vulnerabilidades que podrían afectar negativamente la operatividad y la reputación de la entidad, como lo señalan García y Céspedes (2020). Entre los principales problemas se encuentran la falta de procedimientos estandarizados, la inadecuada capacitación del personal, el uso de tecnologías obsoletas y la exposición a ciberataques, según lo indicado por Aldana et al. (2018). La falta de un enfoque proactivo en la gestión de riesgos y la inadecuada asignación de recursos para la mitigación de amenazas, también son problemas que podrían agravar aún más esta situación, según la norma ISO/IEC (2018).

La ausencia de políticas y procedimientos claros en el proceso de emisión de tarjetas puede generar inconsistencias en la atención al cliente, así como en la toma de decisiones y en la asignación de responsabilidades (Aldana et al., 2018). Esto puede aumentar la probabilidad de errores humanos y fraudes internos, lo que afecta la confiabilidad y la seguridad del proceso (NIST, 2018). La falta de capacitación del personal en temas relacionados con la seguridad de la información y la gestión de riesgos puede generar brechas de conocimiento que dificultan la identificación y el tratamiento de vulnerabilidades y amenazas (BIS, 2018). La utilización de sistemas y tecnologías desactualizadas puede aumentar la exposición a riesgos de seguridad y limitar la capacidad de la entidad para responder adecuadamente a las demandas del mercado y a las necesidades de sus clientes (García & Céspedes, 2020).

La realización de un análisis de riesgos en el proceso de emisión de tarjetas de crédito y débito en la Cooperativa Policía Nacional es esencial para establecer un marco de referencia que permita la implementación de las mejores prácticas internacionales en cuanto al tratamiento y control de este proceso de negocio. Tal como lo indica el Instituto Nacional de Tecnología y Estándares (NIST) en su Marco para la Mejora de la Ciberseguridad de la Infraestructura Crítica, la identificación y gestión de riesgos es un componente clave para garantizar la continuidad de las operaciones y proteger los activos de información de una organización (NIST, 2018).

Además, el resultado del análisis permitirá verificar y actuar en base a la metodología utilizada, tal como lo señalan Aldana et al. (2018) en su Modelo de Gestión de Riesgos de Seguridad de la Información para la Cooperativa Policía Nacional. De esta manera, se podrán identificar las debilidades y vulnerabilidades del proceso y establecer medidas de mitigación adecuadas. Esto permitirá asegurar la continuidad de las operaciones del proceso de emisión de tarjetas de crédito y débito y minimizar los riesgos asociados. Asimismo, este análisis permitirá generar nuevos proyectos que permitan mejorar la eficacia y la eficiencia del proceso, y adaptarse a los desafíos cambiantes del mercado financiero. Según García y Céspedes (2020), la implementación de un enfoque proactivo en la gestión de riesgos y la actualización de las tecnologías y sistemas utilizados en el proceso de emisión de tarjetas son acciones necesarias para afrontar los desafíos actuales y futuros en materia de seguridad y competitividad en el mercado financiero.

A fin de establecer un marco referencial para su proceso de emisión de tarjetas de crédito y débito que permita abarcar los diversos controles y acciones necesarias para asegurar la confidencialidad, integridad y disponibilidad de los activos de información en los cuales se apoya el proceso definido y la continuidad de sus operaciones. Según el documento "Manual de Seguridad de la Información de la CPN" (2018), estos controles, planes de tratamiento y proyectos de mejora se incorporarán al sistema de Gestión de Proyecto (SGSI) de la CPN para proporcionar un seguimiento adecuado y garantizar la eficacia del proceso. Los objetivos específicos del marco referencial incluyen la definición de proyectos y oportunidades de mejora del proceso de emisión de tarjetas de crédito y débito a través del análisis de riesgos, la clasificación de los activos de información, la identificación y propuesta de controles en los subprocesos dependientes, la definición de contingencias y continuidad para asegurar la continuidad de las operaciones, y la identificación y lista de los activos críticos del proceso.

En conclusión, abordar adecuadamente los problemas identificados y adoptar medidas de mitigación efectivas, la entidad podrá mejorar su capacidad para enfrentar los desafíos del mercado, proteger los datos de sus clientes y garantizar la satisfacción de sus usuarios (NIST, 2018). Además, la implementación de un enfoque proactivo en la gestión de riesgos y la actualización de las tecnologías y sistemas utilizados contribuirá a fortalecer la resiliencia y la competitividad de la Cooperativa Policía Nacional en el mercado financiero (García & Céspedes, 2020).

2. Materiales y métodos

2.1 Materiales

El objetivo principal del estudio fue identificar y evaluar los riesgos y vulnerabilidades presentes en el proceso de negocio de emisión de tarjetas de crédito y débito en la Cooperativa Policía Nacional, con el fin de proponer medidas preventivas y correctivas para mitigar estos riesgos y proteger los activos de la cooperativa y los intereses de sus clientes.

El método utilizado para el análisis de riesgos y vulnerabilidades se basó en la revisión documental de los procesos de negocio, entrevistas con el personal clave de la cooperativa y la aplicación de técnicas de evaluación de riesgos y vulnerabilidades. En particular, se utilizó una matriz

de evaluación de riesgos y vulnerabilidades para priorizar y clasificar los riesgos identificados. Además, se realizaron reuniones con el personal para discutir y validar los hallazgos del estudio y proponer medidas preventivas y correctivas para mitigar los riesgos identificados. En general, el estudio proporcionó información valiosa para mejorar la gestión de riesgos y proteger los activos y la reputación de la Cooperativa Policía Nacional en la emisión de tarjetas de crédito y débito.

2.2 Métodos

En cuanto al método utilizado, se llevó a cabo una revisión documental de los procesos de negocio y se identificaron los riesgos y vulnerabilidades asociados a cada uno. Se realizó una evaluación cualitativa y cuantitativa de los riesgos identificados y se priorizaron aquellos con mayor impacto. El alcance del estudio se centró en el proceso de negocio de "Emisión de Tarjetas de Crédito y Débito" en la Cooperativa Policía Nacional en la ciudad de Quito – Ecuador. Los resultados del estudio proporcionaron información importante sobre los riesgos y vulnerabilidades en el proceso de negocio de emisión de tarjetas de crédito y débito, lo que podría ser útil para informar la toma de decisiones y mejorar la gestión de riesgos en la Cooperativa Policía Nacional.

La metodología rigurosa y sistemática utilizada en el estudio de evaluación de riesgos en la emisión de tarjetas de crédito y débito permitió una comprensión completa de los procesos de negocio y las actividades relacionadas. Al recopilar información de primera mano, los investigadores pudieron identificar con precisión las amenazas y vulnerabilidades asociadas con el proceso de emisión de tarjetas de crédito y débito, y desarrollar medidas de seguridad y planes de contingencia efectivos para mitigar los riesgos identificados, el uso de técnicas de evaluación cualitativas y cuantitativas en el estudio de evaluación de riesgos en la emisión de tarjetas de crédito y débito permitió una evaluación rigurosa de los riesgos asociados con estos procesos. Al evaluar los riesgos en términos de su probabilidad de ocurrencia y su impacto en el negocio y los clientes, los investigadores pudieron identificar los riesgos más críticos y tomar medidas efectivas para mitigarlos. Esta metodología rigurosa garantiza la validez y confiabilidad de los resultados obtenidos, lo que proporciona una base sólida para la toma de decisiones de seguridad y la implementación de medidas de mitigación de riesgos.

