CONTRASTE DE LOS RIESGOS VALORADOS PARA LOS TIPOS DE TARJETAS QUE HAN SIDO UTILIZADAS COMO MEDIO DE PAGO EN EL SISTEMA INTEGRADO DE TRANSPORTE PÚBLICO

IVÁN FELIPE MOJICA SÁNCHEZ

SERGIO ANDRÉS LEAL VALERO

UNIVERSIDAD CATÓLICA DE COLOMBIA.

FACULTAD DE INGENIERÍA

PROGRAMA DE INGENIERÍA DE SISTEMAS

PROYECTO DE GRADO

MODALIDAD: INVESTIGACIÓN TECNOLÓGICA

BOGOTA D.C., COLOMBIA

2019

CONTRASTE DE LOS RIESGOS VALORADOS PARA LOS TIPOS DE TARJETAS QUE HAN SIDO UTILIZADAS COMO MEDIO DE PAGO EN EL SISTEMA INTEGRADO DE TRANSPORTE PÚBLICO

IVÁN FELIPE MOJICA SÁNCHEZ
SERGIO ANDRÉS LEAL VALERO

Tesis presentada como requisito parcial para optar al título de:
Ingeniero de Sistemas

Director:
Raúl Bareño Gutiérrez

UNIVERSIDAD CATÓLICA DE COLOMBIA.
FACULTAD DE INGENIERÍA
PROGRAMA DE INGENIERÍA DE SISTEMAS
PROYECTO DE GRADO
MODALIDAD: INVESTIGACIÓN TECNOLÓGICA
BOGOTA D.C., COLOMBIA
2019

Nota de Aceptación

_____
_____
_____
_____

_____

Firma del director del Proyecto

_____

Firma del jurado

_____

Firma del jurado

BOGOTÁ D.C., MAYO 30 DE 2019

AGRADECIMIENTOS

Queremos agradecer en primer lugar a Dios, por guiarnos en el camino y fortalecernos espiritualmente para comenzar un camino lleno de logros. Así, queremos mostrar nuestra gratitud a todas aquellas personas que estuvieron presentes en la realización de este proyecto de investigación, de este sueño que es tan importante para nosotros, agradecer todas sus ayudas, sus palabras motivadoras, sus conocimientos, sus consejos y su dedicación.

A nuestras familias por todo el apoyo y constancia durante estos años de carrera universitaria, por cada una de sus palabras de ánimo que nos motivaban a continuar superando todos los obstáculos que se nos presentaban en el camino.

A los profesores y compañeros de la Universidad Católica de Colombia por todas sus enseñanzas tanto académicas como de vida.

CONTENIDO

LISTA DE TABLAS

LISTA DE ILUSTRACIONES

GLOSARIO

ALGORITMO AES: Es uno de los algoritmos de cifrado más utilizados y seguros actualmente disponibles. Es de acceso público, y es el cifrado que la NSA utiliza para asegurar documentos con la clasificación secreta

AMENAZA: El riesgo se define como la combinación de la probabilidad de que se produzca un evento y sus consecuencias negativas. Los factores que lo componen son la amenaza y la vulnerabilidad.

CRYPTO1: Es un algoritmo de cifrado patentado creado por NXP semiconductors específicamente para las etiquetas mifare RFID, que incluyen la tarjeta mifare classic, mifare plus y mifare Desfire.

EMV: Es un estándar de interoperabilidad de tarjetas inteligentes, para la autenticación de pagos mediante tarjetas de crédito y débito. El nombre EMV es un acrónimo de "europay mastercard VISA", las tres compañías que inicialmente colaboraron en el desarrollo del estándar.

GESTIÓN DE RIESGOS: La norma ISO 27005 contiene diferentes recomendaciones y directrices generales para la gestión de riesgo en Sistemas de Gestión de Seguridad de la Información, La gestión del riesgo es una actividad recurrente que se refiere al análisis, a la planificación, la ejecución, el control y el seguimiento de todas las medidas implantadas y la política de seguridad que ha sido impuesta.

IDENTIFICACIÓN POR RADIOFRECUENCIA: El propósito fundamental de la tecnología RFID es identificar mediante un lector, sin contacto y a distancia, una tarjeta o etiqueta (tag) portada por una persona, un vehículo en movimiento o cualquier producto que se encuentra en un almacén o en una cadena de producción automatizada.

MÓDULO DE SEGURIDAD HARDWARE: Un HSM es un dispositivo criptográfico basado en hardware que genera, almacena y protege claves criptográficas de alto rendimiento que se efectúa dentro del propio hardware para operaciones criptográficas.

MODULO SAM: Un secure access module o módulo de acceso seguro se basa en una smartcard y se utiliza para mejorar la seguridad rendimiento y en los dispositivos la criptografía, comúnmente en dispositivos que necesitan realizar una transacción segura, como terminales de pago.

MIFARE: Es una tecnología de tarjetas inteligentes sin contacto (TISC), de las más instaladas en el mundo con protocolo de alto nivel, con una distancia típica de lectura de 10 cm. Es propiedad de NXP semiconductors (antes parte de philips semiconductors).

RIESGO: Posibilidad de que se produzca un contratiempo o una desgracia, de que alguien o algo sufra perjuicio o daño.

RFID: Es un sistema de almacenamiento y recuperación de datos que usa dispositivos denominados etiquetas, tarjetas o transpondedores RFID. El propósito fundamental de la tecnología RFID es transmitir la identidad de un objeto (similar a un número de serie único) mediante ondas de radio. Las tecnologías RFID se agrupan dentro de las denominadas auto ID (*automatic identification*, o identificación automática).

SMARTCARD: Tarjeta Inteligente del formato estándar de crédito que incorpora un microchip o Microprocesador que almacena información y/o la procesa obteniendo su información por medio de lectores RFID.

TARJETAS INTELIGENTES SIN CONTACTO: Las tarjetas inteligentes sin contacto son una evolución de la tecnología usada desde hace años por los RFID (identificación por radio frecuencia), permitidos para distancias de comunicación de hasta 10 cm.

VULNERABILIDAD: Está íntimamente relacionado con el riesgo y la amenaza y se puede definir como la debilidad o grado de exposición de un sujeto, objeto o sistema. También son aquellas fallas, omisiones o deficiencias de seguridad que puedan ser aprovechadas por los delincuentes.

LISTA DE SÍMBOLOS Y ABREVIATURAS

Tabla 1. Glosario de términos

Abreviatura	Término
AES	Estándar de encriptación avanzado
BRT	Autobuses de tránsito rápido
CPTCRD	CriptoCards
DF	Archivo dedicado
EF	Archivo elemental
EMV	Europay MasterCard VISA
HSM	Módulo de seguridad hardware
HZ	Hertz
IC	Tarjetas con circuito integrado
IFMS	Sistemas interoperables de gestión de tarifas
LSFR	Registro de desplazamiento con retroalimentación lineal
MF	Archivo principal
MHZ	Mega hertzios
NFC	Comunicación de campo cercano
PIN	Número de identificación personal
RIFID	Modulo sensor de tarjeta
RUID	Identificador único aleatorio
SAM	Módulo de acceso seguro
SITP	Sistema integrado de transporte público
SW	Software

Fuente: El autor

RESUMEN

El sistema integrado de transporte público SITP, conocido antes como transmilenio s.a., es uno de los sistemas más grandes y sofisticados de transporte en Colombia; el ingreso a transmilenio se hace mediante tarjetas inteligentes sin contacto entre las cuales se encuentran: la tarjeta monedero, cliente frecuente y la actual tarjeta tu llave bajo la licitación de recaudo Bogotá. Debido a diferentes sucesos presentados, vulneración del medio de pago del sistema de transporte, se realizó una valoración de riesgos por medio de la norma ISO 27005 enfocada a seguridad de la información de activos, basándose en la identificación de amenazas, vulnerabilidades y riesgos de las tarjetas utilizadas en el sistema.

Los resultados encontrados con el presente estudio permiten detectar y contrastar los riesgos asociados del uso de cada una de las tarjetas que han sido utilizadas por esta entidad, aplicando la metodología ISO 27005, además los diferentes mapas de calor resaltan las amenazas y vulnerabilidades dada la valoración de riesgos de la solución planteada, que servirán para mejorar los criterios de seguridad que se deben implementar día a día en el uso de este tipo de tarjetas. Finalmente la seguridad inmersa en la tarjetas inteligente de tullave minimizan vulnerabilidades e incrementan el grado de confiabilidad y de aceptación por el sistema de transmilenio, esta tarjeta permite su masificación y uso dentro del sistema con alto grado de confianza dados los diferentes sistemas de encriptamiento, se recomienda revisar nuevos sistemas autenticación y validación entre otros aspectos que garanticen los principios básicos de seguridad en autenticación, confiabilidad e integridad. Por ello se puede tener una tarjeta única e interoperable entre los sistemas de transporte masivo de Colombia con características de seguridad eficientes.

Palabras clave: INFORMACIÓN, MEDIO URBANO, SEGURIDAD, TECNOLOGÍA DE LA INFOMACIÓN, TRANSPORTE PUBLICO.

ABSTRACT

The integrated public transport system SITP, formerly known as transmienio s.a., is one of the largest and most sophisticated transport systems in Colombia; The entry to transmilenio is done through non-contact smart cards among which are: tarjeta monedero, cliente frecuente and the current card tullave under the Bogota collection tender. Due to different events presented, violation of the means of payment of the transport system, a risk assessment was carried out by means of the ISO 27005 standard focused on the security of the assets information, based on the identification of threats, vulnerabilities and risks of the cards used in the system.

The results found with the present study allow to detect and contrast the associated risks of the use of each of the cards that have been used by this entity, applying the ISO 27005 methodology, in addition the different heat maps highlight the threats and vulnerabilities given the risk assessment of the proposed solution, which will serve to improve the safety criteria that must be implemented day by day in the use of this type of cards. Finally the security immersed in the smart cards of tullave minimize vulnerabilities and increase the degree of reliability and of acceptance by the system of transmilenio, this card allows its overcrowding and use within the system with high degree of trust given the different encryption systems, it is recommended to revise new authentication and validation systems among other aspects that guarantee the basic principles of security in authentication, reliability and integrity. This is why you can have a unique and interoperable card between Colombia's mass transit systems with efficient security features.

Keywords: INFORMATION, INFORMATION TECHNOLOGY, PUBLIC TRANSPORTATION, SECURITY, URBAN ENVIROMENT.

INTRODUCCIÓN

La presente investigación se enmarca en valorar los riesgos asociados a los diferentes tipos de tarjetas inteligentes que han sido utilizadas como medio de pago en el sistema masivo de transporte público de Bogotá D.C., definiéndose como la alteración de la autenticidad de las tarjetas, siendo consecuencia de esto la vulneración de los algoritmos de encriptación y las llaves que contienen estos chips incorporados.

La característica principal de este tipo de vulneraciones es la actividad ilegal llevada a cabo, debido que el dinero por la venta de las tarjetas no lo recibe directamente el sistema de transporte, generando pérdidas económicas para la misma.

Para analizar esta problemática es necesario identificar sus vulnerabilidades y amenazas, una de ellas, y por la cual se inició el proceso de identificación, es la falta de seguridad y control en los protocolos de los diferentes tipos de tarjetas existentes en las tecnologías utilizadas; esto evidenciado en los antecedentes expuestos en el presente documento.

La investigación de esta problemática se llevó a cabo por el interés de conocer los mecanismos existentes de seguridad, identificar vulnerabilidades y amenazas, y valorar los riesgos asociados a las tarjetas inteligentes que han sido utilizadas como medio de pago en el sistema masivo de transporte público de Bogotá D.C.; con esto profundizar en la indagación, desde la perspectiva de la Ingeniería de Sistemas, aportando estudios de investigación referentes a las tarjetas inteligentes en el transporte público masivo.

1. GENERALIDADES

1.1. ANTECEDENTES

El primer inconveniente que se detectó en el sistema masivo de transporte público transmilenio fue en año 2013, se comprobaron las vulnerabilidades de las tarjetas "cliente frecuente – tarjeta monedero" a cargo del operador angelcom, donde fue posible clonar y alterar estas tarjetas de pago, siendo afectados los algoritmos de encriptamiento, y con esto, aumentando la posibilidad de obtención de las llaves[1] . Posteriormente en el 2016, se identificó una organización que se dedicaba a la clonación y adulteración de las tarjetas de transmilenio, que luego de ser clonadas y alteradas eran vendidas a mitad de precio, el desfalco total para el sistema masivo fue de $27.000 millones de pesos[2].

En la actualidad existen trabajos e investigaciones sobre las vulnerabilidades en tarjetas inteligentes denominadas tarjetas "prepago", como lo es el sistema de cobro electrónico de pasajes en el transporte público, una muestra de ello es el estudio presentado por las naciones unidas de Chile en el 2010, donde se establecieron las características operativas de las diferentes tarjetas prepago que existen para el pago de transporte público, realizando una comparación exhaustiva de cada una de las tecnologías, se determinaron los diferentes métodos que maneja cada país según el modelo de transporte y manejo de tarjetas (Brasil y Colombia) [3] , y por último, la universidad de Cantabria - España donde identificaron los diferentes protocolos existentes en las tarjetas con chip y tipos de tarjetas, este trabajo se enfocó en el análisis del modelo de las tarjetas, la memoria que incorpora, ventajas y estándares que mundialmente las rigen [4].

---

[1] Revista Semana, 2013." Transmilenio: tarjetas de las fases I y II se pueden clonar Bogotá – Colombia".(10 Agosto de 2018).Disponible en internet: https://www.semana.com/nacion/articulo/informe-transmilenio-sobre-seguridad-en-tarjetas/356601-3

[2] Noticias RCN, 2016. "Capturan a siete personas acusadas de clonar tarjetas de Transmilenio Bogotá – Colombia".(11 Agosto de 2018).Disponible en internet: https://noticias.canalrcn.com/nacional-bogota/capturan-siete-personas-acusadas-clonar-tarjetas-transmilenio

[3] Gabriel Pérez, 2015. "Sistema de cobro electrónico de pasajes en el transporte público Santiago de Chile". (11 Agosto de 2018). Disponible en internet: https://repositorio.cepal.org/bitstream/handle/11362/6401/1/S026444_es.pdf

[4] Felipe Carrera, 2016. "Seguridad de la Información Política INFOSEC Nacional Cantabria – España ".(13 Agosto de 2018).Disponible en internet: https://books.google.com.co/books?hl=es&lr=lang_es%7Clang_en&id=cQk_Ms6MUfEC&oi=fnd&p=

1.1.1 PLANTEAMIENTO DEL PROBLEMA

1.1.2. Descripción del problema.

El transporte público de Bogotá a través del tiempo ha evolucionado como resultado a las necesidades de los ciudadanos en dirigirse a diferentes lugares, esto dio paso a la articulación operacional de los buses colectivos mediante transmilenio s.a.

De esta manera, transmilenio s.a. surgió a partir del año 2000 prestando un servicio masivo de transporte al ciudadano, aportando rapidez entre desplazamientos debido al modelo de transporte implementado en donde uno de sus principales componentes es el sistema de pago y recaudo electrónico llevado a cabo mediante tarjetas inteligentes sin contacto (TISC) y torniquetes.

Posteriormente, en el año 2003, la empresa angelcom fue contratada con el fin de llevar a cabo el recaudo de las fases I y II de transmilenio mediante el uso de dos tarjetas electrónicas conocidas como monedero y cliente frecuente tipo MIFARE® classic. Sin embargo, en el año 2011 transmilenio s.a. abrió un nuevo proceso de licitación para el recaudo de la fase III del sistema, adjudicando este contrato a la empresa recaudo Bogotá, debido al menor costo que representa para la ciudad dicha propuesta; para esta fase, se implementó una nueva tarjeta para uso del sistema conocida como tullave tipo MIFARE® plus con un estándar definido por la norma ISO 14443, estándar internacional relacionado con las tarjetas de identificación electrónicas[5]:

Así pues, durante 4 años estos dos operadores estuvieron a cargo del proceso de recaudo del anterior sistema de transporte masivo transmilenio s.a. y ahora conocido como sistema integrado de transporte público (SITP) de Bogotá. Por esto, fue a partir del año 2013 que evidenciaron que se estaban alterando las tarjetas monedero y cliente frecuente lo que ocasionó pérdidas financieras y afectación a la reputación del sistema y el contratista a cargo (angelcom) del recaudo, entre estas alteraciones se encuentran la clonación y modificación de saldo.

Un ejemplo de esto es el informe presentado por FTI consultores en el año 2015, la cual denunció clonación y alteración en las tarjetas monedero y cliente frecuente ya

PA9&dq=seguridad+en+tarjetas++&ots=Z09h9OyFCJ&sig=RubJ_L5eXiOvo0BGLfeqIy4sE6s&redir_esc=y#v=onepage&q=seguridad%20en%20tarjetas&f=false

[5] ISO, 2014. “ISO 14443”. (20 Agosto de 2018). Disponible en: https://www.iso.org/standard/50942.html

que, al aplicar pruebas sobre 15 tarjetas, en dos fue posible modificar su saldo y todas fueron clonadas.

