UNIVERSIDAD INTERNACIONAL SEK

FACULTAD DE ARQUITECTURA E INGENIERÍAS

Proyecto de fin de carrera titulado:

"**Diseño de una metodología para la implementación y gestión de un sistema de seguridad para servicios transaccionales en instituciones financieras de la economía popular y solidaria basada en las buenas prácticas de la PCI DSS, caso de estudio Cooperativa de Ahorro y Crédito Construcción Comercio y Producción".**

Realizado por:

Ing. Jean Pierre Rodríguez Guerra.

Director del proyecto:

Ing. Verónica Rodríguez, MBA.

Como requisito para la obtención del título de:

MASTER EN TECNOLOGÍAS DE LA INFORMACIÓN

QUITO, FEBRERO 2019

DECLARACIÓN JURAMENTADA

Yo, JEAN PIERRE RODRÍGUEZ GUERRA, con cédula de identidad #171816489-0, declaro bajo juramento que el trabajo aquí desarrollado es de mi propia autoría, que no ha sido previamente presentado para ningún grado a calificación profesional; y que he consultado las referencias bibliográficas que se incluyen en este documento.

A través de la presente declaración, se cede los derechos de propiedad intelectual correspondientes a este trabajo, a la UNIVERSIDAD INTERNACIONAL SEK, según lo establecido por la Ley de Propiedad Intelectual, por su reglamento y por la normativa institucional vigente.

Ing. Jean Pierre Rodríguez Guerra

C.C.: 171816489-8

DECLARATORIA

El presente trabajo de investigación titulado:

“DISEÑO DE UNA METODOLOGÍA PARA LA IMPLEMENTACIÓN Y GESTIÓN DE UN SISTEMA DE SEGURIDAD PARA SERVICIOS TRANSACCIONALES EN INSTITUCIONES FINANCIERAS DE LA ECONOMÍA POPULAR Y SOLIDARIA BASADA EN LAS BUENAS PRÁCTICAS DE LA PCI DSS, CASO DE ESTUDIO COOPERATIVA DE AHORRO Y CRÉDITO CONSTRUCCIÓN COMERCIO Y PRODUCCIÓN.”

Realizado por:

JEAN PIERRE RODRÍGUEZ GUERRA

Como requisito para la obtención del título de:

MASTER EN TECNOLOGÍAS DE LA INFORMACIÓN

Ha sido dirigido por el docente:

ING. VERÓNICA RODRÍGUEZ, MBA.

Quien considera que constituye un trabajo original de su autor

ING. VERÓNICA RODRÍGUEZ, MBA.

DIRECTOR

PROFESORES INFORMANTES

Los profesores informantes:

ING. ÉDISON ESTRELLA

ING. DIEGO RIOFRÍO.

Después de revisar el trabajo presentado, lo han calificado como apto para su defensa oral ante el tribunal del examinador

ÉDISON ESTRELLA

DIEGO RIOFRÍO

Quito, Abril del 2018

DEDICATORIA

Dedico este trabajo a mi familia, quienes me apoyan día a día.

A mis compañeros de maestría con quienes aprendí a ver el mundo con otros ojos.

A mis profesores y a la Universidad, lugar en el que además de adquirir conocimientos valiosos, conocí a personas grandiosas

.

AGRADECIMIENTO

Agradezco en primer lugar a Dios, por permitirme llegar a este punto de mi vida junto a las personas que amo. A mis padres por apoyarme y demostrarme que nada en la vida es fácil, pero si satisfactorio, a mis hermanos que son el eje fundamental en mi vida, mis consejeros y fortaleza.

Agradezco de manera muy especial a mi maestra la Ing. Verónica Rodríguez, quien me enseñó desde joven el amor a esta hermosa profesión y me recuerda siempre que, no importa que tanto te alejes, siempre puedes encontrar el camino de vuelta.

ÍNDICE GENERAL DE CONTENIDO

LISTA DE FIGURAS

LISTA DE TABLAS

RESUMEN

En los últimos años, el crecimiento de las tecnologías emergentes y su aplicación al sector financiero dieron inicio a las *Fintech*, tecnologías aplicadas para ofrecer por diferentes canales los servicios financieros buscando la transformación digital y la omnicanalidad. Estas nuevas tecnologías abren una ventana de oportunidades que pueden llegar a sectores rurales y ofrecen beneficios para la comunidad, en especial para microempresas. Motivo por el cual son idóneas para aplicarse en las cooperativas de ahorro y crédito. Instituciones financieras que, a diferencia de la banca, su objetivo es servir y fortalecer a una comunidad, grupo de interés o zonas de influencia, buscando destinar las ganancias en pro de buscar una mejora en representativa en sus productos como créditos de bajos intereses y beneficios directos para las familias temas de recreación, cultura y educación. Al conocer los riesgos que existen en los canales electrónicos y nuevos vectores de ataque disponibles al implementar estas nuevas tecnologías, se desarrolló la metodología para la implementación y gestión de un sistema de seguridad de los servicios transaccionales y poder así brindar nuevas oportunidades a los socios con productos seguros y confiables aceptados por los organismos de control y se encuentren disponibles 24/7. El proyecto se desarrolló en la Cooperativa de Ahorro y Crédito Construcción, Comercio y Producción – COOPCCP en la que, tras el análisis de la situación actual y conjunto al desarrollo de un análisis de riesgo basado en las normativas nacionales SEPS-103, JB-2148 y como normativa internacional la PCI DSS, se evidenció la necesidad de implementación de esta metodología ya que, los mecanismos de seguridad actual no definen claramente los responsables de aplicación de estos nuevos servicios, lo que retrasa la gestión de proyectos y salida a producción.

Palabras clave: Sistemas transaccionales, Fintech, instituciones financieras, seguridad de la información, guía metodológica de seguridad, tecnologías emergentes.

ABSTRACT

In recent years, the growth of emerging technologies and their application to the financial sector started the Fintech, technologies applied to offer financial services through different channels seeking digital transformation and omnichannel. These new technologies open a window of opportunities that can reach rural sectors and offer benefits for the community, especially for micro-businesses. Reason why they are suitable to apply in credit unions. Financial institutions that, unlike banking, aim to serve and strengthen a community, interest group or areas of influence, seeking to allocate profits in favor of seeking an improvement in their products as low interest loans and benefits direct for families themes of recreation, culture and education. By knowing the risks that exist in the electronic channels and new vectors of attack available when implementing these new technologies, the methodology for the implementation and management of a security system of the transactional services was developed and thus be able to offer new opportunities to the partners with safe and reliable products accepted by the control organisms and are available 24/7. The project was developed in the Cooperative of Savings and Credit Construction, Trade and Production - COOPCCP in which, after the analysis of the current situation and together to the development of a risk analysis based on national regulations SEPS-103, JB-2148 and as an international standard for the PCI DSS, the need for the implementation of this methodology was evident, since the current security mechanisms do not clearly define those responsible for the application of these new services, which delays project management and production output.

Key words: Transactional Systems, Fintech, financial institutions, information security, methodological security guide, emerging technologies.

CAPÍTULO I

INTRODUCCIÓN

1.1 EL PROBLEMA DE INVESTIGACIÓN

1.1.1 Planteamiento del Problema

Hoy en día los servicios ofrecidos a los usuarios mediante el uso de canales de comunicación electrónica son los principales factores que definen el éxito de una empresa ya que, según la revista de finanzas Bankingly (2017), el mercado está orientado a desenvolverse un 70% en estos medios, lo que quiere decir que existe una gran mayoría de usuarios que optan por el uso de estos servicios e ingresan a dichas plataformas, todo tipo de información personal, por lo que, se convirtieron en los canales en donde existe una mayor cantidad de intrusiones y eventos de riesgo que en su mayoría de veces terminan en delitos tales como robo, sustracción de credenciales, extorsión, entre otros. Lo que se debe en gran medida según Toapanta (2018). A la carencia de criterios de seguridad que existe por parte de los usuarios, pero mucho más importante, la poca importancia a nivel de seguridad que se le da a los canales electrónicos a niveles administrativos dentro de las instituciones.

Teniendo en cuenta que los servicios electrónicos son alcanzables por cualquier dispositivo conectado a Internet que cuente con los permisos básicos, desde el punto de vista de seguridad informática, los vectores de ataque que los rodean crecen exponencialmente, mismos que se enfocan a afectar tanto a los servicios en infraestructuras públicas (como ataques a servidores

web IIS), como a la infraestructura interna (por ejemplo, ataques dedicados a servidores de aplicaciones). Por lo que se evidencia la necesidad de aplicar controles sobre los distintos canales e infraestructura en los que una institución ofrece sus servicios.

Según ESET (2014) típicamente, los scripts maliciosos atacan a diferentes segmentos de la red, probando sus defensas contra alteraciones, tratando de explotar sus vulnerabilidades para tomar control sobre la información y en el peor de los casos, sustraerla, divulgarla o destruirla. Sin embargo, hoy en día existe una gran variedad de códigos que utilizan métodos más sofisticados abarcando nuevos vectores de ataques y en base a ellos, se desarrollaron equipos capaces de monitorear y actuar sobre la infraestructura de una red, incluyendo las comunicaciones con los proveedores de servicios, los enlaces internos, entre otros. Duk, Bjerlobrk & Carapina (2013) mencionan en su estudio que además, también existen otros tipos de ataques que tienen como objetivo afectar el nivel reputacional, estos son los denominados "*Black SEO*"[1] y se enfoca en realizar el mismo trabajo de posicionamiento e indexación de sitios web en Internet, pero a diferencia del SEO tradicional, éste se encarga de que los algoritmos automáticos de Google reconozcan a la página web como fraudulenta y de esta forma, sea incluida en las listas negras de Internet, de esta manera se genera una intermitencia del servicio que brinda dicha dirección e incluso, el buscador (por ejemplo, *www.google.com*) puede dar de baja el sitio web en sus resultados. Para lograrlo, el atacante puede utilizar varios métodos, desde realizar hipervínculos en páginas fraudulentas o los cuales incluyen el uso de código malicioso, sin embargo, no está considerado dentro de ninguna solución de seguridad ya que no interfiere directamente con la infraestructura que se utilizan en una red institucional.

[1] En español: Optimización de motores de búsqueda de sombrero negro, consiste en engañar a los buscadores automáticos para posicionar a un sitio web mediante prácticas no éticas en Internet.

Según ISOTools (2017). Inicialmente la seguridad de la información protege los aspectos relacionados a la confidencialidad, integridad y disponibilidad de los datos que representen algún tipo de valor para la institución en la que se encuentran, sin embargo gracias al creciente uso de tecnologías que manejan grandes cantidades de datos a una gran velocidad (Big Data) y su uso para realizar estrategias de negocio , cada uno de los datos que se puedan recopilar del cliente interno y externo son valiosos, lo que causa que se amplíe el abanico de servicios para los cuales se requieren aplicar controles y monitoreo que atenten contra los principios de los datos.

La falta de consciencia de seguridad de la información existente en gran parte de las instituciones financieras de la economía popular y solidaria de la mano con la amplia gama de soluciones y servicios de seguridad existentes en el mercado, hacen que las responsabilidades que deben recaer sobre los profesionales encargados de la seguridad de la información se vean limitadas al uso de equipos que brindan soluciones basadas en parámetros que no siempre están alineadas a la necesidad del negocio, lo que deja un abanico de opciones limitado.(OEA,2018)

En lugar de realizar un análisis sobre la situación, los eventos de riesgo suscitados se gestionan automáticamente por dispositivos de la infraestructura o se ubican en cuarentena sin un criterio real de seguridad, lo que causa conflictos a niveles administrativos cambiando la percepción de los clientes internos (usuarios de la intranet empresarial) a un sistema de baja calidad y mucho control sin sentido directo. (Calderón & Castro, 2017)

Según el estudio de Goodbody (2018), que una mala práctica común que se da al adquirir servicios tercerizados de seguridad es definir como responsables de la seguridad de la información al área de Tecnología en lugar del área de Riesgos, lo que hace que los datos

entregados pierdan relación de confianza al ser el mismo departamento juez y parte de los eventos de seguridad en la red informática.

1.1.2 Diagnóstico

A nivel mundial, dentro del sector financiero existen dos modelos de negocio. La banca privada y las cooperativas financieras, mismas que en el Ecuador se encuentran controladas por la Superintendencia de Bancos y Seguros (SBS) y la Superintendencia de la Economía Popular y Solidaria (SEPS) respectivamente.

En el caso de estudio se realizó un análisis a una institución financiera perteneciente al segmento 1 de la economía popular y solidaria en la República del Ecuador. La Cooperativa de Ahorro y Crédito Comercio Construcción y Producción (COOPCCP).

Según las entrevistas realizadas a Daniel Zurita, Jefe de Tecnología y Sebastián Ortiz, Oficial de Seguridad de la Información de la COOPCCP sobre los servicios ofrecidos a los usuarios mediante el uso de canales de comunicación telemática en temas de seguridad, se identificó que no existe una metodología que permita realizar una asignación adecuada de recursos, planificación estratégica de implementación por fases de una infraestructura de seguridad y que en general permita proteger integralmente las aplicaciones utilizadas en canales electrónicos mediante controles a todos los nuevos posibles vectores de ataque desarrollando un proceso de configuración independientemente a las prediseñadas por las casas de seguridad. Por lo que las infraestructuras estaban expuestas a ataques de día cero, varios tipos de malware como Ransomware que utilizan nuevos puertos de comunicación tales como smbv1, smbv2, etc. Por lo que era necesario establecer cada una de las configuraciones de manera manual acorde a los servicios utilizados por los diferentes productos de la institución.

La falta de una metodología que permita realizar una configuración aplicando un criterio de seguridad informática ha causado que, pese a existir soluciones informáticas implementadas todavía exista un porcentaje del riesgo informático que no puede ser mitigado, mismo que, sumado a la obsolescencia de los equipos al igual que su efectividad sobre nuevas técnicas y vectores de ataque, no brindan una cobertura real y en efecto, existe la posibilidad de que se dé un evento de riesgo por lo que, la siguiente métrica a tomar en cuenta es el tiempo de respuesta y recuperación de desastres.

1.1.3 Pronóstico

Si esta falta de conciencia sobre seguridad informática continuaba, todos los eventos de riesgo hubiesen sido trasladados a empresas ajenas a la institución prescindiendo de personal especializado en seguridad de la información y atentando contra la relación de confianza de los datos sin tener un control establecido para contar con la disponibilidad de los mismos.

Tanto en el traslado como en el almacenaje de información existen distintas maneras de presentarse un robo o sustracción de datos por lo que, de producirse el caso, el proveedor de servicios de seguridad informática podrá encontrar un punto o segmento en el que los datos salgan de su alcance y de esta manera trasladar la responsabilidad a un tercero, ya que su solución no cubriría todos los canales por los que viaja la información. Un caso particular relacionado fue registrado el 15 de mayo del 2018 en una institución financiera de México, cuya pérdida económica registró más de 8 cifras. (Sinembargo Periodismo Digital & Diario de México, 2018)

La Cooperativa de ahorro y crédito Construcción, Comercio y Producción (COOPCCP) es una institución de intermediación financiera bajo el control de la Superintendencia Económica Popular y Solidaria (SEPS) que cuenta con presencia en las 4 regiones del ecuador divididas para sus 14 sucursales a nivel nacional y la matriz ubicada en la ciudad de Quito, inició sus actividades el 28 de junio de 1988. Ya con más de 30 años en el sector cooperativo, la COOPCCP se dedica a brindar servicios financieros en captaciones (inversiones, ahorros, depósitos a plazo fijo) y colocaciones (créditos de tipo consumo, microcrédito, empresa) con beneficios para sus socios y clientes.

1.1.4 Control del pronóstico:

Si bien es cierto el riesgo inherente al desarrollo de actividades es alto y mitigarlo con controles establecidos de acuerdo a una política o buenas prácticas de seguridad, da como resultado un nivel de riesgo residual aceptable, es posible disminuir el impacto que se generará al presentarse un evento de seguridad informática mediante la intervención de un profesional que aplique una metodología para la gestión de un sistema de seguridad y dicho documento sirva como una guía que contemple eventos que se puedan producir de acuerdo a la realidad de la institución. El seguimiento de estos lineamientos traerá a la institución una conciencia de seguridad que de manera idónea será llevada a nivel administrativo, creando nuevos procesos y procedimientos estableciendo diferentes responsabilidades a los colaboradores de la institución de acuerdo a una mejor segregación de funciones, reduciendo así los tiempos de respuestas a incidentes y entregando productos y servicios de calidad, seguros y siempre disponibles al público.

1.2 Objetivos

1.2.1 Objetivo general

Diseñar una metodología para la implementación y gestión de un sistema de seguridad enfocado en brindar servicios transaccionales dentro de instituciones financieras de la economía popular y solidaria basada en las buenas prácticas de la normativa PCI DSS, caso de estudio Cooperativa de Ahorro y Crédito Construcción Comercio y Producción COOPCCP.

1.2.2 Objetivos específicos

- Analizar los procesos e infraestructura tecnológica de la COOPCCP mediante reuniones con el personal responsable para el diagnóstico de la situación actual de los servicios transaccionales y la infraestructura existente
- Determinar los posibles riesgos a los que están expuestos los procesos de los servicios transaccionales de la COOPCCP mediante un análisis del estado de madurez de la institución basado en la normativa PCI DSS que permita la identificación de las vulnerabilidades de los servicios transaccionales.
- Analizar las buenas prácticas de seguridad de la información de la normativa PCI DSS y las regulaciones vigentes de los organismos de control para determinar los controles que se pueden aplicar a los procesos de gestión de desarrollo, instalación y producción de los servicios transaccionales.
- Desarrollar los controles de la metodología que permita la implementación y gestión de los servicios transaccionales de la COOPCCP a partir del estudio realizado de las buenas prácticas y estado de madurez de la institución.

1.3 Justificación

A pesar del esfuerzo realizado para incrementar los niveles de seguridad de la información y mejorar integralmente su infraestructura tecnológica, existen algunos temas administrativos que no permiten avanzar con los distintos proyectos relacionados con la seguridad ya que, las áreas se dedican a trabajar en sus competencias sin tener una visión integral del negocio y la incidencia que tiene la tecnología en él, lo que ocasiona que no se realice una adecuada asignación de recursos.

Al momento de revisar su infraestructura y manejo de la información, se evidencia una latente falta de criterio de seguridad ya que, el personal del área de tecnología únicamente realiza adquisición de equipos y configuración de los mismos de acuerdo a lo recomendado por profesionales externos ya sean provenientes de una consultoría o como un valor agregado de un *partner* de negocio en la venta de activos de información (como firewalls, switches, etc.). Dicha práctica constituye a una falta en la gestión de la información contenida en su infraestructura ya que son vulnerables a la mayoría de las formas de ataques persistentes que puedan ser desplegados en sus servidores y clientes finales encontrándose vulnerables a cualquier tipo de conexión ya sea interna o externa a la COOPCCP.

Bajo este contexto, se considera necesario el desarrollo de una metodología de seguridad que con un criterio técnico defina una correcta configuración y tipos de seguridades a aplicar homologada en estándares internacionales y las normativas nacionales que contribuyan a la solución del problema y apoyen integralmente al funcionamiento y crecimiento de la institución, definidas en base de su situación actual.

El contar con una metodología de seguridad orientada a los canales y servicios electrónicos aportará con mejoras significativas en muchos ámbitos como: laboral (generando mayores medios de comunicación a potenciales clientes), productivo (mejorando los tiempos de producción de sus servicios), ambiente de trabajo (con controles específicos que genere confianza en sus clientes), etc. Con la aplicación de la metodología propuesta en el presente proyecto, se pretende que los problemas de seguridad en los canales transaccionales y de comunicación sean mínimos y se cuente con un correcto monitoreo en la infraestructura, una solución rápida a las solicitudes de otras áreas y cumplir con lo dispuesto por los organismos de control. La capacitación del personal es parte del proceso de cambio, dentro del mismo se van tipificando la manera de proceder para tener un crecimiento en las distintas áreas organizacionales de la COOPCCP, todo esto se traduce como diferentes tipos de mejoras en la empresa en tiempo de acción, respuestas rápidas, un fuerte control de datos y administración, etc.

El punto más importante es brindar un esquema de seguridad sólido que no solo beneficie a las áreas de tecnología y seguridad de la información, sino también al departamento de negocios y procesos, mejorando integralmente la manera en la que la COOPCCP llega a sus socios y potenciales clientes, ya que permitirá la integración de nuevos elementos tecnológicos que den soporte para una adecuada gestión de los productos y servicios electrónicos.

1.4 Alcance

El presente proyecto se alinea a las diferentes actividades que se desarrollan en la COOPCCP como son:

- **Levantamiento de información inicial:** Este proceso consistió en realizar reuniones iniciales dentro de la COOPCCP para extraer información específica requerida para obtener un punto de partida y conocimiento puntual del manejo de todos los dispositivos de infraestructura utilizados, protocolos de respuesta, certificaciones de seguridad, administración del software de desarrollo interno, bases de datos, proveedores de servicios, formas de administración de accesos y credenciales, entre otros. Además, se elaboró un análisis de documentos existentes como informes de auditorías, acuerdos de nivel de servicios (SLA) y toda la documentación relevante para el desarrollo del proyecto, este proceso se realizó mediante entrevistas al personal técnico competente dentro de la COOPCCP en los temas antes mencionados.

- **Análisis de Riesgos (ERM) a los activos de la información basados en la normativa PCI DSS:** Para el desarrollo de esta actividad fue necesario planificar una reunión con los distintos colaboradores pertenecientes al área de tecnología y al área de riesgos de la COOPCCP quienes brindaron la información técnica necesaria para el desarrollo de un análisis de riesgos basados en la normativa PCI DSS teniendo en cuenta que toda la información será a tratar en los servicios electrónicos son de clientes y socios de la institución. Se deben trata temas de infraestructura, bases de datos, proyectos vigentes y modelos de seguridad aplicados y a aplicarse. El trabajo con estas personas consistió en llevar a cabo un diálogo a manera de entrevista que se divide en 4 partes: Introducción a sus funciones dentro de la institución, perspectiva de seguridad dentro de su ámbito de trabajo, seguridad y planes de contingencia, conclusiones y recomendaciones.

- **Definición de los controles y buenas prácticas basados en normativas y buenas prácticas internacionales y regulaciones de organismos de control:** Se determinó la criticidad de los activos de información en base del levantamiento previamente realizado, con el fin de clasificar los puntos en los que requiere hacer énfasis al momento de definir los controles a ser utilizados en base a la realidad de la institución;

- **Desarrollo de la metodología de seguridad para la implementación segura de canales electrónicos:** Para poder realizar con éxito este paso fue necesario contar con la información levantada previamente hasta este punto, en el cual se toma como referencia diferentes definiciones de estándares de infraestructura, buenas prácticas de normativas internacionales y las regulaciones vigentes de los organismos de control, iniciando con las definiciones de los estados de madurez, los esquemas mínimos y los deseados ajustando el tipo de configuraciones en base a fuentes de conocimiento disponibles de manera libre dentro de repositorios de datos como por ejemplo, la página oficial de la CVE *(Common Vulnerabilities and Exposures)*.

- **Definición del estado de madurez de la Institución:** Se desarrolla en base al ERM tras obtener los resultados cuantificados en la matriz de riesgos, el cual se toma como punto inicial se debe definir los responsables de los diferentes procesos que se llevan a cabo para la gestión de los sistemas de información a nivel de administrativo, una vez formalizada esta información se realizó la preparación en el caso de estudio antes de impartir la metodología propuesta en el presente documento.