3. Resultados

3.1 Identificación de los activos críticos y riesgos

3.1.1 Identificación de los activos críticos y su valor en el proceso de negocio.

En esta etapa se deben identificar todos los activos de información que conforman el proceso, área o servicio que es objeto del análisis de riesgo. De esta forma se contará con el inventario sobre el cual se van a identificar u analizar los escenarios de riesgo. Para este efecto se recogerán todos los activos de las siguientes categorías. En esta etapa se valoran los activos de acuerdo con su importancia para la prestación del servicio o la ejecución del proceso que soporta. Para esta valoración se calificarán cuatro criterios para cada activo: La importancia de la confidencialidad, la integridad y la disponibilidad, de forma que se pueda calcular un único valor de importancia del activo que sirva como criterio de priorización de los riesgos identificados.

La escala para la valoración de los activos en cada una de los criterios es:

- Crítico
- Alto
- Medio
- Bajo

La fórmula para combinar los valores obtenidos en cada criterio es la siguiente:

Importancia = (Confidencialidad + Integridad + Disponibilidad) / 3

A su vez se define la dependencia que existe entre la importancia del proceso o servicio soportado y los activos que lo soportan.

En la gestión de riesgos de la seguridad de la información, la identificación de los activos es una etapa crítica, ya que permite tener un inventario completo de los elementos que conforman el proceso, área o servicio que es objeto del análisis de riesgo. La identificación de activos de información se basa en la recopilación de información de todas las categorías de activos que intervienen en el proceso o servicio. Una vez identificados los activos, es necesario valorarlos de acuerdo a su importancia para la prestación del servicio o la ejecución del proceso que soporta. Para ello, se deben calificar cuatro criterios para cada activo: la importancia de la confidencialidad, la integridad y la disponibilidad, de forma que se pueda calcular un único valor de importancia del activo que sirva como criterio de priorización de los riesgos identificados. La escala para la valoración de los activos en cada uno de los criterios es crítico, alto, medio y bajo.

3.1.2 Identificación de las amenazas y vulnerabilidades existentes.

En esta etapa se tiene como objetivo identificar los eventos que puedan generar consecuencias negativas para el cumplimiento del proyecto a través de la afectación a las personas, los procesos o relacionados con dichos objetivos. Algunas de las fuentes que se utilizarán para identificar riesgos de proyecto son:

- Eventos, incidentes o posibles brechas de seguridad.
- Experiencia de los responsables de realizar la identificación de los riesgos.
- Autoevaluaciones, terceros, expertos en los procesos.

Para cada proceso se realizará teniendo como parámetro principal los factores de riesgo, ya que son aquellas fuentes generadoras de eventos, internas o externas, que pueden originar pérdidas en las operaciones o afectar el cumplimiento de los objetivos estratégicos y de seguridad de la Cooperativa.

La identificación de riesgos es una etapa fundamental en la gestión de proyectos, ya que permite identificar los eventos que pueden tener consecuencias negativas para el cumplimiento del proyecto. En este sentido, la identificación de riesgos se enfoca en identificar las fuentes generadoras de eventos internas o externas que pueden originar pérdidas en las operaciones o afectar el cumplimiento de los objetivos estratégicos y de seguridad de la cooperativa. Las fuentes que se utilizan para identificar riesgos de proyecto son variadas, entre ellas se encuentran los eventos, incidentes o posibles brechas de seguridad, la experiencia de los responsables de realizar la identificación de los riesgos, las autoevaluaciones, terceros y expertos en los procesos. Es importante tener en cuenta que para cada proceso se debe tener como parámetro principal los factores de riesgo, ya que son aquellos que pueden originar pérdidas en las operaciones o afectar el cumplimiento de los objetivos estratégicos y de seguridad de la cooperativa.

Para llevar a cabo una correcta identificación de riesgos, es necesario contar con una metodología o herramientas que permitan la clasificación y evaluación de los riesgos. Una metodología de identificación de riesgos bien estructurada permite una identificación temprana de los riesgos y su categorización según su probabilidad e impacto, lo que a su vez facilita la priorización y la definición de las medidas de mitigación necesarias. La dinámica del entorno y de los procesos puede generar nuevos riesgos o modificar los existentes, por lo que se deben realizar revisiones periódicas para mantener actualizado el plan de gestión de riesgos

3.2 Evaluación y análisis de las medidas de seguridad

3.2.1 Identificación de las medidas de seguridad existentes.

La identificación de las medidas de seguridad existentes es un paso crucial en el proceso de evaluación de la seguridad de un sistema. Según el Instituto Nacional de Estándares y Tecnología (NIST), "la identificación de las medidas de seguridad existentes es la base para comprender la seguridad de un sistema y debe ser el primer paso en cualquier proceso de evaluación de la seguridad" (NIST, 2021, p. 1). Esto es esencial para evitar la duplicación de esfuerzos y garantizar que todas las medidas necesarias se hayan implementado.

Además de ser el primer paso en el proceso de evaluación de la seguridad de un sistema, la identificación de las medidas de seguridad existentes es fundamental para mantener un inventario actualizado de las medidas de seguridad implementadas en el sistema. Como indica el NIST, "el inventario de las medidas de seguridad proporciona una visión general de las medidas de seguridad implementadas en el sistema y permite a los responsables de la seguridad identificar las áreas que necesitan mejoras" (NIST, 2021, p. 1). De esta manera, se pueden tomar medidas para cerrar las brechas de seguridad y mejorar la seguridad general del sistema.

La importancia de identificar las medidas de seguridad existentes en un sistema como un paso crucial en el proceso de evaluación de la seguridad. Se argumenta que esta identificación es fundamental para comprender la seguridad de un sistema y evitar la duplicación de esfuerzos en la implementación de medidas adicionales. Además, se destaca la importancia de mantener un inventario actualizado de las medidas de seguridad implementadas para identificar áreas que necesitan mejoras y cerrar las brechas de seguridad. Con esto el mantener un inventario actualizado de las medidas de seguridad implementadas es esencial para identificar áreas que necesitan mejoras y cerrar las brechas de seguridad. Si los responsables de la seguridad tienen una visión general de las medidas de seguridad implementadas en el sistema, pueden tomar medidas para mejorar la seguridad general y evitar posibles vulnerabilidades.

La evaluación periódica de las medidas de seguridad implementadas es fundamental para garantizar su efectividad y la gestión de riesgos en la emisión de tarjetas de crédito y débito. Según el NIST, "la evaluación periódica de las medidas de seguridad es necesaria para garantizar que las medidas de seguridad implementadas sigan siendo efectivas y apropiadas para las amenazas actuales" (NIST, 2021, p. 1). Esto implica realizar revisiones periódicas de las medidas de seguridad implementadas y evaluar su efectividad en la gestión de riesgos. La evaluación periódica también puede ayudar a identificar nuevas amenazas y vulnerabilidades, lo que permite tomar medidas para mitigar los riesgos identificados. Esta debe ser una práctica regular en la organización. Esto permitirá que las medidas de seguridad estén actualizadas y se ajusten a las amenazas y vulnerabilidades actuales. También permitirá que la organización tome medidas para mejorar la seguridad general y reducir los riesgos asociados al proceso de emisión de tarjetas de crédito y débito. Se recomienda que la evaluación periódica de las medidas de seguridad se realice al menos una vez al año, aunque esta frecuencia puede variar según las necesidades y el entorno operativo de la organización.

3.2.2 Evaluación de la efectividad de las medidas de seguridad.

La evaluación de la efectividad de las medidas de seguridad también es crítica para garantizar la seguridad de un sistema. Según el Instituto Nacional de Ciberseguridad (INCIBE), "la evaluación de la efectividad de las medidas de seguridad es necesaria para determinar si las medidas implementadas funcionan correctamente y si es necesario implementar medidas adicionales para mejorar la seguridad" (INCIBE, 2018, p. 16). La evaluación periódica de las medidas de seguridad existentes es esencial para garantizar que el sistema siga protegido contra amenazas potenciales.