Debido a lo anterior, el SITP unificó el único medio de pago, a través de su contratista (recaudo Bogotá s.a.s.), proceso que se completó el 01 de enero de 2019 con la salida de funcionamiento de la tarjeta cliente frecuente; para esto el SITP creó un plan de personalización de tarjetas tu llave con beneficios tarifarios y de crédito para el usuario.

1.1.3. Formulación del problema.

En conformidad con lo descrito anteriormente, se plantea la siguiente pregunta de investigación: ¿Aplicando la norma ISO 27005, se podrán encontrar fortalezas y debilidades de los diferentes tipos de tarjetas inteligentes que han sido utilizadas como medio de pago en el sistema masivo de transporte público de Bogotá D.C., transmilenio s.a.?

1.2. OBJETIVOS

1.2.1. Objetivo General.

Valorar los riesgos asociados a los tipos de tarjetas que han sido utilizadas como medio de pago electrónico de pasajes del sistema masivo de transporte público de Bogotá D.C., transmilenio s.a., bajo la norma ISO 27005.

1.2.2. Objetivos Específicos.

- Identificar las amenazas, vulnerabilidades y controles existentes en los tipos de tarjetas utilizadas como medio de pago del sistema masivo de transporte público transmilenio s.a.
- Estimar los riesgos de forma semi - cualitativa, obteniendo las consecuencias y probabilidades de ocurrencia vinculadas a los tipos de tarjetas utilizadas como medio de pago del sistema masivo de transporte público transmilenio s.a.
- Evaluar los riesgos relacionados a los tipos de tarjetas utilizadas como medio de pago del sistema masivo de transporte público transmilenio s.a. comparando los niveles de riesgo frente a los criterios de aceptación.

1.3. JUSTIFICACIÓN

Las TISC dentro del contexto de medio de pago utilizado en sistemas de transporte público, surgieron por la necesidad de reemplazar el procedimiento tradicional (pago en efectivo) por medio de la implementación de nuevas tecnologías que aportan mayor agilidad a la hora de satisfacer las necesidades del ser humano en la actualidad. En Colombia, el primer sistema de transporte que implementó este tipo de pago fue transmilenio s.a. en el año 2000, logrando así una nueva visión al sistema actual que para esa época no se contempló como factor clave: la seguridad.

Posteriormente, a partir del año 2013 se empezaron a evidenciar las vulnerabilidades que ocasionan el manejo de los diferentes tipos de tarjetas que se encontraban en producción en su momento como son la tarjeta cliente frecuente y monedero.

Por esta razón, sin controles eficientes, la escritura de saldo y clonación de tarjetas ya era un riesgo materializado y el impacto generado fue mayor puesto que no se identificaron las vulnerabilidades, amenazas y riesgos asociados a la tecnología que se habían adoptado para las TISC en uso del sistema de pago de transmilenio s.a., ahora conocida como SITP.

Para ello, fue necesario plantear la unificación de este medio de pago a través de la tarjeta tullave. Ahora bien, la tecnología de la tarjeta tullave es similar a las que son usadas en las tarjetas crédito y débito, incluye un chip infineon con una infraestructura mifare plus de 4k en donde se proporciona la autenticación mutua y la seguridad de los datos por medio del algoritmo crypto1 integrado con AES para la autenticación, integridad de datos y cifrado, basado en estándares abiertos y globales. [6]

El desarrollo del presente trabajo de investigación aporta y conlleva a generar un impacto positivo en la parte financiera de la organización, ya que, conociendo, aceptando o rechazando los riesgos asociados a los activos de información es posible proponer planes de acción y plantear tratamientos a los mismos (etapas posteriores de la gestión de riesgos que se encuentran fuera del alcance de la investigación), de tal forma que se puedan mitigar pérdidas financieras producto de la vulneración de las TISC, la alteración a la integridad y confidencialidad de la información asociada a estos activos de información.

[6] (MiFare, s.f.) Familia MIFARE Plus. (25 Agosto de 2018). Disponible en: https://www.mifare.net/es/productos/ics-de-tarjetas-con-chip/familia-mifare-plus/

Finalmente, la razón por la cual se desarrolló el presente trabajo de investigación es identificar, estimar y evaluar los riesgos asociados a los tipos de tarjetas que han sido usadas en el SITP, ya que a través del proceso planteado es posible valorar los controles actuales y, en trabajos futuros, identificar falencias en esto, de tal manera que se puedan mejorar los actuales y a su vez proponer nuevos controles, logrando así disminuir su impacto y la probabilidad que se derive en mitigar los riesgos identificados que en conclusión benefician directamente al SITP y a los usuarios.

1.4. MARCO LEGAL

El marco legal en el presente trabajo de investigación proporciona las regulaciones existentes sobre las cuales se basó el problema tratado, donde se encuentran regulaciones, normativas y leyes interrelacionadas entre sí, se describen a continuación:

1.4.1 Ley estatutaria 1266 – 2008 Habeas data: Es el estatuto de las disposiciones generales del Hábeas Data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial y de servicios[7].

1.4.2 Ley 1273 – 2009 Delitos informáticos: Esta ley se define en el código penal, se crea un nuevo bien jurídico tutelado denominado “de la protección de la información y de los datos” y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.

1.4.3 Sistemas de Gestión de la Seguridad de la Información (SGSI): El ministerio de tecnologías de la información y las comunicaciones - MinTIC a través de la dirección de estándares y arquitectura de TI y la subdirección de seguridad y privacidad de TI, dando cumplimiento a sus funciones; pública el modelo de seguridad y privacidad de la Información (MSPI), la implementación del modelo de seguridad y privacidad de la Información, en la entidad está determinado por las necesidades objetivas, los requisitos de seguridad, procesos, el tamaño y la estructura de la misma, todo con el objetivo de preservar la confidencialidad,

[7] Seguridad de la información, Marco legal de seguridad de la información en Colombia 2012. (26 Agosto de 2018).
Disponible en: http://seguridadinformacioncolombia.blogspot.com/2010/02/marco-legal-de-seguridad-de-la.html

integridad, disponibilidad de los activos de información, garantizando su buen uso y la privacidad de los datos.

1.4.4 ISO 7810: La norma ISO/IEC 7810, tarjetas de identificación y características físicas, es el estándar internacional de las tarjetas de identificación, como los documentos de identidad o las tarjetas electrónicas tipo tarjetas de crédito.

Las características especificadas en la norma incluyen:

- Las dimensiones físicas y sus tolerancias.
- La construcción y los materiales de las tarjetas de identificación;
- Las características físicas de las tarjetas, tales como rigidez a la flexión, inflamabilidad, toxicidad, resistencia a productos químicos, la estabilidad dimensional, la adhesión o el bloqueo, la deformación, resistencia al calor, las distorsiones de la superficie, y la contaminación. 32

La ISO 7810 maneja 3 tipos de tamaños:

- ID-1: El formato ID-1 especifica un tamaño de 85,60 × 53,98 mm (3 3⁄8 × 2 1⁄8 pulgadas) y esquinas redondeadas con un radio de entre 2.88 y 3.48 mm., se utiliza comúnmente para las tarjetas de pago, sistemas de cobro automatizado, tarjetas para el transporte público y en las tarjetas de fidelidad comerciales.
- ID-2: El formato ID-2 especifica 105 × 74 mm. Este tamaño es el formato A7, se utiliza, para las visas y diferentes documentos de identidad.
- ID-3: El formato ID-3 especifica un tamaño de 125 × 88 mm., este tamaño es el formato B7, se utiliza comúnmente para pasaportes.

1.4.5 ISO 7816: Es un estándar internacional relacionado con las tarjetas de identificación electrónicas, en especial las tarjetas inteligentes, gestionado conjuntamente por la organización internacional de normalización (ISO) y comisión electrotécnica internacional (IEC). Especifica las características físicas de las tarjetas de circuitos integrados con contactos.

La ISO 7816 maneja diferentes características y referencias:

- 7816-1 - Características físicas: Creada en 1987 especifica las características físicas de las tarjetas de circuitos integrados con contactos.

Se aplica a las tarjetas de identificación del tipo ID-1 de la norma ISO 7810, que puede incluir la grabación en relieve y/o una banda magnética y/o marca de identificación táctil como se especifica en la norma ISO 7811. ISO/IEC 7816-1 se aplica a las tarjetas que tienen un interfaz físico con contactos eléctricos.

- 7816-2 - Dimensiones y ubicación de los contactos: Contactos del chip de una tarjeta con contactos, creada en 1988, especifica las dimensiones y ubicaciones para cada uno de los contactos de una tarjeta de circuito integrado del tipo de tarjeta de identificación ID-1. También proporciona información sobre la manera de identificar y qué normas definen el uso de los contactos.

1.5. ESTADO DEL ARTE

El primer trabajo investigativo, realizado en el 2002, se basó en los riesgos asociados a las tarjetas inteligentes, el desarrollo del trabajo consistió en la creación de controles entre los lectores y las criptocards con el fin de mitigar los riesgos de fraude en los sistemas de transporte, billetera electrónica entre otras, a través del fortalecimiento de la comunicación entre el dispositivo de cobro y la tarjeta inteligente, evitando las situaciones de plagio o clonación[8].

Posteriormente el autor Dominik Haneberg[9] en el 2004, describió las ventajas de los pasajes electrónicos y los riesgos asociados a este tipo de tecnología de pago, los diferentes protocolos existentes, asociado todo a los sistemas de cobro, en las tarjetas inteligentes determinando que los mecanismos que utilizan esta tecnología son vulnerables y deficientes, afectando directamente a este tipo de sistemas con su impacto de materialización frente a una posible ocurrencia de eventos.

En la actualidad existen trabajos e investigaciones sobre los posibles riesgos a los que están sometidos las tarjetas inteligentes en los sistemas de transporte del mundo, es así como los estudiantes de la universidad de Buenos Aires[10] en el 2011, establecieron los potenciales ataques que se podrían producir por medio de las

[8] Gerges Kayanakis, 2002. Contactless or hybrid contact-contactless smart card designed to limit the risks of fraud. (02 Abril de 2019). Disponible en : https://patents.google.com/patent/US6390375B2/en
[9] Dominik Haneberg, 2004. Electronic ticketing: risks in e-commerce applications. (02 Abril de 2019). Disponible en: https://link.springer.com/chapter/10.1007%2F978-3-540-72621-0_5
[10] Marey, 2011. Aspecto de seguridad en sistemas de boletos electrónicos. (03 Abril de 2019). Disponible en: http://bibliotecadigital.econ.uba.ar/download/tpos/1502-0811_MareyAD.pdf

vulnerabilidades de las tarjetas con tecnología MIFARE y los posibles controles preventivos que podrían ser implementados para minimizar su impacto en los sistemas de cobro de pasajes que implementen estas tarjetas MIFARE.

En el año 2012 realizaron un trabajo investigativo de gestión de riesgos, en la universidad técnica de Múnich[11], el cual desarrolló un estudio de las vulnerabilidades que se presentan por medio de la tecnología NFC donde es posible obtener la información de las tarjetas; como es los seriales, id y el saldo disponible en esta criptocard.

Por último se encuentra la gestión de riesgos de recaudo Bogotá s.a.s, responsable de la distribución de las tarjetas de la fase 1 y 2 del sistema integrado de transporte público de la ciudad de Bogotá - Colombia, realizado por estudiantes de la universidad católica de Colombia[12] en el año 2016, este trabajo consistió en la ejecución de un análisis de gestión de los riesgos de TI y asociado a las operaciones principales (recaudo, control de flota y medio de pago), esto a través del marco 4A, que finalmente conllevo a proponer un plan de continuidad del negocio y propuesta de mejoramiento de la base tecnológica.

1.6. METODOLOGÍA

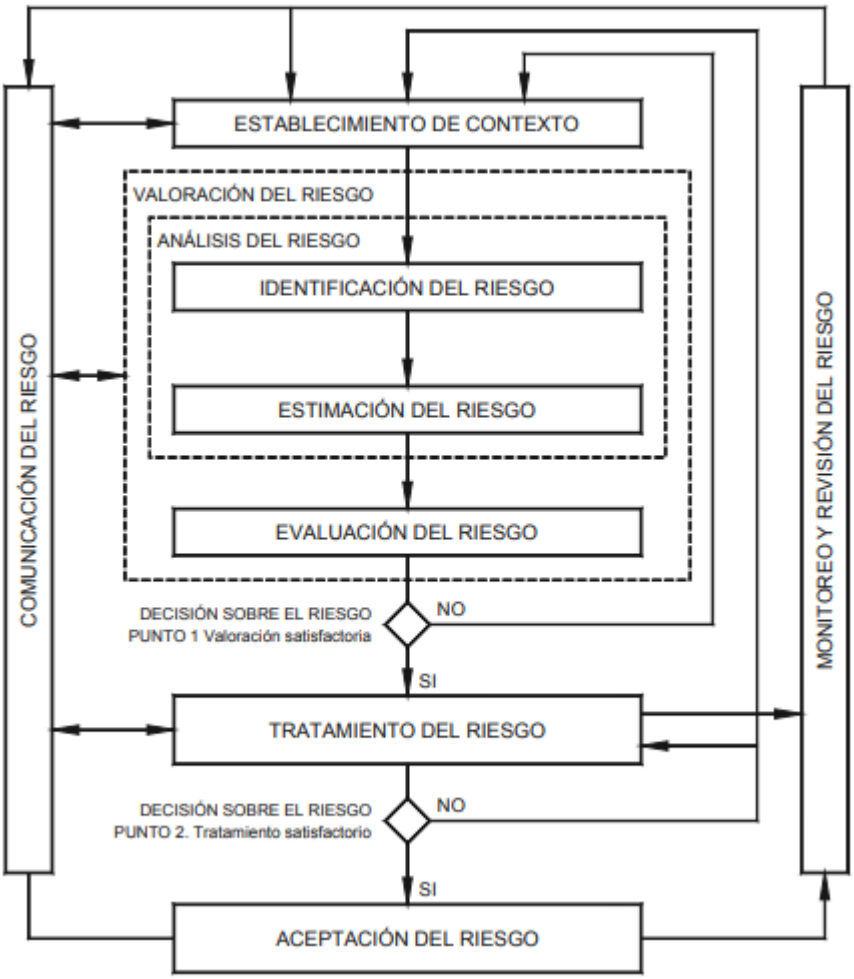
La metodología a aplicar para el correcto desarrollo del proyecto de investigación es la propuesta en la norma ISO/NTC 27005 gestión del riesgo en la seguridad de la información, que consta de la siguiente estructura:[13]

[11] Uwe Trottmann, 2012. NFC – Possibilities and risk. (04 Abril de 2019). Disponible en: https://www.net.in.tum.de/fileadmin/TUM/NET/NET-2013-02-1/NET-2013-02-1_05.pdf

[12] Jóse Leonardo Camacho,2016. Análisis de gestión del riesgo de TI en recaudo Bogota. (05 Abril de 2019). Disponible en: https://repository.ucatolica.edu.co/bitstream/10983/

[13] PMG SGSI, Metodología 27005. (20 Septiembre de 2018). Disponible en: https://www.pmg-ssi.com/2017/06/iso-27005-gestion-del-riesgo-tecnologico/

Ilustración 1. Metodología ISO 27005

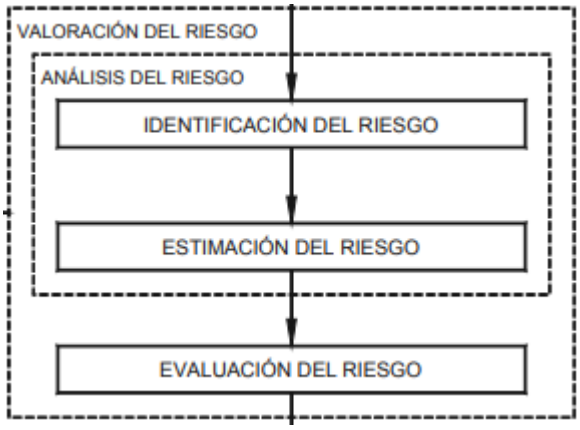


Fuente: ISO 27005 Gestión de riesgos activos de información

Está definido por directrices para la gestión del riesgo en la seguridad de la información en las organizaciones, apoyándose del sistema de gestión de seguridad de la información (SGSI) regida por la ISO/NTC 27001. El estándar 27005 orienta a las organizaciones a definir el enfoque para realizar una óptima gestión del riesgo, esta norma es pertinente para los directores y personal involucrado en la gestión del riesgo en la seguridad de la información.