- **Desarrollo práctico de la metodología:** Una vez obtenidos los datos anteriores se procede a desarrollar la metodología con los lineamientos a seguir según las

características de los sistemas, procesos e infraestructura adquirida, de igual manera se toma en cuenta lo requerido por los entes de control de acuerdo al segmento al que pertenecen,

1.5 Estado del Arte

Según menciona Heredia J. (2017), a nivel mundial, las organizaciones cooperativas financieras son un segmento para el cual no se ha realizado ningún desarrollo específico sobre su adhesión a los servicios transaccionales vigentes y popularizados por la banca, los cuales hoy en día se encuentran ya disponibles en el mercado por empresas denominadas *startups*[2] por lo que actualmente no existe ningún desarrollo puntual sobre trabajos relacionados a metodologías o sistemas de seguridad, mucho menos homologados con las normativas que regula el funcionamiento de estas instituciones. Sin embargo, en base a la documentación vigente, sean actas o resoluciones dirigidas a la banca, se han realizado trabajos sobre guías metodológicas para un sin número de aristas que son de competencia del área de la seguridad de la información, y son basadas en estándares internacionales como la ISO 27000 o COBIT en cualquiera de sus versiones.

Según las investigaciones de Rodríguez (2016), Calderón & Castro (2017) y Constante (2016), disponibles de manera pública en los repositorios de universidades a nivel nacional e internacional, existen modelos y metodologías para la implementación de sistemas de gestión de seguridad de la información, sistemas integrados de gestión, metodologías de gestión y control, entre otros. Mismos que no se encuentran adaptados a la realidad ecuatoriana en conformidad con las normativas de la SEPS o la SBS y tampoco contempla todos los puntos de

[2] Concepto Ligado a los negocios en la era digital: es una gran empresa en su etapa temprana haciendo el uso de tecnologías digitales.

trabajo en la seguridad de la información y las aplicaciones de controles de seguridad informática.

Sin embargo, existen trabajo que destacan por su contenido ya sea en estructura o fin para el cual fueron desarrollados. Entre ellos se encuentran los siguientes:

1. **Metodología para la gestión de seguridad informática**: Se hace referencia al trabajo de Doina (2013). Por su amplio desarrollo en el tratamiento y gestión de incidentes de seguridad, pese a ser un documento perteneciente al año 2013 contiene referencias puntuales sobre los planes de acción en caso de ataques de día cero que se encuentran aún vigentes, con miras a solventar los problemas administrativos relacionados a la seguridad de la información.
2. **Guía metodológica para la implementación de un sistema de gestión de seguridad en instituciones**: Se cita a Miranda (2013) por realizar un trabajo que contempla la integración de varias normativas de seguridad de información así también como con la participación de normativas de gestión de procesos tecnológicos.
3. **Guía metodológica Indicador de seguridad de la información 2018:** Un muy importante trabajo por la Subsecretaría de telecomunicaciones de Colombia (2018) con su aporte en el desarrollo de métricas para el cumplimiento de la planificación de los proyectos de tecnología de la información y aplicación al sector financiero en el transcurso del último año.

4. **ICLG Fintech Ireland 2018:** Este artículo de A&L Goodbody (2018) habla sobre las normativas legales que existen a nivel mundial sobre las Fintech y recalca el gran

crecimiento dado en Irlanda en el último año en transición, menciona los beneficios de tomar en cuenta algunas buenas prácticas sobre seguridad con respecto a las aplicaciones distribuidas.

5. **The Pulse of Fintech 2018:** En el artículo de Pollari & Ruddenklau (2018). Hablan de un estudio sobre el impacto económico que tienen las *Fintech* y la manera en la cual su economía de escala se convirtió en referencia para el desarrollo de estas tecnologías aplicadas al mundo de las instituciones financieras.

Estos proyectos fueron destacados por su fuerte contenido relacionado con diferentes aristas de la seguridad de la información y sobre todo con las similitudes de las normativas a tomar en cuenta para el desarrollo del presente proyecto.

CAPÍTULO II

MARCO TEÓRICO

2.1 Ciberseguridad en el sector bancario en América Latina:

La seguridad informática hace referencia al desarrollo de actividades, métodos y gestión de herramientas con el objetivo de mitigar todo intento de intrusión en una infraestructura específica, así también como el análisis y monitoreo del tráfico en cada segmento de la red, por otro lado, la seguridad de la información trata de la toma de decisiones a nivel técnico y administrativo teniendo en cuenta no solamente la resolución de problemas generados por la automatización de procesos y los eventos de seguridad sino también de cada una de las aristas que pudiesen ocasionar algún tipo de afectación al giro del negocio.

Bajo esta premisa, la Organización de Estados Americanos, (OEA, 2018), presentó un reporte del estado de la ciberseguridad en el sector bancario en américa latina y el caribe, realizando el análisis de 191 entidades bancarias y los aportes de 772 usuarios de sus sistemas con corte al último trimestre de 2018. El objetivo de dicho documento fue analizar el comportamiento tanto administrativo como técnico de los profesionales a nivel mundial dedicados a la seguridad de la información y la seguridad informática respectivamente que se encuentren dentro de las instituciones financieras, denotando no solamente la posición de los CEO´s sobre la importancia de la seguridad de la información sino también el avance obtenido con relación a la postura mantenida años anteriores.

A continuación, se presenta información relevante del mencionado reporte:

Desde la perspectiva de la las instituciones financieras, en promedio, el 41% de las instituciones existen dos niveles jerárquicos entre el profesional encargado de la seguridad de la información y el director ejecutivo de las empresas; en el 74% de las instituciones se tiene un área única responsable de la seguridad digital, lo cual es un avance significativo ya que en el año 2016 solamente el 60% de las empresas encuestadas contaban con profesionales responsables de la seguridad de la información.

Este crecimiento fue necesario tras la creciente tendencia hacia la transformación digital y automatización de procesos que de manera directamente proporcional aumentaron los índices de ataques y delitos informáticos. Por tal motivo el área de seguridad de la información brinda un apoyo importante en la gestión del riesgo exigiendo la adopción de buenas prácticas de seguridad, fortaleciendo la capacitación y sensibilización de seguridad informática e impulsando planes de seguridad. Sin embargo, aún existe una gran brecha en la inversión de equipos dedicados a la gestión de eventos de riesgo, el 60% de las empresas consideran que convencer a la alta dirección de esta inversión tiene un medio grado de dificultad.

A nivel latinoamericano, dentro de los marcos metodológicos más utilizados se encuentran las normas ISO 27001 y COBIT entre el 68% y 50% respectivamente, teniendo como otros marcos de referencia lineamientos como PCI DSS. Para ello, según el tamaño de las empresas, en instituciones grandes, el 27% cuenta con un equipo de 16 – 30 miembros, en instituciones medianas, 48% cuenta con un equipo conformado por 1 – 5 miembros y en instituciones pequeñas, el 94% cuenta con un equipo conformado por 1 – 5 miembros.

Debido al bajo crecimiento del equipo de seguridad, cerca del 65% del trabajo de monitoreo de eventos deberá ser tercerizado, práctica que no es recomendada por los mismos profesionales de seguridad. No obstante, el 85% de las instituciones han logrado implementar una infraestructura medianamente robusta en seguridad con la inclusión de equipos IPS e IDS pero aún no se encargan de realizar sus propios desarrollos en tecnologías emergentes como Big Data, *Machine Learning*, o Inteligencia Artificial, las cuales son importantes para poder combatir las nuevas heurísticas maliciosas.

Por otro lado, en el mismo documento menciona que desde la perspectiva de los usuarios, se obtienen datos de comportamiento relevante tanto como para ayudar a designar los recursos de acuerdo con el uso de canales como para realizar estrategias comerciales que permitan tener un mejor lugar en el *Top of Mind* de su población objetiva. Partiendo de que el grado de confianza en el uso de canales electrónicos es del 88% se obtienen los siguientes datos de interés:

Con respecto a la conciencia de seguridad, el 85% conoce sobre incidentes de seguridad, sin embargo, únicamente un el 20% reconoce ser víctima de *phishing* o detectar actividades inusuales reportadas por su banco.

El 53% de los usuarios prefieren revisar sus transacciones y saldos utilizando teléfonos inteligentes más que los que consultan en el banco (29%) o vía telefónica (18%), de igual manera, en su mayoría (43%) prefieren hacer transferencias de sus fondos a través de banca móvil y solamente un 37% prefieren visitar el banco. Estos números varían en gran medida por la tecnificación y preferencia al uso de terminales móviles.

En conclusión, según el mismo reporte de la (OEA, 2018). Aunque el escenario presentado en el estudio es muy positivo, no es una realidad en todos los países de Latinoamérica y de manera mucho más preocupante, únicamente abarca al grupo bancario del sector financiero, dejando de lado las Cajas de Ahorro o también conocidas Cooperativas Financieras. En las cuales, empezando por el número de profesionales responsables de la seguridad de la información son ínfimos teniendo a únicamente 1 miembro o en otros casos, ninguno. Las herramientas, controles, procesos están en estado de desarrollo inicial y en muchas ocasiones, la normativa y los entes de control no consideran dichas seguridades por lo que, se genera un retraso tecnológico y un alto riesgo en las comunicaciones informáticas de dichas instituciones que deben ser suplidas a su medida de economía a escala con los recursos vigentes. Como consecuencia, en la mayoría de las instituciones, carecen de reportes e identificación de vectores de ataques y eventos de seguridad.

2.2 Instituciones Financieras en el Ecuador:

Las instituciones financieras son entidades que, por naturaleza y actividades diarias, se consideran empresas de alto riesgo y como tal, deben aplicar diferentes normativas y regulaciones que más allá del cumplimiento deben enfocarse en proteger toda información de sus socios y clientes ya que ese es el activo más importante en su posesión. Para cumplir ese objetivo, los organismos de control en el Ecuador disponen el cumplimiento de normas como la resolución de la junta bancaria No. JB-2148-2012 hasta su última modificación en 2015, que si bien es cierto han logrado aumentar su alcance en estos últimos 7 años, no aseguran un nivel adecuado de protección sobre las amenazas que hoy en día existen en el ambiente cibernético.

Pese a aquello, las tecnologías emergentes junto al concepto de internet de las cosas (*IoT)* [3]ponen en el mercado soluciones informáticas que se encuentran en una corriente creciente y luchan por adaptarse a los modelos de negocios de la banca.

Es importante mencionar la diferencia entre cooperativas financieras y la banca, haciendo énfasis en el modelo de negocio que manejan: La banca, tiene en su dirección a socios privados, un grupo selecto que son dueños de las acciones y decisiones de la institución. Así, cada una de las personas que desean ser parte del modelo de intermediación financiera son denominados **clientes**, quienes pagan un porcentaje de su dinero para poder utilizar sus servicios. En este caso, el objetivo de la banca es únicamente el crecimiento de la empresa mediante la captación de clientes y expansión física controlada.

Por otro lado, en una cooperativa financiera, cada persona que desee ingresar debe aportar con una cantidad de dinero que le faculta como un socio de la cooperativa con derechos y obligaciones, teniendo inferencia en las decisiones de la institución, al ser este una organización que trabaja para todos sus socios y no solo un grupo selecto de ellos, las cooperativas financieras reparten el capital ganado por recaudaciones en beneficios para todos sus socios tanto en servicios, capacitaciones, obras o culturización y temas de responsabilidad social, llegando a sectores a los cuales los bancos no acceden. Por tal motivo, existen varios puntos que los diferencian a nivel normativa y uso de tecnologías que son determinantes para el desarrollo de la seguridad de la información y su aplicación en el mercado. Mismas que se especifican más adelante en el presente documento. (Dirección Nacional de Información, 2016)

[3] Internet of Things: Según CISCO (2011), es la interconexión digital de objetos cotidianos con Internet

2.3 Las Fintech en el Ecuador:

Tapia & Maldonado (2018) refieren que pese a que la ola del *Fintech* en América latina surgió alrededor del año 2013, no fue hasta mediados del 2016 y ya en el 2017 que en Ecuador se reconocieron 31 empresas con el modelo de *startups* enfocadas a solucionar el principal problema del modelo B2B (*business to business*) de no llegar directamente al cliente. Y aunque sea un mercado nuevo, no es incierto, pero puede llegar a ser oneroso para las empresas que decidan dirigir sus esfuerzos a este sector. Según encuestas del Banco Central del Ecuador (2017), el 40% de la población accede a los servicios bancarizados, lo que quiere decir que el 60% restante, aunque no haga uso de estos servicios, tiene entero conocimiento del uso de teléfonos e Internet. Es importante recalcar que estos servicios están en boga para los millennials en el Ecuador, que, según datos del INEC con edades entre 20 y 36 años, componen el 23% de la población del país.

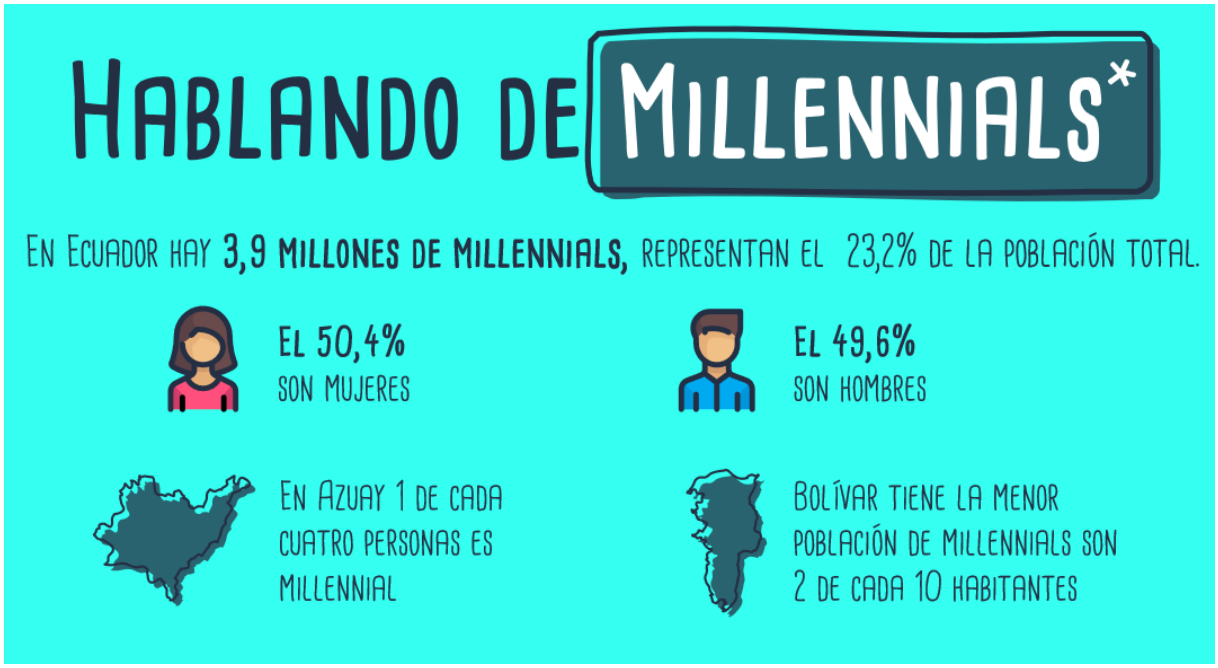


Figura 1: Presencia de un nuevo mercado en Ecuador.
Elaborado por: INEC, 2018

El modelo de las Fintech es uno de los mercados más prometedores, sobre todo porque, según Heredia (2017), se encuentra en un crecimiento que durará alrededor de 20 años más. Sin

embargo, aún no se encuentra maduro como para aseverar que son confiables y podrá resguardar la integridad, confidencialidad y disponibilidad de los usuarios de la banca. Por otro lado, este modelo de negocio encaja de mejor manera en el modelo de las cooperativas y cajas de ahorro ya que, se encuentran orientadas a brindar beneficios para sus socios y no únicamente al crecimiento de la empresa. Además, si se implementan de la mano de una metodología de seguridad que aplique tanto en canales transaccionales como infraestructura, cada arista puede ser solventada.

2.4 Servicios y canales Electrónicos:

Según la Superintendencia de Bancos y Seguros (SBS) y la Superintendencia de Economía Popular y Solidaria (SEPS), en la Resolución No. SEPS-IGT-IR-ISF-ITIC-IGJ-2017-103. (Resolución No. SEPS-103, 2017) A nivel técnico se definen a los canales electrónicos a todos aquellos que contengan información que realice consultas a las tablas de base de datos que contenga información sobre sus socios o clientes, tomando en cuenta diferentes directrices para el tratamiento de los datos que se comparten, preservando por sobre toda otra norma el sigilo bancario, un convenio existente para que la información privada que fue proporcionada por el socio o cliente únicamente esté disponible para las dos partes y el organismo de control si así fuera necesario. Entre las aplicaciones más comunes de servicios en canales electrónicos se pueden encontrar los siguientes:

- **ChatBots Transaccionales:** El uso de asistentes inteligentes con fines transaccionales ha ido incrementándose en los últimos años, permitiendo a los usuarios realizar consultas y afectaciones a bases de datos mediante diferentes servicios web disponibles de manera pública. (SEPS, Resolución No. SEPS-IGT-IR-ISF-ITIC-IGJ-2017-103., 2017)
- **Facebook / Whatsapp Enterprise:** El gran contingente de desarrollo de Facebook y Whatsapp entregan una plataforma segura para el uso de chatbots en sus canales,

condicionados a ser utilizados mediante la acogida de un gran volumen de usuarios y únicamente bajo una licencia empresarial. (Schul, 2018)

- **Botones de pago:** Una de las integraciones que generan un gran retorno de inversión tanto como para la institución financiera como para sus usuarios son los botones de pago, mediante los cuales se realizan órdenes de cobro en línea y se acreditan a la empresa con quien se maneja la alianza. (INTERDIN, 2015).
- **Modelos predictivos de comportamiento de pago – Inteligencia artificial:** Realizar una heurística que logre predecir comportamientos para el sistema crediticio es un arma muy eficaz si se realiza de manera correcta, este es quizás uno de los servicios más importantes para el proceso de colocación de fondos en una institución financiera. (Equifax, 2007)
- **Consultas IVR:** Las consultas con IVR (Interactive Voice Respond) actualmente continúa siendo utilizada como un sistema transaccional realizando consultas a las cuentas de los clientes de manera indirecta. (INTERDIN, 2015).
- **Tarjetas de débito – crédito:** El tratamiento de la información del tarjetahabiente es un proceso delicado en el que interfieren algunos gestores del procesamiento de la información tanto del autorizador, el procesador y el adquiriente, por lo que es necesario asegurar la información que viaja a través de las tramas con encriptaciones y canales certificados. (INTERDIN, 2015).
- **Servicios Web (*Web Services*)– Transaccionales:** Según Baquero (2015), los servicios web son scripts de programación que permiten la comunicación entre plataformas a nivel de enlaces de archivos y bits codificados en un rango seguro que permita el paso de diferente tipo de información a ser procesada por *Stored Procedures*. Esta es una comunicación de doble vía que es utilizada en el sistema financiero para el sistema transaccional en ventanillas de extensión de servicios.

- **Banca / Cooperativa en línea:** Según el trabajo de investigación de Tarifi, Cutillas & Soley (2011), básicamente es una extensión del sistema financiero que permite la afectación de cuentas tras un proceso de validaciones, este servicio financiero es utilizado en gran medida mediante aplicaciones móviles, por lo que es necesario tener en cuenta varias aristas a nivel normativo y funcional para su correcta aplicación.
- **CORE Financieros Manejo de datos:** Según Zauzich (2016), existen algunas distribuciones que se dedican a la tercerización del manejo de datos de sus asociados, esta, si bien es cierto no es un servicio disponible al público, se deben tomar varias consideraciones antes de incursionar en este modelo. En la legislación ecuatoriana no existe una sección clara sobre el tratamiento
- **Sistemas de relaciones con el cliente:** Según Rouse (2015), el tratamiento de grandes cantidades de información a una alta velocidad, es la premisa requerida para la implementación de estructuras que apliquen BigData para un sector financiero, actualmente el uso más relevante de este campo son las aplicaciones en herramientas para la gestión fuera de oficinas y su incorporación con grandes sistemas de archivos, obteniendo un control y seguimiento sobre cada gestión. De igual manera, este es un servicio que no se encuentra directamente visible al público, sino a los colaboradores de cada institución financiera. Sin embargo es un servicio adquirido al momento de aceptar utilizar sus datos para mejorar la experiencia de usuario en la interacción con la institución financiera.
- **SMS – transaccional:** Comparte el mismo esquema que las consultas por IVR, la transaccionalidad se realiza de una manera arcaica ya que para el funcionamiento de este servicio es necesario el uso de tarjetas de coordenadas. (SINERMEDIA, 2016)
- **Billetera Móvil:** Un proyecto que está por arrancar en el Ecuador y pretende que se manejen pequeñas cantidades de dinero (montos de hasta 100 USD) que sean

transaccionales como un monedero digital y aceptados en todos los establecimientos y negocios formales, microempresarios, Pymes medianos, entre otros.(BANRED, 2018)

2.5 Modelo de Negocios a Escalas

Las instituciones financieras utilizan modelos de negocio diferentes de acuerdo a sus distintos tamaños y recursos, puntualmente en las Cooperativas Financieras, existe el modelo de negocios a escala, que según Rodriguez (2011), trata de brindar servicios de manera mixta con su infraestructura, tanto en enlaces y servidores con los beneficios de organismos que se encarguen de actuar como terceros en la adhesión de nuevos servicios.

Eventualmente este tipo de negocios definidos como servicios financieros auxiliares buscan rentabilidad a través de generar un gran volumen de tráfico en el uso de sus servicios, dejando una alta rentabilidad que es tangible a partir del segundo o tercer año una vez realizada la inversión. Y para lograrlo, se requiere manejar estrategias de negocio que estén orientadas a promover el uso de tecnologías que les permita concretar el objetivo. De este modelo, Rodríguez (2011) define las siguientes operaciones:

- **Operaciones Pasivas:** Se trata de operaciones por las que la entidad financiera capta, recibe o recolecta dinero de sus socios y clientes, dichas operaciones se ven respaldadas por depósitos que puede reflejarse en ahorros, inversiones y depósitos a plazo fijo.
- **Operaciones activas:** Colocar recursos significa posicionarlos entre personas que permitan generar un retorno dependiendo de algunas aristas como el destino de los fondos, la capacidad de pago del beneficiario y la calificación de buró, una heurística que permite predecir el comportamiento crediticio. Estos créditos se otorgan a personas y empresas.

- **Servicios Financieros complementarios:** Por normativa, las instituciones financieras no pueden realizar la comercialización de servicios no financieros como seguros o equipos, sin embargo, el modelo y normativa permite participar como intermediario financiero en estas transacciones que son elegidas por el socio o cliente de manera libre y voluntaria. Lo que genera movimiento a las cuentas y posteriormente, colocación del dinero. Lo que también genera ingresos para la institución.

Por dar estos préstamos el banco cobra, dependiendo del tipo de préstamo, unas cantidades de dinero que se llaman intereses (intereses de colocación) y comisiones. Al diferencial entre lo que los bancos cobran por el dinero que prestan y el que abonan a los que les ceden sus ahorros en depósito, se le llama diferencial de tipos de interés, y junto con los ingresos por comisiones bancarias constituyen el negocio bancario. (Rodríguez C. E., 2011)

2.6 Gestión de seguridad en instituciones de la SEPS:

Hoy en día las instituciones pertenecientes a la SEPS tienen la obligación de cumplir con la Resolución No. SEPS-IGT-IR-ISF-ITIC-IGJ-2017-103. (Resolución No. SEPS-103, 2017). Misma que habla específicamente sobre temas de seguridad de la información orientadas a las transferencias electrónicas aplicando seguridad sobre gestión de perfiles de usuarios administradores, finales y seguridad a nivel de comunicación. Lo que deja normativamente una brecha de seguridad en temas de infraestructura e incrustación de diferentes ataques de día cero. Por lo que, la SEPS decidió continuar cumpliendo a manera de buenas prácticas lo mencionado en las resoluciones de la junta bancaria SEPS 103 (2017), puntalmente iniciando en la norma JB-2005-834 incluyendo sus reformas en las resoluciones (JB-2012-2148 ,2012) ; (JB-2014-3066, 2014). Mismas que disponen a la seguridad de la información bajo el área de riesgo operativo y lo tratan como eventos tecnológicos y servicios transaccionales. Lo que, nuevamente deja abierta la gestión integral de un sistema de seguridad de la información íntegro

que pueda responder ante cualquier tipo de ataque o vector existente al que esté expuesta la institución financiera de acuerdo con los servicios que ofrecen.