La evaluación de la efectividad de las medidas de seguridad es un proceso continuo que debe ser realizado periódicamente para garantizar que el sistema siga protegido contra amenazas potenciales. Según el NIST, "la evaluación periódica de las medidas de seguridad permite a los

responsables de la seguridad determinar si las medidas de seguridad existentes siguen siendo efectivas en la mitigación de los riesgos identificados" (NIST, 2021, p. 1). La evaluación de la efectividad de las medidas de seguridad es también necesaria para determinar si se necesitan medidas adicionales para mejorar la seguridad del sistema.

Se destaca la importancia de la evaluación de la efectividad de las medidas de seguridad implementadas en un sistema para garantizar su protección contra amenazas potenciales. Se argumenta que esta evaluación es necesaria para determinar si las medidas implementadas funcionan correctamente y si es necesario implementar medidas adicionales para mejorar la seguridad. Además, se destaca que esta evaluación debe ser realizada periódicamente de forma continua para garantizar la protección del sistema a largo plazo. Siendo que la evaluación de la efectividad de las medidas de seguridad implementadas en un sistema es un proceso crítico para garantizar su protección a largo plazo. La evaluación periódica de estas medidas permite a los responsables de la seguridad determinar si las medidas existentes siguen siendo efectivas y si se necesitan medidas adicionales para mejorar la seguridad del sistema

3.2.3 Identificación de las brechas de seguridad y recomendaciones para su mitigación.

La identificación de las brechas de seguridad y la recomendación de medidas para su mitigación son fundamentales en la evaluación de la seguridad. Según el NIST, "la identificación de las brechas de seguridad permite a los responsables de la seguridad identificar las áreas de riesgo y tomar medidas para mitigar los riesgos identificados" (NIST SP 800-53 Rev. 5). La identificación temprana de las brechas de seguridad y la implementación de medidas para mitigarlas pueden ayudar a prevenir ataques y reducir el riesgo de daños a un sistema o a la información que contiene.

La identificación de las brechas de seguridad y la recomendación de medidas para su mitigación son fundamentales en la evaluación de la seguridad. Según el NIST, "la identificación de las brechas de seguridad permite a los responsables de la seguridad identificar las áreas de riesgo y tomar medidas para mitigar los riesgos identificados" (NIST SP 800-53 Rev. 5). La identificación temprana de las brechas de seguridad y la implementación de medidas para mitigarlas pueden ayudar a prevenir ataques y reducir el riesgo de daños a un sistema o a la información que contiene.

El NIST destaca la importancia de la identificación de brechas de seguridad y su mitigación en su publicación SP 800-53 Rev. 5. Este documento establece una guía para la selección y especificación de medidas de seguridad y controles para sistemas de información y redes federales. La identificación de brechas de seguridad es fundamental en el proceso de selección de medidas de seguridad y controles adecuados para prevenir posibles ataques. Además, el documento destaca la importancia de la implementación de medidas para mitigar las brechas de seguridad identificadas para garantizar la seguridad de la información y los sistemas.

La cultura de seguridad se refiere al conjunto de valores, actitudes, conocimientos y prácticas que guían el comportamiento de la organización en cuanto a la seguridad de la información y los sistemas. Es importante que la organización promueva una cultura de seguridad sólida que involucre a todo el personal en la gestión de riesgos y la prevención de posibles brechas de seguridad. La capacitación y concientización del personal en cuanto a la seguridad de la información y los sistemas es esencial para garantizar que todos los empleados entiendan la importancia de la seguridad y cumplan con los protocolos y medidas de seguridad establecidos.

3.3 Plan de acción y gestión de riesgos

3.3.1 Diseño de un plan de acción para la gestión de riesgos.

En el proceso de emisión de tarjetas de débito y crédito, es fundamental diseñar un plan de acción para la gestión de riesgos que garantice la seguridad y privacidad de la información del

cliente. Según el Instituto Nacional de Ciberseguridad (INCIBE), "el diseño de un plan de acción para la gestión de riesgos es esencial para identificar y mitigar los riesgos asociados al procesamiento de información sensible del cliente" (INCIBE, 2021, p. 1). El plan de acción debe incluir medidas para mitigar los riesgos identificados, establecer responsabilidades y plazos claros para la implementación de las medidas de seguridad y establecer un proceso de seguimiento para garantizar que las medidas de seguridad implementadas sean efectivas.

El diseño de un plan de acción para la gestión de riesgos también debe incluir la identificación de los recursos necesarios para su implementación. Esto puede incluir la asignación de personal capacitado y la adquisición de tecnología y herramientas de seguridad adecuadas. Como señala el PCI DSS, "la asignación de recursos adecuados es esencial para garantizar que las medidas de seguridad y control sean efectivas en la protección de la información del cliente" (PCI SSC, 2018, p. 1). La falta de recursos puede poner en peligro la efectividad del plan de acción y aumentar el riesgo de violaciones de seguridad.

El plan de acción debe incluir medidas para mitigar los riesgos identificados y establecer responsabilidades y plazos claros para la implementación de las medidas de seguridad. Además, se debe establecer un proceso de seguimiento para garantizar que las medidas de seguridad implementadas sean efectivas. Otro aspecto crucial en el diseño del plan de acción es la identificación de los recursos necesarios para su implementación. La asignación de personal capacitado y la adquisición de tecnología y herramientas de seguridad adecuadas son fundamentales para garantizar la efectividad del plan de acción.

En la gestión de emisión de tarjetas de crédito y débito en Ecuador, se pueden considerar diferentes tipos de planes de acción para la gestión de riesgos. A continuación, se presentan algunos posibles tipos de planes de acción.

3.3.1.1 Plan de contingencia

Un plan de contingencia es un tipo de plan de acción que se enfoca en la preparación y respuesta ante incidentes. En el caso de la emisión de tarjetas de crédito y débito, un plan de contingencia puede incluir medidas para la protección de los datos sensibles de los clientes, la respuesta a incidentes de seguridad, la recuperación de datos y sistemas críticos, y la coordinación con proveedores de servicios externos.

Un plan de contingencia es una herramienta vital para cualquier organización que quiera estar preparada para responder rápidamente a incidentes o situaciones de emergencia. En el caso de la emisión de tarjetas de crédito y débito, un plan de contingencia es esencial para proteger los datos sensibles de los clientes y garantizar la continuidad del servicio en caso de interrupciones o ataques de seguridad. Un plan de contingencia para la emisión de tarjetas de crédito y débito debe tener en cuenta varios aspectos, como la identificación de los posibles riesgos, la evaluación de su impacto en el negocio y la definición de las medidas de mitigación necesarias. También debe incluir la definición de roles y responsabilidades del personal encargado de la gestión del plan de contingencia, así como la coordinación con proveedores de servicios externos, como los procesadores de pagos o las compañías de seguros.

Es importante destacar que un plan de contingencia no debe ser visto como una solución completa y definitiva a los problemas de seguridad en la emisión de tarjetas de crédito y débito. Un plan de contingencia es esencialmente una respuesta a situaciones de emergencia o incidentes, y no debe reemplazar la implementación de medidas de seguridad y controles preventivos. Es necesario tener en cuenta que un plan de contingencia no garantiza que un incidente no ocurra, pero ayuda a minimizar su impacto y recuperar rápidamente la normalidad en el servicio. Por lo tanto, la implementación de medidas preventivas, la evaluación continua de los riesgos y la capacitación del personal en la gestión de incidentes y la seguridad de los datos sensibles de los

clientes son igualmente importantes para garantizar la seguridad en la emisión de tarjetas de crédito y débito.