Por lo anterior, la metodología a seguir en el presente trabajo de investigación es la valoración del riesgo que comprende la identificación, estimación y la evaluación del riesgo:

Ilustración 2. Valoración de riesgos ISO 27005



Fuente: ISO 27005 Gestión de riesgos activos de información

1.6.1. Identificación del riesgo.

El propósito de la identificación del riesgo es determinar qué podría suceder en caso de una pérdida potencial y llegar a comprender el cómo, dónde y porqué podría ocurrir esta pérdida. Como subprocesos de la identificación del riesgo se encuentran las siguientes etapas para la correcta identificación de los riesgos:

- Identificación de los activos: Determinar los activos importantes para la organización por lo cual requieren una protección y donde influyen factores de hardware y software, identificar los activos es de gran de importancia para proporcionar la información suficiente para la valoración del riesgo. En esta etapa de reconocimiento es adecuado asignar propietarios y roles de responsabilidad a los activos de la organización.

  En el presente trabajo de investigación se realizó la identificación de activos por medio de la documentación que el sistema masivo de transporte público transmilenio hace público mediante su página web, el foco principal y el activo a utilizar para el correcto funcionamiento del trabajo son las tarjetas inteligentes que han sido utilizadas como medio de pago para ingresar al sistema de transporte.

- Identificación de las amenazas: Está relacionado con el anterior proceso de reconocimiento, referente a los responsables de los activos, ya que estos son los que determinan y analizan las posibles amenazas que

pueden afectar los activos representando impactos a la organización; las amenazas se presentan de dos formas:

- Origen natural: Todo lo relacionado con catástrofes naturales.
- Origen humano: Orientadas a las personas que pueden ser amenazas accidentales o deliberadas.

La identificación de amenazas se realizó basado en lo sugerido por la norma ISO 27005 anexo C.

- Identificación de controles existentes: Se debe realizar la identificación de los controles existentes para evitar contratiempos y costos innecesarios, así mismo evaluar su eficiencia que reduce la probabilidad y/o impacto de las vulnerabilidades, estos controles deben contener documentación y tratamientos de los riesgos.

  Los controles existentes se determinaron por medio de la documentación técnica pública que tiene cada fabricante de los tipos de tarjetas que fueron valoradas.

- Identificación de vulnerabilidades: Se debe tener presente las vulnerabilidades existentes en la organización, con una correcta identificación se evita las amenazas no detectadas donde se podría explotar la vulnerabilidad afectando directamente a los activos, cada vulnerabilidad debe tener asociado amenazas.

  La identificación de las vulnerabilidades se realizó por medio de documentación de investigaciones académicas, antecedentes y situaciones conocidas en la actualidad

- Identificación de consecuencias: Después de la identificación de activos, amenazas, vulnerabilidades, controles, se debe determinar los daños y consecuencias, basado en que una amenaza explote la vulnerabilidad, que afecten la confidencialidad, integridad y disponibilidad de los activos.

  Las consecuencias se determinaron por medio de los escenarios incidente, identificando afectación a la confidencialidad, integridad y disponibilidad, y también, la afectación financiera, reputacional y recurso humano.

1.6.2. Estimación del riesgo.

El propósito de la estimación del riesgo es asociar una escala de calificación de criticidad de los activos, vulnerabilidades e incidentes presentados que afectaron a la organización, se clasifican en dos estimaciones:

- Estimación cualitativa: Es una escala de atributos calificativos para describir algún tipo de magnitud de las consecuencias potenciales y así mismo su probabilidad, una ventaja que tiene la estimación cualitativa es la facilidad de entendimiento y comprensión por parte de las personas de la organización, normalmente la escala que se utiliza es (muy alta - alta - intermedia - baja - muy Baja).

- Estimación cuantitativa: Es una escala de valoraciones numéricas a diferencia de la anterior estimación que es descriptiva, tanto la consecuencia como la probabilidad, esta estimación es acertada y exacta.

La estimación del riesgo se compone de las siguientes fases:

- Valoración de las consecuencias: Es la calificación que se determinó por medio de alguna de las anteriores opciones, según el impacto en el negocio, después de un incidente presentado ya materializado, evaluando factores como la pérdida de confidencialidad, integridad o disponibilidad.

- Valoración de los incidentes: Posteriormente de identificar los escenarios de los incidentes, se evaluó la probabilidad de cada escenario presentado y el impacto de ocurrencia, se tuvo en cuenta la periodicidad de la amenaza en el que se presentan los escenarios donde las vulnerabilidades pueden ser explotadas.

- Nivel de estimación del riesgo: En esta fase se determinaron las valoraciones de probabilidad y consecuencia de los riesgos identificados, considerando el beneficio en costo e intereses de las partes involucradas.

En el presente trabajo de investigación la estimación de los riesgos se valoró por medio de un método semi - cualitativo aplicando rangos y escalas, dando calificaciones dependiendo la ocurrencia y afectación a los activos de la organización, se estimó tanto impacto como probabilidad según las escalas definidas en el establecimiento del contexto.

1.6.3. Evaluación del riesgo.

El propósito de la evaluación del riesgo es tomar planes de acción o la toma de decisiones sobre las evaluaciones de riesgo y los criterios de evaluación, determinando una prioridad entre los riesgos de acuerdo con los criterios de evaluación y aceptación de riesgo definidos en el establecimiento del contexto.

La evaluación del riesgo se realizó priorizando los niveles de riesgo, de acuerdo con su valor y criterios para la evaluación y aceptación del riesgo.

1.6.4. Método.

El presente trabajo de investigación adopta una metodología descriptiva, iniciándose con la valoración el riesgo bajo el marco NTC/ISO 27005 donde se identificaron vulnerabilidades, amenazas, riesgos y controles actuales, posteriormente la estimación de valoraciones de consecuencia y probabilidad de la incidencia de los riesgos en la organización.

La metodología de medición para el trabajo de investigación será (semi - cualitativa) donde estará definida por las siguientes escalas de valoración y su valor numérico asignado:[14]

- Probabilidad:

Tabla 2. Especificación probabilidad

Nivel	Descripción	Definición	Frecuencia
1	Rara Vez	El evento puede ocurrir solo en circunstancias excepcionales (poco comunes o anormales).	No se ha presentado en los últimos 5 años.
2	Improbable	El evento puede ocurrir en forma esporádica	Al menos 1 vez en los últimos 5 años.
3	Posible	El evento podrá ocurrir en algunas circunstancias.	Al menos 1 vez en los últimos 2 años.
4	Frecuente	Es viable que el evento ocurra en la mayoría de las circunstancias	Al menos 1 vez en el último año.
5	Casi Seguro	Se espera que el evento ocurra en la mayoría de las circunstancias	Más de 1 vez al año.

[14] Transmilenio, 2017. “Gestión de riesgo Transmilenio”. (21 Septiembre de 2018).Disponible en: http://www.transmilenio.gov.co/loader.php?lServicio=Publicaciones&lTipo=WFactionA&lFuncion=visualizar&id=14538&bd=m

Fuente: Transmilenio - https://www.transmilenio.gov.co/publicaciones/149398/m-op-002-manual-para-la-gestin-del-riesgo-en-transmilenio-s-a/

- Consecuencia:

Tabla 3. Especificación consecuencia

Nivel	Descripción	Impacto
1	Insignificante	• No hay interrupción de las operaciones de la entidad. • No se generan sanciones económicas o administrativas. • No se afecta la imagen institucional de forma significativa.
2	Menor	• Interrupción de las operaciones de la entidad por algunas horas. • Reclamaciones o quejas de los usuarios que implican investigaciones internas disciplinarias. • Imagen institucional afectada localmente por retrasos en la prestación del servicio a los usuarios o ciudadanos
3	Moderado	• Interrupción de las operaciones de la entidad por un (1) día. • Reclamaciones o quejas de los usuarios que podrían implicar una denuncia ante los entes reguladores o una demanda de largo alcance para la entidad. • Inoportunidad en la información ocasionando retrasos en la atención a los usuarios.

4	Mayor	• Interrupción de las operaciones de la entidad por más de dos (2) días. • Pérdida de información crítica que puede ser recuperada de forma parcial o incompleta. • Sanción por parte del ente de control u otro ente regulador. • Incumplimiento en las metas y objetivos institucionales afectando el cumplimiento en las metas de gobierno.
5	Catastrófico	• Interrupción de las operaciones de la entidad por más de cinco (5) días. • Intervención por parte de un ente de control u otro ente regulador. • Pérdida de Información crítica para la entidad que no se puede recuperar.

Fuente: Transmilenio - https://www.transmilenio.gov.co/publicaciones/149398/m-op-002-manual-para-la-gestin-del-riesgo-en-transmilenio-s-a/

Nivel de riesgo:

Tabla 4. Nivel de riesgo

Nivel de severidad	**Puntaje**
Bajo	1 a 2
Medio	3 a 4
Alto	5 a 12
Extremo	15 a 25

Fuente: Transmilenio - https://www.transmilenio.gov.co/publicaciones/149398/m-op-002-manual-para-la-gestin-del-riesgo-en-transmilenio-s-a/

1.7. CRONOGRAMA

Tabla 5. Cronograma de desarrollo del proyecto

Fase	Nombre	Duración	Semana 1	Semana 2	Semana 3	Semana 4	Semana 5	Semana 6	Semana 7	Semana 8	Semana 9	Semana 10	Semana 11	Semana 12	Semana 13	Semana 14	Semana 15	Semana 16	Semana 17	Semana 18	Semana 19	Semana 20	Semana 21	Semana 22	Semana 23	Semana 24	Semana 25	Semana 26
Planteamiento del proyecto	Formulación del anteproyecto	2 mss																										
	Correcciones al documento de anteproyecto	2 sem.																										
Establecimiento del contexto	Definición de criterios de evaluación del riesgo	1 sem																										
	Definición de criterios de impacto	1 sem																										
	Definición de criterios de aceptación del riesgo	1 sem																										
Análisis del riesgo	Identificar los activos	0,5 sem.																										
	Identificar las amenazas	1,5 sem.																										
	Identificar controles existentes	1 sem																										
	identificar las vulnerabilidades	1,5 sem.																										
	Identificar las consecuencias	1 sem																										
Estimación del riesgo	Elegir el metodo de estimación	0,5 sem.																										
	Valorar las consecuencias	1 sem																										
	Valorar los incidentes	1 sem																										
	Estimar el nivel de riesgo	3 sem.																										
Evaluación del riesgo	Comparar los niveles de riesgo frente a los criterios	1 sem																										
	Priorizar los riesgos de acuerdo a los criterios	1 sem																										

Fuente: El autor

1.8. PRODUCTOS A ENTREGAR

- Documentación de las vulnerabilidades, amenazas, riesgos y controles existentes asociados a las tarjetas que han sido utilizadas como medio de pago en el sistema masivo de transporte público transmilenio.
- Listado de identificación de vulnerabilidades, amenazas y riesgos, con sus respectivas valoraciones, detectados en el presente trabajo de investigación.
- Documento formal de la valoración del riesgo acorde a la norma ISO 27005, gestión de activos en la seguridad de la información.

1.8.1 ESTRATEGIAS DE COMUNICACIÓN Y DIVULGACIÓN

Con el fin de divulgar y comunicar los resultados obtenidos del presente proyecto de grado, se establece como principal medio el “repositorio institucional de la Universidad Católica de Colombia”, donde se publicará el documento completo con el desarrollo de la propuesta expuesta anteriormente. Como complemento, el desarrollo y conclusiones serán plasmados en un paper, de tal forma que el conocimiento generado no solo sea divulgado en la organización objeto de estudio, sino también en el ámbito académico.

1.9. PRESUPUESTO

Tabla 6. Presupuesto

		HORA(S)	CANTIDAD	COSTO/Hora	TOTAL
RECURSO FISICO	Computador	384	2	$ 5,208	$ 1.999,872
	Internet	384	2	$ 97,22	$ 113.553
	SUBTOTAL	4	4	$ 102,43	$ 115.553
RECURSO HUMANO	Ingenieros de Sistemas	384	2	$ 41.000	$ 15.744.000
	Asesoría	40	1	$ 16.000	$ 640.000
	SUBTOTAL	2	2	$ 57.000	$ 16.384.000
COSTOS	Gastos Papelería	-	-	-	$ 100.000
	Material físico de investigación	-	-	-	$ 300.000
	Gastos de publicación	-	-	-	$ 150.000
	SUBTOTAL	0	0	0	$ 550.000
OTROS	Imprevistos	-	-	-	$ 500.000
	SUBTOTAL	0	0	0	$ 500.000

TOTAL	$ 17.049.553
TOTAL (Imprevistos)	$ 17.549.553

Fuente: El autor

2. ESTABLECIMIENTO DEL CONTEXTO

El contexto estratégico consiste en la definición de los parámetros internos y externos que deben tenerse en cuenta para la gestión del riesgo y su ámbito de aplicación; está compuesto por la determinación del entorno externo y del ambiente interno de transmilenio s.a., todo esto pretende alcanzar sus objetivos.

2.1. CONTEXTO EXTERNO

- Las obligatoriedades o compromisos normativos institucionales con las regulaciones, aplicaciones y los planes ya determinados.
- Los factores clave y que tengan impacto en el logro de los objetivos, metas y planes de transmilenio s.a., o del proceso.
- Las relaciones con las partes interesadas, proveedores y usuarios.
- Las consecuencias sociales y culturales, legales, regulatorias, financieras, tecnológicas, económicas, naturales, entre otras, de la gestión de las partes interesadas.[15]

2.2. CONTEXTO INTERNO

- El gobierno corporativo, la estructura organizacional, la determinación de responsabilidades, los niveles de autoridad y los flujos de comunicación.
- Los objetivos, las metas, las estrategias y las políticas dispuestas por transmilenio s.a., como parte de la cadena de valor de la entidad, donde se evidencian los procesos.
- La forma y el alcance de las relaciones contractuales desarrolladas en transmilenio s.a.
- Las normas, directrices y modelos adoptados por transmilenio s.a.
- Capacidades expresadas en términos de recursos y el conocimiento (Por ejemplo, capital, tiempo, personas, tecnologías, entre otros).

[15] Transmilenio, 2017. “Contexto Transmilenio”. (05 Febrero de 2019). Disponible en: http://www.transmilenio.gov.co/loader.php?lServicio=Publicaciones&lTipo=WFactionA&lFuncion=visualizar&id=14538&bd=m

2.3. CRITERIOS DE EVALUACIÓN DEL RIESGO

Estos criterios especifican la prioridad con la que se brindará tratamiento al riesgo (etapa no incluida en el presente trabajo de investigación).[16]

Tabla 7. Contexto nivel de riesgo

Nivel de riesgo	Puntaje
Bajo	1 a 2
Medio	3 a 4
Alto	5 a 12
Extremo	15 a 25

Fuente: Transmilenio - https://www.transmilenio.gov.co/publicaciones/149398/m-op-002-manual-para-la-gestin-del-riesgo-en-transmilenio-s-a/

2.4. CRITERIOS DE PROBABILIDAD

Se refiere al nivel de probabilidad[17] , que se determina con base en la frecuencia con la que se ha presentado el evento anteriormente.

Tabla 8. Criterios de probabilidad transmilenio s.a

Nivel	Descripción	Definición	Frecuencia
1	Rara Vez	El evento puede ocurrir solo en circunstancias excepcionales (poco comunes o anormales).	No se ha presentado en los últimos 5 años.
2	Improbable	El evento puede ocurrir en forma esporádica	Al menos 1 vez en los últimos 5 años.
3	Posible	El evento podrá ocurrir en algunas circunstancias.	Al menos 1 vez en los últimos 2 años.

16 Eric Morana.2018. "Niveles de riesgos aceptable versus criterios de aceptacion del riesgo". (05 Febrero de 2019). Disponible en: https://ericmorana.wordpress.com/2012/10/29/niveles-de-riesgo-aceptable-versus-criterios-de-aceptacion-del-riesgo/.

17 Transmilenio, 2017. "Objetivos del sistema integrado de gestión". (05 Febrero de 2019). Disponible en: https://www.transmilenio.gov.co/publicaciones/146051/objetivos_del_sistema_integrado_de_gestion/

4	Frecuente	Es viable que el evento ocurra en la mayoría de las circunstancias	Al menos 1 vez en el último año.
5	Casi Seguro	Se espera que el evento ocurra en la mayoría de las circunstancias	Más de 1 vez al año.

Fuente: Transmilenio - https://www.transmilenio.gov.co/publicaciones/149398/m-op-002-manual-para-la-gestin-del-riesgo-en-transmilenio-s-a/

2.5. CRITERIOS DE IMPACTO

Se entiende como la magnitud de las pérdidas que podrían resultar de una exposición dada, teniendo en cuenta la capacidad que tiene la empresa de afrontar estas pérdidas.

Tabla 9. Criterios de impacto transmilenio s.a.