Como actualmente no se encuentra detallado a fondo la gestión de la seguridad para las entidades financieras y principalmente al no poder establecer resoluciones y normativas que se encuentren en el tiempo y acorde al avance tecnológico, los profesionales dedicados a resguardar la seguridad informática se ven obligados a realizar un manual de gestión de seguridad de la información (SGSI) que adopte buenas prácticas de diferentes normativas internacionales tales como la ISO 27000 en gestión de seguridad de la información, la PCI DSS para la seguridad en la información de los tarjetahabientes, prácticas de ISACA o libros de ITIL para concatenar con la aplicación de seguridad en los procesos e incluso COBIT en cualquiera de sus versiones para poder definir el esquema de seguridad.

2.7 Aspectos de la seguridad

La empresa consultora ISOTools Excellence (2017) realizó una breve descripción sobre los aspectos clave de la seguridad de la información según la normativa especialista en el tema, la ISO 27001:2013. Es necesario recordar que ningún sistema de seguridad es completamente seguro y de acuerdo a la línea de negocio, se prioriza cierto aspecto sobre los otros con el objetivo de tener un sistema menos vulnerable, los puntos que se toman en cuenta son:

- **Confidencialidad:** Se refiere a los mecanismos o artificios diseñados para prevenir la divulgación de la información a personas o sistemas no autorizados que busquen de manera directa o indirecta acceder a los archivos. El principio de confidencialidad es fundamental en líneas de negocio en la que dependan únicamente del estado del archivo o documento.

- **Integridad:** Se refiere a la manera en la que los datos se mantienen intactos desde la primera vez que fueron concebidos en su estado final y original y en la que únicamente hayan participado los dueños de la información y los programas definidos por los mismos. Este principio puede ser el más importante ya que de este depende las afectaciones directas que se realizan fruto de un proceso automatizado y muchas de las veces, atentar contra este principio puede tener afectar temas legales, (desestimando la veracidad de una prueba en un proceso judicial) tecnológicos (ocultando riesgos de las acciones sobre la infraestructura de red), entre otros.
- **Disponibilidad:** El tercer piar de la seguridad de la información describe la capacidad que se posee para tener disponible la información cuando el usuario o sistema necesita realizar la consulta.

Estos tres pilares fundamentales son aquellos en los que se debe basar el profesional responsable del resguardo de la información para poder ofrecer y evaluar soluciones a los problemas que resultan del riesgo inherente de realizar las actividades. Se puede determinar que la seguridad consiste en mantener el equilibrio adecuado entre estos tres factores. Ya que, no tiene sentido conseguir la confidencialidad para un archivo si es a costa de no poder acceder a él, inclusive con permisos de administrador o usuario privilegiado. O que se encuentre libre de modificaciones no consentidas y se encuentre disponible al momento de ser requerido, pero no es confidencial de cualquier persona que desee visualizarlo.

2.8 Ataques informáticos:

Según Tarazona (2018), hoy en día los ataques informáticos constituyen un mal común dentro de la actividad que se realiza en línea a tal manera en que no se puede asegurar que un dispositivo se encuentre seguro ya que los ataques pueden ser tan simples como un gusano o tan destructivos como un *Randsomware* si se habla a nivel de daño a los equipos de cómputos,

sin embargo ese no es el objetivo de todos los virus informáticos desarrollados, por lo que es importante informar sobre la evolución que han tenido gracias a las nuevas tecnologías emergentes derivadas del *data Ware House* y la minería de datos aplicadas para su uso en actividades diarias, buscando transformar el mundo a un ambiente digital.

Según los autores de ACIMED, Bello & Ileana (2003). Los virus informáticos tienen propiedades inspiradas en el sistema orgánico biológico de un proceso viral en el cual se pueden reproducir, aprender e incluso protegerse. Por tales variaciones es imposible llevar un registro de todos los tipos de virus existentes y aunque ciertos de ellos son desconocidos, muchos otros gozan de una gran popularidad debido al daño que ocasionaron en su momento:

Como se menciona en el mismo artículo, el más conocido de ellos es el denominado viernes 13, que fue lanzado en 1987, infectando los documentos con extensión .EXE y replicando esta actividad hasta tener una gran cantidad de procesamiento ocupado, el objetivo era la desactivación de información militar. Por lo que tras un proceso de investigación se encontró la manera de mitigar el efecto. Fue el primer daño masivo registrado por un gusano. Seguido de grandes hitos de su evolución con la portabilidad a los disquetes y posteriormente a las comunicaciones gracias a la red de redes.

Según Prieto & Pan (2006) en su proyecto de identificación de virus informáticos se definió de manera puntual los tipos de scripts maliciosos y su comportamiento, del análisis se clasificaron a los virus informáticos en los siguientes tipos:

- Virus Transaccionales
- Virus Encriptados

- Virus Polimórficos
- Gusanos
- Troyanos
- Virus Falsos
- Bombas Lógicas
- Bug – Ware
- MIRC

Según Ruiz (2016), estas definiciones que fueron válidas hasta el año 2016, ya que a partir de dicho punto, el mundo de la informática surgió un cambio rotundo por la aparición de los primeros scripts maliciosos que aplican Inteligencia Artificial, heurísticas diseñadas con el fin de emular el comportamiento de selección y sobrevivencia, cualidad que les permitió defenderse ante las medidas de seguridad tradicionales como antivirus y conmutadores de tráfico en puertos, dando vida a la nueva generación de *Ransomware*. En respuesta a esta evolución, para poder combatir esta nueva generación de software, también se desarrollaron sistemas que emulan el sistema inmunológico, conjuntos con el uso de métodos como sandbox, se construyeron los primeros sistemas de respuesta en base a anomalías del sistema.

2.9 Clasificación de ataques por segmentos de red:

Según Moreira & Alcívar (2018), pueden existir varios tipos de agrupaciones para explicar los tipos de ataques existentes y en su estudio hacen referencia a vulnerabilidades en las capas del modelo OSI y de acuerdo a dicha investigación, para los fines del presente proyecto, se los clasifica según el vector de ataque que utilizan como medio para propagarse o causar afectaciones:

- **Vulnerabilidades a nivel de puertos:** Los puertos de comunicación deben ser censados y su conexión debe ser permitida o rechazada según el requerimiento de los programas que se utilizan ya que existen diferentes tipos de vulnerabilidades que aprovechan el bajo control de los puertos para enviar información del computador objetivo con el fin de tener un ataque persistente. Las herramientas comúnmente usadas para explotar las vulnerabilidades en puertos son:
    - ***Bot nets*. –** Según Kaspersky Labs (2013). Son pequeñas sentencias de código que recopilan información de los computadores y permiten al atacante o administrador de los *bot nets* conocer el ambiente e infraestructura manejada. Este tipo de ataques persistentes están presentes comúnmente en archivos adjuntos enviados por e-mail camuflados en extensiones .PDF, .DOC o .DOCX.
    - ***Backdoors*. –** Según Albors (2015). Son métodos que tienen como objetivo permitir la comunicación entre el computador del objetivo con el del atacante, con el fin de iniciar estas sesiones y buscar realizar escalamiento por medio de toda la información reportada por los *botnets.*

- **Vulnerabilidad a nivel de archivos:** Tanto las comunicaciones como los archivos son considerados un vector de ataque cuando los *payloads* se ven alterados, atentando directamente contra la integridad de la información. Para evitar que existan este tipo de ataques hay diferentes soluciones que permiten realizar una segmentación discriminante sobre los documentos que se encuentran en los computadores, es importante mencionar también que la existencia de archivos en directorios ligados al sistema operativo es de por sí, una posible amenaza de virus.

- **Vulnerabilidad a nivel de aplicaciones:** Similar a la vulnerabilidad a nivel de puertos, es importante censar la comunicación y tiempos de escucha y acción que existe configurado en las aplicaciones que se utilizan ya que, el permitir comunicación mediante una aplicación conectada a un servidor puede ser el causal perfecto para que el atacante pueda realizar movimientos laterales o simplemente busque abrir un backdoor para tratar de obtener escalabilidad en el tipo de ataque persistente que se esté realizando.

- **Vulnerabilidades en los enlaces de datos:** Los enlaces de datos mantienen un esquema punto a punto mediante el cual la información puede comprometerse si no se encuentra debidamente protegida, algunos de los ataques que fuerzan las posibles vulnerabilidades de estoy sitios son:
    - **Ataque de denegación de servicios (DoS).-** Este tipo de ataque trata de prohibir o denegar el uso de una red a usuarios, normalmente este es un tipo de explotación que busca bajar los servicios y aplicar otros tipos de ataques. En general provoca la pérdida de conexión a la red por sobre consumo de ancho de banda o sobrecarga de recursos; haciendo que el servidor se sobrecargue impidiendo su funcionamiento. Como dato importante, según el estudio realizado por la empresa ARBOR NETWORKS (2018), en el Ecuador existió un alza de 258% en los ataques en relación con el año 2017. Lo que se traduce en 9.150 ataques por mes o 305 por día, que muy por fuera de ser solo intentos, el 90% registró baja de servicios y detección de *exploits*.

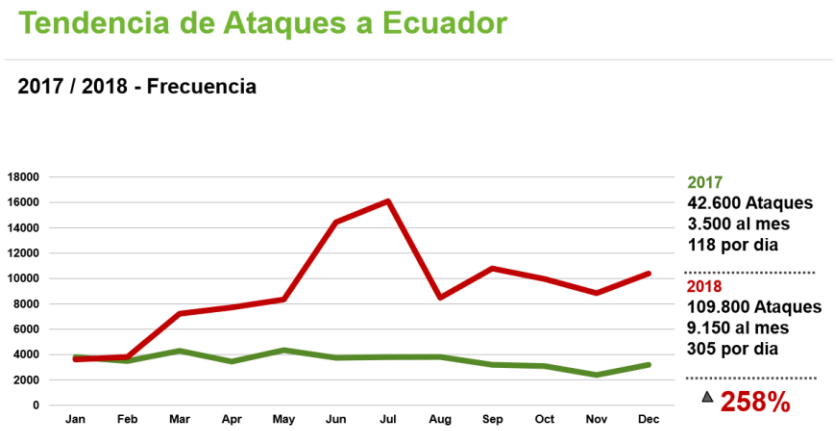


Figura 2: Tendencias ataques DDoS Ecuador – Frecuencia
Elaborado por: ARBOR NETWORKS, 2018

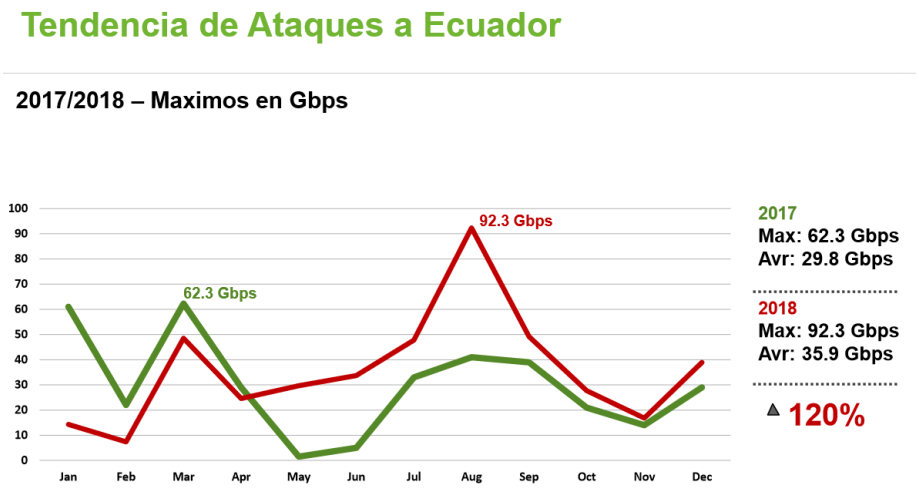


Figura 3:Tendencias ataques DDoS Ecuador – Máximo en Gbps
Elaborado por: ARBOR NETWORKS, 2018

- **Ataque *Man In the Middle*. –** Según Karspersky (2013), su premisa básica es redireccionar y reenviar (Con la opción a modificar el contenido de los datos incrustados en la trama de comunicación) datos alterando dirección MAC en las tablas ARP de cada computador (este ataque utiliza el método de *ARPSPOOFING*), esto es posible ya que el protocolo ARP no tiene ningún mecanismo de validación de datos por tanto si recibe nuevos datos simplemente los acepta y actualiza por parámetros ya existentes en la tabla.

- **Explotaciones día cero. -** Conocida como una reingeniería a realizada a los equipos y aplicaciones informáticas que consiste en explotar fallas que no hayan sido reportadas por los desarrolladores de la aplicación y de esta manera, comprometer el sistema ofreciendo una ventana de oportunidades a los atacantes. En la mayoría de las ocasiones, los ataques de día cero son solucionables con las actualizaciones o parches que los desarrolladores publican tiempo después de haberse presentado, sin embargo, es altamente recomendable que existan otros niveles de seguridad para prevenir daños de este tipo. Uno de los daños más memorables fue los miles de afectaciones a nivel mundial del virus *Ransomware.*

  Según el estudio realizado en noviembre por ESET (2018) se informó que Ecuador se encuentra en el puesto 7 de los países con más casos de virus de tipo Ransomware. Como resumen del reporte, se expresa la siguiente gráfica:

País	Porcentaje de Ataques
Colombia	28%
Perú	17%
México	15%
Brasil	11%
Argentina	9%
Chile	1.33%
Ecuador	1.33%
Venezuela	1.33%
Resto de América Latina	6%

Tabla 1: Países con más ciberataques de América Latina.
Elaborado por: ESET (2018).

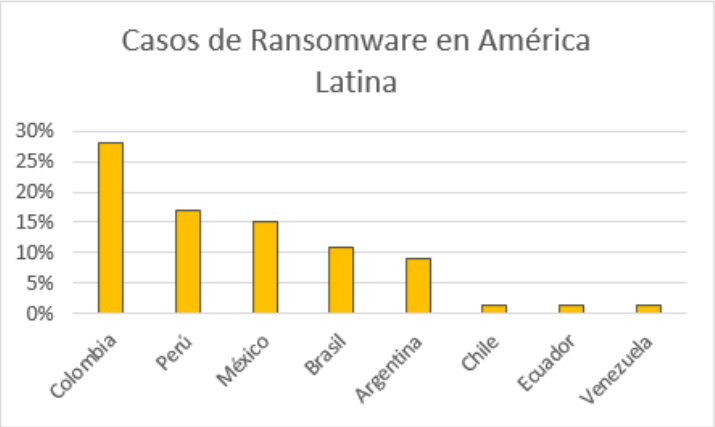


Figura 4: Países con más ciberataques de América Latina.
Elaborado por: ESET (2018).

- **Ataques a IoT. –** Hoy en día existen también nuevos vectores de ataques encontrados, dichas vulnerabilidades no siempre son explotables sin embargo representan un riesgo cuando se presentan a nivel de protocolos como el ya conocido exploit en el protocolo de transferencia de archivos de bluetooth, lo que abre las puertas a nuevas posibilidades de explotar vulnerabilidades que se encontraban blindadas por esta seguridad primaria.

2.10 Equipos de infraestructura y gestión de seguridad de la información.

Como lo define la normativa SEPS 103 (2017), los equipos de infraestructura son componentes sin los cuales una institución de alto riesgo no podría continuar sus operaciones, ya que su funcionamiento depende únicamente de su capacidad de adaptarse al medio en el que se encuentran. Actualmente se encuentran catalogados de manera estándar como: equipos de seguridad perimetral, equipos de seguridad de punto a punto, equipos de seguridad de usuarios finales, protección antivirus, emuladores de comportamientos, detectores de intrusos, detectores de anomalías, correlacionadores de eventos, entre otros.

Con el tiempo se fueron convirtiendo en dispositivos y soluciones multipropósito mismas que, con diferentes integraciones se desarrollaron como módulos mixtos. De manera básica, según la SEPS (2017), para propósitos del desarrollo de un sistema para servicios transaccionales, los equipos de infraestructura dedicados a la seguridad son:

- ***Security Information and Event Management*** **(SIEM) - Monitoreo:** Este tipo de soluciones en realidad son una evolución de los sistemas de administración de eventos de seguridad de la información, que proporciona el censo en tiempo real de una red o infraestructura informática, incluyendo todas las conexiones entrantes y salientes. Estas soluciones se presentan como software, *appliance* o en administración de terceros en un modelo SAS. Una de las características más importantes es que esta herramienta permite obtener pistas de auditoría que de manera técnica, ofrecen información acerca de toda conexión expuesta en la red.

  Esta herramienta y servicio se entrega con el fin de poder recolectar y correlacionar todos los eventos que se encuentren en la red, dispositivos de seguridad, aplicaciones de gestión de identidades, eventos de aplicaciones, sistema operativo, bases de datos, entre otros. También, es una herramienta que ayuda en gran medida a gestionar las vulnerabilidades y los instrumentos de cumplimiento de diferentes políticas, principalmente de la normativa PCI DSS, ayudando a controlar los permisos y privilegios de usuarios de un sistema o servicio. (IMPERVA, 2017)

- **Firewall Seguridad Perimetral:** Un firewall o corta fuegos es un dispositivo que puede ser tanto físico como lógico que permite administrar y filtrar el tráfico entrante y saliente que existe entre los dispositivos de una red que además se maneja con un conjunto de reglas modificables tomando la acción de bloquear todo tráfico que no se encuentre de acuerdo con lo existente. La correcta configuración de un firewall junto con el registro

de los eventos en un correlacionador pueden ser una fuerte herramienta para la identificación de posibles intrusos en una red o tratar temas de fuga de información, comunicaciones forzadas, análisis de los puertos abiertos en la red, entre otros. (OWASP, 2016)

- **WAF - Seguridad Perimetral:** El protocolo de transferencia de hipertexto y su amplio uso en Internet lo hizo el foco principal de los ataques dirigidos, motivo por el cual se vio la necesidad de implementar una solución de cortafuegos que aplique únicamente a este segmento, lo que lo convierte en una puerta primaria de seguridad que aplica una serie de reglas en las conversaciones de http, por defecto, se encuentra preconfigurado para que se pueda proteger a la red contra diversos ataques:

    - *Cross-site scripting* que consiste en la inclusión de código script malicioso en el cliente que consulta el servidor web.
    - *SQL injection* que consiste en introducir un código SQL que vulnere la Base de Datos del servidor.
    - *Denial-of-service* que consiste en que el servidor de aplicación sea incapaz de servir peticiones correctas de usuarios.

  Hay 2 tipos de WAF: Los que se residen en la red (es decir son un elemento más de la red) y los que se basan en el servidor de aplicaciones (residen en el servidor). Los WAF son elementos complementarios a las medidas de seguridad que soportan los Firewall clásicos. (OWASP, 2016)

- **Seguridad Perimetral – IPS:** Los investigadores de la NIST, Scarfone & Mell (2007). Un sistema de prevención de intrusos se encarga de, como su nombre lo indica, tomar

acciones al momento de recibir un condicionante previamente programado y poder según sea el caso, permitir la conexión, informar del evento o aislar el computador infectado de la red para iniciar un proceso de emulación. Dependiendo de las configuraciones existentes este dispositivo puede ser ampliamente explotado teniendo en cuenta también su ubicación dentro de la topología de red ya que censará únicamente el tráfico que pase a través de él.

- **Seguridad Perimetral - ADS:** De igual manera Scarfone & Mell (2007) mencionan que un sistema de detección de anomalías consiste en registrar cualquier actividad que no se encuentre dentro del sentido normal del proceso, teniendo para ello dos maneras de recopilar esta información, mediante firmas digitales obtenidas de las casas de seguridad que proveen el servicio de actualización o de un aprendizaje diario programado utilizando tecnología de Inteligencia Artificial. El primer método no es del todo seguro ya que tiene como particularidad que la frecuencia de actualización es muy baja, por lo que el sistema queda inútil para tipos de ataques de día cero o nuevas actualizaciones en los comportamientos del script, evolución natural de un virus.

- **Seguridad en última milla - DLP:** Según Andrade (2015). Los mecanismos de prevención de pérdida de datos o DLP por su significado en español, son aquellos que se encuentran instalados a manera de agentes en los dispositivos finales de usuario y tienen como objetivo dar continuidad al seguimiento y organización de los archivos que sean considerados críticos según la matriz de archivos de la información. Actualmente los DLP también incluyen funcionalidades que tratan de llevar el control a dispositivos móviles, agregando capas adicionales de seguridad. Para cumplir este fin, se utiliza bloqueo de puertos o comunicaciones.

- **Emulación de comportamiento- *SandBox*:** Según Carles (2017). Un sandbox es un mecanismo de seguridad para disponer de un entorno aislado del resto del sistema operativo y segmentos de red. Todos los programas que se ejecutan dentro de un sandbox lo hacen de forma controlada mediante los siguientes aspectos:
    1. Se les asigna un espacio en disco. Estos programas no podrán acceder a ningún espacio del disco que no les haya sido asignado previamente.
    2. Se puede hacer que los programas se ejecuten en un sistema de archivos temporal (tmpfs) para aislarlos del resto del sistema operativo.
    3. También se les asigna un espacio en memoria. Los programas no podrán acceder a otras partes de la memoria que nos les hayan sido asignadas.
    4. Se les puede dar o restringir la capacidad para acceder y consultar dispositivos de almacenamiento externos.
    5. Se puede restringir la capacidad para que puedan inspeccionar la máquina anfitriona.
    6. Se puede restringir el acceso de los programas a la red, al servidor de aplicaciones, al servidor de sonido, entre otros.
    7. Se puede limitar el ancho de banda que usa un determinado programa

Software de seguridad - Reglas YARA:

Según ESET (2017). Hoy en día existe una nueva manera de combatir las afectaciones por scripts existentes en una página web que tenga como objetivo minar información o utilizar los recursos del sistema para infectar un equipo, las reglas YARA son cadenas de código que reconocen scripts a nivel de capa 7 (aplicación) y pueden almacenar una base de datos para guardar las diferentes conductas aprendidas y en base a ellas poder tomar decisiones sobre los motores que corren tras todo el código descargado de una página web evitando ejecución de

código y uso no consentido de los recursos de un equipo para actividades como minería de crypto-monedas.

Software de seguridad – Encriptación:

Según Agulló, Guerra, Silva & Vivanco, (2012). Los algoritmos criptográficos o de encriptación son soluciones que modifican un mensaje original en función a una contraseña que contiene métodos aritméticos teniendo como objetivo que el mensaje no sea funcional sin la llave y algoritmo, método que evita revelar su contenido. Existen diferentes tipos de encriptación y uso de la misma.

Algoritmos Simétricos. - En este caso se utiliza una clave para cifrar y descifrar la información,

Algoritmos Asimétricos. - Son los que utilizan para su cifrado dos tipos de claves, una pública y una privada, la pública será la cual el mediador cifre la información que se está enviando y la privada será de único acceso y conocimiento del remitente, haciendo que el mensaje sea fácil de encriptar, pero muy difícil de desencriptar. Existen algunos ejemplos de este tipo de cifrado sin embargo no se puede igualar a la seguridad que brinda la longitud del rango de asignación de un cifrado simétrico.

Es importante mencionar que un buen sistema de cifrado pone toda la seguridad en la clave y ninguna en el algoritmo ya que es mucho más fácil para el atacante tener la clave.