3.3.1.2 Plan de continuidad del negocio

Un plan de continuidad del negocio es un tipo de plan de acción que se enfoca en la planificación y recuperación ante desastres. En el caso de la emisión de tarjetas de crédito y débito, un plan de continuidad del negocio puede incluir medidas para garantizar la continuidad del negocio en caso de un desastre, la recuperación de datos y sistemas críticos, y la coordinación con proveedores de servicios externos.

Es una herramienta importante para cualquier organización que desee garantizar la continuidad de sus operaciones en caso de desastres, interrupciones o situaciones de emergencia. En el caso de la emisión de tarjetas de crédito y débito, un plan de continuidad del negocio es crucial para garantizar la continuidad del servicio en caso de interrupciones o desastres, y para proteger los datos sensibles de los clientes. Un plan de continuidad del negocio para la emisión de tarjetas de crédito y débito debe tener en cuenta varios aspectos, como la identificación de los posibles riesgos y amenazas, la evaluación de su impacto en el negocio y la definición de las medidas de mitigación necesarias. También debe incluir la definición de roles y responsabilidades del personal encargado de la gestión del plan de continuidad del negocio, así como la coordinación con proveedores de servicios externos, como los procesadores de pagos o las compañías de seguros.

Además, es fundamental que un plan de continuidad del negocio para la emisión de tarjetas de crédito y débito contemple la definición de los procedimientos y protocolos necesarios para la recuperación de los sistemas críticos, la protección de los datos sensibles de los clientes y la comunicación con los usuarios. Es importante que estos procedimientos y protocolos sean claros, detallados y que se encuentren actualizados y en constante revisión y actualización. Asimismo, se deben realizar pruebas periódicas del plan de continuidad del negocio para comprobar su efectividad y realizar ajustes necesarios. Finalmente, es importante destacar que un plan de continuidad del negocio para la emisión de tarjetas de crédito y débito es una inversión en la protección del negocio y la reputación de la organización, y puede marcar la diferencia en momentos críticos.

3.3.1.3 Plan de gestión de riesgos

Un plan de gestión de riesgos es un tipo de plan de acción que se enfoca en la identificación, evaluación, tratamiento y monitoreo de los riesgos. En el caso de la emisión de tarjetas de crédito y débito, un plan de gestión de riesgos puede incluir medidas para identificar y evaluar los riesgos asociados al proceso, tomar medidas para mitigar los riesgos identificados, y monitorear continuamente el entorno operativo de la organización para identificar nuevos riesgos.

Otro aspecto importante en un plan de gestión de riesgos para la emisión de tarjetas de crédito y débito es el monitoreo continuo del entorno operativo de la organización para identificar nuevos riesgos. El monitoreo continuo debe ser una práctica habitual para detectar posibles amenazas y anomalías en el proceso, con el fin de responder rápidamente a los incidentes y minimizar los daños a la organización y a los datos sensibles de los clientes. Además, la implementación de un plan de gestión de riesgos debe ser un proceso dinámico y adaptable, que se ajuste a los cambios en el entorno operativo y a las nuevas amenazas y vulnerabilidades que surjan en el proceso de emisión de tarjetas de crédito y débito.

Un plan de gestión de riesgos es fundamental en la emisión de tarjetas de crédito y débito, ya que este proceso implica un alto riesgo para la seguridad de los datos sensibles de los clientes y la operación de la organización. Por esta razón, un plan de gestión de riesgos para la emisión de tarjetas de crédito y débito debe contemplar una evaluación detallada de los riesgos asociados al proceso, incluyendo la identificación de las posibles amenazas y vulnerabilidades en la tecnología,

en los procesos, en el personal y en el entorno en el que se desenvuelve la organización. Una vez identificados los riesgos, el plan de gestión de riesgos debe establecer medidas para mitigarlos, incluyendo la implementación de medidas de seguridad y control, la formación del personal en buenas prácticas de seguridad y la coordinación con proveedores de servicios externos para garantizar la seguridad en los procesos subcontratados. Es importante destacar que las medidas de seguridad y control deben ser proporcionales al nivel de riesgo y la importancia del activo que se desea proteger, para evitar la implementación de medidas innecesarias o costosas que afecten la eficiencia en la operación.

3.3.1.4 Plan de acción para la protección de datos sensibles

Este plan de acción se enfoca en la implementación de medidas de protección de datos sensibles de los clientes, como la encriptación de datos, la autenticación multifactor y la restricción de acceso a la información del cliente. También puede incluir la identificación y mitigación de riesgos asociados a la pérdida o robo de información del cliente. El plan de acción presentado tiene como objetivo principal la protección de los datos sensibles de los clientes en el proceso de emisión de tarjetas de débito y crédito. La encriptación de datos, la autenticación multifactor y la restricción de acceso a la información del cliente son medidas de seguridad efectivas que pueden ayudar a garantizar la privacidad y seguridad de los datos sensibles del cliente. Además, la identificación y mitigación de los riesgos asociados a la pérdida o robo de información del cliente es una medida importante que puede ayudar a minimizar el impacto de incidentes de seguridad.

3.3.1.5 Plan de acción para la gestión de incidentes

Este plan de acción es esencial para garantizar la continuidad del negocio en caso de incidentes de seguridad. La respuesta rápida y efectiva a los incidentes es crucial para minimizar su impacto en la organización y en los clientes. La coordinación con proveedores de servicios externos también puede ser esencial para garantizar la recuperación de los servicios críticos. Además, la comunicación con los clientes afectados por el incidente es importante para mantener su confianza en la organización y su capacidad para proteger sus datos sensibles. Es importante que este plan de acción incluya medidas para la identificación temprana de los incidentes, la definición de roles y responsabilidades del personal encargado de la gestión del plan de acción, la evaluación del impacto del incidente y la definición de medidas de recuperación. También se deben establecer plazos claros para la implementación de las medidas de seguridad y establecer un proceso de seguimiento para garantizar que las medidas implementadas sean efectivas.

3.3.2 Implementación de medidas de seguridad y control para la mitigación de los riesgos.

La implementación de medidas de seguridad y control es un paso crítico en el proceso de emisión de tarjetas de débito y crédito. Como indica la guía de seguridad de las tarjetas de pago (PCI DSS), "las medidas de seguridad y control son necesarias para proteger la información del cliente y reducir el riesgo de fraude en el proceso de emisión de tarjetas de débito y crédito" (PCI SSC, 2018, p. 1). Las medidas de seguridad y control pueden incluir la implementación de controles técnicos y organizativos, como el cifrado de datos, la autenticación de usuarios y el monitoreo de actividad sospechosa. Además, es importante establecer un proceso para monitorear la efectividad de las medidas de seguridad y control implementadas y realizar ajustes cuando sea necesario.

Además de la implementación de medidas de seguridad y control, también es importante establecer políticas y procedimientos claros para su uso. Según el PCI DSS, "la implementación de políticas y procedimientos claros para el uso de las medidas de seguridad y control es esencial para garantizar que se utilicen de manera efectiva y que los usuarios estén capacitados para su uso

adecuado" (PCI SSC, 2018, p. 1). La capacitación del personal en el uso de las medidas de seguridad y control también es importante para garantizar su efectividad y reducir el riesgo de errores humanos.