Nivel	Descripción	Impacto Cualitativo
1	Insignificante	• No hay interrupción de las operaciones de la entidad. • No se generan sanciones económicas o administrativas. • No se afecta la imagen institucional de forma significativa.
2	Menor	• Interrupción de las operaciones de la entidad por algunas horas. • Reclamaciones o quejas de los usuarios que implican investigaciones internas disciplinarias. • Imagen institucional afectada localmente por retrasos en la prestación del servicio a los usuarios o ciudadanos

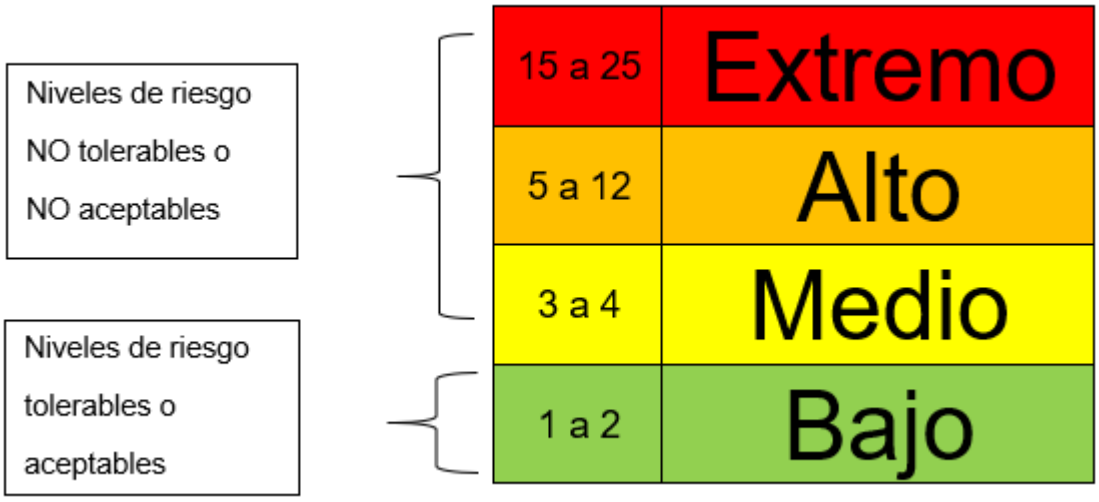
3	Moderado	• Interrupción de las operaciones de la entidad por un (1) día. • Reclamaciones o quejas de los usuarios que podrían implicar una denuncia ante los entes reguladores o una demanda de largo alcance para la entidad. • Inoportunidad en la información ocasionando retrasos en la atención a los usuarios.
4	Mayor	• Interrupción de las operaciones de la entidad por más de dos (2) días. • Pérdida de información crítica que puede ser recuperada de forma parcial o incompleta. • Sanción por parte del ente de control u otro ente regulador. • Incumplimiento en las metas y objetivos institucionales afectando el cumplimiento en las metas de gobierno.
5	Catastrófico	• Interrupción de las operaciones de la entidad por más de cinco (5) días. • Intervención por parte de un ente de control u otro ente regulador. • Pérdida de Información crítica para la entidad que no se puede recuperar.

Fuente: Transmilenio - https://www.transmilenio.gov.co/publicaciones/149398/m-op-002-manual-para-la-gestin-del-riesgo-en-transmilenio-s-a/

2.6. CRITERIOS DE LA ACEPTACIÓN DEL RIESGO

Durante la etapa de evaluación de riesgos se aceptan todos aquellos que tengan el nivel “bajo” [18] en un rango de 1 a 2 y no se aceptan los que tengan nivel “medio” de 3 a 4, nivel “alto” de 5 a 12 y nivel “extremo” de 15 a 25, los cuales deben ser tratados. A pesar de que esta información no se encuentra pública explícitamente, se definen los criterios de la aceptación del riesgo a partir del mapa de calor o colorimétrico de nivel de riesgo inherente que se encuentra público en la página web de transmilenio s.a., todo esto alineado a lo definido por la norma ISO 27001, de gestión de seguridad de la información[19] para los criterios de la aceptación del riesgo[20].

Tabla 10. Criterios de la aceptación del riesgo alineado a la norma ISO 27001



Fuente: Eric Morana - https://ericmorana.wordpress.com/2012/10/29/niveles-de-riesgo-aceptable-versus-criterios-de-aceptacion-del-riesgo/

[18] Transmilenio, 2017. “Gestión de riesgo Transmilenio”. (10 Febrero de 2019). Disponible en: http://www.transmilenio.gov.co/loader.php?lServicio=Publicaciones&lTipo=WFactionA&lFuncion=visualizar&id=14538&bd=m

[19] Normas-ISO, 2018. “ISO 27001 Seguridad de la información”. (11 Febrero de 2019). Disponible en: https://www.normas-iso.com/iso-27001/

[20] Eric Morana.2018. “Niveles de riesgos aceptable versus criterios de aceptacion del riesgo”. (11 Febrero de 2019). Disponible en: https://ericmorana.wordpress.com/2012/10/29/niveles-de-riesgo-aceptable-versus-criterios-de-aceptacion-del-riesgo/.

3. IDENTIFICACIÓN DE RIESGOS

El propósito de la identificación de riesgos de la norma ISO 27005 es determinar el posible suceso de eventos de pérdida y de qué forma podría ocurrir, de esta forma la identificación de riesgos establece varios procedimientos que se desarrollan a continuación.

3.1. IDENTIFICACIÓN DE LOS ACTIVOS

Tabla 11. Relación de activos de información

Nombre del activo	Descripción	Tipo de activo	Proceso asociado
Tarjeta mifare classic	Tarjeta monedero y cliente frecuente	Información	Pago del sistema
Tarjeta EMV	Tarjetas débito y crédito		
Tarjeta mifare plus	Tarjeta tullave		

Fuente: El autor

3.2. IDENTIFICACIÓN DE LAS AMENAZAS

Tabla 12. Relación de amenazas

Tipo	Amenaza	Origen
Compromiso de la información	Manipulación con hardware	D
	Manipulación con software	A, D
Fallas técnicas	Mal funcionamiento del software	A
Acciones no autorizadas	Uso de software falso o copiado	A, D

	Uso no autorizado del equipo	D

Fuente: Norma ISO 27005 - Anexo C

Convención de origen:

Tabla 13. Convención origen de amenazas

Abreviatura	Detalle
A	Accidentales
D	Deliberadas

Fuente: Norma ISO 27005 - Anexo C

3.3. IDENTIFICACIÓN DE LOS CONTROLES EXISTENTES

Para evaluar la eficacia de un control se emplean los siguientes criterios[21] para la evaluación de controles:

Tabla 14. Criterios para la evaluación de control

Criterio de evaluación	Opción de respuesta	Peso
1. Asignación del responsable	Asignado	15
	No Asignado	0
2. Periodicidad	Oportuna	15
	No Oportuna	0
3. Propósito	Preventivo	15
	Detectivo	15
	Correctivo	0
	No es un Control	0
4. Cómo se realiza la actividad del control	Estandarizada	15
	No Estandarizada	0

[21] Mintic, 2018. “Seguridad y privacidad de la información”. (25 Febrero de 2019). Disponible en: https://www.mintic.gov.co/gestionti/615/articles-5482_G7_Gestion_Riesgos.pdf

5. Evidencia de Ejecución del control	Completa	25
	Incompleta	10
	No Existe	0

Fuente: El autor

La única excepción para asignar peso a más de una opción aplica para el criterio de evaluación tres (3), solo si el tipo de control a evaluar reduce impacto es posible asignar peso a la opción correctivo y/o detectivo, según aplique.

La identificación de controles existentes se lleva a cabo por cada activo de información existente en el presente trabajo de investigación, a continuación, se describe y evalúa cada control relacionado a su respectivo activo de información.

3.3.1 Mifare classic.

Pese a que actualmente el fabricante de este tipo de TISC [22] no recomienda el uso de estas en sistemas donde su seguridad es relevante, es importante mencionar su importancia y relevancia a partir de su aparición en el año 1994; donde a raíz de las debilidades evidenciadas en este tipo de TISC surgieron otras TISC con controles más efectivos a los mencionados a continuación.

3.3.1.1. (CTRL - MC01) UID – NUID.

También conocido como CSN (*Card Serial Number*), es un identificador único que el fabricante le asigna a cada chip incorporado en cada tarjeta, este identificador se encuentra definido en la norma ISO 14443-3A. Este tipo de tarjetas contienen identificadores simples de 4 bytes (NUID) o dobles de 7 bytes (UID)[23].

Tabla 15. Calificación de eficacia CTRL_MC01

Criterio de evaluación	Opción de respuesta	Peso
1. Asignación del responsable	Asignado	15

[22] MiFare, 2016. “Chip MiFare Classic”. (10 Marzo de 2019). Disponible en: https://www.mifare.net/es/productos/ics-de-tarjetas-con-chip/familia-mifare-classic

[23] StackOverFlow, 2015. “MiFare - Difference between UID and Serial Number of MiFare Card”. (12 Marzo de 2019). Disponible en: https://stackoverflow.com/questions/17608670/mifare-difference-between-uid-and-serial-number-of-mifare-card.

	No Asignado	0
2. Periodicidad	Oportuna	15
	No Oportuna	0
3. Propósito	Preventivo	15
	Detectivo	0
	Correctivo	0
	No es un Control	0
4. Cómo se realiza la actividad del control	Estandarizada	15
	No Estandarizada	0
5. Evidencia de Ejecución del control	Completa	25
	Incompleta	0
	No Existe	0

Fuente: El autor

3.3.1.2. (CTRL - MC02) RID.

Es un indicador aleatorio dinámico el cual tiene definido un tamaño no variable de 4 bytes.

Tabla 16. Calificación de eficacia CTRL_MC02

Criterio de evaluación	Opción de respuesta	Peso
1. Asignación del responsable	Asignado	15
	No Asignado	0
2. Periodicidad	Oportuna	0
	No Oportuna	0
3. Propósito	Preventivo	15
	Detectivo	0

	Correctivo	0
	No es un Control	0
4. Cómo se realiza la actividad del control	Estandarizada	15
	No Estandarizada	0
5. Evidencia de Ejecución del control	Completa	25
	Incompleta	0
	No Existe	0

Fuente: El autor

3.3.1.3. (CTRL - MC03) Protocolo de autenticación mutua de tres pasos de clave simétrica.

Es un protocolo el cual lleva como nombre de tres pasos, debido a que entre el remitente y receptor se intercambian tres mensajes cifrados, dando seguridad en el envío de mensajes entre dos partes[24].

Tabla 17. Calificación de eficacia CTRL_MC03

Criterio de evaluación	Opción de respuesta	Peso
1. Asignación del responsable	Asignado	15
	No Asignado	0
2. Periodicidad	Oportuna	15
	No Oportuna	0
3. Propósito	Preventivo	15
	Detectivo	0
	Correctivo	0
	No es un Control	0
4. Cómo se realiza la actividad	Estandarizada	0

[24] Crypto, 2016. “Three-pass protocol”. (25 Marzo de 2019).Disponible en https://crypto.stackexchange.com/tags/three-pass-protocol/info

del control	No Estandarizada	0
5. Evidencia de Ejecución del control	Completa	0
	Incompleta	10
	No Existe	0

Fuente: El autor

3.3.1.4. (CTRL - MC04) Conjunto individual de dos claves por sector para admitir aplicaciones múltiples con jerarquía de claves.

Cada sector de la tarjeta maneja 2 crypto llaves, de tal forma que se condiciona el acceso por sector de doble forma.

Tabla 18. Calificación de eficacia CTRL_MC04

Criterio de evaluación	Opción de respuesta	Peso
1. Asignación del responsable	Asignado	15
	No Asignado	0
2. Periodicidad	Oportuna	15
	No Oportuna	0
3. Propósito	Preventivo	15
	Detectivo	0
	Correctivo	0
	No es un Control	0
4. Cómo se realiza la actividad del control	Estandarizada	0
	No Estandarizada	0
5. Evidencia de Ejecución del control	Completa	0
	Incompleta	10
	No Existe	0

Fuente: El autor

3.3.1.5. (CTRL - MC05) Crypto1.

Es un algoritmo de encriptación con patente del fabricante (NXP) creado con el fin de ser implementado en este tipo de tarjetas mifare[25].

Tabla 19. Calificación de eficacia CTRL_MC05

Criterio de evaluación	Opción de respuesta	Peso
1. Asignación del responsable	Asignado	15
	No Asignado	0
2. Periodicidad	Oportuna	0
	No Oportuna	0
3. Propósito	Preventivo	15
	Detectivo	0
	Correctivo	0
	No es un Control	0
4. Cómo se realiza la actividad del control	Estandarizada	0
	No Estandarizada	0
5. Evidencia de Ejecución del control	Completa	0
	Incompleta	10
	No Existe	0

Fuente: El autor

3.3.2 Mifare plus.

Este tipo de TISC tiene como base los controles de seguridad, no todos, implementados en mifare classic, pero con mejoras significativas; este tipo es un

[25] University of Virginia, 2017. “Crypto 1”. (01 Abril de 2019). Disponible en: https://www.cs.virginia.edu/~kn5f/Mifare.Cryptanalysis.htm

punto de referencia dentro de las TISC debido a que cuenta con seguridad AES y facilidad migratoria de su antecesora (mifare classic) a esta[26]. Los controles tecnológicos de seguridad implementados en mifare plus son:

3.3.2.1. (CTRL - MP01) UID – NUID.

Tiene el mismo funcionamiento del implementado en mifare classic, esto con el fin de garantizar compatibilidad y facilidad migratoria desde mifare classic a mifare plus.

Tabla 20. Calificación de eficacia CTRL_MP01

Criterio de evaluación	Opción de respuesta	Peso
1. Asignación del responsable	Asignado	15
	No Asignado	0
2. Periodicidad	Oportuna	15
	No Oportuna	0
3. Propósito	Preventivo	15
	Detectivo	0
	Correctivo	0
	No es un Control	0
4. Cómo se realiza la actividad del control	Estandarizada	15
	No Estandarizada	0
5. Evidencia de Ejecución del control	Completa	25
	Incompleta	0
	No Existe	0

Fuente: El autor

[26] MiFare, 2018. “Familia MiFare Plus”. (02 Abril de 2019).Disponible en: https://www.mifare.net/es/productos/ics-de-tarjetas-con-chip/familia-mifare-plus/

3.3.2.2. (CTRL - MP02) Crypto1 con integración AES.

El algoritmo de encriptación crypto1 fue utilizado en la mifare classic, ya en mifare plus el fabricante integró un esquema de cifrado por bloques conocido como AES (*Advanced Encryption Standard* o Estándar de Encriptación Avanzado) a este algoritmo base.

Tabla 21. Calificación de eficacia CTRL_MP02

Criterio de evaluación	Opción de respuesta	Peso
1. Asignación del responsable	Asignado	15
	No Asignado	0
2. Periodicidad	Oportuna	15
	No Oportuna	0
3. Propósito	Preventivo	15
	Detectivo	0
	Correctivo	0
	No es un Control	0
4. Cómo se realiza la actividad del control	Estandarizada	15
	No Estandarizada	0
5. Evidencia de Ejecución del control	Completa	25
	Incompleta	0
	No Existe	0

Fuente: El autor

3.3.2.3. (CTRL - MP03) Key length.

La longitud de clave consiste en un determinado número de bits en la clave del algoritmo de cifrado, la longitud de la clave determina el número máximo de combinaciones necesarias para romper un algoritmo de cifrado, estos algoritmos de

clave simétrica utilizan la misma clave para el cifrado y el descifrado, mientras que un algoritmo de clave asimétrica utiliza claves diferentes. Hoy en día, la mayoría de los algoritmos de clave simétrica comunes están destinados a tener una seguridad igual a la longitud de su clave[27].

Tabla 22. Calificación de eficacia CTRL_MP03

Criterio de evaluación	Opción de respuesta	Peso
1. Asignación del responsable	Asignado	15
	No Asignado	0
2. Periodicidad	Oportuna	15
	No Oportuna	0
3. Propósito	Preventivo	15
	Detectivo	0
	Correctivo	0
	No es un Control	0
4. Cómo se realiza la actividad del control	Estandarizada	15
	No Estandarizada	0
5. Evidencia de Ejecución del control	Completa	25
	Incompleta	0
	No Existe	0

Fuente: El autor

3.3.2.4. (CTRL - MP04) Authentication key / password.

La autenticación basada en claves es un tipo de autenticación que se puede utilizar como alternativa a la autenticación de contraseña. En lugar de requerir la

[27] Techopedia, 2015. “Key Length”. (02 Abril de 2019) Disponible en: https://www.techopedia.com/definition/3999/key-length

contraseña de un usuario, es posible confirmar la identidad del cliente mediante el uso de algoritmos de criptografía asimétrica, con claves públicas y privadas[28].