La encriptación se ve como el tipo de seguridad que puede ser utilizada para evitar atentar contra la integridad de la información que haya sido compartida por canales no censados o seguros, sin embargo, en la actualidad se utilizó este método para realizar ataques informáticos tales como *Randsomware.*

2.11 Riesgo Operativo - Análisis de riesgos

Según Amaya (2012), como parte del Sistema de Gestión de Seguridad de la Información, es necesario hacer una adecuada gestión de riesgos que le permita saber cuáles son las principales vulnerabilidades de sus activos de información y cuáles son las amenazas que podrían explotar las vulnerabilidades. En la medida que la empresa tenga clara esta identificación de riesgos podrá establecer las medidas preventivas y correctivas viables que garanticen mayores niveles de seguridad en su información.

También menciona que son muchas las metodologías utilizadas para la gestión de riesgos, pero todas parten de un punto común: la identificación de activos de información, es decir todos aquellos recursos involucrados en la gestión de la información, que va desde datos y hardware hasta documentos escritos y el recurso humano. Sobre estos activos de información es que hace la identificación de las amenazas o riesgos y las vulnerabilidades

Por lo tanto, Amaya menciona que una amenaza se puede definir entonces como un evento que puede afectar los activos de información y están relacionadas con el recurso humano, eventos naturales o fallas técnicas. Algunos ejemplos pueden ser ataques informáticos externos, errores u omisiones del personal de la empresa, infecciones con malware, terremotos, tormentas eléctricas o sobrecargas en el flujo eléctrico.

Por otra parte, también dice que una vulnerabilidad es una característica de un activo de información y que representa un riesgo para la seguridad de la información. Cuando se materializa una amenaza y hay una vulnerabilidad que pueda ser aprovechada hay una exposición a que se presente algún tipo de pérdida para la empresa. Por ejemplo, el hecho de tener contraseñas débiles en los sistemas y que la red de datos no esté correctamente protegida puede ser aprovechado para los ataques informáticos externos.

Como conclusión, en el artículo se menciona que para tomar decisiones sobre cómo actuar ante los diferentes riesgos es necesario que la empresa realice una valoración para determinar cuáles son los más críticos para la empresa. Esta valoración suele hacerse en términos de la posibilidad de ocurrencia del riesgo y del impacto que tenga la materialización del riesgo. La valoración del impacto puede medirse en función de varios factores: la pérdida económica si es posible cuantificar la cantidad de dinero que se pierde, la reputación de la empresa dependiendo si el riesgo pueda afectar la imagen de la empresa en el mercado o de acuerdo al nivel de afectación por la pérdida o daño de la información.

En este punto se deberían tener identificados y valorados los principales riesgos que pueden afectar los activos de información de la empresa. Pero ¿es suficiente con saber qué puede pasar? La respuesta es no. Una vez identificadas las amenazas, lo más importante del análisis de riesgos es la identificación de controles ya sea para mitigar la posibilidad de ocurrencia de la amenaza o para mitigar su impacto. Las medidas de control que puede asumir una empresa van a estar relacionadas con el tipo de amenaza y el nivel de exposición que represente para la información corporativa.

Una empresa puede afrontar un riesgo de cuatro formas diferentes: aceptarlo, transferirlo, mitigarlo o evitarlo. Si un riesgo no es lo suficientemente crítico para la empresa la medida de control puede ser aceptarlo, es decir, ser consciente de que el riesgo existe y hacer un monitoreo sobre él. Si el riesgo representa una amenaza importante para la seguridad de la información se puede tomar la decisión de transferir o mitigar el riesgo.

La primera opción está relacionada con tomar algún tipo de seguro que reduzca el monto de una eventual pérdida, y la segunda tiene que ver con la implementación de medidas preventivas o correctivas para reducir la posibilidad de ocurrencia o el impacto del riesgo. Finalmente, si el nivel de riesgo es demasiado alto para que la empresa lo asuma, puede optar por evitar el riesgo, eliminando los activos de información o la actividad asociada.

La gestión de riesgos debe garantizarle a la empresa la tranquilidad de tener identificados sus riesgos y los controles que le van a permitir actuar ante una eventual materialización o simplemente evitar que se presenten. Esta gestión debe mantener el equilibrio entre el costo que tiene una actividad de control, la importancia del activo de información para los procesos de la empresa y el nivel de criticidad del riesgo.

2.12 Planes de continuidad del negocio

Como mencionan Calderón & Castro (2013), hoy en día como parte fundamental de las operaciones del negocio, la información ahora toma un papel determinante para el funcionamiento de las instituciones y es parte de la gestión del riesgo operativo el velar por que tras cualquier evento de riesgo que se suscite, siempre se pueda tener continuidad en la operatividad para lo cual, se requiere salvaguardar los equipos de tecnología que deben ser sometidos a proceso de gestión y mejora continua.

Un plan de respuesta de incidentes debe contemplar la definición de una política, segregación de responsabilidades, procedimientos y canales de comunicación, Notificación a terceras partes afectadas, Evaluación de incidentes, capacitación, entre otros.

La gestión de un plan de continuidad es vital a nivel de contingencia de los activos de seguridad de la información.

2.13 Concientización de seguridad informática

Mucho se habla sobre concientización en seguridad informática, sin embargo, existe una confusión sobre cómo estructurar la comunicación ya que, no todos los usuarios son iguales ni tienen el mismo nivel de acceso por lo que, muy aparte de la teoría que se pueda transmitir, es necesario primero estudiar las necesidades de la organización, ya que esta es una tarea imprescindible para entender el nivel de conocimiento general. Para ello el profesional puede apoyarse en encuestas, reuniones, política de seguridad de la información vigente y eventos suscitados en la empresa.

Con tales insumos identificados, para desarrollar y definir el plan de concientización, se debe incluir elementos como:

- A quién se dirige el plan. Cuando ya se han conocido los requisitos de la organización ya es conocido quien necesita mayor atención respecto a formación y concienciación.
- Ley o norma que nos obliga, en caso de haberla. La concienciación a los trabajadores en materia de Seguridad de la Información puede ser una obligación legal o un requisito de una norma voluntaria.
- Objetivos para cada uno de los apartados del programa. Deben estar muy claros estos objetivos para después poder medir si las tareas que estamos ejecutando sobre concienciación han sido efectivas o no.
- Instrucciones sobre cómo se va a concienciar. Sobre todo, qué medios se van a usar, pueden ser algunos de los descritos anteriormente u otros.
- Repetición o frecuencia. La concienciación no puede ser algo puntual, debe repetirse con cierta frecuencia y esa frecuencia ha de estar detallada previamente.

El siguiente punto es planificar un calendario y preparar el material, para lo cual es necesario desarrollar un plan comunicacional que se encuentre de acuerdo a la línea gráfica de la empresa y previo al cumplimiento del cronograma, desarrollar pruebas de concepto sobre los temas a

abordar, esto incluye inyección de código, método de *phishing* o pruebas de vulnerabilidades. (ISOTools Excellence, 2014)

2.14 Sistemas de Gestión de Seguridad de la Información

Como menciona Allende & Gui (2011). Un sistema de gestión de la seguridad de la información (SGSI) (en inglés: *information security management system*, ISMS) es, como el nombre lo sugiere, un conjunto de políticas de administración de la información. El término es utilizado principalmente por la ISO/IEC 27001, aunque no es la única normativa que utiliza este término o concepto.

Un SGSI es para una organización el diseño, implantación, mantenimiento de un conjunto de procesos para gestionar eficientemente la accesibilidad de la información, busca asegurar la confidencialidad, integridad y disponibilidad de los activos de información minimizando a la vez los riesgos de seguridad de la información.

Como todo proceso de gestión, un SGSI debe ser eficiente y adaptándose a los cambios internos de la organización, así como los externos del entorno.

ISO / IEC 27001, parte de la creciente ISO / IEC 27000 familia de normas, es un (ISMS) estándar de sistema de gestión de la seguridad de la información publicada en octubre de 2005 por la Organización Internacional de Normalización (ISO) y la Comisión Electrotécnica Internacional (IEC). Su nombre completo es la norma ISO / IEC 27001: 2013 - Técnicas de seguridad - - Tecnología de la información sistemas de gestión de seguridad de la información - Requisitos pero se conoce comúnmente como "ISO 27001".

ISO / IEC 27001 especifica formalmente un sistema de gestión que pretende aportar seguridad de la información bajo el control explícito de la dirección administrativa. Al ser una especificación formal significa que en ella se prevén requisitos puntuales. Organizaciones que dicen han adoptado, por tanto, la norma ISO / IEC 27001 puede ser auditado y certificado conforme a la norma.

La mayoría de las organizaciones tienen una serie de controles de seguridad de la información, sin un SGSI sin embargo, los controles tienden a ser un poco desorganizado y desarticulada, después de haber puesto en práctica a menudo como soluciones puntuales a situaciones específicas o simplemente como una cuestión de convención. Los modelos de madurez normalmente se refieren a esta etapa como "ad hoc". Los controles de seguridad en el funcionamiento suelen abordar ciertos aspectos de TI y seguridad de datos, en concreto, dejando activos de información (tales como trámites y conocimiento de su propiedad) bien protegidos en el conjunto. La planificación de la continuidad del negocio y la seguridad física, por ejemplo, pueden ser manejados con total independencia de TI o de seguridad de la información, mientras que las prácticas de recursos humanos pueden hacer poca referencia a la necesidad de definir y asignar roles y responsabilidades de seguridad de la información en toda la organización. Veritas (2005).

2.15 Diccionario de Controles

Según Grijalva (2018), los diccionarios de controles son básicamente una aplicación que se compagina con los datos extraídos del levantamiento de información y los levantamientos de procesos, éste es desarrollado para la metodología de seguridad y va alineado de acuerdo a los métodos en función de su situación inicial. El diccionario de controles es una guía que justifica cuáles son los puntos importantes en dónde se debe llevar a cabo la implementación y la cual

nos da los parámetros necesarios para la implementación de la metodología, como un extra, el diccionario de controles nos ayuda también a realizar (si es necesario) una cotización de cuánto se debe invertir, pero este proceso se debe llevar a cabo a través del tiempo y no hay una fecha límite para acabar la implementación.

También menciona que debe contener la actividad de la cual se empieza a derivar los procesos, el número de proceso asignado, los controles existentes y la norma a la cual se está alienando el trabajo, en este caso la ISO 27000, estos datos son también extraídos del ERM, que puede llegar a ser vital para el desarrollo del mismo. Y se justifica por qué se aplica o no se aplica un control, todo esto ajustado a la realidad de la empresa, sus lineamientos y métodos de operación que tengan.

Un diccionario de controles es único para cada empresa, ya que es un trabajo que se realiza con muchas variables extraídas de la organización y dependiendo del avance en su implementación puede ser sujeto a cambios en el tiempo y el espacio requerido.

2.16 Normativas utilizadas en la investigación:

Para el desarrollo del proyecto, se realizó un análisis de diferentes normativas que, por su fuerte incidencia a nivel nacional e internacional, se consideran los pilares sobre los cuales se construyó la metodología y estas son:

- **PCI DSS v 3.2:** PCI Council (2016), *Payment Card Industry Data Security Standart*. En el presente trabajo se habla la importancia de las Fintech como alternativa en medios de pago y servicios transaccionales, por tal motivo, se tomó en cuenta como normativa principal con la cual se desarrollaron los controles sobre la matriz de riesgos informáticos. Sus dominios y objetivos de control son:

- Desarrollo y mantenimiento de red segura
- Protección de datos de tarjetahabientes / Usuarios
- Programa de gestión de vulnerabilidades
- Métodos de control de acceso
- *Testing* regular de las redes
- Mantenimiento de un SGSI.

- **ISO 27000:** Como pilar complementario, se encuentra la normativa ISO de seguridad de la información, para poder cubrir algunos puntos adicionales como seguridad en el desarrollo, en la contratación de contingente humano, descripción de controles y medios extraíbles. Esta normativa internacional es indispensable para el desarrollo de cualquier metodología de seguridad informática y seguridad de la información. (ISO/IEC 27001, 2018)

- **Resolución No. SEPS-IGT-IR-ISF-ITIC-IGJ-2017-103:** El cumplimiento normativo de la normativa vigente en el Ecuador es indispensable para la homologación del presente proyecto y adhesión en cualquier institución financiera controlada por la SEPS, en su última versión disponible, la resolución 103 destaca por la descripción de los reportes necesarios y controles de auditoría en los sistemas para la gestión de servicios transaccionales.

- **Resoluciones de la junta bancaria No. JB -2014-3066 y No. JB-2005-834:** Conjunto con cada una de sus reformas, las resoluciones de la junta bancaria para la gestión del riesgo operativo y gestión de servicio financieros toca temas importantes sobre el riesgo informático en el Ecuador, que si bien es cierto las Cooperativas financieras no están

obligadas a reportar, son buenas prácticas que aseguran el crecimiento y transparencia de las instituciones. El cumplimiento de estas resoluciones ayuda a la institución para mejorar la calificación de riesgo, acción que permite la adhesión de nuevos servicios para el crecimiento de la institución.

- **COBIT 5:** Para el correcto desarrollo de la metodología objeto del presente proyecto, se tomó en cuenta los lineamientos del marco de trabajo de COBIT 5, que permite reestructurar la gestión del gobierno de TI y alinear los temas operativos en función a las necesidades de la empresa, además permite la visualización y definición del alcance para el desarrollo de la metodología y aplicación sobre cualquier institución perteneciente a la economía popular y solidaria.

CAPÍTULO III

ANÁLISIS SITUACIONAL

3.1. ANÁLISIS

3.1.1 Introducción a las instituciones financieras pertenecientes a la Economía popular y solidaria Ecuador:

En la actualidad la Superintendencia de la Economía Popular y Solidaria estructura 5 niveles funcionales en los que se ubican un total de 145 cooperativas de ahorro y crédito y 4 mutualistas que suman un total de 149 instituciones divididas en:

Clasificación	Instituciones pertenecientes	Porcentaje
Segmento 1	26	17.45%
Segmento 2	38	25.50%
Segmento 3	81	54.36%
Mutualistas	4	2.68%

***Tabla 2*: Entidades financieras de la SEPS.**
Elaborado por: SEPS (2018).

De las cuales únicamente 30 cuentan con un sistema de transaccionalidad electrónica, servicio que antes de ser lanzado al mercado debe ser autorizado por la SEPS y deben contar con el cumplimiento de las regulaciones vigentes en relación con la seguridad de la información perteneciente a la misma institución y a la Junta Bancaria del Ecuador. Con estos datos, se puede decir que únicamente el 20.13% de las instituciones cuentan con un sistema de seguridad que permita la integración de este tipo de servicios de manera normativa.

Algunos de los indicadores tomados en cuenta para poder segmentar a las instituciones financieras de la SEPS son: Cartera por vencer, cartera vencida, índice de morosidad, valor de

los activos adquiridos, liquidez, solvencia, vulnerabilidad del patrimonio, entre otros. Por lo que, es importante señalar que el índice financiero es vital para poder implementar soluciones de seguridad que se encuentren actualizados así también como destinar personal a cargo exclusivamente de dichos temas, motivo por el cual una buena parte de dicho 80% restante no ha aplicado medidas de seguridad y tampoco han destinado fondos para dicha gestión.

3.2 Conciencia de seguridad de la información en el Ecuador:

La firma auditora DELOITTE (2017) realizó un estudio en empresas de mediano y gran tamaño en diferentes líneas de negocios con el objetivo de realizar un análisis a las tendencias de cyber seguridad y cultura de seguridad de la información en el Ecuador. El muestreo fue realizado según la tabla que se muestra a continuación:

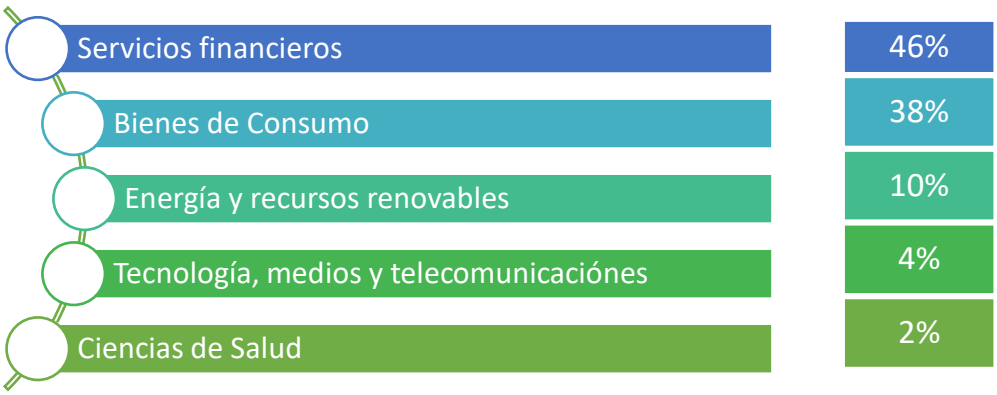


Figura 5: Análisis de riesgos – Porcentaje de estudio DELOITTE (2017).
Elaborado por: DELOITTE (2017)

De las empresas encuestadas, el 68% se ubican en la región Sierra y el 32% pertenecen a la región costa, enfocándose más en el sector financiero, 46% del total. Dentro del análisis se encontraron algunos datos interesantes:

- Casi el 50% de las empresas participantes, tuvieron un ataque informático en los que, el 20% no pudo determinar un impacto de dichas intrusiones.

- Existe una capacitación muy baja o nula en seguridad de la información por parte de las instituciones participantes y solo el 50% tienen planeado iniciar programas de capacitaciones.
- Más del 50% de las instituciones que participaron del estudio manifestaron que la mayor dificultad para poder aplicar seguridad de la información es la falta de asignación de presupuesto, entre otros temas administrativos.

En el Ecuador, cada año son más las empresas encargadas a importar servicios y productos de infraestructura de seguridad informática que, con un modelo Software as Service (SAS) o tipo Appliance In-House, mantienen un costo elevado que muchas veces no es accesible según el presupuesto de las cooperativas de segmentos más bajos. Incluso se ofrecen soluciones que trasladan toda la gestión del riesgo informático (monitoreo, respuesta a incidentes, reportes y control de enlaces) a un centro de respuesta a incidentes conocido como CSIRT (*Computer Segurity Incident Response Team)* y en Ecuador con el nombre EcuCert. Estas prácticas de seguridad buscan prescindir de un profesional dedicado a la seguridad de la información y trasladar todas las funciones tanto activas como pasivas en el tratamiento de riesgo informático a un equipo externo a la institución. Esta práctica, aunque vigente y puesta en marcha por algunas instituciones, no es recomendable ya que, ante un evento de seguridad se incrementarán los tiempos de ejecución del plan de respuesta ya que, en un servicio transaccional al menos se requieren diferentes proveedores para los enlaces de red, organismo de compensación, ISP, Desarrollador de la aplicación. Lo que ocasionará que cada uno responda ante la incidencia en el tiempo que cada uno defina según su SLA descrito en el contrato de adquisición de servicios.

Con el objetivo de proporcionar controles de seguridad de la información a las instituciones reguladas por la superintendencia de la economía popular y solidaria que satisfagan las

necesidades de una institución de intermediación financiera que ofrece servicios transaccionales, se realiza la presente investigación que además de dar los lineamientos para el crecimiento y fortalecimiento institucional, permite manejar adecuadamente los incidentes internos y gestionar los eventos de riesgo con proveedores de manera rápida y ágil.

3.3 Caso de estudio COOPCCP

Tras la integración de una política de seguridad de la información estructurada, la Cooperativa de Ahorro y Crédito Construcción Comercio y Producción COOPCCP, mejoró integralmente la institución facilitando el manejo de la información de la manera más adecuada y la automatización de sus procesos, ayudó también a reconocer los fallos instaurados por los servicios transaccionales vigentes. Según la definición de la SEPS, los servicios transaccionales definidos en la resolución son:

1. Tarjeta de Débito
2. Canales de comunicación con instituciones compensadoras
3. Cajero automático ATM
4. Consulta de saldo en Línea de contacto 1800
5. SMS programados
6. Cooperativa en línea
7. *Web Services*
8. Transferencias SMS
9. Transferencias Whatsapp
10. Chatbots

De los cuales, al momento de su integración, la normativa vigente no contemplaba el riesgo informático que conlleva tener activos dichos servicios por lo que, en cada uno de ellos, el área de Seguridad de la Información logró identificar vulnerabilidades y vectores de ataques que de ser explotados pueden tener una incidencia representativa para la institución.

Con la gran acogida del tratamiento de riesgo informático, el ente de control SEPS, emitió la resolución No. SEPS-IGT-IR-ISF-ITIC-IGJ-2017-103, que habla sobre el mínimo de nivel de cumplimiento que deben contar todo canal transaccional, definiéndolo como cualquier servicio, aplicación o interacción que pueda llegar a tener un socio directamente o por medio de terceros, con la información existente en la base de datos que sea relacionada a su operatividad. Por lo que, incluso una consulta de saldo a través de un SMS o llamada telefónica a partir del 23 de noviembre de 2017 debe contar con controles. Al ser retroactiva, la COOPCCP y todas las Cooperativas de ahorro y crédito (COAC) deben ajustarse a esta disposición, por lo que se genera la duda e incertidumbre sobre ¿Cuál es el punto en donde me encuentro?; ¿Cómo debo capacitar al personal de mi institución?; ¿Qué inversión debo priorizar para no incurrir en sanciones económicas con el organismo de control?

Sobre dicho tema, muchas empresas de asesoría, ofrecen acompañamientos para certificar el cumplimiento de lo expuesto sin embargo, no llegan más lejos de emitir un criterio y sugerencias sobre el tratamiento de los eventos de riesgo por lo que, se genera una sensación falsa de seguridad ya que, a pesar de existir un documento reglamentario sobre seguridad de la información, no tiene la capacidad de actualizarse ante los eventos de riesgo que hoy en día se desarrollan a través de *Machine Learning* e inteligencia artificial aplicada en ataques

persistentes y por lo tanto, no asegura que la institución esté preparada para soportar todo tipo de ataques por intrusiones.

Para ello se definió que, mediante el uso de la normativa PCI DSS (Estándar de seguridad de datos para la industria de tarjetas de pago) apegado a las buenas prácticas de seguridad ISO 27000 y los reglamentos internos como el SGSI, se puede desarrollar un esquema que no solo permita generar tranquilidad a nivel de cumplimiento de la resolución sino también contra ataques. Y para ello, se realizó el acompañamiento metodológico estructurado en la COOPCCP para así poder determinar el estado de madurez en el que se encuentra, los roles de cada uno de sus colaboradores, estado de servidores, correlación de eventos de riesgo informático, maneras prácticas de encontrar información relacionada a la seguridad de la información que puedan poner en práctica en el día a día según las tendencias en ataques vigentes, entre otros temas de interés.

3.4 Levantamiento de Información – Declaración de trabajo.

Existen varios temas tomados en consideración para determinar el camino a seguir en la implementación y gestión de un sistema de seguridad, resultado del desarrollo de la metodología, se presenta un documento de declaración de trabajo (SOW) que, entre otros puntos, detalla el alcance esperado del trabajo:

3.4.1 Resumen general

- **Desarrollo:** Diseño de una metodología para la implementación y gestión de un sistema de seguridad para servicios transaccionales en instituciones financieras de la economía popular y solidaria basada en las buenas prácticas de la PCI DSS.
- **Tipo de Proyecto:** Teórico – Práctico.
- **Tamaño del diseño:** Grande.

- **Ubicación del diseño:** Quito – Ecuador. - Extensión a nivel nacional
- **Fecha de inicio del diseño:** 10 de octubre de 2018.
- **Fecha de Finalización del diseño:** 31 de marzo de 2019.
- **Tiempo estimado – Duración (meses):** 5 meses
- **Sector de la industria de la metodología:** Financiero.
- **Tipos de Servicio de la metodología:** Transaccionalidad en línea.
- **Portafolio /área:** Tecnología – Seguridad de la información – Negocios
- **Cliente:** Cooperativa Financiera CCP
- **Ubicación del Cliente:** Av 10 de agosto y Atahualpa.
- **Líder del proyecto:** Jean Pierre Rodríguez.
- **Fecha de Elaboración:** 01 de octubre de 2018.
- **Declaración de trabajo elaborada por:** Jean Pierre Rodríguez.