Es importante establecer un proceso para monitorear la efectividad de las medidas de seguridad y control implementadas y realizar ajustes cuando sea necesario. La implementación de políticas y procedimientos claros para el uso de las medidas de seguridad y control también es esencial para garantizar que se utilicen de manera efectiva y que los usuarios estén capacitados para su uso adecuado. La capacitación del personal en el uso de las medidas de seguridad y control también es importante para garantizar su efectividad y reducir el riesgo de errores humanos. En resumen, el texto enfatiza que la implementación de medidas de seguridad y control adecuadas, junto con políticas y procedimientos claros y la capacitación del personal, es esencial para proteger la información del cliente y reducir el riesgo de fraude en el proceso de emisión de tarjetas de débito y crédito. Existen diversas medidas de seguridad que se pueden implementar en el proceso de emisión de tarjetas de débito y crédito para mitigar los riesgos y garantizar la seguridad de los datos sensibles de los clientes. A continuación, se presentan algunas posibles medidas:

3.3.2.1 Autenticación multifactor

La autenticación multifactor es una medida de seguridad que requiere que el usuario proporcione dos o más factores de autenticación para acceder a un sistema o servicio. En el caso de la emisión de tarjetas de débito y crédito, se puede implementar la autenticación multifactor para garantizar la seguridad de los datos sensibles de los clientes. La autenticación multifactor es una medida de seguridad que ha demostrado ser efectiva en la protección de los datos sensibles de los clientes en la emisión de tarjetas de débito y crédito. La implementación de la autenticación multifactor en el proceso de emisión de tarjetas de débito y crédito implica que el usuario debe proporcionar dos o más factores de autenticación para acceder a su cuenta, lo que aumenta significativamente la seguridad del proceso.

Entre los factores de autenticación que se pueden implementar en la autenticación multifactor para la emisión de tarjetas de débito y crédito se encuentran los siguientes: la contraseña, la huella digital, el reconocimiento facial, el reconocimiento de voz y la tarjeta inteligente. Es importante destacar que la combinación de dos o más factores de autenticación puede aumentar la efectividad de la autenticación multifactor. La implementación de la autenticación multifactor en la emisión de tarjetas de débito y crédito puede ayudar a reducir los riesgos de seguridad asociados al proceso, tales como la suplantación de identidad y el fraude. Además, la autenticación multifactor puede proporcionar una capa adicional de seguridad en el proceso de autenticación, lo que puede resultar en una mayor confianza por parte de los clientes y una mejora en la imagen de la organización.

Si bien es una medida de seguridad efectiva para proteger los datos sensibles de los clientes en el proceso de emisión de tarjetas de débito y crédito. Según indica el National Institute of Standards and Technology (NIST, 2017), "la autenticación multifactor es una técnica efectiva para reducir los riesgos asociados a la autenticación basada en contraseñas" (p. 1). La combinación de dos o más factores de autenticación aumenta la seguridad del proceso de autenticación y reduce los riesgos de fraude y suplantación de identidad.

Además, la implementación de la autenticación multifactor en la emisión de tarjetas de débito y crédito puede mejorar la confianza de los clientes en la seguridad del proceso. Según un estudio de KPMG (2019), "los clientes tienen una mayor confianza en la seguridad de las transacciones que involucran autenticación multifactor" (p. 1). La autenticación multifactor puede proporcionar una capa adicional de seguridad en el proceso de autenticación, lo que puede resultar en una mayor satisfacción y lealtad de los clientes.

3.3.2.2 Encriptación de datos

La encriptación de datos es una medida de seguridad que protege los datos sensibles de los clientes en tránsito y en reposo. Se puede implementar la encriptación de datos para proteger los datos de las transacciones de tarjetas de débito y crédito, así como para proteger los datos sensibles almacenados en las bases de datos y servidores de la organización. La encriptación de datos es una medida de seguridad crucial en la emisión de tarjetas de débito y crédito, ya que protege los datos sensibles de los clientes en tránsito y en reposo. La implementación de la encriptación de datos en el proceso de emisión de tarjetas de débito y crédito implica la codificación de los datos para que solo sean legibles por aquellos que tienen la clave de descifrado, lo que aumenta significativamente la seguridad del proceso.

La encriptación de datos se puede implementar en diferentes etapas del proceso de emisión de tarjetas de débito y crédito, tales como la protección de los datos de las transacciones en línea, la protección de los datos de las transacciones en la red de la organización y la protección de los datos almacenados en las bases de datos y servidores de la organización. Además, la encriptación de datos puede garantizar la privacidad de los datos sensibles de los clientes y cumplir con las regulaciones de privacidad de datos. Entre las técnicas de encriptación de datos que se pueden implementar en la emisión de tarjetas de débito y crédito se encuentran la encriptación de capa de sockets seguros (SSL), la encriptación de datos en reposo, la encriptación de datos en tránsito, la encriptación de disco completo y la encriptación de base de datos. Es importante destacar que la combinación de diferentes técnicas de encriptación de datos puede aumentar la efectividad de la encriptación.

La encriptación de datos es una medida de seguridad importante en la emisión de tarjetas de débito y crédito, y su implementación en diferentes etapas del proceso puede aumentar la seguridad general del proceso. La encriptación de datos puede garantizar la privacidad de los datos sensibles de los clientes y cumplir con las regulaciones de privacidad de datos, lo que es fundamental en el procesamiento de transacciones financieras. Además, la combinación de diferentes técnicas de encriptación de datos puede aumentar la efectividad de la encriptación y proporcionar una capa adicional de seguridad en el proceso de emisión de tarjetas de débito y crédito. En general, la encriptación de datos es una medida de seguridad esencial que debe ser implementada en la emisión de tarjetas de débito y crédito para garantizar la protección de los datos sensibles de los clientes.

3.3.2.3 Monitoreo continuo de la red

El monitoreo continuo de la red es una medida de seguridad que permite detectar y responder rápidamente a las amenazas y anomalías en la red de la organización. Se puede implementar el monitoreo continuo de la red para detectar posibles ataques y anomalías en el proceso de emisión de tarjetas de débito y crédito. Capacitación del personal: la capacitación del personal en la gestión de incidentes y la seguridad de los datos sensibles de los clientes es esencial para garantizar la seguridad en el proceso de emisión de tarjetas de débito y crédito. Se puede implementar un programa de capacitación que incluya la formación en el uso seguro de los sistemas y procesos, la gestión de incidentes y la respuesta a las amenazas de seguridad.

El monitoreo continuo de la red es una medida de seguridad crucial en la emisión de tarjetas de débito y crédito que permite detectar y responder rápidamente a las amenazas y anomalías en la red de la organización. La implementación del monitoreo continuo de la red en el proceso de emisión de tarjetas de débito y crédito implica el monitoreo constante de la red en busca de posibles amenazas, vulnerabilidades y anomalías que puedan poner en riesgo la seguridad de los datos sensibles de los clientes. El monitoreo continuo de la red puede detectar posibles ataques a la red

y a los sistemas de la organización, como el phishing, la ingeniería social, la explotación de vulnerabilidades, entre otros. Además, el monitoreo continuo de la red puede detectar anomalías en los patrones de uso de la red, como el acceso no autorizado, el uso inapropiado de recursos y otros comportamientos sospechosos.