Tabla 23. Calificación de eficacia CTRL_MP04

Criterio de evaluación	Opción de respuesta	Peso
1. Asignación del responsable	Asignado	15
	No Asignado	0
2. Periodicidad	Oportuna	15
	No Oportuna	0
3. Propósito	Preventivo	15
	Detectivo	0
	Correctivo	0
	No es un Control	0
4. Cómo se realiza la actividad del control	Estandarizada	15
	No Estandarizada	0
5. Evidencia de Ejecución del control	Completa	25
	Incompleta	0
	No Existe	0

Fuente: El autor

3.3.3. EMV.

Es un acrónimo de Europay MasterCard Visa, este tipo de tarjetas inteligentes cuentan con un circuito integrado para la autenticación de pagos mediante tarjetas de crédito y débito que permite una interoperabilidad segura en cada transacción, esta tecnología lo que implica es mayor seguridad, por lo cual una reducción en el

[28] Crypto.net. “Key-Based Authentication (Public Key Authentication)”. (03 Abril de 2019) . Disponible en: http://www.crypto-it.net/eng/tools/key-based-authentication.html

fraude, esto se logra por medio de los algoritmos de cifrado que manejan este tipo de tarjetas, a continuación, se indicarán los controles tecnológicos EMV:

3.3.3.1. (CTRL - EMV01) Niveles EMV.

Cuenta con dos tipos de niveles que son: interfaces a nivel físico y transporte, y el último que se considera de segundo nivel cubre las aplicaciones de pago y el procesamiento de transacciones financieras mediante tarjetas de crédito[29].

Tabla 24. Calificación de eficacia CTRL_EMV01

Criterio de evaluación	Opción de respuesta	Peso
1. Asignación del responsable	Asignado	0
	No Asignado	0
2. Periodicidad	Oportuna	15
	No Oportuna	0
3. Propósito	Preventivo	15
	Detectivo	0
	Correctivo	0
	No es un Control	0
4. Cómo se realiza la actividad del control	Estandarizada	15
	No Estandarizada	0
5. Evidencia de Ejecución del control	Completa	25
	Incompleta	0
	No Existe	0

Fuente: El autor

[29] Gemalto, 2016. “Explaining EMV payment”. (03 Abril de 2019). Disponible en: https://www.gemalto.com/latam/servicios-financieros/tarjertas/emv/acerca

3.3.3.2. (CTRL - EMV02) Esquemas de autenticación robustos.

La tecnología de tarjetas inteligentes EMV utiliza algoritmos de encriptación, que se componen de tres algoritmos (3Des - SDA - DDA) fundamentales para la seguridad de los sistemas de acceso, para evitar ataques a las transacciones en línea y que sean indescifrables. Estos algoritmos aplican diferentes operaciones básicas para convertir texto en otro tipo de cifrado y empleando claves criptográficas en tres iteraciones[30].

Tabla 25. Calificación de eficacia CTRL_EMV02

Criterio de evaluación	Opción de respuesta	Peso
1. Asignación del responsable	Asignado	15
	No Asignado	0
2. Periodicidad	Oportuna	15
	No Oportuna	0
3. Propósito	Preventivo	15
	Detectivo	0
	Correctivo	0
	No es un Control	0
4. Cómo se realiza la actividad del control	Estandarizada	15
	No Estandarizada	0
5. Evidencia de Ejecución del control	Completa	0
	Incompleta	0
	No Existe	0

Fuente: El autor

[30] By, 2017. “Algoritmos de encryptamiento AES”. (04 Abril de 2019). Disponible en: https://www.by.com.es/blog/algoritmos-encriptacion-aes-3des/

3.3.3.3. (CTRL - EMV03) Cuatro fases de autenticación.

La tarjeta EMV cumple con el estándar ISO 14443 tipo A, que se refiere a 4 ciclos de autenticaciones, donde se considera los métodos de modulación, codificación de las llaves únicas, inicialización y transmisión de la información contenida en la tarjeta y el lector o palenquera para evitar posibles fraudes [31] e interferencia de información.

Tabla 26. Calificación de eficacia CTRL_EMV03

Criterio de evaluación	Opción de respuesta	Peso
1. Asignación del responsable	Asignado	15
	No Asignado	0
2. Periodicidad	Oportuna	15
	No Oportuna	0
3. Propósito	Preventivo	15
	Detectivo	0
	Correctivo	0
	No es un Control	0
4. Cómo se realiza la actividad del control	Estandarizada	15
	No Estandarizada	0
5. Evidencia de Ejecución del control	Completa	0
	Incompleta	0
	No Existe	0

Fuente: El autor

3.3.3.4. (CTRL - EMV04) Comandos de tarjeta (apdu's).

Basado en la norma ISO 7816, hecha para las tarjetas inteligentes e identificaciones electrónicas, contiene 3 archivos primordiales, el primero se denomina archivo

[31] Fodafin, 2015. "Seminario de Transporte tarjetas inteligentes". (04 Abril de 2019). Disponible en: http://www.fonadin.gob.mx/wp-ontent/uploads/2016/08/SeminarioTransporte_FONADIN_FIMPE.pdf

principal (MF) que es el que contiene toda la información contenida de la tarjeta; el segundo, archivo dedicado (DF), consta de subdivisiones dentro de la tarjeta para segmentar información en sectores; y como último, se encuentra el archivo elemental (EF), que almacena los datos en cualquier tipo de formato (binario, bytes, etc.)[32].

Tabla 27.Calificación de eficacia CTRL_EMV04

Criterio de evaluación	Opción de respuesta	Peso
1. Asignación del responsable	Asignado	15
	No Asignado	0
2. Periodicidad	Oportuna	15
	No Oportuna	0
3. Propósito	Preventivo	0
	Detectivo	0
	Correctivo	15
	No es un Control	0
4. Cómo se realiza la actividad del control	Estandarizada	15
	No Estandarizada	0
5. Evidencia de Ejecución del control	Completa	0
	Incompleta	0
	No Existe	0

Fuente: El autor

3.3.3.5. (CTRL - EMV05) Módulo de acceso seguro SAM.

Se utiliza para mejorar la seguridad en los dispositivos que cuentan con algún tipo de criptografía, comúnmente en dispositivos que necesitan realizar transacciones

[32] CardWerk, 21015. “ISO 7816 Part 4”. (05 Abril de 2019). Disponible en: https://cardwerk.com/iso-7816-part-4/

seguras, como terminales de pago. El módulo SAM se encarga de toda la gestión de llaves y de la criptografía[33].

Tabla 28. Calificación de eficacia CTRL_EMV05

Criterio de evaluación	Opción de respuesta	Peso
1. Asignación del responsable	Asignado	15
	No Asignado	0
2. Periodicidad	Oportuna	15
	No Oportuna	0
3. Propósito	Preventivo	15
	Detectivo	0
	Correctivo	0
	No es un Control	0
4. Cómo se realiza la actividad del control	Estandarizada	15
	No Estandarizada	0
5. Evidencia de Ejecución del control	Completa	0
	Incompleta	10
	No Existe	0

Fuente: El autor

3.4. IDENTIFICACIÓN DE VULNERABILIDADES

Dentro de lo contemplado en la norma ISO 27005, se identificarán vulnerabilidades en las siguientes áreas:

- Configuración del sistema de información.
- Software o hardware (de los activos de información de la investigación).

[33] CardLogix, 2017. “Modelo SAM”. (06 Abril de 2019).Disponible en: https://www.cardlogix.com/glossary/sam-card-secure-access-module-secure-application-module/

A continuación, se presenta un listado de vulnerabilidades identificadas con relación al activo de información, amenaza y control existente:

Tabla 29. Identificación de vulnerabilidades

Activo	Amenaza	Control	Vulnerabilidad
Mifare classic	Mal funcionamiento del software, manipulación con software y manipulación con hardware	CTRL - MC03, CTRL - MC04 y CTRL - MC05	Mezcla de la capa de enlace de datos y la capa de comunicación.[34]
Mifare classic	Mal funcionamiento del software y manipulación con software	CTRL - MC04	Filtración de 32 bits de los 48 bits que comprenden la clave de un sector, conociendo la clave completa de cualquier otro sector.
Mifare classic	Manipulación con software	CTRL - MC04 y CTRL - MC05	Longitud corta de la clave asignada por sector (48 bits).[35]
Mifare classic	Mal funcionamiento del software	CTRL - MC02	Ausencia de aleatoriedad en los números únicos generados (RUID).[36]
Mifare classic	Mal funcionamiento del software, manipulación con software y manipulación con hardware	CTRL - MC05	Filtración de 4 bits de clave por error en autenticación.[37]
Mifare classic	Mal funcionamiento del software y manipulación con software	CTRL - MC03, CTRL - MC04 y CTRL - MC05	Facilidad en el cálculo de un estado anterior del LSFR (registro de desplazamiento con retroalimentación lineal).[38]

[34] Radboud University. 2019. “Wirelessly Pickpocketing a Mifare Classic Card”. (07 Abril de 2019). Disponible en: https://repository.ubn.ru.nl/handle/2066/75545

[35] Defense Technical Information Center, 1996. “Minimal Key Lengths for Symmetric Ciphers to Provide Adequate Commercial Security. A Report by an Ad Hoc Group of Cryptographers and Computer Scientists”.(07 Abril de 2019).Disponible en: https://apps.dtic.mil/docs/citations/ADA389646

[36] Springer, 2014. “A Practical Attack on Patched MIFARE Classic.”. (08 Abril de 2019). Disponible en: https://link.springer.com/book/10.1007/978-3-319-12087-4

[37] Nicolas T. Courtois. “The dard side of security by obscurity”. (08 Abril de 2019). Disponible en: http://www.scitepress.org/Papers/2009/22380/22380.pdf

[38] F.D Garcia, 2008. “Dismantling MIFARE Classic”. (08 Abril de 2019). Disponible en: https://research.tue.nl/en/publications/dismantling-mifare-classic

Mifare classic	Mal funcionamiento del software	CTRL - MC03, CTRL - MC04 y CTRL - MC05	Configuración incorrecta de parámetros de la función que toma las entradas del LSFR.
EMV	Manipulación con hardware, uso no autorizado del equipo	CTRL - EMV03	Autorización de transacciones por medio de código PIN erróneo en los dispositivos de cobro.[39]
EMV	Mal funcionamiento del software, uso no autorizado del equipo	CTRL - EMV02	Transacciones en línea por medio de clonación y falsificación de tarjetas EMV.
EMV	Manipulación con hardware, manipulación con software	CTRL - EMV03, CTRL - EMV02, CTRL - EMV04	Alteración de dispositivos de lectura de la tecnología EMV, con la posibilidad de realizar modificaciones en las transacciones.[40]
EMV	Manipulación con software	CTRL - EMV01	Falsificación de las firmas electrónicas realizadas durante las transacciones.
EMV	Mal funcionamiento del software	CTRL - EMV01	Confidencialidad de la información de la tarjeta EMV de forma visible, como es el PIN y fecha de caducidad.
EMV	Manipulación con hardware, uso no autorizado del equipo	CTRL - EMV01, CTRL - EMV03	Perturbación de la comunicación de la tarjeta EMV y el dispositivo lector por medio de snnifers o algún otro tipo de equipo para interrumpir las transacciones.

Fuente: El autor

[39] Mike Bond, 2015. “The EMV preplay attack”. (09 Abril de 2019) Disponible en: https://ieeexplore.ieee.org/document/7085649

[40] Emmanuel Bertin, 2018. “An Overview of the EMV Protocol and Its Security Vulnerabilities”. (09 Abril de 2019).Disponible en: https://www.researchgate.net/publication/323073718_An_Overview_of_the_EMV_Protocol_and_Its_Security_Vulnerabilities

3.5. IDENTIFICACIÓN DE CONSECUENCIAS

La identificación de daños o consecuencias, con su respectiva causa o escenario incidente, se compone de un listado de consecuencias relacionadas a cada escenario de incidente, activo de información (que tenga asociado una vulnerabilidad y amenaza) y proceso del negocio.

Tabla 30. Identificación de consecuencias

Escenario de incidente	Consecuencia	Activo	Proceso del negocio
Mal funcionamiento del software debido a la mezcla de la capa de enlace de datos y la capa de comunicación, permitiendo establecer un canal lateral a partir de un código de error (que contiene parte de la clave del sector) obtenido luego de un intento de autenticación fallido.	Pérdida de la confidencialidad de la clave cifrada, lo que conlleva a pérdidas económicas por ingresos no percibidos producto de la carga de saldo no autorizada.	Mifare classic	Pago del sistema
Manipulación con software que toma ventaja de la mezcla de la capa de enlace de datos y la capa de comunicación, permitiendo establecer un canal lateral a partir de un código de error (que contiene parte de la clave del sector) obtenido luego de un intento de autenticación fallido.	Pérdida de la confidencialidad de la clave cifrada, lo que conlleva a pérdidas económicas por ingresos no percibidos producto de la carga de saldo no autorizada.	Mifare classic	Pago del sistema
Manipulación con hardware que a partir de la mezcla de la capa de enlace de datos y la capa de comunicación, permite establecer un canal lateral a partir de un código de error (que contiene parte de la clave del sector) obtenido luego de un intento de autenticación fallido.	Pérdida de la confidencialidad de la clave cifrada, lo que conlleva a pérdidas económicas por ingresos no percibidos producto de la carga de saldo no autorizada.	Mifare classic	Pago del sistema

Mal funcionamiento del software debido a la mezcla de la capa de enlace de datos y la capa de comunicación, permitiendo establecer un canal lateral a partir de un código de error (que contiene parte de la clave del sector) obtenido luego de un intento de autenticación fallido.	Pérdida de la confidencialidad de la clave cifrada, trayendo como consecuencia la afectación reputacional de la organización debido al fácil acceso al cifrado.	Mifare classic	Pago del sistema
Manipulación con software que toma ventaja de la mezcla de la capa de enlace de datos y la capa de comunicación, permitiendo establecer un canal lateral a partir de un código de error (que contiene parte de la clave del sector) obtenido luego de un intento de autenticación fallido.	Pérdida de la confidencialidad de la clave cifrada, trayendo como consecuencia la afectación reputacional de la organización debido al fácil acceso al cifrado.	Mifare classic	Pago del sistema
Manipulación con hardware que a partir de la mezcla de la capa de enlace de datos y la capa de comunicación, permite establecer un canal lateral a partir de un código de error (que contiene parte de la clave del sector) obtenido luego de un intento de autenticación fallido.	Pérdida de la confidencialidad de la clave cifrada, trayendo como consecuencia la afectación reputacional de la organización debido al fácil acceso al cifrado.	Mifare classic	Pago del sistema
Mal funcionamiento del software por filtración de 32 bits de los 48 bits que comprenden la clave de un sector, teniendo como premisa el conocimiento de la clave completa de cualquier otro sector.	Pérdida de la confidencialidad de la clave cifrada del sector, afectando económicamente a la organización debido a la posible escritura de los sectores que contienen el saldo, dejando así de recibir ingresos por el pago de pasajes.	Mifare classic	Pago del sistema

Mal funcionamiento del software por filtración de 32 bits de los 48 bits que comprenden la clave de un sector, teniendo como premisa el conocimiento de la clave completa de cualquier otro sector.	Pérdida de la confidencialidad de la clave cifrada del sector, afectando la imagen de la organización producto del fácil acceso al contenido cifrado.	Mifare classic	Pago del sistema
Manipulación con software que conlleva a la filtración de 32 bits de los 48 bits que comprenden la clave de un sector, teniendo como premisa el conocimiento de la clave completa de cualquier otro sector.	Pérdida de la confidencialidad de la clave cifrada del sector, afectando económicamente a la organización debido a la posible escritura de los sectores que contienen el saldo, dejando así de recibir ingresos por el pago de pasajes.	Mifare classic	Pago del sistema
Manipulación con software que conlleva a la filtración de 32 bits de los 48 bits que comprenden la clave de un sector, teniendo como premisa el conocimiento de la clave completa de cualquier otro sector.	Pérdida de la integridad de la información, teniendo como posibilidad la copia de la información contenida en todos los sectores de la tarjeta resultando esto en la clonación del activo, afectando financieramente a la organización.	Mifare classic	Pago del sistema
Manipulación con software que conlleva a la filtración de 32 bits de los 48 bits que comprenden la clave de un sector, teniendo como premisa el conocimiento de la clave completa de cualquier otro sector.	Pérdida de la confidencialidad de la clave cifrada de los sectores, afectando la imagen de la organización debido a la clonación de las tarjetas.	Mifare classic	Pago del sistema

Fuente: El autor

Para más información sobre el listado de identificación de consecuencias, dirigirse al (Anexo A).

4. ESTIMACIÓN DE RIESGOS

El propósito de la estimación de riesgos, en la norma ISO 27005, es establecer las escalas de medición a evaluar sobre la criticidad de activos, vulnerabilidades e incidentes tanto su consecuencia y probabilidad de ocurrencia de eventos. La estimación de este trabajo de investigación se basó con las escalas de evaluación que maneja transmilenio s.a., información que se encuentra en su página web oficial [41] .El método de estimación a utilizar es de forma semi - cualitativa basándose en una combinación de variables cualitativas y cuantitativas que permiten la estimación de consecuencia y probabilidad del riesgo.