3.4.2 Resumen ejecutivo

Enunciado de la visión

"En el Ecuador, la oferta de servicios electrónicos está en boga debido a la gran facilidad de acceso existente en el mundo digital, mismo que ha provocado grandes cambios sobre las infraestructuras de una gran variedad de negocios y el sector financiero no es la excepción, sin embargo, existe un riesgo inherente mucho más alto en esta línea de negocios ya que el producto y servicio que se comercializa es intangible y vulnerable ante eventos de seguridad. Para poner en línea un sistema transaccional para los socios y clientes de la COOPCCP existen ciertas configuraciones avanzadas que se deben realizar con respecto a sus equipos de seguridad y servicios adquiridos.

El presente proyecto pretende dar los lineamientos específicos sobre cómo realizar una integración sobre los servicios adoptados por las instituciones financieras de la economía popular y solidaria para salvaguardar sus datos según la normativa vigente, misma que entre otros, menciona la importancia de proteger la información de sus clientes y colaboradores por un periodo de tiempo elevado sean estas transaccionales o de movimientos laterales sobre la infraestructura de la institución.

Para lograrlo se presenta la estructura de una metodología que permita integrar diferentes tipos de soluciones dotando de herramientas y conocimiento oportuno a los colaboradores de la institución responsables de la seguridad de la información para que puedan aplicar un buen criterio profesional con respecto al tipo de aplicativos que la institución posee, así mismo del giro que está dando en base a la segmentación en la que se encuentra y de este modo, poder configurar adecuadamente los sistemas adquiridos, correlacionar información de manera adecuada y poder administrar un sistema de recuperación de desastres con respecto al volumen de transaccionalidad que maneje la institución."

3.4.3 Objetivos

OBJETIVO PRINCIPAL	
Diseñar un sistema de seguridad para servicios transaccionales de la COOPCCP basada en las buenas prácticas de la normativa PCI DSS.	
Objetivos detallados	
1	Identificar el estado de madurez de la institución mediante un levantamiento de información de eventos relacionados a seguridad de la información a nivel técnico, operativo y administrativo.
2	Formular un diccionario de controles que mitiguen el riesgo al que la institución está expuesta
3	Definir los lineamientos mínimos a conseguir para el estado de madurez de la institución que asegure el cumplimiento normativo de los organismos de control para servicios transaccionales.

Tabla 3: Objetivos – SOW
Elaborado por: Jean P. Rodríguez

3.4.4 Alcance de necesidades

Necesidades Funcionales	
PROCESOS/SERVICIOS	
Código	**Necesidad**
N1	Proceso de plan de respuesta operativo
N2	Procesos de comunicación y respuesta de incidentes
N3	Proceso de atención y servicio automatizado al público.
Necesidades de Infraestructura	
PROCESOS/SERVICIOS	
Código	**Necesidad**
NECESIDADES GENERALES	
N4	Herramienta de control de tráfico de red en la web (WAF)
N5	Certificados de seguridad en modalidad wildcard
NECESIDADES DESARROLLO	
N6	Ambientes de desarrollo
N8	Adaptación de los SP del Core a los nuevos servicios electrónicos
NECESIDADES BASE DE DATOS BDD	
N10	Segmentación de bases de datos
N11	Métodos de acceso a base de datos

Tabla 4: Alcance de necesidades – SOW
Elaborado por: Jean P. Rodríguez

3.4.5 Entregables y criterios

N. de serie	Fase	Detalle
	Creación	✓ Documento de Requerimientos para levantamiento de la información ✓ Statement of Work (SOW) firmado. - Sentencia de trabajo en el cual se detalla el alcance Del proyecto.
	Inicio del análisis (PSU)	✓ Acta de reunión de Kick Off. Documento que contiene los acuerdos alcanzados al inicio del proyecto.

N. de serie	Fase	Detalle
		✓ Gantt resultado del primer kick off. (Nota: Primera línea base será grabada por el cliente).
	Análisis, Construcción	✓ Especificaciones Funcionales. ✓ Manual de la aplicación de la metodología.
	Pruebas	✓ Evidencia de análisis y calificación de riesgo.
	Cierre de Proyecto	✓ Resultados Inspección Final ✓ Acta de Finiquito. Reporte de Errores ✓ Formato Encuesta de Satisfacción

Tabla 5: Entregables y criterios - SOW
Elaborado por: Jean P. Rodríguez

3.4.6 Cronograma de creación de la metodología

#	Detalle	Duración	Fecha de inicio	Fecha Fin	Predecesora
1	Presentación del Statemen of Work	2d	06/08/2018	07/08/2018	
2	Firma de acuerdos de confidencialidad	1d	08/08/2018	08/08/2018	1
3	Firma de carta de auspicio Tesis UISEK	1d	08/08/2018	08/08/2018	1
4	Levantamiento y análisis de información	82d	09/08/2018	30/11/2018	3
5	Organigrama	1d	09/08/2018	09/08/2018	3
6	Matriz de riesgos y procesos	10d	10/08/2018	23/08/2018	5
7	Matriz de riesgos informáticos cotejada PCI	20d	24/08/2018	20/09/2018	6
8	Política de seguridad de la Información	3d	21/09/2018	25/09/2018	7
9	Acceso de usuarios a aplicaciones	2d	26/09/2018	27/09/2018	8
10	Sistemas para uso transaccional	1d	28/09/2018	28/09/2018	9
11	Reportes de eventos encontrados	4d	01/10/2018	04/10/2018	10
12	Gestión de auditoría interna y externa	15d	05/10/2018	25/10/2018	11
13	Pruebas de penetración de vulnerabilidades	51d	21/09/2018	30/11/2018	7
14	Clasificación de activos de la información	5d	26/10/2018	01/11/2018	12
15	Inventario de activos de la información	10d	02/11/2018	15/11/2018	14
16	Servidores físicos	3d	16/11/2018	20/11/2018	15
17	Servidores virtuales	3d	21/11/2018	23/11/2018	16
18	Bases de Datos	3d	26/11/2018	28/11/2018	17
19	Proveedores de servicio	1d	29/11/2018	29/11/2018	18
20	Análisis de requisitos PCI DSS a ser utilizados	3d	30/11/2018	04/12/2018	19
21	Desarrollo de la metodología	45d	05/12/2018	05/02/2019	20
22	Descripción de la metodología	5d	05/12/2018	11/12/2018	20
23	Definición de valores de estado de madurez	2d	12/12/2018	13/12/2018	22
24	Esquema general de madurez	2d	14/12/2018	17/12/2018	23
25	Cotejo de controles - Diccionario de controles PCI DSS	3d	18/12/2018	20/12/2018	24
26	Análisis de estado de madurez de la empresa	2d	21/12/2018	24/12/2018	25
27	Definición de roles de usuarios	3d	25/12/2018	27/12/2018	26
28	Definición y documentación requerida para el proyecto	2d	28/12/2018	31/12/2018	27

#	Detalle	Duración	Fecha de inicio	Fecha Fin	Predecesora
29	Requisitos recomendados para el proyecto	2d	01/01/2019	02/01/2019	28
30	Cambios normativos internos	3d	03/01/2019	07/01/2019	29
31	Cumplimiento y seguimiento	2d	08/01/2019	09/01/2019	30
32	Mejoras de equipos	2d	10/01/2019	11/01/2019	31
33	Definición de alcance de los Pentest	2d	14/01/2019	15/01/2019	32
34	Plan de capacitación de seguridad	5d	16/01/2019	22/01/2019	33
35	Pasos a seguir en la implementación.	10d	23/01/2019	05/02/2019	34
36	Formulación del documento	5d	06/02/2019	12/02/2019	35

Tabla 6: Cronograma de creación de la metodología.
Elaborado por: Jean P. Rodríguez.

3.4.7 Roles y responsabilidades

Roles	Responsabilidades
Project Manager	• Seguimiento de los Líderes de desarrollo de la metodología (costo/tiempo/asignaciones) • Coordinación de cumplimiento y Control de Calidad de los proyectos • Difundir temas corporativos referentes a cambios de la institución o de los proyectos
Líder de desarrollo de la metodología	• Soporte en la definición de alcance del proyecto • Soporte en levantamiento de especificaciones funcionales del proyecto • Planificación y ejecución del proyecto • Control y Monitoreo del proyecto en las diferentes fases • Levantamiento y ejecución de controles de cambios que se generen • Revisión de documentación del proyecto
Arquitecto	• Validación de la arquitectura de la aplicación • Soporte en aplicación de pruebas técnicas • Certificación de la aplicación para su paso a diseño de la metodología.

Tabla 7: Roles y responsabilidades – SOW
Elaborado por: Jean P. Rodríguez

El documento completo consta de los siguientes puntos:

- Objetivos
- Beneficios previstos
- Alcance de la solución
- Modelo de la solución propuesta
- Ciclo de vida de la metodología
- Entregables y criterios

- Componentes de terceros y acuerdos
- Plataforma, hardware, software y productos.
- Reuniones y reportes
- Cronograma de la metodología
- Recursos
- Modelo de respaldo
- Roles y responsabilidades
- Patrocinadores de la metodología
- Control de cambios
- Glosario de términos
- Aprobaciones

A continuación, se muestran las etapas en las que se basa el desarrollo de la estructura de la metodología presentada.

3.4.8 Acuerdo de Confidencialidad

Antes de obtener información sensible sobre el manejo interno de la institución, se desarrolló un acuerdo de confidencialidad firmado por el Ing. Daniel Zurita, Jefe de Tecnologías de la COOPCCP y el Ing. Jean Rodríguez. Estructurado de la siguiente manera: antecedentes, objeto, exposición y cláusulas. En cumplimiento del documento aceptado y firmado, la COOPCCP se reserva el derecho de presentar documentos e información que se encuentre vigente para la operatividad del año 2019 así como también de la información proporcionada por consultorías externas que se encuentren activos en el periodo que se desarrolla el presente proyecto.

3.4.9 Análisis de información preliminar

Para el desarrollo de la metodología fue muy importante tabular la información a través de una matriz de riesgos desarrollada en base a la información extraída de todos los datos relacionados a la seguridad de la información y realizar un cruce con los controles definidos por la normativa PCI DSS enfatizando en la red e infraestructura tecnológica con el que la institución cuenta y los servicios transaccionales activos y definidos para el desarrollo del plan operativo anual (POA).

3.4.9.1 Organigrama

La estructura organizacional de la COOPCCP ha sufrido cambios a través del tiempo, el último aprobado el 30 de enero de 2019 se enfoca en realizar una gestión por procesos tipificados en gestión gobernante, gestión productiva y gestión de apoyo. Esta estructura permite a los colaboradores de la institución tener una participación dentro de los diferentes comités tanto de gestión productiva como de gobernanza. La metodología se centró en todas las áreas de la COOPCCP poniendo especial atención en los procesos del área de Operaciones, Tecnología, Riesgos y Negocios.

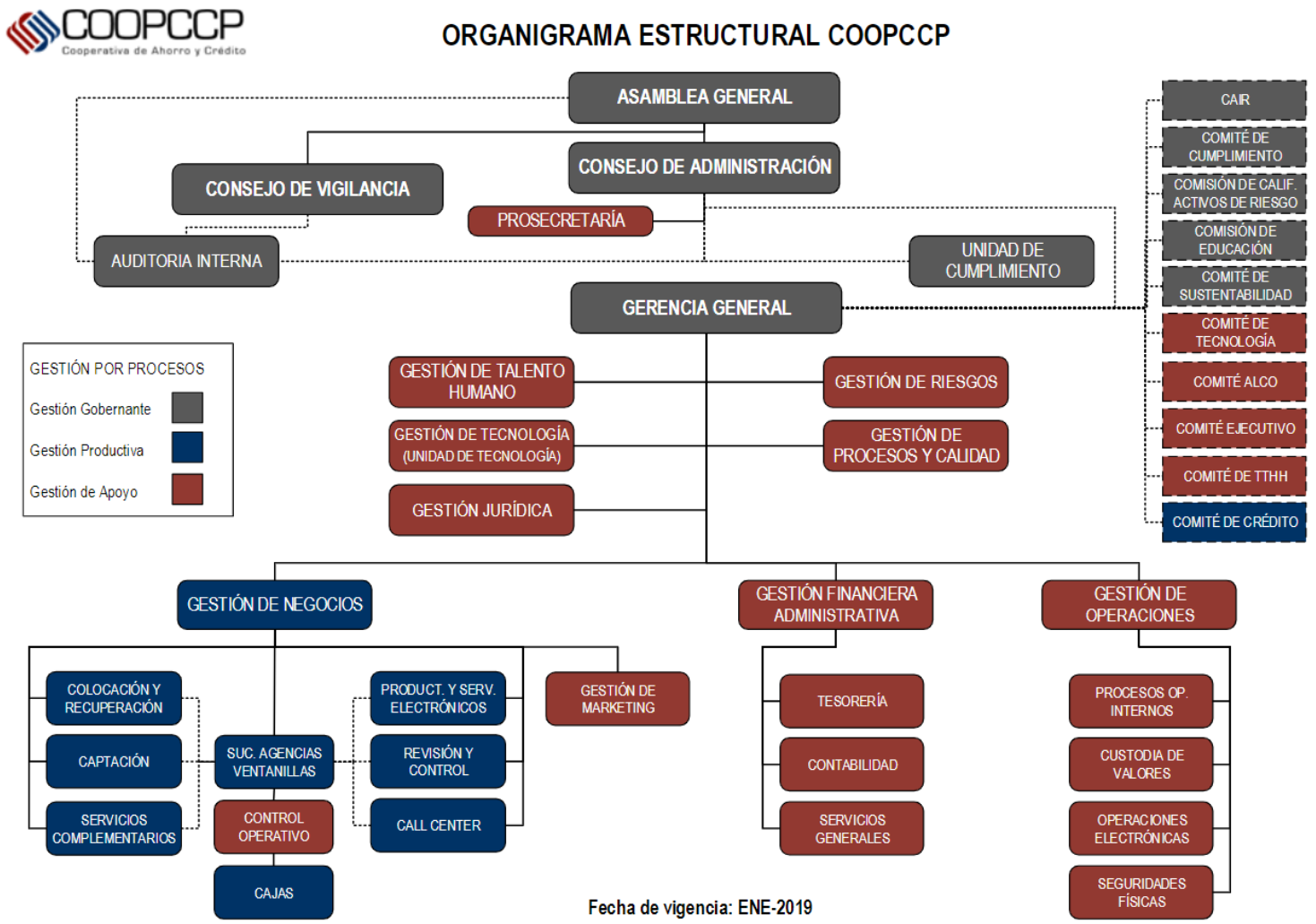


Figura 6: Organigrama Estructural Posicional COOPCCP – enero 2019
Elaborado por: COAC COOPCCP

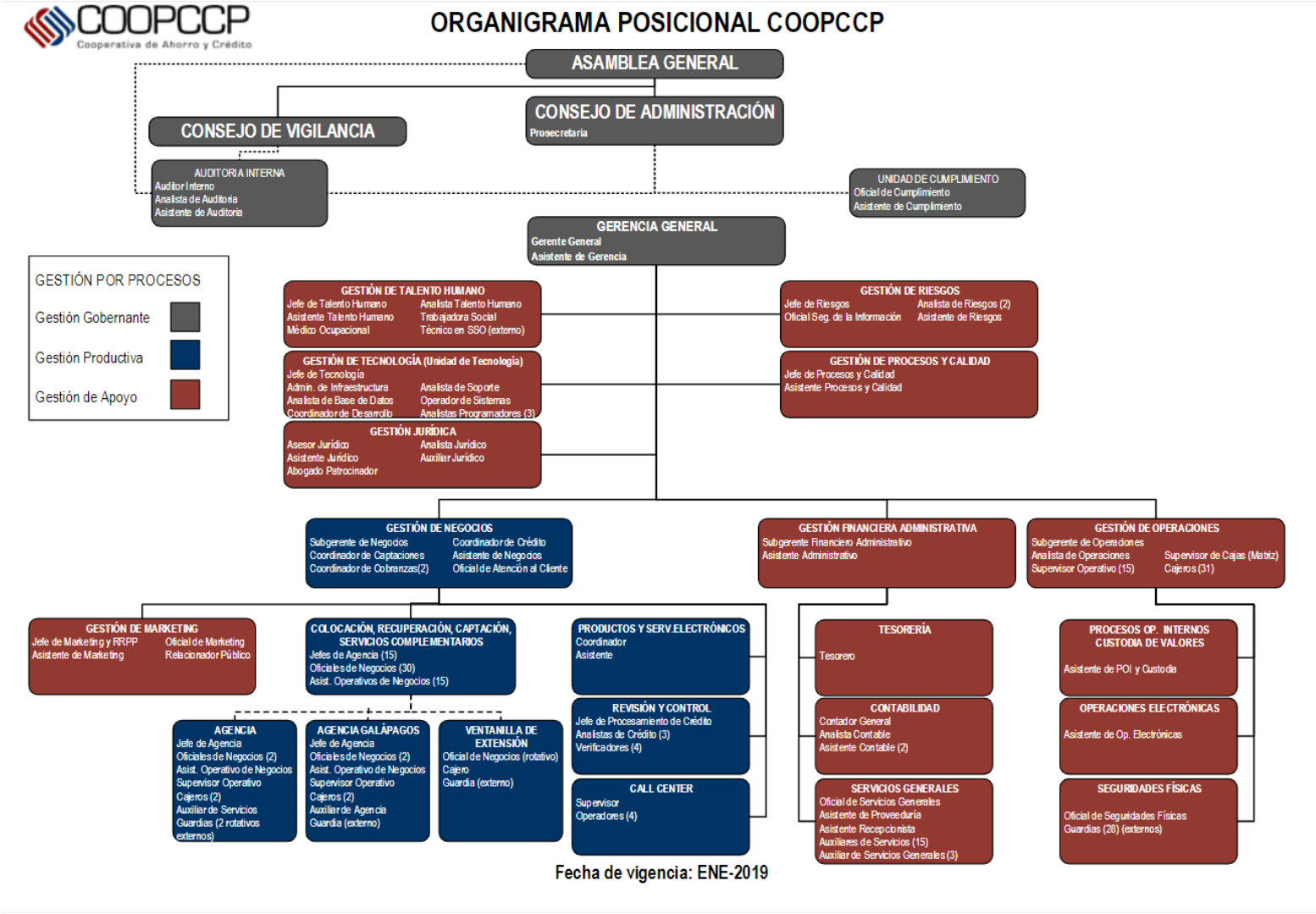


Figura 7: Organigrama Posicional COOPCCP – enero 2019
Elaborado por: COAC COOPCCP

3.4.9.2 Análisis de riesgos y procesos

Para realizar el análisis de riesgos se tomaron en cuenta cada uno de los eventos y actividades realizadas dentro de la COOPCCP relacionadas con procesos de tecnología, operaciones, riesgos y negocios; e intervienen en el proceso de gestión de los servicios transaccionales vigentes y futuros. Por tal motivo se desarrolló un formato de análisis de riesgos que contiene los siguientes campos:

Área del proceso, líder del proceso responsable, descripción del riesgo tipificado, riesgo evaluado de acuerdo con el diccionario de controles, control relacionado con la normativa PCI DSS y buenas prácticas de la ISO 27002.

Matriz de análisis de riesgos informáticos para el desarrollo y aplicación de servicios transaccionales en la COOPCCP														
Tema: Eventos de Riesgo **Elaborado por:** Jean P. Rodríguez. **Fecha:** 10/10/2018 Área: Negocios					**Descripción:** La matriz presentada está realizada en base a los eventos de riesgo encontrados en la Cooperativa en las áreas de: - Aspectos Generales -Tecnología de la Información. - Riesgos - Seguridad de la Información									**Documento N° 2018-COOPCCP-023-SE**
COD	**Proceso**	**Lider de proceso**	**Tipificación del riesgo**	**Riesgo Evaluado**	**Observación**	**Control relacionado (PCI DSS / ISO27002)**	**Criticidad**	**Vulnerabilidad**	**Impacto**	**Voto/Cargos**	**Calificación Funcionario 1**	**Calificación Funcionario 2**	**Calificación Funcionario 3**	**Notas**
G01							Bajo	1,0	1,0	Voto Impacto	1,0	1,0	1,0	
										Voto Vulnerabilidad	1,0	1,0	1,0	
G02							Bajo	1,0	1,0	Voto Impacto	1,0	1,0	1,0	
										Voto Vulnerabilidad	1,0	1,0	1,0	
G03							Bajo	1,0	1,0	Voto Impacto	1,0	1,0	1,0	
										Voto Vulnerabilidad	1,0	1,0	1,0	
G04							Bajo	1,0	1,0	Voto Impacto	1,0	1,0	1,0	
										Voto Vulnerabilidad	1,0	1,0	1,0	
G05							Bajo	1,0	1,0	Voto Impacto	1,0	1,0	1,0	
										Voto Vulnerabilidad	1,0	1,0	1,0	
G06							Bajo	1,0	1,0	Voto Impacto	1,0	1,0	1,0	
										Voto Vulnerabilidad	1,0	1,0	1,0	
G07							Bajo	1,0	1,0	Voto Impacto	1,0	1,0	1,0	
										Voto Vulnerabilidad	1,0	1,0	1,0	

Figura 8: Formato de análisis de riesgo COOPCCP
Elaborado por: Jean P. Rodríguez.

En estos campos se buscó calcular el riesgo en función al impacto por su vulnerabilidad, esta fórmula definirá la criticidad del evento de riesgo y dará prioridad sobre los cambios a ser realizados. Para este fin fue necesario contar con la opinión de al menos tres personas del área o dueños de procesos para, posteriormente concatenar la matriz de riesgos encontrados en la institución que afecten a los servicios transaccionales así también como los puntos normativos que existen en base a la aplicación de resolución No. SEPS-IGT-IR-ISF-ITIC-IGJ-2017-103. Posteriormente se presentó un mapa de calor con el que se evidencia el punto inicial de criticidad en el que se encuentra la Cooperativa previo a los cambios tras la metodología.

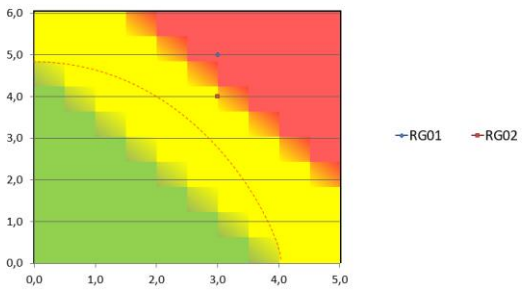


Figura 9: Mapa de Calor – Matriz de riesgos COOPCCP.
Elaborado por: Jean P. Rodríguez.

A continuación, se muestra un extracto de las áreas más relevantes sobre las cuales se realizó el análisis de riesgos y que fueron cotejadas con la normativa ISO 27002 que dan un punto de partida para el desarrollo de la presente metodología.

En el desarrollo de actividades se realizó el análisis de riesgos informáticos existentes levantados con el área de Riesgos – Seguridad de la información y el área de tecnología, también se realizó una comparativa con la matriz levantada en el año 2016 en la que se evidenciaron varias vulnerabilidades principalmente ocasionadas por los sistemas informáticos. En respuesta al informe presentado en 2016, la COOPCCP inició el proyecto de cambio de su Core Financiero con el cual, se implementaron la mayoría de los controles propuestos. Sin embargo, de los eventos de riesgo resultantes, se inició el proceso de cambio conjunto con los líderes de

proceso. De lo resultante se extrajeron la matriz de riesgos informáticos que se encuentra vigente en la institución y se presentan de acuerdo con su criticidad por interacción con los sistemas transaccionales en línea.