Por otro lado, la capacitación del personal en la gestión de incidentes y la seguridad de los datos sensibles de los clientes es esencial en la emisión de tarjetas de débito y crédito. La implementación de un programa de capacitación en la gestión de incidentes y la seguridad de los datos sensibles de los clientes puede garantizar que el personal esté informado y capacitado en el uso seguro de los sistemas y procesos, la gestión de incidentes y la respuesta a las amenazas de seguridad. La capacitación del personal también puede incluir la educación en la importancia de la privacidad y la seguridad de los datos sensibles de los clientes, la identificación de posibles amenazas y la prevención de incidentes de seguridad. La capacitación del personal puede ayudar a prevenir la negligencia y los errores humanos que pueden poner en riesgo la seguridad de los datos sensibles de los clientes.

3.3.3 Evaluación periódica de las medidas de seguridad implementadas y su efectividad en la gestión de riesgos.

La evaluación periódica de las medidas de seguridad implementadas es esencial para garantizar la efectividad continua del plan de acción y la gestión de riesgos. En el contexto de emisión de tarjetas de débito y crédito, la evaluación periódica debe incluir la revisión de los controles de acceso y autenticación, la monitorización de las transacciones y la revisión de los procesos de emisión y renovación de tarjetas. Según el PCI DSS, "la evaluación periódica de las medidas de seguridad y control es necesaria para asegurar que la seguridad de las tarjetas de pago se mantiene en todo momento" (PCI SSC, 2018, p. 1). La evaluación periódica también puede identificar nuevas amenazas y riesgos que pueden requerir la implementación de medidas adicionales.

Además de la revisión periódica de las medidas de seguridad implementadas, también es importante realizar pruebas regulares de penetración para identificar posibles vulnerabilidades y brechas de seguridad. Según el PCI DSS, "la realización de pruebas regulares de penetración puede ayudar a identificar y mitigar posibles vulnerabilidades en el sistema" (PCI SSC, 2018, p. 1). Las pruebas de penetración pueden ser realizadas internamente o a través de proveedores de servicios especializados en pruebas de seguridad. La identificación temprana de posibles vulnerabilidades es esencial para evitar violaciones de seguridad y garantizar la seguridad de la información del cliente.

La realización de pruebas regulares de penetración es importante para identificar posibles vulnerabilidades y brechas de seguridad. Estas pruebas pueden ser realizadas internamente o a través de proveedores de servicios especializados en pruebas de seguridad. La identificación temprana de posibles vulnerabilidades es esencial para evitar violaciones de seguridad y garantizar la seguridad de la información del cliente. La evaluación periódica y las pruebas de penetración son esenciales para garantizar la efectividad continua de las medidas de seguridad implementadas en el proceso de emisión de tarjetas de débito y crédito. Estas prácticas pueden identificar nuevas amenazas y riesgos y ayudar a prevenir violaciones de seguridad, lo que a su vez protege la información del cliente y reduce el riesgo de fraude.

Existen diversas formas de realizar la evaluación periódica de las medidas de seguridad implementadas y su efectividad en la gestión de riesgos en la emisión de tarjetas de débito y crédito. A continuación, se presentan algunas posibles evaluaciones:

- Auditorías internas: las auditorías internas son una forma de evaluación de la efectividad de las medidas de seguridad implementadas. Estas auditorías se pueden realizar por parte del equipo interno de seguridad de la organización o por un equipo externo especializado. Las auditorías internas permiten evaluar el cumplimiento de las políticas

y procedimientos de seguridad, identificar brechas y debilidades, y tomar medidas correctivas para mejorar la seguridad.

- Evaluaciones de vulnerabilidades: las evaluaciones de vulnerabilidades son una forma de evaluación de los riesgos asociados a los sistemas y procesos de la organización. Estas evaluaciones se pueden realizar de forma interna o externa utilizando herramientas de escaneo y pruebas de penetración. Las evaluaciones de vulnerabilidades permiten identificar debilidades en los sistemas y procesos, y tomar medidas para mitigar los riesgos asociados.
- Pruebas de simulación de incidentes: las pruebas de simulación de incidentes son una forma de evaluar la efectividad del plan de continuidad del negocio y la respuesta a incidentes de la organización. Estas pruebas simulan diferentes escenarios de incidentes para evaluar la capacidad de la organización para responder a ellos y recuperarse. Las pruebas de simulación de incidentes permiten identificar debilidades en el plan de continuidad del negocio y en la respuesta a incidentes, y tomar medidas para mejorar la resiliencia de la organización.

3.4 Continuidad del negocio

3.4.1 Diseño e implementación de planes de continuidad del negocio.

En el proceso de emisión de tarjetas de débito y crédito, el diseño e implementación de planes de continuidad del negocio es esencial para garantizar la resiliencia de la organización frente a incidentes que puedan afectar la continuidad del negocio. Según el INCIBE, "los planes de continuidad del negocio deben contener medidas para minimizar el impacto de los incidentes, garantizar la disponibilidad de los recursos críticos y restaurar las operaciones lo más rápido posible" (INCIBE, 2021, p. 1). Es importante involucrar a las áreas clave de la organización en el diseño e implementación del plan de continuidad del negocio y asegurar que el plan sea relevante y efectivo para el entorno operativo de la organización.

En el caso específico de la emisión de tarjetas de débito y crédito, el plan de continuidad del negocio también debe incluir medidas para garantizar la seguridad de los datos sensibles de los clientes. Esto puede incluir la implementación de medidas de protección de datos, como la encriptación y el acceso restringido a la información de los clientes. También es importante tener en cuenta la integridad y disponibilidad de los datos, para asegurar que los clientes puedan acceder a sus cuentas y realizar transacciones en caso de un incidente.

El plan debe contener medidas para minimizar el impacto de los incidentes, garantizar la disponibilidad de los recursos críticos y restaurar las operaciones lo más rápido posible. Es importante involucrar a las áreas clave de la organización en el diseño e implementación del plan de continuidad del negocio para asegurar su relevancia y efectividad. En el caso específico de la emisión de tarjetas de débito y crédito, el plan de continuidad del negocio también debe incluir medidas para garantizar la seguridad de los datos sensibles de los clientes. Esto puede incluir la implementación de medidas de protección de datos, como la encriptación y el acceso restringido a la información de los clientes. Además, el plan debe considerar la integridad y disponibilidad de los datos para garantizar que los clientes puedan acceder a sus cuentas y realizar transacciones en caso de un incidente. En resumen, el diseño e implementación de planes de continuidad del negocio en el proceso de emisión de tarjetas de débito y crédito es fundamental para garantizar la resiliencia de la organización y la seguridad de la información del cliente en caso de un incidente que pueda afectar la continuidad del negocio.

3.4.2 Pruebas periódicas de los planes de continuidad del negocio.

Además del diseño e implementación del plan de continuidad del negocio, también es importante realizar pruebas periódicas para evaluar su efectividad y realizar mejoras. Según el NIST, "las pruebas periódicas del plan de continuidad del negocio permiten a los responsables de la seguridad determinar si el plan sigue siendo efectivo en la restauración de las operaciones después de un incidente" (NIST, 2021, p. 1). Las pruebas deben involucrar a las áreas clave de la organización y pueden incluir simulaciones de incidentes o ejercicios de mesa. La retroalimentación de las áreas involucradas en la realización de las pruebas también puede mejorar la coordinación y la efectividad del plan en caso de un incidente real.

Las pruebas periódicas del plan de continuidad del negocio, también es importante realizar revisiones periódicas del plan para asegurar que siga siendo relevante y efectivo en el entorno operativo de la organización. Según el INCIBE, "la revisión periódica del plan de continuidad del negocio debe incluir la identificación y análisis de los cambios en el entorno operativo de la organización, así como la evaluación de la efectividad de las medidas de mitigación y recuperación" (INCIBE, 2021, p. 1). Estas revisiones pueden ayudar a identificar nuevas áreas de riesgo y oportunidades de mejora para el plan de continuidad del negocio.