4.1. VALORACIÓN DE CONSECUENCIAS

El objetivo de la valoración de consecuencias es llevar a cabo el análisis del impacto en la organización, que pueda resultar de incidentes posibles o reales en la seguridad de la información teniendo en cuenta las consecuencias de la posible afectación de más de un activo, asociado a amenazas y vulnerabilidades, donde su evaluación tendrá impactos diferentes en los activos evaluados.

Tabla 31. Valoración de consecuencias

Escenario de incidente	Consecuencia	Impacto	Nivel	Activo
Mal funcionamiento del software debido a la mezcla de la capa de enlace de datos y la capa de comunicación, permitiendo establecer un canal lateral a partir de un código de error (que contiene parte de la clave del sector) obtenido luego de un intento de autenticación fallido.	Pérdida de la confidencialidad de la clave cifrada, lo que conlleva a pérdidas económicas por ingresos no percibidos producto de la carga de saldo no autorizada.	Mayor	4	Mifare classic

[41] Transmilenio, 2018. “Manual para la gestión de riesgos TRANSMILENIO S.A”. (02 Mayo de 2019) Disponible en: https://www.transmilenio.gov.co/publicaciones/149398/m-op-002-manual-para-la-gestin-del-riesgo-en-transmilenio-s-a/

Manipulación con software que toma ventaja de la mezcla de la capa de enlace de datos y la capa de comunicación, permitiendo establecer un canal lateral a partir de un código de error (que contiene parte de la clave del sector) obtenido luego de un intento de autenticación fallido.	Pérdida de la confidencialidad de la clave cifrada, lo que conlleva a pérdidas económicas por ingresos no percibidos producto de la carga de saldo no autorizada.	Mayor	4	Mifare classic
Manipulación con hardware que a partir de la mezcla de la capa de enlace de datos y la capa de comunicación, permite establecer un canal lateral a partir de un código de error (que contiene parte de la clave del sector) obtenido luego de un intento de autenticación fallido.	Pérdida de la confidencialidad de la clave cifrada, lo que conlleva a pérdidas económicas por ingresos no percibidos producto de la carga de saldo no autorizada.	Mayor	4	Mifare classic
Mal funcionamiento del software debido a la mezcla de la capa de enlace de datos y la capa de comunicación, permitiendo establecer un canal lateral a partir de un código de error (que contiene parte de la clave del sector) obtenido luego de un intento de autenticación fallido.	Pérdida de la confidencialidad de la clave cifrada, trayendo como consecuencia la afectación reputacional de la organización debido al fácil acceso al cifrado.	Menor	2	Mifare classic
Manipulación con software que toma ventaja de la mezcla de la capa de enlace de datos y la capa de comunicación, permitiendo establecer un canal lateral a partir de un código de error (que contiene parte de la clave del sector) obtenido luego de un intento de autenticación fallido.	Pérdida de la confidencialidad de la clave cifrada, trayendo como consecuencia la afectación reputacional de la organización debido al fácil acceso al cifrado.	Menor	2	Mifare classic

Manipulación con hardware que a partir de la mezcla de la capa de enlace de datos y la capa de comunicación, permite establecer un canal lateral a partir de un código de error (que contiene parte de la clave del sector) obtenido luego de un intento de autenticación fallido.	Pérdida de la confidencialidad de la clave cifrada, trayendo como consecuencia la afectación reputacional de la organización debido al fácil acceso al cifrado.	Menor	2	Mifare classic
Mal funcionamiento del software por filtración de 32 bits de los 48 bits que comprenden la clave de un sector, teniendo como premisa el conocimiento de la clave completa de cualquier otro sector.	Pérdida de la confidencialidad de la clave cifrada del sector, afectando económicamente a la organización debido a la posible escritura de los sectores que contienen el saldo, dejando así de recibir ingresos por el pago de pasajes.	Mayor	4	Mifare classic
Mal funcionamiento del software por filtración de 32 bits de los 48 bits que comprenden la clave de un sector, teniendo como premisa el conocimiento de la clave completa de cualquier otro sector.	Pérdida de la confidencialidad de la clave cifrada del sector, afectando la imagen de la organización producto del fácil acceso al contenido cifrado.	Menor	2	Mifare classic
Manipulación con software que conlleva a la filtración de 32 bits de los 48 bits que comprenden la clave de un sector, teniendo como premisa el conocimiento de la clave completa de cualquier otro sector.	Pérdida de la confidencialidad de la clave cifrada del sector, afectando económicamente a la organización debido a la posible escritura de los sectores que contienen el saldo,	Mayor	4	Mifare classic

	dejando así de recibir ingresos por el pago de pasajes.			
Manipulación con software que conlleva a la filtración de 32 bits de los 48 bits que comprenden la clave de un sector, teniendo como premisa el conocimiento de la clave completa de cualquier otro sector.	Pérdida de la integridad de la información, teniendo como posibilidad la copia de la información contenida en todos los sectores de la tarjeta resultando esto en la clonación del activo, afectando financieramente a la organización.	Mayor	4	Mifare classic
Manipulación con software que conlleva a la filtración de 32 bits de los 48 bits que comprenden la clave de un sector, teniendo como premisa el conocimiento de la clave completa de cualquier otro sector.	Pérdida de la confidencialidad de la clave cifrada de los sectores, afectando la imagen de la organización debido a la clonación de las tarjetas.	Menor	2	Mifare classic
Manipulación con software que aprovecha la longitud corta de la clave asignada por sector (48 bits).	Pérdida de la confidencialidad de la clave cifrada para un sector, permitiendo escribir sobre sectores que contienen información de saldo y afectando económicamente a la empresa.	Mayor	4	Mifare classic

Fuente: El autor

Para más información sobre el listado de valoración de consecuencias, dirigirse al (Anexo B).

4.2. VALORACIÓN DE LOS INCIDENTES

El objetivo de la valoración de incidentes es establecer la probabilidad de cada escenario identificado y frecuencia de ocurrencia, utilizando la estimación semi - cualitativa teniendo presente los controles existentes por cada activo de información, en el *(Anexo C)* se recopilan todos los incidentes identificados.

Tabla 32. Valoración de incidentes

Escenario de incidente	Probabilidad	Nivel
Mal funcionamiento del software debido a la mezcla de la capa de enlace de datos y la capa de comunicación, permitiendo establecer un canal lateral a partir de un código de error (que contiene parte de la clave del sector) obtenido luego de un intento de autenticación fallido.	Improbable	2
Manipulación con software que toma ventaja de la mezcla de la capa de enlace de datos y la capa de comunicación, permitiendo establecer un canal lateral a partir de un código de error (que contiene parte de la clave del sector) obtenido luego de un intento de autenticación fallido.	Posible	3
Manipulación con hardware que a partir de la mezcla de la capa de enlace de datos y la capa de comunicación, permite establecer un canal lateral a partir de un código de error (que contiene parte de la clave del sector) obtenido luego de un intento de autenticación fallido.	Posible	3

Mal funcionamiento del software debido a la mezcla de la capa de enlace de datos y la capa de comunicación, permitiendo establecer un canal lateral a partir de un código de error (que contiene parte de la clave del sector) obtenido luego de un intento de autenticación fallido.	Improbable	2
Manipulación con software que toma ventaja de la mezcla de la capa de enlace de datos y la capa de comunicación, permitiendo establecer un canal lateral a partir de un código de error (que contiene parte de la clave del sector) obtenido luego de un intento de autenticación fallido.	Posible	3
Manipulación con hardware que a partir de la mezcla de la capa de enlace de datos y la capa de comunicación, permite establecer un canal lateral a partir de un código de error (que contiene parte de la clave del sector) obtenido luego de un intento de autenticación fallido.	Posible	3
Mal funcionamiento del software por filtración de 32 bits de los 48 bits que comprenden la clave de un sector, teniendo como premisa el conocimiento de la clave completa de cualquier otro sector.	Frecuente	4
Mal funcionamiento del software por filtración de 32 bits de los 48 bits que comprenden la clave de un sector, teniendo como premisa el conocimiento de la clave completa de cualquier otro sector.	Frecuente	4

Manipulación con software que conlleva a la filtración de 32 bits de los 48 bits que comprenden la clave de un sector, teniendo como premisa el conocimiento de la clave completa de cualquier otro sector.	Frecuente	4
Manipulación con software que conlleva a la filtración de 32 bits de los 48 bits que comprenden la clave de un sector, teniendo como premisa el conocimiento de la clave completa de cualquier otro sector.	Frecuente	4
Manipulación con software que conlleva a la filtración de 32 bits de los 48 bits que comprenden la clave de un sector, teniendo como premisa el conocimiento de la clave completa de cualquier otro sector.	Frecuente	4
Manipulación con software que aprovecha la longitud corta de la clave asignada por sector (48 bits).	Casi Seguro	5
Manipulación con software que aprovecha la longitud corta de la clave asignada por sector (48 bits).	Casi Seguro	5
Mal funcionamiento del software debido a la ausencia de aleatoriedad en los números únicos generados (RUID).	Frecuente	4
Mal funcionamiento del software debido a la ausencia de aleatoriedad en los números únicos generados (RUID).	Frecuente	4
Mal funcionamiento del software producto de la filtración de 4 bits de clave de sector por error en autenticación.	Frecuente	4

Fuente: El autor

Para más información sobre el listado de valoración de incidentes, dirigirse al (Anexo C).

4.3. NIVEL DE ESTIMACIÓN DEL RIESGO

El nivel de estimación del riesgo fija valores de impacto y probabilidad a cada riesgo por medio de la estimación semi-cualitativa, se puede encontrar como se realiza de la combinación del impacto por la probabilidad de ocurrencia de los escenarios incidentes identificados (impacto * probabilidad) determinando los niveles de severidad de cada riesgo.

Tabla 33. Nivel de estimación del riesgo

Código	Riesgo	Nivel Impacto	Nivel Probabilidad	Nivel de Riesgo	Nivel de Severidad
RSK-01	Pérdida de la confidencialidad de la clave cifrada lo que conlleva a pérdidas económicas, debido a la mezcla de la capa de enlace de datos y la capa de comunicación, permitiendo establecer un canal lateral a partir de un código de error (que contiene parte de la clave del sector) obtenido luego de un intento de autenticación fallido, producto del mal funcionamiento del software.	4	2	8	Alto
RSK-02	Pérdida de la confidencialidad de la clave cifrada lo que conlleva a pérdidas económicas, debido a la mezcla de la capa de enlace de datos y la capa de comunicación, permitiendo establecer un canal lateral a partir de un código de error (que contiene parte de la clave del sector) obtenido luego	4	3	12	Alto

	de un intento de autenticación fallido, producto de la manipulación con software.				
RSK-03	Pérdida de la confidencialidad de la clave cifrada lo que conlleva a pérdidas económicas, debido a la mezcla de la capa de enlace de datos y la capa de comunicación, permitiendo establecer un canal lateral a partir de un código de error (que contiene parte de la clave del sector) obtenido luego de un intento de autenticación fallido, producto de la manipulación con hardware.	4	3	12	Alto
RSK-04	Pérdida de la confidencialidad de la clave cifrada, trayendo como consecuencia la afectación reputacional de la organización, debido a la mezcla de la capa de enlace de datos y la capa de comunicación, permitiendo establecer un canal lateral a partir de un código de error (que contiene parte de la clave del sector) obtenido luego de un intento de autenticación fallido, producto del mal funcionamiento del software.	2	2	4	Medio

RSK-05	Pérdida de la confidencialidad de la clave cifrada, trayendo como consecuencia la afectación reputacional de la organización, debido a la mezcla de la capa de enlace de datos y la capa de comunicación, permitiendo establecer un canal lateral a partir de un código de error (que contiene parte de la clave del sector) obtenido luego de un intento de autenticación fallido, producto de la manipulación con software.	2	3	6	Alto
RSK-06	Pérdida de la confidencialidad de la clave cifrada, trayendo como consecuencia la afectación reputacional de la organización, debido a la mezcla de la capa de enlace de datos y la capa de comunicación, permitiendo establecer un canal lateral a partir de un código de error (que contiene parte de la clave del sector) obtenido luego de un intento de autenticación fallido, producto de la manipulación con software.	2	3	6	Alto

Fuente: El autor

Para más información sobre el listado de nivel de estimación del riesgo, dirigirse al (Anexo D).

5. EVALUACIÓN DE RIESGOS

La evaluación de riesgos es una fase clave dentro de la valoración de riesgos, ya que se comparan los niveles de riesgo frente a los criterios de evaluación y aceptación del riesgo, donde el resultado de esto es el insumo para la toma de decisiones al momento de formular controles o mejorar los actuales (fase no incluida dentro del presente trabajo de investigación).

5.1. PRIORIZACIÓN DE RIESGOS

En el anexo *(Anexo E)*, se presenta una tabla con el nivel de severidad del riesgo priorizado (de mayor a menor) de acuerdo con los criterios de evaluación del riesgo.

Tabla 34. Lista de riesgos priorizados con respecto a los criterios de evaluación y aceptación del riesgo.

Código	Riesgo	Nivel de riesgo	Nivel de severidad	Criterio de aceptación
RSK-12	Pérdida de la confidencialidad de la clave cifrada para un sector, afectando económicamente a la empresa, debido a la longitud corta de la clave asignada por sector (48 bits), producto de la manipulación con software.	20	Extremo	NO tolerable o NO aceptable
RSK - 07	Pérdida de la confidencialidad de la clave cifrada del sector, afectando económicamente a la organización, debido a la filtración de 32 bits de los 48 bits que comprenden la clave de un sector, teniendo como premisa el conocimiento de la clave	16	Extremo	NO tolerable o NO aceptable

	completa de cualquier otro sector, producto del mal funcionamiento del software.			
RSK-09	Pérdida de la confidencialidad de la clave cifrada del sector, afectando económicamente a la organización, debido a la filtración de 32 bits de los 48 bits que comprenden la clave de un sector, teniendo como premisa el conocimiento de la clave completa de cualquier otro sector, producto de la manipulación con software.	16	Extremo	NO tolerable o NO aceptable
RSK-10	Pérdida de la integridad de la información, afectando financieramente a la organización, debido a la filtración de 32 bits de los 48 bits que comprenden la clave de un sector, teniendo como premisa el conocimiento de la clave completa de cualquier otro sector, producto de la manipulación con software.	16	Extremo	NO tolerable o NO aceptable
RSK-14	Pérdida de la integridad de la información de la tarjeta, impactando de forma negativa la parte económica de la organización, debido a la ausencia de aleatoriedad en los números únicos generados (RUID), producto del mal	16	Extremo	NO tolerable o NO aceptable

	funcionamiento del software.			
RSK-33	Pérdida de la confidencialidad de la información personal de los usuarios, teniendo como consecuencia la afectación financiera de la organización debido al procedimiento de la información contenida en las tarjetas de crédito, efectuando algún tipo de transacción en línea producto de la utilización de forma no autorizada	16	Extremo	NO tolerable o NO aceptable
RSK-35	Pérdida de la integridad en las transacciones, teniendo como consecuencia la afectación financiera debido a las interrupciones de la comunicación en las transferencias, para realizar actos de clonación, fraudes o modificaciones producto del uso indebido de las interrupciones de la comunicación.	16	Extremo	NO tolerable o NO aceptable

Fuente: El autor

Para más información sobre el listado de priorización de riesgo, dirigirse al (Anexo E).

5.2. REGISTRO E INFORME

Una herramienta útil para mostrar los resultados de la evaluación de riesgos es el mapa colorimétrico ya que brinda una visión general del riesgo, facilitando la visualización y comprensión de datos para comunicar los riesgos identificados y estimados que enfrenta la organización. El mapa colorimétrico del presente trabajo de investigación será el implementado en transmilenio s.a. en su gestión de riesgos[42].