	Proceso	Líder de proceso	Tipificación del riesgo	Riesgo Evaluado	Observación	Control relacionado (ISO27002)	Criticidad	Vulnerabilidad	Impacto	Voto/Cargos	Calificación Funcionario 1	Calificación Funcionario 2	Calificación Funcionario 3
RG01	General	General	RG01	No existencia / desconocimiento del documento de la política de seguridad de la información	Existe conocimiento / aplicación de alguna norma de la política de seguridad vigente	5.1.1 Documento de SGSI / 5.1.2. Revisión	Bajo	1,0	2,0	Voto Impacto	2,0	2,0	2,0
										Voto Vulnerabilidad	1,0	1,0	1,0
RG02	General	General	RG02	Falta de conocimiento de coordinación de la seguridad de la información	Conoce algún tipo de organización o responsables de la empresa sobre el tema	6.1.2. Coordinación de la seguridad de la información	Bajo	1,0	2,0	Voto Impacto	2,0	2,0	2,0
										Voto Vulnerabilidad	1,0	1,0	1,0
RG03	General	General	RG03	Personas no designadas a resguardar la Seguridad de la información	Conoce alguna persona encargada de regular esto dentro de la empresa	6.1.3. Asignación de responsabilidades relativas a la seguridad de la información	Bajo	1,0	3,0	Voto Impacto	3,0	3,0	3,0
										Voto Vulnerabilidad	1,0	1,0	1,0
RG04	General	General	RG04	Falta de personal para la asignación de recursos	Existe alguien a quién se le deba buscar por motivos de seguridad de la información	6.1.4. Proceso de autorización de recursos para el tratamiento de seguridad de la información	Medio	1,0	4,0	Voto Impacto	4,0	4,0	4,0
										Voto Vulnerabilidad	1,0	1,0	1,0
RG05	General	General	RG05	Carencia de acuerdos de confidencialidad para la información sensible	Maneja Ud. Acuerdos de confidencialidad con las personas que trabaja	6.1.5. Acuerdos de confidencialidad	Medio	2,0	5,0	Voto Impacto	5,0	5,0	5,0
										Voto Vulnerabilidad	2,0	2,0	2,0
RG06	General	General	RG06	Falta de conocimiento del funcionamiento del SGSI	Revisa independiente de las capacitaciones los manuales o políticas de seguridad de la información	6.1.8. Revisión independiente de la seguridad de la información.	Alto	4,0	5,0	Voto Impacto	5,0	5,0	5,0
										Voto Vulnerabilidad	4,0	4,0	4,0
RG07	General	General	RG07	No clasificar la información de acuerdo a políticas de la empresa	Maneja algún método para clasificar la sensibilidad de su información. Sea personal u organizacional	7.2.1. Directrices de clasificación de la información	Alto	5,0	5,0	Voto Impacto	5,0	5,0	5,0
										Voto Vulnerabilidad	5,0	5,0	5,0
RG08	General	General	RG08	Mal manejo de la información	Existe un debido etiquetado de la información y manipulación del mismo	7.2.2. Etiquetado y manipulado de la información	Medio	3,5	4,0	Voto Impacto	4,0	4,0	4,0
										Voto Vulnerabilidad	3,5	3,5	3,5
RG09	General	General	RG09	Falta de controles de acceso físicos	Facilidad para ingresar a diferentes áreas físicas de la organización	9.1.2. Control físico de entradas	Medio	3,5	4,0	Voto Impacto	4,0	4,0	4,0
										Voto Vulnerabilidad	3,5	3,5	3,5
RG10	General	General	RG10	Seguridad en el ambiente de trabajo	Seguridad física, de la información dentro de la empresa	9.1.3. Seguridad de oficinas, despachos e instalaciones	Alto	3,0	5,0	Voto Impacto	5,0	5,0	5,0
										Voto Vulnerabilidad	3,0	3,0	3,0
RG11	General	General	RG11	No existencia de un procesos para realizar copias de seguridad	Realiza respaldos de su información etiquetada y clasificada debidamente con algún protocolo, explique frecuencia	10.5.1 Copias de seguridad de la información	Alto	4,0	5,0	Voto Impacto	5,0	5,0	5,0
										Voto Vulnerabilidad	4,0	4,0	4,0

	Proceso	Líder de proceso	Tipificación del riesgo	Riesgo Evaluado	Observación	Control relacionado (ISO27002)	Criticidad	Vulnerabilidad	Impacto	Voto/Cargos	Calificación Funcionario 1	Calificación Funcionario 2	Calificación Funcionario 3
RG12	General	General	RG12	Falta de controles para el uso de medios extraíbles	Conoce de alguna política de medios extraíbles vigente	10.7.1. Gestión de soportes extraíbles	Medio	1,0	4,0	Voto Impacto	4,0	4,0	4,0
										Voto Vulnerabilidad	1,0	1,0	1,0
RG13	General	General	RG13	Falta de ayuda técnica para generar una contraseña adecuada	Cuál es la manera que usa para asignar sus contraseñas en equipos personales y plataformas web	11.3.1. Uso de contraseñas	Bajo	1,0	3,0	Voto Impacto	3,0	3,0	3,0
										Voto Vulnerabilidad	1,0	1,0	1,0
RG14	General	General	RG14	Ambiente de trabajo no debidamente manejado	Conoce cuales son los riesgos de tener un puesto de trabajo limpio, qué políticas lleva al respecto	11.3.3. Política de puesto de trabajo despejado y pantalla limpia.	Bajo	1,0	3,0	Voto Impacto	3,0	3,0	3,0
										Voto Vulnerabilidad	1,0	1,0	1,0
RG15	General	General	RG15	Falta de seguridad dentro de los pc´s de la empresa	Tiene controles seguros para el acceso a los sistemas operativos de su pc, qué otros accesos utiliza	11.5.1. Procedimientos seguros de inicio de sesión (SO)	Medio	2,0	5,0	Voto Impacto	5,0	5,0	5,0
										Voto Vulnerabilidad	2,0	2,0	2,0
RG16	General	General	RG16	Libertad de manejo, compartición de la información	Tienes alguna restricción a páginas web, red interna de la empresa, web mail	11.6.1. Restricción del acceso a la información	Medio	1,0	5,0	Voto Impacto	5,0	5,0	5,0
										Voto Vulnerabilidad	1,0	1,0	1,0
RG17	General	General	RG17	Falta de normalización en el teletrabajo	Cuáles son las políticas del teletrabajo conocidas y mantenidas por el usuario	11.7.2. Teletrabajo	Alto	5,0	5,0	Voto Impacto	5,0	5,0	5,0
										Voto Vulnerabilidad	5,0	5,0	5,0
RG18	General	General	RG18	No uso de controles criptográficos	Maneja algún tipo de control criptográfico para la información sensible	12.3.1. Política de uso de los controles criptográficos	Alto	5,0	4,0	Voto Impacto	4,0	4,0	4,0
										Voto Vulnerabilidad	5,0	5,0	5,0
RG19	General	General	RG19	Falta de conocimiento en caso de eventos emergentes	A quién y de qué manera notifica los eventos de seguridad que no sean ajustados a sus niveles de acceso	11.3.1. Notificación de los eventos de la seguridad de la información	Bajo	1,0	3,0	Voto Impacto	3,0	3,0	3,0
										Voto Vulnerabilidad	1,0	1,0	1,0
RG20	General	General	RG20	Falta de regulación en el cumplimiento del SGSI	Dentro del departamento, existe el encargado de hacer cumplir las normas y políticas de seguridad	15.2.1. Cumplimiento de las normas y políticas de seguridad	Alto	4,0	4,0	Voto Impacto	4,0	4,0	4,0
										Voto Vulnerabilidad	4,0	4,0	4,0
R01	Tecnología de la información	Daniel Zurita	R01	Soporte a usuarios: El cableado estructural no se encuentra debidamente implementado lo que genera fallo de comunicaciones	¿Se cuenta con una infraestructura certificada que asegure la disponibilidad de las comunicaciones? Qué tan eficiente es el control?	9.2.3 Seguridad del cableado	Alto	4,3	5,0	Voto Impacto	5,0	5,0	5,0
										Voto Vulnerabilidad	4,3	4,3	4,3
R02	Tecnología de la información	Daniel Zurita	R02	Daños a equipo de la empresa por falta de mantenimiento preventivo y posible pérdida de la información	¿Se realizan mantenimiento preventivo a los equipos de las áreas para garantizar su continua disponibilidad e integridad?	9.2.4. Mantenimiento de equipos	Alto	5,0	4,0	Voto Impacto	4,0	4,0	4,0
										Voto Vulnerabilidad	5,0	5,0	5,0
R03			R03				Alto	5,0	5,0	Voto Impacto	5,0	5,0	5,0

	Proceso	Líder de proceso	Tipificación del riesgo	Riesgo Evaluado	Observación	Control relacionado (ISO27002)	Criticidad	Vulnerabilidad	Impacto	Voto/Cargos	Calificación Funcionario 1	Calificación Funcionario 2	Calificación Funcionario 3
	Tecnología de la información	Daniel Zurita		Desorganización en el manejo de solicitudes de soporte a usuarios lo que no asegura la continuidad del servicio	Existe un responsable de los eventos de comunicaciones y operaciones quien segregue las tareas a realizar dentro del soporte a usuario?	10.1.3 Segregación de tareas				Voto Vulnerabilidad	5,0	5,0	5,0
R04	Tecnología de la información	Daniel Zurita	R04	El no registro, análisis y toma de decisiones apropiadas de las averías.	Se cuenta con algún sistema de monitoreo y análisis de datos masivos procedente de redes, aplicaciones, equipos, etc. Que permita detectar y solucionar problemas e incidentes de seguridad con rapidez?	10.10.5 Registro de fallos	Alto	5,0	4,0	Voto Impacto	4,0	4,0	4,0
										Voto Vulnerabilidad	5,0	5,0	5,0
R05	Tecnología de la información	Daniel Zurita	R05	Cierre del día: BDD : Posible pérdida de datos de la DB	Existe algún protocolo para realizar copias de seguridad a la BDD que asegure la continuidad del negocio?	10.5.1. Copias de la seguridad de la información	Medio	3,0	4,0	Voto Impacto	4,0	4,0	4,0
										Voto Vulnerabilidad	3,0	3,0	3,0
R06	Tecnología de la información	Daniel Zurita	R06	Fuga de información y uso inadecuado de los respaldos	Existe una política de manipulación de dichos soportes declarando un responsable de los mismos ?	10.7 Manipulación de soportes	Medio	1,0	5,0	Voto Impacto	5,0	5,0	5,0
										Voto Vulnerabilidad	1,0	1,0	1,0
R07	Tecnología de la información	Daniel Zurita	R07	Fuga de información y pérdida de datos por malware	Existen controles contra el código malicioso que aplique tanto al proceso de respaldos como a los medios extraíbles?	10.4.1. Controles contra el código malicioso	Medio	1,0	5,0	Voto Impacto	5,0	5,0	5,0
										Voto Vulnerabilidad	1,0	1,0	1,0
R08	Tecnología de la información	Daniel Zurita	R08	Vulnerabilidades dentro de la BDD o en los computadores adyacentes que guarden comunicación directa	Existe algún control contra el código malicioso especial en el manejo de la BDD? Qué tan eficiente es?	10.4.2.Controles contra el código descargado en el cliente	Alto	5,0	5,0	Voto Impacto	5,0	5,0	5,0
										Voto Vulnerabilidad	5,0	5,0	5,0
R09	Tecnología de la información	Daniel Zurita	R09	Planificación y manejo de proyectos: Fuga de la información, explotación de vulnerabilidades	Existen controles apropiados para antes de conceder el ingreso de terceros dentro de la gestión y manejo de proyectos	6.2.1 Identificación de los riesgos derivados con el acceso de terceros	Medio	1,0	5,0	Voto Impacto	5,0	5,0	5,0
										Voto Vulnerabilidad	1,0	1,0	1,0
R10	Tecnología de la información	Daniel Zurita	R10	Posible fuga de información, Mal uso de la información obtenida	Existen protocolos que generen acuerdos de confidencialidad generales y su modificación sea avalada por la empresa para el manejo de la información en la gestión de proyectos que involucre personal interno y terceros?	6.1.5. Acuerdos de confidencialidad	Bajo	1,0	3,0	Voto Impacto	3,0	3,0	3,0
										Voto Vulnerabilidad	1,0	1,0	1,0
R11	Tecnología de la información	Daniel Zurita	R11	Información gestionada indebidamente	Existen aristas que sean necesarias cumplir para la correcta clasificación de la información dentro del manejo y planificación de proyectos?	7.2. Clasificación de la información	Medio	3,0	4,0	Voto Impacto	4,0	4,0	4,0
										Voto Vulnerabilidad	3,0	3,0	3,0

	Proceso	Líder de proceso	Tipificación del riesgo	Riesgo Evaluado	Observación	Control relacionado (ISO27002)	Criticidad	Vulnerabilidad	Impacto	Voto/Cargos	Calificación Funcionario 1	Calificación Funcionario 2	Calificación Funcionario 3
R12	Tecnología de la información	Daniel Zurita	R12	Falta de supervisión y mal manejo de información dentro de proyectos	Existen responsables de los proyectos que se encarguen de supervisar el uso de datos, recursos y seguimiento del plan de acción ?	8.2.1. Responsabilidades de la Dirección	Alto	4,0	4,0	Voto Impacto	4,0	4,0	4,0
										Voto Vulnerabilidad	4,0	4,0	4,0
R13	Tecnología de la información	Daniel Zurita	R13	Falta de sanciones para quien genere vulnerabilidades	Existe algún proceso disciplinario formal para los empleados que generen brechas de seguridad ya sean internos o terceros en la gestión de proyectos ?	8.2.3. Proceso disciplinario	Alto	3,0	5,0	Voto Impacto	5,0	5,0	5,0
										Voto Vulnerabilidad	3,0	3,0	3,0
R14	Tecnología de la información	Daniel Zurita	R14	Posible problemas a la continuidad del negocio	Existen ambientes separados para el desarrollo e implementación de proyectos antes de ponerlos en línea ?	10.1.4. Separación de los recursos de desarrollo, prueba y operación.	Medio	2,0	4,0	Voto Impacto	4,0	4,0	4,0
										Voto Vulnerabilidad	2,0	2,0	2,0
R15	Tecnología de la información	Daniel Zurita	R15	Vulnerabilidades vigentes dentro de la empresa por falta de conocimiento en el proceso de mitigación.	Se encuentran documentados los procedimientos de operación antes problemas de seguridad de la información y puestos en conocimiento con todos los miembros de la organización ?	10.1.1. Documentación de los procedimientos de operación	Medio	2,0	5,0	Voto Impacto	5,0	5,0	5,0
										Voto Vulnerabilidad	2,0	2,0	2,0
R16	Tecnología de la información	Daniel Zurita	R16	Pérdidas de datos por falta de control en los sistemas implementados y los proyectos propuestos.	Se controlan los cambios en los sistemas y los recursos de tratamiento de la información?	10.1.2. Gestión de cambios	Bajo	1,0	3,0	Voto Impacto	3,0	3,0	3,0
										Voto Vulnerabilidad	1,0	1,0	1,0
R17	Tecnología de la información	Daniel Zurita	R17	Mal manejo de la información	Existen controles que aseguren el uso correcto de la información obtenida por terceros así también como protocolos para supervisar el trabajo realizado?	10.2.2. Supervisión y revisión de los servicios prestados por terceros	Medio	1,0	5,0	Voto Impacto	5,0	5,0	5,0
										Voto Vulnerabilidad	1,0	1,0	1,0
R18	Tecnología de la información	Daniel Zurita	R18	Pérdida de la información y posibles daños al equipos	Existe alguna medida contra el código malicioso dentro de los equipos que gestionan los proyectos?	10.4.2. Controles contra el código descargado en el cliente	Medio	2,0	5,0	Voto Impacto	5,0	5,0	5,0
										Voto Vulnerabilidad	2,0	2,0	2,0

	Proceso	Líder de proceso	Tipificación del riesgo	Riesgo Evaluado	Observación	Control relacionado (ISO27002)	Criticidad	Vulnerabilidad	Impacto	Voto/Cargos	Calificación Funcionario 1	Calificación Funcionario 2	Calificación Funcionario 3
R19	Tecnología de la información	Daniel Zurita	R19	Pérdida de información y seguridad en redes	Existen controles dentro de las redes que aseguren el tráfico limpio dentro de los canales de compartición de datos en la gestión de proyectos?	10.6. Gestión de seguridades de redes	Bajo	1,0	3,0	Voto Impacto	3,0	3,0	3,0
										Voto Vulnerabilidad	1,0	1,0	1,0
R20	Tecnología de la información	Daniel Zurita	R20	Pérdida de información	Existen acuerdos de intercambio de información con terceros a la empresa en la gestión de proyectos?	10.8.2. Acuerdos de intercambio	Alto	5,0	5,0	Voto Impacto	5,0	5,0	5,0
										Voto Vulnerabilidad	5,0	5,0	5,0
R21	Tecnología de la información	Daniel Zurita	R21	Fuga de información	Existen soportes específicos para el tratamiento de proyectos que aseguren la integridad de la información?	10.8.3. Soportes físicos en tránsito	Medio	2,0	5,0	Voto Impacto	5,0	5,0	5,0
										Voto Vulnerabilidad	2,0	2,0	2,0
R22	Tecnología de la información	Daniel Zurita	R22	Sigilo Bancario	Dentro de la implementación y gestión de proyectos se contempla la protección de los datos usados por los programas en fase de desarrollo?	15.1.4. Protección de datos de carácter personal y de la intimidad de las personas	Medio	1,0	4,5	Voto Impacto	4,5	4,5	4,5
										Voto Vulnerabilidad	1,0	1,0	1,0
R23	Tecnología de la información	Daniel Zurita	R23	Pérdida de datos e integridad de información	Existe alguna política que gestione el uso de soportes extraíbles en tránsito de la gestión de proyectos?	10.7.1. Gestión de soportes extraíbles	Medio	2,0	4,8	Voto Impacto	4,8	4,8	4,8
										Voto Vulnerabilidad	2,0	2,0	2,0
R24	Tecnología de la información	Daniel Zurita	R24	Monitoreo y notificaciones	Existe algún protocolo conocido para la notificación de puntos débiles que se encuentren en el desarrollo de proyectos?	13.1. Notificación de eventos y puntos débiles de la seguridad de la información	Medio	1,0	4,5	Voto Impacto	4,5	4,5	4,5
										Voto Vulnerabilidad	1,0	1,0	1,0
R25	Tecnología de la información	Daniel Zurita	R25	PETI	Se cuenta con controles que monitoreen el uso de recursos así como de las proyecciones de los requisitos de las capacidades adecuadas para el futuro en aplicación de proyectos	10.3.1 Planificación de capacidades	Alto	4,0	4,8	Voto Impacto	4,8	4,8	4,8
										Voto Vulnerabilidad	4,0	4,0	4,0
R26			R26	Revisión de seguridad			Medio	1,0	3,8	Voto Impacto	3,8	3,8	3,8

	Proceso	Líder de proceso	Tipificación del riesgo	Riesgo Evaluado	Observación	Control relacionado (ISO27002)	Criticidad	Vulnerabilidad	Impacto	Voto/Cargos	Calificación Funcionario 1	Calificación Funcionario 2	Calificación Funcionario 3
	Tecnología de la información	Daniel Zurita			Existe algún protocolo que asegure la aceptación del sistema antes de su implementación	10.3.2. Aceptación del sistema				Voto Vulnerabilidad	1,0	1,0	1,0
R27	Tecnología de la información	Daniel Zurita	R27	Monitoreo de la infraestructura y BDD: Falta de conocimiento de equipo dedicado requerido para el funcionamiento de la infraestructura o BDD	¿Todos los activos se encuentran debidamente identificados para su debido inventariado?	7.1.1. Inventario de activos	Medio	1,0	4,7	Voto Impacto	4,7	4,7	4,7
										Voto Vulnerabilidad	1,0	1,0	1,0
R28	Tecnología de la información	Daniel Zurita	R28	Equipo no designado o subutilizado	Existe algún control que designe la propiedad de los activos dentro de la organización ?	7.1.2. Propiedad de los activos	Medio	1,0	4,5	Voto Impacto	4,5	4,5	4,5
										Voto Vulnerabilidad	1,0	1,0	1,0
R29	Tecnología de la información	Daniel Zurita	R29	Uso inadecuado de los activos	Existe algún control que designe el correcto uso de los activos dentro de la organización?	7.2.3. Uso aceptable de los activos	Alto	5,0	3,8	Voto Impacto	3,8	3,8	3,8
										Voto Vulnerabilidad	5,0	5,0	5,0
R30	Tecnología de la información	Daniel Zurita	R30	Vulnerabilidades causadas por el personal	Existe una debida capacitación a las personas encargadas de monitorear la infraestructura y la BDD dentro de la empresa?	8.2.2. Concienciación, formación y capacitación en seg. De la información	Alto	5,0	4,9	Voto Impacto	4,9	4,9	4,9
										Voto Vulnerabilidad	5,0	5,0	5,0
R31	Tecnología de la información	Daniel Zurita	R31	Fuga de información , manipulación de la misma	Existen controles de acceso a la red que sean reflejados en el monitoreo de la infraestructura?	11.4 Control de Acceso a la Red	Medio	3,3	4,0	Voto Impacto	4,0	4,0	4,0
										Voto Vulnerabilidad	3,3	3,3	3,3
R32	Tecnología de la información	Daniel Zurita	R32	Vulnerabilidad de la información	Existen controles de acceso a las aplicaciones de la organización que maneje información interna?	11.6 Control de acceso a las aplicaciones y a la información	Alto	5,0	4,2	Voto Impacto	4,2	4,2	4,2
										Voto Vulnerabilidad	5,0	5,0	5,0
R33	Tecnología de la información	Daniel Zurita	R33	Información sensible sin un correcto manejo.	Se contempla el uso de controles criptográficos dentro de la infraestructura y la BDD?	12.3. Controles criptográficos	Alto	4,5	4,6	Voto Impacto	4,6	4,6	4,6
										Voto Vulnerabilidad	4,5	4,5	4,5
R34	Tecnología de la información	Daniel Zurita	R34	Manipulación de la información no autorizada	Existen controles de control de acceso al código fuente de los programas con los que se manejan en la infraestructura?	12.4.3. Control de acceso al código fuente de los programas	Medio	1,0	3,9	Voto Impacto	3,9	3,9	3,9
										Voto Vulnerabilidad	1,0	1,0	1,0
R35	Tecnología de la información	Daniel Zurita	R35	Vulnerabilidades existentes en el ámbito técnico de los sistemas utilizados	Se cuenta con la información de la vulnerabilidad técnica de los sistemas de información que se usen?	12.6.1. Control de las vulnerabilidades técnicas	Medio	3,0	4,6	Voto Impacto	4,6	4,6	4,6
										Voto Vulnerabilidad	3,0	3,0	3,0
R36	Tecnología de la información	Daniel Zurita	R36	Generación de reportes: Pérdida de información por código malicioso	Se cuenta con controles contra el código malicioso dentro de los equipos destinados a guardar la información de reportes?	10.4 Protección contra el código malicioso y descargable	Alto	5,0	4,6	Voto Impacto	4,6	4,6	4,6
										Voto Vulnerabilidad	5,0	5,0	5,0
R37			R37	Pérdida de la información			Alto	4,0	4,0	Voto Impacto	4,0	4,0	4,0