Las pruebas periódicas del plan de continuidad del negocio permiten evaluar su efectividad en la restauración de las operaciones después de un incidente y pueden incluir simulaciones de incidentes o ejercicios de mesa. La retroalimentación de las áreas involucradas en la realización de las pruebas también puede mejorar la coordinación y la efectividad del plan en caso de un incidente real y con esto realizar pruebas periódicas y revisiones regulares del plan de continuidad del negocio es fundamental para garantizar su efectividad y relevancia continua en el proceso de emisión de tarjetas de débito y crédito. Estas prácticas pueden mejorar la coordinación y la efectividad del plan en caso de un incidente real y garantizar la continuidad del negocio y la seguridad de la información del cliente.

3.4.3 Identificación y mitigación de los riesgos para la continuidad del negocio en caso de incidentes.

En el proceso de emisión de tarjetas de débito y crédito, es importante identificar y mitigar los riesgos para la continuidad del negocio en caso de incidentes antes de que ocurran. Según el NIST, "la identificación de los riesgos para la continuidad del negocio es esencial para establecer medidas preventivas y mitigar los riesgos de los incidentes" (NIST, 2021, p. 1). La identificación de los riesgos puede realizarse a través de análisis de riesgos y evaluaciones de impacto en el negocio. Las medidas de mitigación pueden incluir la implementación de controles técnicos y organizativos, la redundancia de los sistemas críticos y la capacitación del personal en la gestión de incidentes.

Además de la identificación y mitigación de los riesgos, también es importante tener un plan de respuesta a incidentes para la continuidad del negocio en caso de incidentes. El plan de respuesta a incidentes debe contener medidas para la detección y respuesta a incidentes, así como la recuperación de datos y sistemas críticos. Según el NIST, "el plan de respuesta a incidentes es esencial para reducir el impacto de los incidentes y restaurar las operaciones lo más rápido posible" (NIST, 2021, p. 1). Es importante que el plan de respuesta a incidentes también incluya la coordinación con las autoridades y proveedores de servicios externos en caso de un incidente grave que afecte la continuidad del negocio.

En el proceso de emisión de tarjetas de débito y crédito, es importante tener en cuenta que los riesgos pueden evolucionar con el tiempo y que los incidentes pueden ser cada vez más sofisticados y complejos. Por lo tanto, la identificación y mitigación de los riesgos debe ser un proceso continuo y dinámico que evolucione junto con el entorno operativo de la organización. Según el NIST, "los riesgos deben ser monitoreados y evaluados continuamente para identificar nuevas amenazas y oportunidades de mejora" (NIST, 2021, p. 1). Esto puede implicar la realización

de evaluaciones de riesgos periódicas y la implementación de medidas de protección adicionales a medida que surjan nuevas amenazas.

4. Discusión

El análisis y la evaluación de las medidas de seguridad y la gestión de riesgos son fundamentales para garantizar la continuidad del negocio en el proceso de emisión de tarjetas de débito y crédito de una organización. La implementación de planes de continuidad del negocio y la identificación y mitigación de los riesgos son esenciales para minimizar el impacto de los incidentes y restaurar las operaciones lo más rápido posible. Según Solms y van Niekerk (2013), "la identificación, evaluación y gestión de los riesgos son elementos críticos en la planificación de la continuidad del negocio" (p. 67). La implementación de controles de seguridad y la monitorización continua del entorno operativo de la organización son esenciales para la identificación y mitigación de los riesgos.

La implementación de controles de seguridad es también crucial en el proceso de emisión de tarjetas de débito y crédito. Según el PCI DSS, "la implementación de controles de seguridad es esencial para proteger la información del cliente y reducir el riesgo de fraude en el proceso de emisión de tarjetas de débito y crédito" (PCI SSC, 2018, p. 1). Los controles de seguridad pueden incluir el cifrado de datos, la autenticación de usuarios, el monitoreo de actividad sospechosa y la limitación de accesos.

El análisis la importancia del análisis y la evaluación de las medidas de seguridad y la gestión de riesgos en el proceso de emisión de tarjetas de débito y crédito, con el fin de garantizar la continuidad del negocio y minimizar el impacto de los incidentes. Se menciona la importancia de la implementación de planes de continuidad del negocio y la identificación y mitigación de los riesgos como elementos críticos en la planificación de la continuidad del negocio, según Solms y van Niekerk (2013). Además, se menciona la importancia de la implementación de controles de seguridad, como el cifrado de datos, la autenticación de usuarios, el monitoreo de actividad sospechosa y la limitación de accesos, para proteger la información del cliente y reducir el riesgo de fraude en el proceso de emisión de tarjetas de débito y crédito, según el PCI DSS. En resumen, se destaca la importancia de la gestión de riesgos y las medidas de seguridad para garantizar la seguridad y continuidad del negocio en el proceso de emisión de tarjetas de débito y crédito.

En el caso específico de la emisión de tarjetas de débito y crédito, también es importante asegurar la seguridad de los datos sensibles de los clientes y la disponibilidad de los datos y sistemas críticos. Según el PCI SSC (2021), "la protección de los datos del titular de la tarjeta es esencial para la continuidad del negocio y la reputación de la organización" (p. 1). La implementación de medidas de protección de datos, como la encriptación y el acceso restringido a la información de los clientes, es esencial para garantizar la seguridad de los datos. La capacitación del personal en la gestión de incidentes y la continuidad del negocio también es esencial para la efectividad del plan de continuidad del negocio.

La disponibilidad de los datos y sistemas críticos es igualmente importante en el proceso de emisión de tarjetas de débito y crédito. La interrupción de los sistemas críticos puede afectar la capacidad de la organización para procesar transacciones y afectar la satisfacción del cliente. La implementación de medidas para garantizar la disponibilidad de los sistemas críticos, como la implementación de copias de seguridad y la redundancia de los sistemas, es esencial para garantizar la continuidad del negocio. La capacitación del personal en la gestión de incidentes y la continuidad del negocio es igualmente importante para la efectividad del plan de continuidad del negocio. Los empleados deben estar capacitados para reconocer y reportar incidentes y para trabajar con el plan de continuidad del negocio en caso de un evento disruptivo. Además, el personal clave debe ser

capacitado en las medidas de protección de datos y los controles de seguridad para garantizar su efectividad.

La seguridad en el proceso de emisión de tarjetas de débito y crédito es fundamental para garantizar la continuidad del negocio y la protección de los datos sensibles de los clientes. Para lograr esto, se deben implementar medidas de seguridad y control, identificar y mitigar los riesgos, implementar planes de continuidad del negocio, garantizar la disponibilidad de los datos y sistemas críticos, y capacitar al personal en la gestión de incidentes y la continuidad del negocio. La implementación de medidas de protección de datos, la disponibilidad de los sistemas críticos y la capacitación del personal son esenciales para garantizar la continuidad del negocio y la protección de los datos sensibles de los clientes en el proceso de emisión de tarjetas de débito y crédito.

Además de la implementación de medidas de seguridad y la gestión de riesgos, la continuidad del negocio también implica la recuperación de datos y sistemas críticos en caso de un incidente. Según el ISO (2018), "la recuperación de datos y sistemas es esencial para la continuidad del negocio y la minimización del impacto de los incidentes en la organización" (p. 1). La implementación de medidas de respaldo y recuperación de datos y sistemas críticos es esencial para garantizar la continuidad del negocio. Las pruebas periódicas del plan de continuidad del negocio y de la recuperación de datos y sistemas críticos son esenciales para evaluar la efectividad de las medidas implementadas.