Ilustración 3. Mapa colorimétrico del riesgo

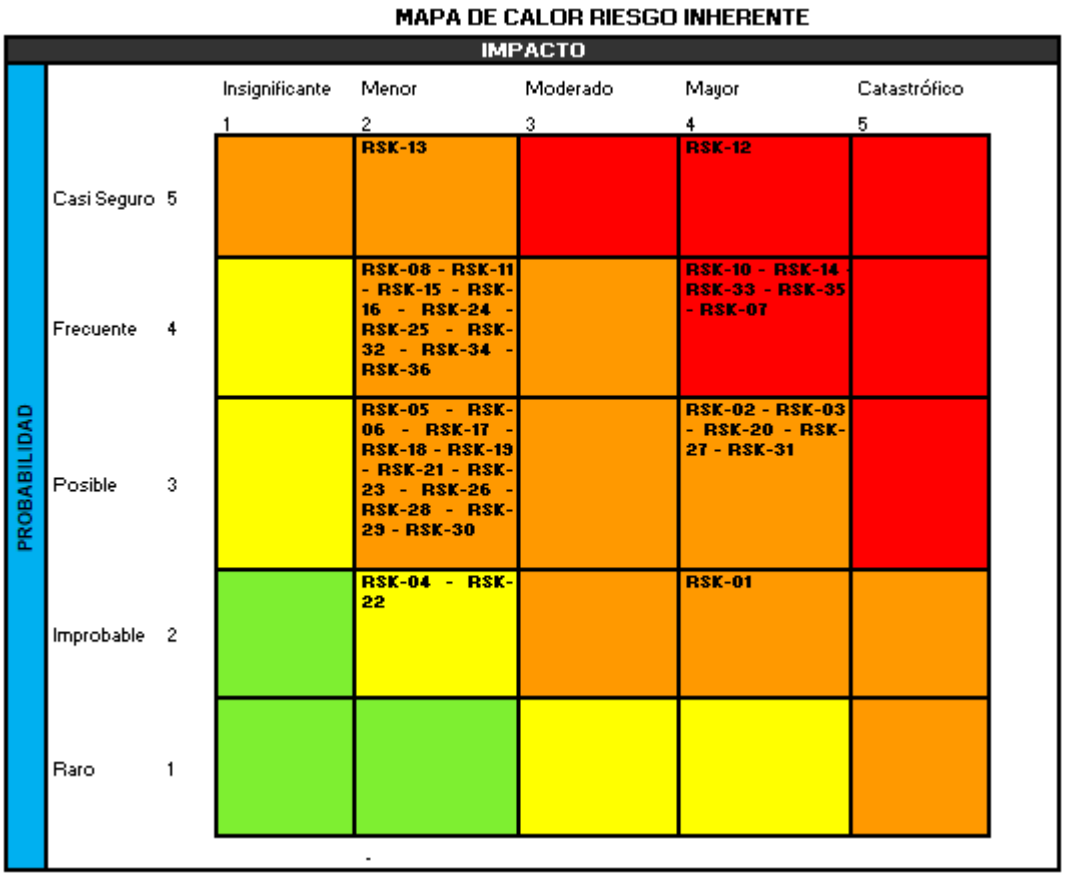
PROBABILIDAD	5	Casi seguro	5	10	15	20	25
	4	Frecuente	4	8	12	16	20
	3	Posible	3	6	9	12	15
	2	Improbable	2	4	6	8	10
	1	Rara vez	1	2	3	4	5
IMPACTO			Insignificante	Menor	Moderado	Mayor	Catastrófico
			1	2	3	4	5

Fuente: transmilenio - https://www.transmilenio.gov.co/publicaciones/149398/m-op-002-manual-para-la-gestin-del-riesgo-en-transmilenio-s-a/

A continuación, se presentan el mapa colorimétrico donde se muestra el resultado final de la evaluación del riesgo inherente para la tarjeta mifare classic y EMV (combinado):

[42] Transmilenio, 2018. “Gestión de riesgos Transmilenio S.A”. (06 Mayo de 2019). Disponible en: https://www.transmilenio.gov.co/publicaciones/149398/m-op-002-manual-para-la-gestin-del-riesgo-en-transmilenio-s-a/

Ilustración 4. Riesgo inherente mifare classic – EMV

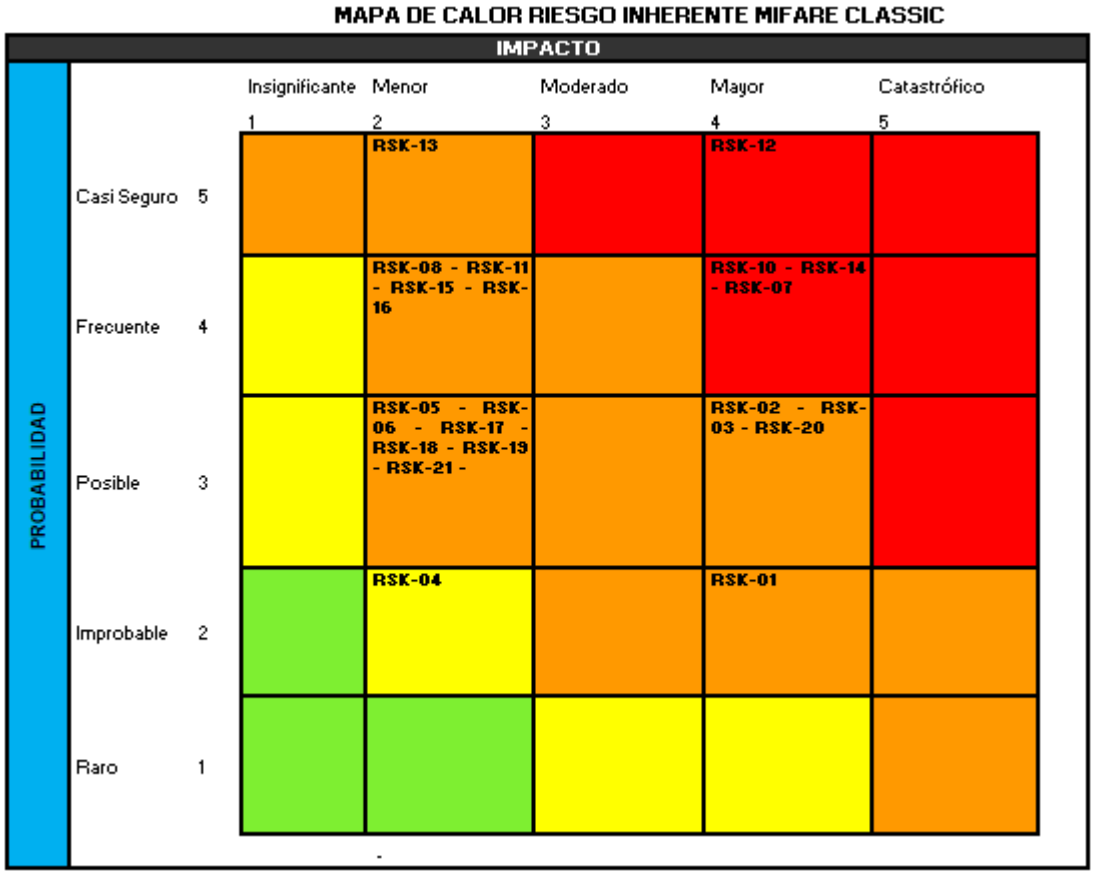


Fuente: El autor

Se puede resaltar que en la ilustración 4 (riesgo inherente mifare classic - EMV) se presentan riesgos con un nivel de severidad extremo (color rojo), los cuales pueden materializarse con mayor frecuencia.

El siguiente mapa colorimétrico refleja los resultados de la evaluación de los riesgos inherentes asociados a la tarjeta mifare classic:

Ilustración 5. Riesgo inherente mifare classic



Fuente: El autor

En la anterior ilustración se presentan riesgos con un nivel de severidad extremo (color rojo) y severidad alta (color naranja) exclusivamente de la tarjeta mifare classic, los cuales pueden materializarse con mayor frecuencia.

Por último, se relaciona a continuación el mapa colorimétrico con la evaluación de los riesgos asociados a la tarjeta mifare classic, pero que aplican a la tarjeta mifare plus con sus controles.

La disminución o desplazamiento de cuadrantes, para el riesgo inherente de la tarjeta mifare plus, se realizó de acuerdo con la siguiente tabla:

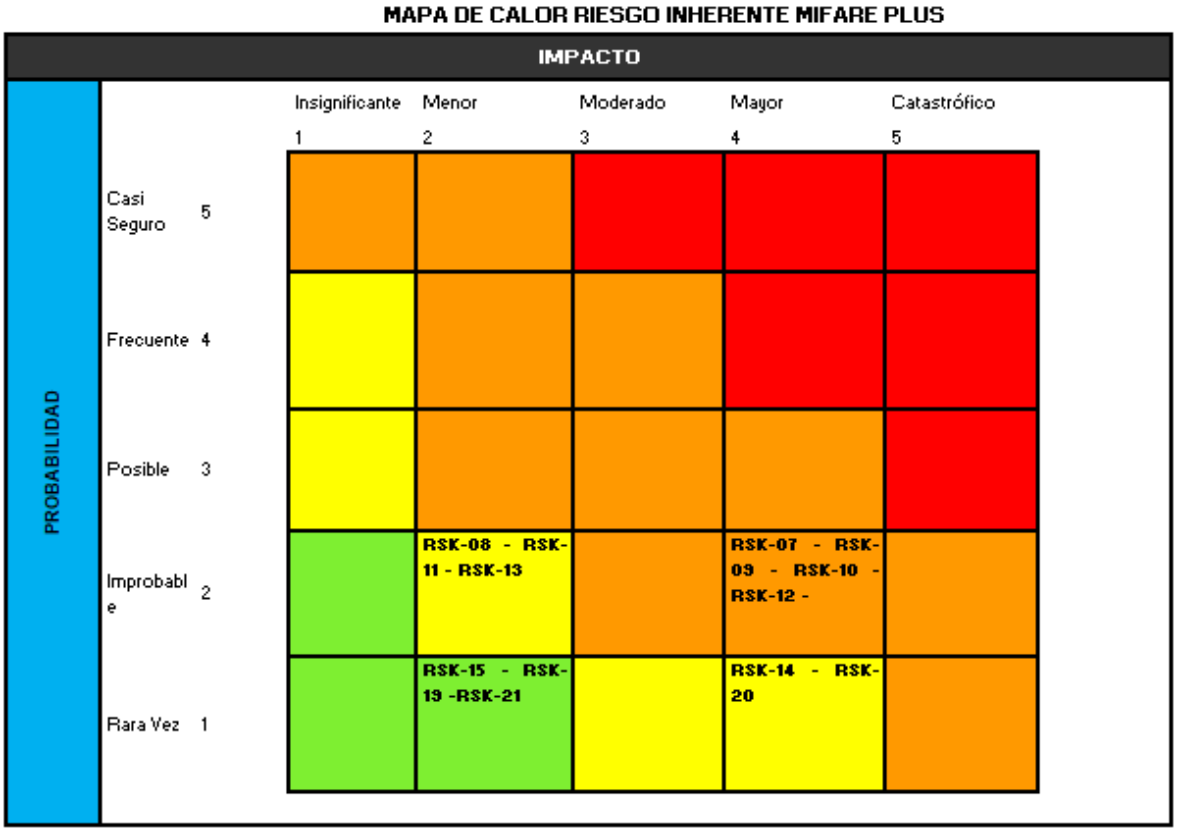
Tabla 35. Desplazamiento en escalas del riesgo de acuerdo con sus controles.

Rango de calificación de los controles	Dependiendo si el control afecta probabilidad o impacto desplaza en la matriz de evaluación del riesgo así: en probabilidad avanza hacia abajo en impacto avanza hacia la izquierda
	Cuadrantes para disminuir
Entre 0-50	0
Entre 51-75	1
Entre 76-100	2

Fuente: Transmilenio - *https://www.transmilenio.gov.co/publicaciones/149398/m-op-002-manual-para-la-gestin-del-riesgo-en-transmilenio-s-a/*

La calificación del control corresponde a la realizada en el capítulo 3., identificación del riesgo; sección 3.3., identificación de los controles existentes; el total de la calificación por control es la sumatoria de los valores respectivamente, esto asociado a los controles evaluados para la tarjeta mifare plus.

Ilustración 6. Riesgo inherente mifare plus



Fuente: El autor

En la anterior ilustración se presentan riesgos con severidad media (color naranja) y severidad media (color amarillo) exclusivamente de la tarjeta mifare plus, esta tarjeta se tiene riesgos moderados que se pueden presentar con una frecuencia menor de ocurrencia.

6. CONCLUSIONES

- En la ilustración 6 es posible ver los resultados del riesgo inherente para mifare classic y EMV, de esta forma se pudieron comparar dichos resultados encontrando una probabilidad de ocurrencia de los riesgos entre ambos activos de información no cercano a la actualidad dado que las tarjetas EMV tienen como fin el uso en actividades bancarias, por lo tanto su seguridad es mayor; ahora bien, si el resultado es distante a la realidad, para EMV, es a causa de la confidencialidad que tienen las características de este tipo de tarjetas, dado que esta información no es de fácil acceso ya que es de carácter privado debido al contexto de mercado en que se encuentran y la principal fuente de información del presente trabajo de investigación fue documentos de investigaciones académicas previas.

- En cuanto a la ilustración 5 (riesgo inherente mifare classic), se puede evidenciar la alta probabilidad de ocurrencia en 18 de los 20 riesgos (90%) asociados a este activo de información, que al ser contrastado contra las mejoras en los controles de seguridad implementados en mifare plus es posible ver un cambio en dicha probabilidad; por otra parte, en 8 de los 20 riesgos (40%) presentan un impacto mayor en caso de materializarse, estos pueden ser tratados por medio de controles de seguridad detectivos y/o correctivos.

- La tarjeta mifare plus tiene similares, pero con mejoras significativas, características de seguridad a mifare classic, esto puede ser justificado a través de los resultados obtenidos y plasmados en la ilustración 6 (Riesgo residual mifare plus), de tal forma que es correcto afirmar que mifare plus presenta una probabilidad baja de ocurrencia de los riesgos asociados, dado que se encuentran dentro de los dos niveles de probabilidad más bajos; esto no quiere decir que no sea vulnerable.

- Al comparar la ilustración 6 (riesgo residual mifare plus) con la ilustración 5 (riesgo inherente mifare classic), es factible evidenciar que existen menos riesgos (9) en comparación con mifare classic, esto se justifica debido a que las actividades (código de error por autenticación fallida) que generaban estos riesgos, en su antecesora, desaparecieron, causando esto la desaparición de los riesgos asociados.

- Los criterios de impacto definidos por transmilenio s.a. no tienen en cuenta en todas sus escalas uno de los principales valores de una organización: la reputación o imagen institucional, dado que solo en dos (los más bajos), de los cinco niveles definidos, se tiene en cuenta este valor.

- La probabilidad de ocurrencia de las vulnerabilidades explotadas y evidenciadas en los antecedentes, pudo ser disminuida en gran medida al haber tenido en cuenta las vulnerabilidades consignadas en la literatura académica (fuente del presente trabajo de investigación), ya que según los resultados de los mapas colorimétricos, presentados en la evaluación de riesgos, para la tarjeta mifare classic y la tarjeta mifare plus, su probabilidad de ocurrencia disminuye considerablemente de la primera a la segunda.

- Actualmente hay riesgos (en las áreas contempladas en el presente trabajo de investigación) que dentro de sus características tienen un impacto alto para la organización en caso de materializarse, es por eso que transmilenio s.a. puede tratar estos riesgos formulando controles de tipo correctivos y/o detectivos.

- La aplicación y alineación de una gestión de riesgos enfocada a seguridad de la información con una norma ajustada a sus necesidades, como por ejemplo la aplicada en el presente trabajo de investigación: ISO 27005, garantiza el correcto desarrollo y cumplimiento del propósito de la actividad, trayendo como consecuencia el aumento en la probabilidad de éxito de esta y su impacto favorable en una organización.

7. RECOMENDACIONES Y TRABAJOS FUTUROS

7.1. RECOMENDACIONES

Con el cumplimiento total de los objetivos planteados en el presente trabajo de investigación, es posible evidenciar oportunidades de mejora que pueden ser aprovechadas para beneficio de la organización como la siguiente:

- Incluir dentro de los criterios de impacto definidos por transmilenio s.a. la afectación reputacional de la organización en todas sus escalas, ya que según lo evidenciado en el capítulo de establecimiento del contexto, únicamente se asocia este tipo de afectación a las escalas más bajas (insignificante y menor), lo cual debería ser incorporado, también, en las demás escalas (moderado, mayor y catastrófico), dado que la reputación es un valor importante dentro de cualquier organización, por ende, si esta se ve afectada (de cualquier forma), la organización también lo estará.

7.2. TRABAJOS FUTUROS

Como continuación del presente trabajo de investigación existen diversas líneas de investigación que quedan abiertas y en las que es posible continuar trabajando, como son las siguientes:

- Generación y aplicación de nuevos controles tecnológicos a las tarjetas inteligentes del sistema integrado de transporte público en la ciudad de Bogotá D.C. - Colombia.

- Detección de nuevas vulnerabilidades por medio de mecanismos físicos y lógicos para realizar un análisis más profundo de las brechas de seguridad en las tarjetas inteligentes.

- Aplicación de nuevas metodologías de gestión de riesgo enfocadas en nuevos tipos de evaluación de los diferentes tipos de impactos reputacionales de la organización.