	Proceso	Líder de proceso	Tipificación del riesgo	Riesgo Evaluado	Observación	Control relacionado (ISO27002)	Criticidad	Vulnerabilidad	Impacto	Voto/Cargos	Calificación Funcionario 1	Calificación Funcionario 2	Calificación Funcionario 3
	Tecnología de la información	Daniel Zurita			Existe un protocolo para realizar copias de seguridad ?	10.5 Copias de seguridad				Voto Vulnerabilidad	4,0	4,0	4,0
R38	Tecnología de la información	Daniel Zurita	R38	Acceso indebido a la información	Existen controles de red que garanticen el uso adecuado de la información ?	10.6.1 Controles de red	Medio	3,0	4,7	Voto Impacto	4,7	4,7	4,7
										Voto Vulnerabilidad	3,0	3,0	3,0
R39	Tecnología de la información	Daniel Zurita	R39	Fuga de la información	Existe algún protocolo de intercambio de la información ?	10.8 Intercambio de la información	Medio	5,0	1,0	Voto Impacto	1,0	1,0	1,0
										Voto Vulnerabilidad	5,0	5,0	5,0
R40	Tecnología de la información	Daniel Zurita	R40	Planificación de TI: Fuga de información e intervención de procedimiento de los procesos de implementación	Existen protocolo de intercambio para intercambiar la información relacionada a la planificación de TI?	10.8 Intercambio de la información	Alto	5,0	4,2	Voto Impacto	4,2	4,2	4,2
										Voto Vulnerabilidad	5,0	5,0	5,0
R41	Tecnología de la información	Daniel Zurita	R41	Mantenimientos	Existen controles que aseguren la integridad de los datos de un computador con los permisos necesarios para cada nivel organizacional?	10.4 Protección contra el código malicioso y descargable	Alto	5,0	4,7	Voto Impacto	4,7	4,7	4,7
										Voto Vulnerabilidad	5,0	5,0	5,0
R42	Tecnología de la información	Daniel Zurita	R42	Pérdida de información general	Existe un protocolo de seguridad que contemple el uso y manejo de copias de seguridad en cada mantenimiento realizado?	10.5 Copias de seguridad	Alto	4,0	4,0	Voto Impacto	4,0	4,0	4,0
										Voto Vulnerabilidad	4,0	4,0	4,0
R43	Tecnología de la información	Daniel Zurita	R43	Posibles pasos de datos no consentidos en la seguridad de la información	¿Existen controles que den mantenimiento a la red de la empresa?	10.6.1 Controles de red	Medio	3,0	3,3	Voto Impacto	3,3	3,3	3,3
										Voto Vulnerabilidad	3,0	3,0	3,0
R44	Tecnología de la información	Daniel Zurita	R44	Operación de recursos de tecnología de información: Desconocimiento de los activos	¿Existe un correcto inventariado de los activos disponibles para la seguridad de la información?	7.1.1. Inventario de activos	Medio	2,0	2,8	Voto Impacto	2,8	2,8	2,8
										Voto Vulnerabilidad	2,0	2,0	2,0
R45	Tecnología de la información	Daniel Zurita	R45	Uso inadecuado de los activos	Existe alguna designación de la información y activos asociados a los recursos para el tratamiento de la información ?	7.1.2. Propiedad de los activos	Medio	4,5	3,4	Voto Impacto	3,4	3,4	3,4
										Voto Vulnerabilidad	4,5	4,5	4,5
R46	Tecnología de la información	Daniel Zurita	R46	Uso inadecuado de los activos	Se encuentran documentados, identificados e implementados regulaciones para el uso adecuado de la información y los activos asociados a los recursos de tratamiento de la información	7.2.3. Uso aceptable de los activos	Medio	1,0	3,9	Voto Impacto	3,9	3,9	3,9
										Voto Vulnerabilidad	1,0	1,0	1,0
R47	Tecnología de la información	Daniel Zurita	R47	Mal uso de las herramientas en el tratamiento de los recursos de tecnología de la información	Exista capacitación acerca de los controles y herramientas para el tratamiento de la seguridad de la información y un correcto uso del mismo?	8.2.2. Concienciación, formación y capacitación en seg. De la información	Medio	2,0	5,0	Voto Impacto	5,0	5,0	5,0
										Voto Vulnerabilidad	2,0	2,0	2,0

	Proceso	Líder de proceso	Tipificación del riesgo	Riesgo Evaluado	Observación	Control relacionado (ISO27002)	Criticidad	Vulnerabilidad	Impacto	Voto/Cargos	Calificación Funcionario 1	Calificación Funcionario 2	Calificación Funcionario 3
R48	Tecnología de la información	Daniel Zurita	R48	Pérdida de información por recursos no comprobados con anterioridad	Dentro del área de TI existe separación de ambientes en las actividades de seguridad de la información dentro del uso de los recursos?	10.1.4 Separación de los recursos de prueba, desarrollo y operación	Medio	1,0	5,0	Voto Impacto	5,0	5,0	5,0
										Voto Vulnerabilidad	1,0	1,0	1,0
R49	Tecnología de la información	Daniel Zurita	R49	Posible navegación no consentida dentro de la empresa	Se cuenta con la identificación del personal que está haciendo la gestión de los recursos de la tecnología de la información?	11.4 Control de Acceso a la Red	Bajo	1,0	2,6	Voto Impacto	2,6	2,6	2,6
										Voto Vulnerabilidad	1,0	1,0	1,0
R50	Tecnología de la información	Daniel Zurita	R50	Acceso indebido del personal	Existe algún tipo de control a las aplicaciones que sigan en la administración de los recursos de tecnología de la información?	11.6 Control de acceso a las aplicaciones y a la información	Medio	1,0	4,5	Voto Impacto	4,5	4,5	4,5
										Voto Vulnerabilidad	1,0	1,0	1,0
R51	Tecnología de la información	Daniel Zurita	R51	Fuga de información, Pérdidas de información	Existen controles criptográficos dentro del área de TI que aseguren el acceso de personas autorizadas a la operación de recursos de tecnología de la información?	12.3. Controles criptográficos	Medio	1,0	3,1	Voto Impacto	3,1	3,1	3,1
										Voto Vulnerabilidad	1,0	1,0	1,0
R52	Tecnología de la información	Daniel Zurita	R52	Seguridad y control de la información hardware y software: Desconocimiento de herramientas disponibles	Existe un inventario debidamente manejado con el hardware y software referente a la seguridad y control de la información?	7.1.1 Inventario de activos	Medio	1,0	3,1	Voto Impacto	3,1	3,1	3,1
										Voto Vulnerabilidad	1,0	1,0	1,0
R53	Tecnología de la información	Daniel Zurita	R53	Uso inapropiado de los activos	Existe la documentación debida que tipifique la propiedad de los activos en su uso, condiciones de uso y registro del mismo ?	7.1.2. Propiedad de los activos	Alto	4,0	4,5	Voto Impacto	4,5	4,5	4,5
										Voto Vulnerabilidad	4,0	4,0	4,0
R54	Tecnología de la información	Daniel Zurita	R54	Uso indebido de los activos	Existen los documentos o certificados del uso destinado para los recursos con los que cuente la empresa?	7.1.3. Uso aceptable de los activos	Medio	2,0	5,0	Voto Impacto	5,0	5,0	5,0
										Voto Vulnerabilidad	2,0	2,0	2,0
R55	Tecnología de la información	Daniel Zurita	R55	Evitar las amenazas del entorno	Se cuenta con la ubicación adecuada para reducir las oportunidades de accesos no autorizados reduciendo las amenazas del entorno ?	9.2.1 Emplazamiento y protección de los equipos	Bajo	1,0	3,0	Voto Impacto	3,0	3,0	3,0
										Voto Vulnerabilidad	1,0	1,0	1,0
R56	Tecnología de la información	Daniel Zurita	R56	Pérdida de los equipos fuera de la empresa	Existen protocolos para la seguridad de los equipos que se encuentren fuera de la empresa considerando los riesgos a los que está expuesto?	9.2.5 Seguridad de los equipos fuera de las instalaciones	Medio	3,0	3,5	Voto Impacto	3,5	3,5	3,5
										Voto Vulnerabilidad	3,0	3,0	3,0
R57	Tecnología de la información	Daniel Zurita	R57	Fuga de información por mal manejo de equipo separado o	Existen vigentes protocolos de retirada segura del equipo o	9.2.6 Reutilización o retirada segura de equipos	Medio	3,0	3,6	Voto Impacto	3,6	3,6	3,6
										Voto Vulnerabilidad	3,0	3,0	3,0

	Proceso	Líder de proceso	Tipificación del riesgo	Riesgo Evaluado	Observación	Control relacionado (ISO27002)	Criticidad	Vulnerabilidad	Impacto	Voto/Cargos	Calificación Funcionario 1	Calificación Funcionario 2	Calificación Funcionario 3
				nuevamente asignado perteneciente a la empresa	reutilización del mismo dentro de la organización?								
R58	Tecnología de la información	Daniel Zurita	R58	Código descargado de terceros perjudicial para la seguridad de la información	Existen controles que eviten la descarga de código malicioso o la ejecución de scrips alojados en el SW propiedad de la empresa?	10.4.2 Controles contra el código descargado en el cliente	Medio	2,0	4,3	Voto Impacto	4,3	4,3	4,3
										Voto Vulnerabilidad	2,0	2,0	2,0
R59	Tecnología de la información	Daniel Zurita	R59	Posible punto vulnerable dentro de la empresa	Existe algún protocolo de tratamiento de usuarios desatendidos?	11.3.2. Equipo de usuario desatendido	Medio	1,0	4,0	Voto Impacto	4,0	4,0	4,0
										Voto Vulnerabilidad	1,0	1,0	1,0
R60	Tecnología de la información	Daniel Zurita	R60	Sistemas o equipos con contenido de alta importancia sin resguardo adecuado y fácil acceso	Existe algún control para el tratamiento de sistemas sensibles en los que se alojen aplicaciones importantes o bases de datos sensibles?	11.6.2 Aislamiento de sistemas sensibles	Alto	5,0	4,2	Voto Impacto	4,2	4,2	4,2
										Voto Vulnerabilidad	5,0	5,0	5,0
R61	Tecnología de la información	Daniel Zurita	R61	Mala gestión de la información en equipos tecnológicos portátiles y cualquier dispositivo usado en telemática	Existen controles para el uso de los ordenadores portátiles dentro de la organización y el teletrabajo que se puede realizar con los mismos?	11.7.1 Ordenadores portátiles y comunicaciones móviles	Medio	1,0	3,8	Voto Impacto	3,8	3,8	3,8
										Voto Vulnerabilidad	1,0	1,0	1,0
R62	Tecnología de la información	Daniel Zurita	R62	Falta de seguridad del HW y SW utilizado en el teletrabajo	Existen protocolos de teletrabajo que asegure la disponibilidad e integridad tanto del HW como del SW usado en la telemática?	11.7.2 Teletrabajo	Medio	2,0	4,2	Voto Impacto	4,2	4,2	4,2
										Voto Vulnerabilidad	2,0	2,0	2,0
R63	Tecnología de la información	Daniel Zurita	R63	Fuga de información	Existe algún procedimiento o manera de control que se encargue de controlar la instalación de software en sistemas que estén operativos?	12.4.1 Control de software en explotación	Bajo	1,0	3,0	Voto Impacto	3,0	3,0	3,0
										Voto Vulnerabilidad	1,0	1,0	1,0
R64	Tecnología de la información	Daniel Zurita	R64	Corrupción de los datos del sistema	Existe algún tipo de control que asegure la seguridad de los datos de prueba del sistema	12.4.2 Protección de los datos de prueba del sistema	Medio	1,0	3,1	Voto Impacto	3,1	3,1	3,1
										Voto Vulnerabilidad	1,0	1,0	1,0
R65	Tecnología de la información	Daniel Zurita	R65	Fuga de información y protocolos	Existen protocolos de seguridad en los procesos de desarrollo y soporte?	12.5. Seguridad de los procesos de desarrollo y soporte	Medio	1,5	4,8	Voto Impacto	4,8	4,8	4,8
										Voto Vulnerabilidad	1,5	1,5	1,5
R66	Tecnología de la información	Daniel Zurita	R66	Personal inadecuado manejando protocoles criptográficos	Existe alguna política de controles criptográficos en las operaciones y tratamiento de la seguridad de la información?	12.3.1 Política de uso de los controles criptográficos	Medio	1,0	5,0	Voto Impacto	5,0	5,0	5,0
										Voto Vulnerabilidad	1,0	1,0	1,0
R67	Tecnología de la información	Daniel Zurita	R67	Toma de documentación inválida	Existe alguna política de intercambio de información como la documentación de cada solicitud?	10.8.1 Políticas y procedimientos de intercambio de la información	Medio	3,0	4,7	Voto Impacto	4,7	4,7	4,7
										Voto Vulnerabilidad	3,0	3,0	3,0
R68			R68				Medio	1,0	4,0	Voto Impacto	4,0	4,0	4,0

	Proceso	Líder de proceso	Tipificación del riesgo	Riesgo Evaluado	Observación	Control relacionado (ISO27002)	Criticidad	Vulnerabilidad	Impacto	Voto/Cargos	Calificación Funcionario 1	Calificación Funcionario 2	Calificación Funcionario 3
	Tecnología de la información	Daniel Zurita		Áreas inseguras para resguardar la información	Existen un perímetro definido para resguardar el equipo y el software que se encarga de dar tratamiento a la seguridad de la información?	9.1.1. Perímetro de seguridad f física				Voto Vulnerabilidad	1,0	1,0	1,0
R69	Tecnología de la información	Daniel Zurita	R69	Personal indebido realizando tareas técnicas	Existe segregación de tareas documentadas dentro de la	10.1.3 Segregación de tareas	Medio	2,0	3,0	Voto Impacto	3,0	3,0	3,0
										Voto Vulnerabilidad	2,0	2,0	2,0
R70	Riesgos	Gabriel Ripalda	R70	Falta de clasificación de archivos de administración dentro del área de riesgos	Dentro de los análisis de la evolución de la cartera de crédito, concentración de cartera, colocaciones, morosidad por tipo de créditos. Hace falta clasificar este tipo de información como sensible, abierta, no clasificada.	7.2.1. Directrices para la clasificación de la información	Medio	5,0	1,0	Voto Impacto	1,0		
										Voto Vulnerabilidad	5,0		
R71	Riesgos	Gabriel Ripalda	R71	Posible daño de equipos por virus	Existe protección para dichos archivos de análisis contra los códigos maliciosos que puedan encontrarse dentro de los equipos de trabajo	10.4 Protección contra el código malicioso y descargable	Alto	5,0	4,2	Voto Impacto	4,2	4,2	4,2
										Voto Vulnerabilidad	5,0	5,0	5,0
R72	Riesgos	Gabriel Ripalda	R72	Falta de copias de seguridad dentro de los computadores de trabajo	Se realizan copias de seguridad debidas para este proceso en específico, cuáles son las maneras de guardar dicha información y cómo se la maneja en caso de desastre.	10.5 Copias de seguridad	Alto	5,0	4,7	Voto Impacto	4,7	4,7	4,7
										Voto Vulnerabilidad	5,0	5,0	5,0
R73	Riesgos	Gabriel Ripalda	R73	Libere acceso a las plataformas y modificación de datos	Cuáles son los controles que se tienen dentro de la intranet y portales web para la persona designada de hacer dichas tareas	10.6.1 Controles de red	Alto	4,0	4,0	Voto Impacto	4,0	4,0	4,0
										Voto Vulnerabilidad	4,0	4,0	4,0
R74	Riesgos	Gabriel Ripalda	R74	Intercambio de los análisis sin una medida de seguridad	¿El intercambio de dicha información lleva un procedimiento acorde al nivel de importancia que la sostiene? Cuál es la política para que dicha información sea compartida	10.8.1 Políticas de Intercambio de la información	Medio	3,0	3,3	Voto Impacto	3,3	3,3	3,3
										Voto Vulnerabilidad	3,0	3,0	3,0
R75	Riesgos	Gabriel Ripalda	R75	posibles pérdidas de archivos o contaminación de los mismos al pasarse por medios magnéticos	Existe algún dispositivo que se encuentre en tránsito capaz de asegurar la integridad y disponibilidad de dicha información	10.8.3. Soportes físicos en tránsito	Medio	2,0	2,8	Voto Impacto	2,8	2,8	2,8
										Voto Vulnerabilidad	2,0	2,0	2,0
R76	Riesgos	Gabriel Ripalda	R76	Comunicación interna de la empresa vía web	En el caso de tener que enviar el archivo vía mail, consta éste de una manera segura de compartirse?	10.8.4. Mensajería electrónica	Medio	4,5	3,4	Voto Impacto	3,4	3,4	3,4
										Voto Vulnerabilidad	4,5	4,5	4,5

	Proceso	Líder de proceso	Tipificación del riesgo	Riesgo Evaluado	Observación	Control relacionado (ISO27002)	Criticidad	Vulnerabilidad	Impacto	Voto/Cargos	Calificación Funcionario 1	Calificación Funcionario 2	Calificación Funcionario 3
R77	Riesgos	Gabriel Ripalda	R77	Protocolos para subir información general	En caso de tener que compartir algún archivo por la herramienta ISOTOOLS, existe algún protocolo de hacerlo?	10.8.5. Sistemas de información empresariales	Medio	1,0	3,9	Voto Impacto	3,9	3,9	3,9
										Voto Vulnerabilidad	1,0	1,0	1,0
R78	Riesgos	Gabriel Ripalda	R78	Problemas en quién sube la información a los portales o herramientas web	Nivel de servicio en el control de acceso que tiene el empleado para la compartición de la información	11.1.1. Políticas de control de acceso.	Medio	2,0	5,0	Voto Impacto	5,0	5,0	5,0
										Voto Vulnerabilidad	2,0	2,0	2,0
R79	Riesgos	Gabriel Ripalda	R79	Falta de conocimiento de alguna actualización de las autoridades que rigen la empresa	Se deben mantener los contactos apropiados con las autoridades pertinentes para estar al corriente del tratamiento de los riesgos que se puedan dar en todas las áreas organizacionales, dentro de ellas pueden estar empresas del sector público y privado.	6.1.6. Contacto con las autoridades	Medio	1,0	5,0	Voto Impacto	5,0	5,0	5,0
										Voto Vulnerabilidad	1,0	1,0	1,0
R80	Riesgos	Gabriel Ripalda	R80	Falta de conocimiento de temas específicos por los que la ayuda sea solicitada	En el caso de requerir algún tipo de ayuda con temas específicos poder tener un contacto o acercamiento a las recomendaciones que hacen diferentes empresas, puede ser en referencia a Tecnología (ESET, MICROSOFT, etc.), ámbitos legales (SEPS, Código de Basilea, etc.), Financiero (Portal del SRI, Programas contables dedicados, etc.), etc.	6.1.7. Contacto con grupos de interés social	Bajo	1,0	2,6	Voto Impacto	2,6	2,6	2,6
										Voto Vulnerabilidad	1,0	1,0	1,0
R81	Riesgos	Gabriel Ripalda	R81	Desconocimiento de herramientas existentes y mal uso de dichos activos	Se deben identificar, documentar y tener regulaciones para el uso adecuado de la información implantadas en caso de presentarse un evento de riesgo y poder solucionarlo eficientemente. (INTECO – Guía del uso de TI en el ámbito organizacional)	7.1.3. Uso aceptable de los activos	Medio	1,0	4,5	Voto Impacto	4,5	4,5	4,5
										Voto Vulnerabilidad	1,0	1,0	1,0
R82	Riesgos	Gabriel Ripalda	R82	Falta de organización en lo que se refiere a tipos de riesgos reportados	Existe algún directriz para clasificar la información de riesgos de acuerdo a su criticidad	7.2.1. Directrices de clasificación de la información	Medio	1,0	3,1	Voto Impacto	3,1	3,1	3,1
										Voto Vulnerabilidad	1,0	1,0	1,0
R83	Riesgos	Gabriel Ripalda	R83	Desorganización de la información sin etiquetas de pertenencia protocolizado	Se debe contar con procedimientos de etiquetado de la información de acuerdo al	7.2.2. Etiquetado y manipulado de la información	Medio	1,0	3,1	Voto Impacto	3,1	3,1	3,1
										Voto Vulnerabilidad	1,0	1,0	1,0

	Proceso	Líder de proceso	Tipificación del riesgo	Riesgo Evaluado	Observación	Control relacionado (ISO27002)	Criticidad	Vulnerabilidad	Impacto	Voto/Cargos	Calificación Funcionario 1	Calificación Funcionario 2	Calificación Funcionario 3
					esquema de clasificación designado por la organización.								
R84	Riesgos	Gabriel Ripalda	R84	Errores constantes y llamadas innecesarias en apoyo del área de riesgos	Se debe contar con que todo el personal esté capacitado en las incidencias referentes a fallas de la seguridad de la información y no objeto de otro tipo de fallos, es importante notar la diferencia de fallo en la seguridad y un fallo funcional.	8.2.2. Formación y capacitación en seguridad de la información	Alto	4,0	4,5	Voto Impacto	4,5	4,5	4,5
										Voto Vulnerabilidad	4,0	4,0	4,0
R85	Riesgos	Gabriel Ripalda	R85	No existe sanciones por no aplicar el SGSI ocasionando brechas de seguridad	De ser el caso, se cuenta con un proceso disciplinario para las personas que causen eventos de riesgo o brechas de seguridad	8.2.3. Procedimiento disciplinario	Medio	2,0	5,0	Voto Impacto	5,0	5,0	5,0
										Voto Vulnerabilidad	2,0	2,0	2,0
R86	Riesgos	Gabriel Ripalda	R86	Problemas con la designación de tareas provisionales que potencialmente causen eventos de riesgo	Se debe contar con la designación de responsabilidades tras un cese de actividades para que los posibles eventos de seguridad no sean reportados de manera frecuente.	8.3.1. Cese de responsabilidades	Bajo	1,0	3,0	Voto Impacto	3,0	3,0	3,0
										Voto Vulnerabilidad	1,0	1,0	1,0
R87	Riesgos	Gabriel Ripalda	R87	Errores en procesos críticos por aplicar medidas sin probarlas antes.	Tras definir una solución o propuesta de aquella, de ser necesario realizar un cambio grande es prudente tener una correcta separación de ambientes para que los procesos no se vean afectados directamente (es un control preventivo).	10.1.4. Separación de los recursos para desarrollo y producción	Medio	3,0	3,5	Voto Impacto	3,5	3,5	3,5
										Voto Vulnerabilidad	3,0	3,0	3,0
R88	Riesgos	Gabriel Ripalda	R88	Pérdida de la solución o avance de la misma a un problema emergente.	Se deben implementar controles para detectar, prevenir y recuperar los archivos afectados por virus, esto en el proceso de verificación en un estudio de campo	10. 4. 1. Medidas y controles contra software malicioso	Medio	3,0	3,6	Voto Impacto	3,6	3,6	3,6
										Voto Vulnerabilidad	3,0	3,0	3,0
R89	Riesgos	Gabriel Ripalda	R89	Pérdida de los reportes de soluciones anteriores para formar un manual de soluciones rápidas.	Es necesario contar con las respectivas copias de seguridad de la información en caso de que el evento haya corrompido datos importantes.	10.5.1. Copias de seguridad de la información.	Medio	2,0	4,3	Voto Impacto	4,3	4,3	4,3
										Voto Vulnerabilidad	2,0	2,0	2,0
R90	Riesgos	Gabriel Ripalda	R90	No registro de reuniones en el trabajo conjunto con el líder de proceso	Es necesario mantener los acuerdos de intercambio de información planteados para tratar un evento de riesgo, al	10.8.2. Acuerdos de intercambio de información.	Medio	1,0	4,0	Voto Impacto	4,0	4,0	4,0
										Voto Vulnerabilidad	1,0	1,0	1,0