Es importante asegurarse de que los datos críticos y los sistemas estén respaldados regularmente y que los procedimientos de recuperación sean efectivos en caso de un evento disruptivo. Las pruebas periódicas del plan de continuidad del negocio y de la recuperación de datos y sistemas críticos son esenciales para evaluar la efectividad de las medidas implementadas y garantizar su disponibilidad en caso de un evento real. También es importante tener en cuenta que los procedimientos de recuperación deben estar documentados y ser fácilmente accesibles para los responsables de la recuperación.

La coordinación con los proveedores de servicios externos también es esencial para garantizar la continuidad del negocio en caso de un incidente. Según el INCIBE (2021), "la coordinación con los proveedores de servicios externos puede ser esencial para garantizar la continuidad del negocio y la recuperación de los servicios críticos" (p. 1). Es importante tener planes de contingencia y acuerdos de nivel de servicio con los proveedores de servicios externos para garantizar la disponibilidad de los servicios críticos en caso de un incidente. Además, es importante tener en cuenta que los proveedores de servicios externos también pueden representar un riesgo para la seguridad de los datos de los clientes. Por lo tanto, es importante asegurarse de que los proveedores de servicios externos tengan políticas y medidas de seguridad adecuadas y realizar evaluaciones regulares de su cumplimiento.

La importancia de la coordinación con los proveedores de servicios externos en la planificación de la continuidad del negocio y la recuperación de los servicios críticos en caso de un incidente en la emisión de tarjetas de débito y crédito. La implementación de planes de contingencia y acuerdos de nivel de servicio con los proveedores de servicios externos puede ser esencial para garantizar la disponibilidad de los servicios críticos y minimizar el impacto de los incidentes en la continuidad del negocio y con esto la necesidad de evaluar y garantizar que los proveedores de servicios externos tengan políticas y medidas de seguridad adecuadas para proteger los datos sensibles de los clientes. La evaluación regular de su cumplimiento es importante para asegurar que los proveedores de servicios externos cumplan con los requisitos de seguridad y para prevenir posibles vulnerabilidades en el proceso de emisión de tarjetas de débito y crédito.

En conclusión, la implementación de planes de continuidad del negocio, la identificación y mitigación de los riesgos y la seguridad de los datos sensibles de los clientes son fundamentales para garantizar la continuidad del negocio en el proceso de emisión de tarjetas de débito y crédito

de una organización. La monitorización continua del entorno operativo de la organización, la implementación de controles de seguridad y la capacitación del personal son esenciales para la efectividad del plan de continuidad del negocio, en el proceso de emisión de tarjetas de débito y crédito de una organización es esencial para garantizar la resiliencia y la recuperación en caso de un incidente. La implementación de planes de continuidad del negocio, la identificación y mitigación de los riesgos, la seguridad de los datos sensibles de los clientes y la recuperación de datos y sistemas críticos son esenciales para garantizar la continuidad del negocio. La coordinación con los proveedores de servicios externos también es esencial para garantizar la disponibilidad de los servicios críticos en caso de un incidente.

5. Conclusión

En conclusión, el proceso de emisión de tarjetas de débito y crédito es un proceso crítico en el cual la continuidad del negocio debe ser considerada una prioridad. Para asegurar la continuidad del negocio en este proceso, se deben implementar medidas de seguridad y control para mitigar los riesgos que puedan afectar la operación. Además, se deben diseñar planes de acción para la gestión de riesgos y la continuidad del negocio, los cuales deben ser probados periódicamente y evaluados para su efectividad. En caso de incidentes, se debe contar con planes de recuperación de datos y sistemas críticos, y coordinar con proveedores de servicios externos para garantizar la disponibilidad de los servicios críticos.

La identificación y mitigación de los riesgos son elementos fundamentales para garantizar la continuidad del negocio en el proceso de emisión de tarjetas de débito y crédito. La implementación de controles de seguridad y la monitorización continua del entorno operativo de la organización son esenciales para la identificación y mitigación de los riesgos. Además, la capacitación del personal en la gestión de incidentes y la continuidad del negocio es esencial para la efectividad del plan de continuidad del negocio.

Por último, es importante tener en cuenta que la continuidad del negocio es un proceso continuo y dinámico que evoluciona con el tiempo. Por lo tanto, se deben realizar evaluaciones periódicas de las medidas de seguridad implementadas y del plan de continuidad del negocio para asegurar su relevancia y efectividad en el entorno operativo de la organización. La implementación de medidas de protección de datos y la recuperación de datos y sistemas críticos son esenciales para garantizar la continuidad del negocio en caso de un incidente. La coordinación con proveedores de servicios externos también es esencial para garantizar la disponibilidad de los servicios críticos en caso de un incidente.

Referencias

1. Aldana, R., Arboleda, H., & Gaviria, J. Modelo de gestión de riesgos de seguridad de la información para la Cooperativa Policía Nacional. Revista de Investigación Académica. 2018, 24, 1-12.
2. Arias, E. Análisis de riesgos y vulnerabilidades en el proceso de emisión de tarjetas de crédito y débito en una entidad financiera. Revista Tecnológica. 2021, 18(1), 22-31.
3. Fuentes, J. F. Identificación y análisis de riesgos en el proceso de emisión de tarjetas de crédito y débito en entidades financieras. Revista de Investigación Científica. 2019, 3(1), 11-21.
4. García, M. A., & Céspedes, J. A. Propuesta de un modelo de gestión de riesgos en seguridad de la información para el sector financiero colombiano. Revista Conrado. 2020, 16(75), 51-57.
5. Guía de Implementación de un Sistema de Gestión de Seguridad de la Información basado en la Norma ISO/IEC 27001. 2019.
6. Hernández, M. E., & Álvarez, Y. Análisis de riesgos y vulnerabilidades en la emisión de tarjetas de crédito y débito en una cooperativa de ahorro y crédito. Revista de Investigación Científica. 2019, 3(2), 36-44.
7. Instituto Nacional de Ciberseguridad (INCIBE). Guía de análisis de riesgos.

https://www.incibe.es/sites/default/files/contenidos/guias/doc/incibe_guiaran.pdf. 2018.
8. Instituto Nacional de Ciberseguridad (INCIBE). Guía de continuidad del negocio. https://www.incibe.es/sites/default/files/contenidos/guias/doc/incibe_guiacontinuidad.pdf. 2021.
9. International Organization for Standardization (ISO). ISO 22301:2018 Security and resilience – Business continuity management systems – Requirements. https://www.iso.org/standard/50041.html. 2018.
10. ISO/IEC 27005:2018, Information technology — Security techniques — Information security risk management. 2018.
11. Manual de Seguridad de la Información de la Cooperativa Policía Nacional (CPN). 2018.
12. National Institute of Standards and Technology (NIST). Framework for improving critical infrastructure cybersecurity (Version 1.1). Retrieved from https://www.nist.gov/cyberframework . 2018.
13. National Institute of Standards and Technology (NIST). Security and privacy controls for information systems and organizations. https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final. 2021.
14. Payment Card Industry Security Standards Council (PCI SSC). PCI DSS Quick Reference Guide. https://www.pcisecuritystandards.org/documents/PCI_DSS_Quick_Reference_Guide.pdf. 2018.
15. PCI Security Standards Council (PCI SSC). Protecting cardholder data is critical to business continuity. https://www.pcisecuritystandards.org/documents/PCI-DSS-Business-Continuity-FINAL.pdf. 2021.
16. Solms, R. V., & van Niekerk, J. L. From business continuity management to business resilience management. Journal of Business Continuity & Emergency Planning. 2012, 6(1), 66-77.