- Teniendo en cuenta la información consignada en la siguiente tabla, asociada a las TISC de los principales sistemas BRT (autobuses de tránsito rápido) de Colombia:

Tabla 36. Tecnologías TISC de los principales BRT de Colombia

Nombre	Ubicación	Estaciones	Valor/Pasaje	Tarjeta Inteligente	Tecnología - Tarjeta
Transmilenio	Bogotá D.C. - Colombia[43]	147	$2.400 COP	TuLlave	Mifare classic, mifare plus y EMV
Metro Medellín	Medellín - Colombia[44]	76	$2.550 COP	Cívica	Mifare plus y EMV
Megabus	Pereira - Colombia[45]	3	$2.100 COP	MegaBus	Mifare classic, calypso y EMV
MÍO	Cali - Colombia	55	$2.100 COP	Tarjeta MIO	Mifare classic y EMV
Cable aéreo Manizales	Manizales - Colombia[46]	4	$2.000 COP	Tarjeta Cable Aéreo Manizales	Mifare classic
Metrolínea	Bucaramanga - Colombia[47]	11	$2.300 COP	Metrolínea	Mifare classic y EMV
Transmetro	Barranquilla - Colombia[48]	2	$2.300 COP	Transmetro	Mifare classic y EMV
Transcaribe	Cartagena - Colombia[49]	17	$2.500 COP	TransCaribe	Mifare classic y calypso

Fuente: El autor

[43] Secop, 2018. "Manual de operaciones transmilenio".(07 Mayo de 2019).Disponible en: https://community.secop.gov.co/Public/Tendering/ContractDetailView/Index?UniqueIdentifier=CO1.PCCNTR.492201&isModal=true&asPopupView=true

[44] Noticias, 2015. "Asistencia técnica para palma tolos para la nueva tarjeta cívica del metro de Medellín". Disponible en: https://palmatools.com/asistencia-tecnica-palma-tools-la-nueva-tarjeta-civica-del-metro-medellin/

[45] Dinero, 2010. "Megatarjetas, ejemplo eficiente de sistemas de pago". (07 Mayo de 2019). Disponible en: https://www.dinero.com/pais/articulo/megatarjetas-ejemplo-eficiente-sistemas-pago/101667

[46] La patria, 2018. "Inficaldas pide más claridad al cable aéreo por recientes irregularidades encontradas". (08 Mayo de 2019).Disponible en: http://www.lapatria.com/manizales/inficaldas-pide-mas-claridad-al-cable-aereo-por-recientes-irregularidades-encontradas

[47] Vanguardia, 2010. "Usted se sube a metrolinea en solo una tarjeta". (08 Mayo de 2019).Disponible en: https://www.vanguardia.com/area-metropolitana/bucaramanga/usted-se-sube-a-metrolinea-solocon-esta-tarjeta-KPVL49804

[48] Transmetro, 2018. "Mi tarjeta". (08 Mayo de 2019). Disponible en: https://www.transmetro.gov.co/mi-tarjeta/#!

[49] Transcaribe, 2010. "Especificaciones técnicas del sistema intregrado de recaudo transcaribe". (08 Mayo de 2019).Disponible en: http://www.transcaribe.gov.co/documentos/Licitaciones%202010/TC-LPN-001-10/APENDICES/Apendice%20No2.Esp.%20Tecnicas%20del%20sistema%20de%20recaudo%20y%20Control%20de%20Flota.pdf

Y partiendo de las siguientes consideraciones:

- Las TISC de los principales BRT de Colombia tienen diversas tecnologías.
- En 6 de los 8 BRT de Colombia (75%), que fueron mencionados en la anterior tabla, tienen en producción TISC con tecnología mifare classic, representando una alta probabilidad de ocurrencia de los riesgos valorados.
- Una materialización de uno o más riesgos, de los valorados en el presente trabajo de investigación, tiene como consecuencia la afectación financiera y/o reputacional de la organización y de la ciudad.

Proponemos como trabajo futuro el diseño y creación de la primera TISC interoperable para los BRT de Colombia teniendo como principal característica la seguridad, todo esto aprovechando los resultados del presente trabajo de investigación y aplicando la norma ISO 24014, la cual proporciona la base para el desarrollo de sistemas de gestión de tarifas de transporte público en superficie de múltiples operadores o servicios múltiples interoperables a nivel nacional (IFMS)[50].

[50] ISO 24014, 2015. “Public transport interoperable fare management system”. (08 Mayo de 2019). Disponible en: https://www.iso.org/standard/61545.html

8. ANEXOS

Tabla 37. Listado de anexos

Nombre	Descripción
Anexo A	Identificación de consecuencias
Anexo B	Valoración de consecuencias
Anexo C	Valoración de incidentes
Anexo D	Nivel de estimación
Anexo E	Evaluación del riesgo

Fuente: El autor

9. REFERENCIAS

Alvarez, A. (s.f.). *Agustin Alvarez, 2016. "Tarjeta inteligente de contacto Tarjeta inteligente sin contacto:". Disponible en: https://www.tangoid.com.ar/noticias/historia-sobre-las-tarjetas-inteligentes-smartcards*.

Atlas, G. (s.f.). Grupo Atlas, 2015. "¿En qué consiste un servicio de pagos y recaudos?". Disponible en: https://blog.atlas.com.co/en-qu%C3%A9-consiste-un-servicio-de-pagos-y-recaudos.

BY. (s.f.). Portal BY, ¿Qué es RFID? 2014 disponible en: https://www.by.com.es/blog/que-es-rfid/.

MiFare. (s.f.). *Mifare*. Obtenido de https://www.mifare.net/es/productos/ics-de-tarjetas-con-chip/familia-mifare-plus/

Cagliostro, C. (s.f.). Charles Cagliostro, Tarjeta con Circuito Integrado 2017 Disponible en: http://carlosmgalvis.com/index.php/tarjeta-con-circuito-integrado.

Cancilleria. (s.f.). Cancillería, Colombia 2017 Disponible en: http://www.cancilleria.gov.co/ministra.

Carrera, F. (s.f.). Felipe Carrera, Seguridad de la Información Política INFOSEC Nacional Cantabria – España 2016 Disponible en internet: https://books.google.com.co/books?hl=es&lr=lang_es%7Clang_en&id=cQk_Ms6MUfEC&oi=fnd&pg=PA9&dq=seguridad+en+tarjetas++&ots=Z09h9OyFCJ&sig=.

Colombia, S. d. (s.f.). Seguridad de la información, Marco legal de seguridad de la información en Colombia 2012 Disponible en: http://seguridadinformacioncolombia.blogspot.com/2010/02/marco-legal-de-seguridad-de-la.html.

D, F. (s.f.). Flavio D. GarciaGerhard de Koning Gans, Dismantling Mifare classic Netherlands 2014 Disponible en : https://link.springer.com/chapter/10.1007/978-3-540-88313-5_7.

Digimentore. (s.f.). Digimentore, Modelo sam 2014 Disponible en: http://www.digimentore.com.ec/index.php/2017/08/19/di9_modelo_sam/.

DMA. (s.f.). DMA, Introducción de la Criptografía Fecha desconocida, Disponible en: http://www.dma.fi.upm.es/recursos/aplicaciones/matematica_discreta/web/aritmetica_modular/criptografia.html.

Duarte, M. R. (s.f.). Mario Ramón Duarte, Las cripto tarjetas en el mercado financiero: una realidad global ascendente 2018 Disponible en : https://www.alainet.org/es/articulo/194089.

FM, L. (s.f.). LA FM, Los problemas de la tarjeta tu llave de Transmilenio Bogotá – Colombia, 2018 Disponible en internet: https://www.lafm.com.co/bogota/los-problemas-de-la-tarjeta-tullave-de-transmilenio.

Hoy, S. p. (s.f.). Guillem Alsina, Tecnología para tarjetas de identificación 2014 Disponible en: https://www.seguridadprofesionalhoy.com/tecnologia-para-tarjetas-de-identificacion/.

MIFARE. (s.f.). MiFare, ¿Familia Mifare classic? 2017 Disponible en: https://www.mifare.net/es/productos/ics-de-tarjetas-con-chip/familia-mifare-classic/.

Orange. (s.f.). Orange, ¿Que es NFC? 2011 Disponible en: https://ayuda.orange.es/particulares/otros-productos/nfc/505-que-es-el-nfc-como-funciona-y-para-que-sirve.

Perez, G. (s.f.). *Gabriel Pérez, Sistema de cobro electrónico de pasajes en el transporte público Santiago de Chile – Chile, 2015 Disponible en internet: https://repositorio.cepal.org/bitstream/handle/11362/6401/1/S026444_es.pdf*

Presidencia. (s.f.). Presidencia, Bogotá Distrito Capital 2018 Disponible en: https://id.presidencia.gov.co/Paginas/presidencia.aspx.

RADIO, C. (s.f.). CARACOL RADIO, Esta es la historia del lío de la doble tarjeta para acceder a Transmilenio Bogotá – Colombia, 2013. Disponible en internet: http://caracol.com.co/radio/2013/06/27/bogota/1372330800_923463.html.

RCN, N. (s.f.). Noticias RCN, Capturan a siete personas acusadas de clonar tarjetas de Transmilenio Bogotá – Colombia, 2016. Disponible en internet: https://noticias.canalrcn.com/nacional-bogota/capturan-siete-personas-acusadas-clonar-tarjetas-transmilenio.

Sabadell, B. (s.f.). Banco Sabadell, Terminales de punto de venta (TPVs) Disponible en : https://www.bancsabadell.com/cs/Satellite/SabAtl/Terminales-punto-de-venta-(TPV)/1191332198568/es/.

Semana, R. (s.f.). Revista Semana, Transmilenio: tarjetas de las fases I y II se pueden clonar Bogotá – Colombia, 2013. Disponible en internet: https://www.semana.com/nacion/articulo/informe-transmilenio-sobre-seguridad-en-tarjetas/356601-3.

SGSI. (s.f.). PMG SGSI, Metodología 27005 Disponible en: https://www.pmg-ssi.com/2017/06/iso-27005-gestion-del-riesgo-tecnologico/.

Sistemas. (s.f.). Sistemas, Definición de Hertz 2014 Disponible en: https://sistemas.com/hertz.php.

Sistemas. (s.f.). Sistemas, Definición de MHZ 2015 Disponible en : https://sistemas.com/mhz.php.

Soledispa, R. (s.f.). Rossy Soledispa, ¿Qué es el HSM? 2014 Disponible en: http://comunidad.todocomercioexterior.com.ec/profiles/blogs/qu-es-el-hsm-hardware-security-module.

Tiempo, R. E. (s.f.). Redacción el Tiempo, Así clonaban las tarjetas de Transmilenio Bogotá – Colombia, 2016. Disponible en internet: https://www.eltiempo.com/bogota/clonacion-de-tarjetas-de-transmilenio-43493.

Transmilenio. (s.f.). *Transmilenio, 2017. "Gestión de riesgo Transmilenio". Disponible en: http://www.transmilenio.gov.co/loader.php?lServicio=Publicaciones&lTipo=WFactionA&lFuncion=visualizar&id=14538&bd=m.*

WeLiveSecurity. (s.f.). EMV, ¿Qué es EMV, y por qué es un tema candente? 2014 Disponible en: https://www.welivesecurity.com/la-es/2014/04/08/que-es-emv-y-por-que-es-un-tema-candente/.

ISO 24014, 2015. "Public transport interoperable fare management system". Disponible en: https://www.iso.org/standard/61545.html

Transmilenio, 2018. "Mapa de corrupción". Disponible en: https://www.transmilenio.gov.co/descargar.php?idFile=815

CardLogix, 2017. "Modelo SAM". Disponible en: https://www.cardlogix.com/glossary/sam-card-secure-access-module-secure-application-module/

CardWerk, 21015. "ISO 7816 Part 4". Disponible en: https://cardwerk.com/iso-7816-part-4/

Fodafin, 2015. "Seminario de Transporte tarjetas inteligentes". Disponible en: http://www.fonadin.gob.mx/wp-ontent/uploads/2016/08/SeminarioTransporte_FONADIN_FIMPE.pdf

By, 2017. "Algoritmos de encryptamiento AES". Disponible en: https://www.by.com.es/blog/algoritmos-encriptacion-aes-3des

Gemalto, 2916. "Explaining EMV payment". Disponible en: https://www.gemalto.com/latam/servicios-financieros/tarjertas/emv/acerca

Crypto.net. "Key-Based Authentication (Public Key Authentication)". Disponible en: http://www.crypto-it.net/eng/tools/key-based-authentication.html

Techopedia, 2015. "Key Length" Disponible en: https://www.techopedia.com/definition/3999/key-length

MiFare, 2018. “Familia MiFare Plus” Disponible en: https://www.mifare.net/es/productos/ics-de-tarjetas-con-chip/familia-mifare-plus/

StackOverFlow, 2015. “MiFare - Difference between UID and Serial Number of MiFare Card” Disponible en: https://stackoverflow.com/questions/17608670/mifare-difference-between-uid-and-serial-number-of-mifare-card.

Mintic, 2018. “Seguridad y privacidad de la información” Disponible en: https://www.mintic.gov.co/gestionti/615/articles-5482_G7_Gestion_Riesgos.pdf

Eric Morana.2018. “Niveles de riesgos aceptable versus criterios de aceptacion del riesgo”. Disponible en: https://ericmorana.wordpress.com/2012/10/29/niveles-de-riesgo-aceptable-versus-criterios-de-aceptacion-del-riesgo/

Radboud University. 2019. “Wirelessly Pickpocketing a Mifare Classic Card”. Disponible en: https://repository.ubn.ru.nl/handle/2066/75545

Defense Technical Information Center, 1996. “Minimal Key Lengths for Symmetric Ciphers to Provide Adequate Commercial Security. A Report by an Ad Hoc Group of Cryptographers and Computer Scientists”. Disponible en: https://apps.dtic.mil/docs/citations/ADA389646

Springer, 2014. “A Practical Attack on Patched MIFARE Classic.”. Disponible en: https://link.springer.com/book/10.1007/978-3-319-12087-4

Nicolas T. Courtois. “The dard side of security by obscurity”. Disponible en: http://www.scitepress.org/Papers/2009/22380/22380.pdf

F.D Garcia, 2008. “Dismantling MIFARE Classic”. Disponible en: https://research.tue.nl/en/publications/dismantling-mifare-classic

Mike Bond, 2015. “The EMV preplay attack”. Disponible en: https://ieeexplore.ieee.org/document/7085649

Emmanuel Bertin, 2018. “An Overview of the EMV Protocol and Its Security Vulnerabilities”. Disponible en: https://www.researchgate.net/publication/323073718_An_Overview_of_the_EMV_Protocol_and_Its_Security_Vulnerabilities

Secop, 2018. “Manual de operaciones”. Disponible en: https://community.secop.gov.co/Public/Tendering/ContractDetailView/Index?UniqueIdentifier=CO1.PCCNTR.492201&isModal=true&asPopupView=true

Noticias, 2015. “Asistencia técnica para palma tolos para la nueva tarjeta cívica del metro de Medellín”. Disponible en: https://palmatools.com/asistencia-tecnica-palma-tools-la-nueva-tarjeta-civica-del-metro-medellin/

Dinero, 2010. “Megatarjetas, ejemplo eficiente de sistemas de pago”. Disponible en: https://www.dinero.com/pais/articulo/megatarjetas-ejemplo-eficiente-sistemas-pago/101667

La patria, 2018. “Inficaldas pide más claridad al cable aéreo por recientes irregularidades encontradas”. Disponible en: http://www.lapatria.com/manizales/inficaldas-pide-mas-claridad-al-cable-aereo-por-recientes-irregularidades-encontradas

Vanguardia, 2010. “Usted se sube a metrolinea en solo una tarjeta”. Disponible en: https://www.vanguardia.com/area-metropolitana/bucaramanga/usted-se-sube-a-metrolinea-solocon-esta-tarjeta-KPVL49804

Transmetro, 2018. “Mi tarjeta”. Disponible en: https://www.transmetro.gov.co/mi-tarjeta/#!

Transcaribe, 2010. “Especificaciones técnicas del sistema intregrado de recaudo transcaribe”. Disponible en: http://www.transcaribe.gov.co/documentos/Licitaciones%202010/TC-LPN-001-10/APENDICES/Apendice%20No2.Esp.%20Tecnicas%20del%20sistema%20de%20recaudo%20y%20Control%20de%20Flota.pdf

Gerges Kayanakis, 2002. Contactless or hybrid contact-contactless smart card designed to limit the risks of fraud. Disponible en : https://patents.google.com/patent/US6390375B2/en

Dominik Haneberg, 2004. Electronic ticketing: risks in e-commerce applications. Disponible en: https://link.springer.com/chapter/10.1007%2F978-3-540-72621-0_5

Marey, 2011. Aspecto de seguridad en sistemas de boletos electrónicos. Disponible en: http://bibliotecadigital.econ.uba.ar/download/tpos/1502-0811_MareyAD.pdf

Uwe Trottmann, 2012. NFC – Possibilities and risk. Disponible en: https://www.net.in.tum.de/fileadmin/TUM/NET/NET-2013-02-1/NET-2013-02-1_05.pdf

Jóse Leonardo Camacho,2016. Análisis de gestión del riesgo de TI en recaudo Bogota. Disponible en: https://repository.ucatolica.edu.co/bitstream/10983/