	Proceso	Líder de proceso	Tipificación del riesgo	Riesgo Evaluado	Observación	Control relacionado (ISO27002)	Criticidad	Vulnerabilidad	Impacto	Voto/Cargos	Calificación Funcionario 1	Calificación Funcionario 2	Calificación Funcionario 3
					estar involucrado el personal interno no hace falta un acuerdo de confidencialidad.								
R91	Riesgos	Gabriel Ripalda	R91	Acceso vulnerable a los equipos en los que se desarrollan soluciones	Toda actividad que se haga dentro de un PC es responsabilidad del usuario, desde el manejo de contraseñas, incluyendo el equipo que tenga la información y registro de dichos eventos.	11.3.1 Uso de contraseñas.	Alto	5,0	4,2	Voto Impacto	4,2	4,2	4,2
										Voto Vulnerabilidad	5,0	5,0	5,0
R92	Riesgos	Gabriel Ripalda	R92	Mala práctica profesional por desconocimiento específico de otra área.	En caso de ser necesario y que el evento de riesgo tenga consecuencias graves es prudente prepararse para el apoyo con la interacción de otras áreas para solucionar el evento de riesgo.	15.1.1. Identificación de la legislación aplicable	Medio	1,0	3,8	Voto Impacto	3,8	3,8	3,8
										Voto Vulnerabilidad	1,0	1,0	1,0
R93	Riesgos	Gabriel Ripalda	R93	Demasiada carga en atención de eventos de cualquier tipo	Asegurar el cumplimiento es una de las mejores maneras de prevenir eventos de riesgo.	15.2.1. Cumplimiento de normas y políticas de seguridad	Medio	2,0	4,2	Voto Impacto	4,2	4,2	4,2
										Voto Vulnerabilidad	2,0	2,0	2,0
R94	Riesgos	Gabriel Ripalda	R94	Modificación indebida de planes de contingencia	Las políticas de accesos a los planes contingentes deben ser debidamente controlados para evitar la modificación no consentida del mismo.	11.1.1. Política de control de acceso	Bajo	1,0	3,0	Voto Impacto	3,0	3,0	3,0
										Voto Vulnerabilidad	1,0	1,0	1,0
R95	Riesgos	Gabriel Ripalda	R95	Confusiones o dualidad de documentación de protocolos al no documentar cada recepción de datos relevantes	Todos los planes, protocolos e información aquí presente deben intercambiarse con todo el personal de manera adecuada siguiendo un procedimiento diferente al de documentación de alta criticidad.	10.8.1. Políticas y procedimientos de intercambio de la información	Medio	1,0	3,1	Voto Impacto	3,1	3,1	3,1
										Voto Vulnerabilidad	1,0	1,0	1,0
R96	Riesgos	Gabriel Ripalda	R96	Desinformación al no acatar un plan de contingencia en fase aplicable	En fase de desarrollo, (continuamente) debe revisarse continuamente que solo se pueda acceder a este tipo de información.	11.2.4. Revisión de los derechos de acceso de usuario.	Medio	1,5	4,8	Voto Impacto	4,8	4,8	4,8
										Voto Vulnerabilidad	1,5	1,5	1,5
R97	Riesgos	Gabriel Ripalda	R97	Pérdida de los planes de contingencia aplicados, en fase de desarrollo o en mejora continua.	Se debe tener una política especial que asegure la disponibilidad de esta información al 100%	10.5.1. Copias de la seguridad de la información.	Medio	1,0	5,0	Voto Impacto	5,0	5,0	5,0
										Voto Vulnerabilidad	1,0	1,0	1,0

	Proceso	Líder de proceso	Tipificación del riesgo	Riesgo Evaluado	Observación	Control relacionado (ISO27002)	Criticidad	Vulnerabilidad	Impacto	Voto/Cargos	Calificación Funcionario 1	Calificación Funcionario 2	Calificación Funcionario 3
R98	Riesgos	Gabriel Ripalda	R98	Pérdida de datos y posibles intrusiones en el proceso de recuperación	Se cuenta con un plan de continuidad que contemple las principales aristas de la seguridad de la información?	14.1.1. Inclusión de la seguridad de la información en el proceso de gestión de la continuidad del negocio.	Medio	3,0	4,7	Voto Impacto	4,7	4,7	4,7
										Voto Vulnerabilidad	3,0	3,0	3,0
R99	Riesgos	Gabriel Ripalda	R99	Gastos innecesarios por estimar pérdidas no comprobadas	Estamos en capacidad de evaluar las consecuencias de los riesgos tras un evento emergente	14.1.2. Continuidad del negocio y evaluación de riesgos.	Medio	1,0	4,0	Voto Impacto	4,0	4,0	4,0
										Voto Vulnerabilidad	1,0	1,0	1,0
R100	Riesgos	Gabriel Ripalda	R100	Pérdida de información de cualquier tipo en caso de evento de alto riesgo	En caso de un evento emergente, se perdería mucha información ? De qué tipo es ?	14.1.3. Desarrollo e implantación de planes de continuidad que incluyan la seguridad de la información.	Medio	2,0	3,0	Voto Impacto	3,0	3,0	3,0
										Voto Vulnerabilidad	2,0	2,0	2,0
R101	Riesgos	Gabriel Ripalda	R101	Pérdida de la continuidad descriptiva para la mejora continua de protocolos de recuperación.	Se cuenta con las bases tomadas en cuenta para el desarrollo de los planes de contingencia documentados adecuadamente?	14.1.4. Marco de referencia para la planificación de la continuidad del negocio.	Medio	1,0	3,6	Voto Impacto	3,6	3,6	3,6
										Voto Vulnerabilidad	1,0	1,0	1,0
R102	Riesgos	Gabriel Ripalda	R102	Desactualización del plan de contingencia	Se cuenta con pruebas, mantenimientos y revalidación de los protocolos de seguridad?	14.1.5. Pruebas, mantenimiento y reevaluación de planes de continuidad.	Medio	1,0	4,0	Voto Impacto	4,0	4,0	4,0
										Voto Vulnerabilidad	1,0	1,0	1,0
R103	Riesgos	Gabriel Ripalda	R103	Errores por desconocimiento técnico	Al ser un evento de alta importancia y manejo de información con otras áreas se deben prestar atención especial a los controles que priman dicho proceso	6.1.7. Contacto con los grupos de especial interés	Medio	1,0	5,0	Voto Impacto	5,0	5,0	5,0
										Voto Vulnerabilidad	1,0	1,0	1,0
R104	Riesgos	Gabriel Ripalda	R104	Fuga de información por uso de instalaciones inseguras	Es importante contar con un área seguro para tratar este tipo de información acorde a diferentes puntos de la seguridad.	9.1.3. Seguridad de oficinas, despachos e instalaciones	Medio	1,0	3,7	Voto Impacto	3,7	3,7	3,7
										Voto Vulnerabilidad	1,0	1,0	1,0
R105	Riesgos	Gabriel Ripalda	R105	Carga laboral mal distribuida y trabajo desarrollado a la fuerza	Se debe contar con una correcta segregación de tareas para evitar la manipulación malintencionada de los datos resultados de dichas reuniones con diferentes personas.	10.1.3. Segregación de tareas	Medio	3,2	4,6	Voto Impacto	4,6	4,6	4,6
										Voto Vulnerabilidad	3,2	3,2	3,2
R106	Riesgos	Gabriel Ripalda	R106	Pérdida de la integridad de los datos a compartir	Es importante mantener el contacto en este tipo de reuniones mediante la compartición de archivos personales por dispositivos	10.7.1. Gestión de soportes extraíbles	Bajo	1,0	1,0	Voto Impacto	1,0	1,0	1,0
										Voto Vulnerabilidad	1,0	1,0	1,0

	Proceso	Líder de proceso	Tipificación del riesgo	Riesgo Evaluado	Observación	Control relacionado (ISO27002)	Criticidad	Vulnerabilidad	Impacto	Voto/Cargos	Calificación Funcionario 1	Calificación Funcionario 2	Calificación Funcionario 3
					físicos, para evitar el camino funcional de la comunicación. De un punto A un punto B								
R107	Riesgos	Gabriel Ripalda	R107	Ingreso de virus a las máquinas propiedad de la empresa	Así también como una correcta administración de los soportes físicos en tránsito.	10.8.3 Soportes físicos en tránsito	Bajo	1,0	1,0	Voto Impacto	1,0	1,0	1,0
										Voto Vulnerabilidad	1,0	1,0	1,0
R108	Riesgos	Gabriel Ripalda	R108	Información no confirmada tomada en el resultado final	Es importante definir las políticas de intercambio de información en este tipo de actividades que involucran a más de una persona.	10.8.1. Políticas y procedimientos de intercambio de la información	Medio	2,0	3,0	Voto Impacto	3,0	3,0	3,0
										Voto Vulnerabilidad	2,0	2,0	2,0
R109	Riesgos	Gabriel Ripalda	R109	Fuga de información, Datos dañados, perdidos o equipos con malware	Es importante cumplir las políticas de seguridad para evitar eventos de riesgo en este tipo de reuniones y acuerdos grupales.	15.2.1. Cumplimiento de las políticas y normas de seguridad .	Medio	1,0	3,1	Voto Impacto	3,1	3,1	3,1
										Voto Vulnerabilidad	1,0	1,0	1,0
R110	Seguridad	Jean Rodríguez	R110	Perdida sustancial de datos y posibles vulnerabilidades fuertes	Es necesario aplicar una política de seguridad de la información que proteja la empresa	5.1.1. Documento de política de seguridad de la información.	Alto	5,0	5,0	Voto Impacto	5,0	5,0	5,0
										Voto Vulnerabilidad	5,0	5,0	5,0
R111	Seguridad	Jean Rodríguez	R111	Desactualización de manuales de uso, protocolos, etc.	Se cuenta con un periodo de revisión de la política con las normas nacionales e internacionales	5.1.2. Revisión de la política de seguridad de la información.	Medio	3,0	3,0	Voto Impacto	3,0	3,0	3,0
										Voto Vulnerabilidad	3,0	3,0	3,0
R112	Seguridad	Jean Rodríguez	R112	Falta de un responsable del manejo de la seguridad de la información	¿Se cuenta con un profesional capacitado para el manejo de la seguridad de la información?	6.1.1. Compromiso de la dirección con la seguridad de la información.	Alto	4,0	4,0	Voto Impacto	4,0	4,0	4,0
										Voto Vulnerabilidad	4,0	4,0	4,0
R113	Seguridad	Jean Rodríguez	R113	No se aplica ninguno de los controles del SGSI	Existe una manera coordinada de aplicar la seguridad de la información?	6.1.2. Coordinación de la seguridad de la información.	Bajo	2,0	2,0	Voto Impacto	2,0	2,0	2,0
										Voto Vulnerabilidad	2,0	2,0	2,0
R114	Seguridad	Jean Rodríguez	R114	Carga laboral demasiado fuerte para la persona encargada y posible mal manejo de las responsabilidades	Existen personas que colaboren con el encargado de la seguridad de la información?	6.1.3. Asignación de responsabilidades relativas a la seguridad de la información.	Alto	5,0	3,0	Voto Impacto	3,0	3,0	3,0
										Voto Vulnerabilidad	5,0	5,0	5,0
R115	Seguridad	Jean Rodríguez	R115	Recursos mal utilizados o imposibilidad de aplicación de controles	Se cuenta con un proceso de autorización de recursos actualmente?	6.1.4. Proceso de autorización de recursos para el tratamiento de la información.	Alto	5,0	4,0	Voto Impacto	4,0	4,0	4,0
										Voto Vulnerabilidad	5,0	5,0	5,0
R116	Seguridad	Jean Rodríguez	R116	Manejo de información sensible por cualquier área	Existen acuerdos de confidencialidad desarrollados	6.1.5. Acuerdos de confidencialidad.	Medio	1,0	4,0	Voto Impacto	4,0	4,0	4,0

	Proceso	Líder de proceso	Tipificación del riesgo	Riesgo Evaluado	Observación	Control relacionado (ISO27002)	Criticidad	Vulnerabilidad	Impacto	Voto/Cargos	Calificación Funcionario 1	Calificación Funcionario 2	Calificación Funcionario 3
					para las diferentes personas que interactúan con la empresa?					Voto Vulnerabilidad	1,0	1,0	1,0
R117	Seguridad	Jean Rodríguez	R117	Desconexión de las entidades que trabajan en relación a la empresa	Se tiene un adecuado contacto con las autoridades que rigen la organización ?	6.1.6. Contacto con las autoridades.	Alto	5,0	3,0	Voto Impacto	3,0	3,0	3,0
										Voto Vulnerabilidad	5,0	5,0	5,0
R118	Seguridad	Jean Rodríguez	R118	Mala aplicación de controles por desconocimiento específico de cada área	Se cuenta con soporte, contacto o algún servicio con empresas técnicas que puedan brindar soluciones oportunas?	6.1.7. Contacto con grupos de especial interés.	Alto	5,0	3,0	Voto Impacto	3,0	3,0	3,0
										Voto Vulnerabilidad	5,0	5,0	5,0
R119	Seguridad	Jean Rodríguez	R119	Desactualización interna del SGSI	Se cuenta con un periodo de revisión de la política por parte de los empleados de la política de seguridad?	6.1.8. Revisión independiente de la seguridad de la información.	Medio	2,0	4,0	Voto Impacto	4,0	4,0	4,0
										Voto Vulnerabilidad	2,0	2,0	2,0
R120	Seguridad	Jean Rodríguez	R120	Mala administración de accesos a terceros	Existe conciencia del riesgo de la entrada de un tercero a la empresa?	6.2.1. Identificación de los riesgos derivados de los accesos de terceros.	Bajo	1,0	2,0	Voto Impacto	2,0	2,0	2,0
										Voto Vulnerabilidad	1,0	1,0	1,0
R121	Seguridad	Jean Rodríguez	R121	Vulnerabilidades externar	Existe un buen nivel de seguridad física, lógica y financiera de los clientes dentro de la empresa?	6.2.2. tratamiento de la seguridad en relación a los clientes.	Bajo	1,0	3,0	Voto Impacto	3,0	3,0	3,0
										Voto Vulnerabilidad	1,0	1,0	1,0
R122	Seguridad	Jean Rodríguez	R122	Acceso a modificaciones internas por medios legales que no sean beneficiosas para la entidad	Se cuenta con una revisión segura de los contratos con terceros, oportuna y rápida para identificar los posibles problemas legales?	6.2.3. tratamiento de la seguridad en contratos con terceros.	Alto	5,0	3,0	Voto Impacto	3,0	3,0	3,0
										Voto Vulnerabilidad	5,0	5,0	5,0
R123	Seguridad	Jean Rodríguez	R123	Pérdida o sustracción de recursos de la entidad	Se tiene conocimiento de todos los activos para usarse en la seguridad de la información así también como los que actúan con los procesos?	7.1.1. Inventario de los activos.	Bajo	1,0	3,0	Voto Impacto	3,0	3,0	3,0
										Voto Vulnerabilidad	1,0	1,0	1,0
R124	Seguridad	Jean Rodríguez	R124	Mal uso de herramientas, adquisición de material ya disponible con anterioridad	Se usan al 100% todas las herramientas ya disponibles dentro de la entidad?	7.1.3. Uso aceptable de los activos.	Alto	4,3	5,0	Voto Impacto	5,0	5,0	5,0
										Voto Vulnerabilidad	4,3	4,3	4,3
R125	Seguridad	Jean Rodríguez	R125	Información mal clasificada a nivel organizacional	Existen protocolos de clasificación de la información para cada área desarrollada por el profesional de seguridad de la información ?	7.2.1. Directrices de clasificación	Alto	5,0	4,0	Voto Impacto	4,0	4,0	4,0
										Voto Vulnerabilidad	5,0	5,0	5,0
R126	Seguridad	Jean Rodríguez	R126	Falta de uniformidad en los el manejo de la información y su etiquetado	Existe protocolos para etiquetar y manipular la información ?	7.2.2. Etiquetado y manipulado de la información.	Alto	5,0	5,0	Voto Impacto	5,0	5,0	5,0
										Voto Vulnerabilidad	5,0	5,0	5,0

	Proceso	Líder de proceso	Tipificación del riesgo	Riesgo Evaluado	Observación	Control relacionado (ISO27002)	Criticidad	Vulnerabilidad	Impacto	Voto/Cargos	Calificación Funcionario 1	Calificación Funcionario 2	Calificación Funcionario 3
R127	Seguridad	Jean Rodríguez	R127	Contratos que no se alineen al SGSI	Existen términos ligados a la seguridad de la información incluidos en un contrato antes del ingreso de la persona?	8.1.3. Términos y condiciones de contratación.	Alto	5,0	4,0	Voto Impacto	4,0	4,0	4,0
										Voto Vulnerabilidad	5,0	5,0	5,0
R128	Seguridad	Jean Rodríguez	R128	Mal uso de la política de seguridad de la información	Existe conciencia organizacional sobre la importancia del uso de una política de seguridad de la información?	8.2.2. Concientización, formación y capacitación sobre la seguridad de la información.	Medio	3,0	4,0	Voto Impacto	4,0	4,0	4,0
										Voto Vulnerabilidad	3,0	3,0	3,0
R129	Seguridad	Jean Rodríguez	R129	Sin sanción los errores se repiten causando vulnerabilidades frecuentes	¿Existen sanciones por no respetar el manual de políticas de seguridad de la información o alguno de sus procesos delegados?	8.2.3. Proceso disciplinario.	Medio	1,0	5,0	Voto Impacto	5,0	5,0	5,0
										Voto Vulnerabilidad	1,0	1,0	1,0
R130	Seguridad	Jean Rodríguez	R130	Al terminar un trabajo, Vulnerabilidad de inicio de sesión de personal antiguo	Existe medidas de seguridad que aseguren que las personas dejen de acceder a cualquier red de la empresa?	8.3.3. Retirada de los derechos de acceso	Medio	1,0	5,0	Voto Impacto	5,0	5,0	5,0
										Voto Vulnerabilidad	1,0	1,0	1,0
R131	Seguridad	Jean Rodríguez	R131	Posibles accidentes y pérdidas de información física o digital	Existe un perímetro seguro para su uso en herramientas de seguridad física, lógica y financiera ?	9.1.1. Perímetro de la seguridad física.	Alto	5,0	5,0	Voto Impacto	5,0	5,0	5,0
										Voto Vulnerabilidad	5,0	5,0	5,0
R132	Seguridad	Jean Rodríguez	R132	Acceso no autorizado a la organización u otras áreas restringidas	Existen controles físicos que aseguren la integridad de la información y brinden seguridad física, lógica y financiera ?	9.1.2. Controles físicos de entrada	Medio	1,0	5,0	Voto Impacto	5,0	5,0	5,0
										Voto Vulnerabilidad	1,0	1,0	1,0
R133	Seguridad	Jean Rodríguez	R133	Ambientes inseguros para los empleados	Todos los ambientes aseguran la seguridad de la información manejada por la empresa así también como de su personal?	9.1.3. Seguridad de oficinas, despachos e instalaciones	Bajo	1,0	3,0	Voto Impacto	3,0	3,0	3,0
										Voto Vulnerabilidad	1,0	1,0	1,0
R134	Seguridad	Jean Rodríguez	R134	Daños colaterales por agentes externos	Existe en consideración eventos externos que puedan afectar a la entidad de alguna manera?	9.1.4. Protección contra las amenazas externas y de origen ambiental.	Medio	3,0	4,0	Voto Impacto	4,0	4,0	4,0
										Voto Vulnerabilidad	3,0	3,0	3,0
R135	Seguridad	Jean Rodríguez	R135	Eventos emergentes consecuentes	Existe un estudio que asegure que el área de funcionamiento sea segura?	9.1.5. Trabajo en áreas seguras.	Alto	4,0	4,0	Voto Impacto	4,0	4,0	4,0
										Voto Vulnerabilidad	4,0	4,0	4,0
R136	Seguridad	Jean Rodríguez	R136	Acceso no autorizado a personal	Existe una correcta designación de áreas de acceso público y laboral?	9.1.6. Áreas de acceso público y de carga y descarga.	Alto	3,0	5,0	Voto Impacto	5,0	5,0	5,0
										Voto Vulnerabilidad	3,0	3,0	3,0
R137	Seguridad	Jean Rodríguez	R137	Fuga de información, pérdida de equipo electrónico de oficina	Existen medidas de seguridad protocolizadas para el		Medio	2,0	4,0	Voto Impacto	4,0	4,0	4,0

	Proceso	Líder de proceso	Tipificación del riesgo	Riesgo Evaluado	Observación	Control relacionado (ISO27002)	Criticidad	Vulnerabilidad	Impacto	Voto/Cargos	Calificación Funcionario 1	Calificación Funcionario 2	Calificación Funcionario 3
					transporte de equipo, uso y devolución ?	9.2.5. Seguridad de los equipos fuera de las instalaciones				Voto Vulnerabilidad	2,0	2,0	2,0
R138	Seguridad	Jean Rodríguez	R138	Información accesible a terceros por mala retirada de material	Existen medidas de destrucción de equipo electrónico o materiales de información salientes de la empresa?	9.2.7. Retirada de los materiales propiedad de la empresa.	Medio	2,0	5,0	Voto Impacto	5,0	5,0	5,0
										Voto Vulnerabilidad	2,0	2,0	2,0
R139	Seguridad	Jean Rodríguez	R139	Aplicación inadecuada de la política de seguridad al manejar mucho flujo de trabajo	Existe delegación de tareas para el control y manejo de la seguridad de la información?	10.1.3. Segregación de tareas.	Bajo	1,0	3,0	Voto Impacto	3,0	3,0	3,0
										Voto Vulnerabilidad	1,0	1,0	1,0
R140	Seguridad	Jean Rodríguez	R140	Se compromete la integridad de los datos así también como el funcionamiento de los procesos	Existe un proceso de implementación de soluciones o cambios sin afectar la línea de producción ?	10.1.4. Separación de los recursos de desarrollo, prueba y operación.	Medio	1,0	5,0	Voto Impacto	5,0	5,0	5,0
										Voto Vulnerabilidad	1,0	1,0	1,0
R141	Seguridad	Jean Rodríguez	R141	Incumplimiento de los acuerdos y contratos con terceros	Existe una manera estándar de supervisar el trabajo de terceros dentro de la empresa?	10.2.2. Supervisión y revisión de los servicios prestados por terceros	Medio	2,0	5,0	Voto Impacto	5,0	5,0	5,0
										Voto Vulnerabilidad	2,0	2,0	2,0
R142	Seguridad	Jean Rodríguez	R142	Malware dentro de los dispositivos de la empresa	Existen controles contra el código malicioso?	10.4.1. Controles contra el código malicioso	Bajo	1,0	3,0	Voto Impacto	3,0	3,0	3,0
										Voto Vulnerabilidad	1,0	1,0	1,0
R143	Seguridad	Jean Rodríguez	R143	Pérdida de la información parcial o total	Existen políticas de copias de seguridad ?	10.5.1. Copias de seguridad de la información	Alto	5,0	5,0	Voto Impacto	5,0	5,0	5,0
										Voto Vulnerabilidad	5,0	5,0	5,0
R144	Seguridad	Jean Rodríguez	R144	Flujo de usuarios no administrados	Existen controles de red vigentes en la coopccp que aseguren la correcta administración de usuarios	10.6.1. Controles de red	Medio	2,0	5,0	Voto Impacto	5,0	5,0	5,0
										Voto Vulnerabilidad	2,0	2,0	2,0
R145	Seguridad	Jean Rodríguez	R145	mala administración de la información	existe protocolos que indiquen cómo manipular la diferente información dentro de redes ?	10.7.3. Procedimiento de manipulación de la información	Medio	1,0	4,5	Voto Impacto	4,5	4,5	4,5
										Voto Vulnerabilidad	1,0	1,0	1,0
R146	Seguridad	Jean Rodríguez	R146	Información falsa tomada como real	Tienen alguna política que asegure que la información intercambiada es verdadera?	10.8.1. Políticas y procedimientos de intercambio de información	Medio	3,0	4,0	Voto Impacto	4,0	4,0	4,0
										Voto Vulnerabilidad	3,0	3,0	3,0
R147	Seguridad	Jean Rodríguez	R147	Información compartida indebidamente, Fuga de información	Se establecen acuerdos con intercambio de información o software con otras empresas ?	10.8.2. Acuerdos de intercambios	Alto	4,0	5,0	Voto Impacto	5,0	5,0	5,0
										Voto Vulnerabilidad	4,0	4,0	4,0
R148	Seguridad	Jean Rodríguez	R148	Política de seguridad estática, sin procesos de mejora	Se cuentan con los registros de auditoria debidamente	10.10.1. Registros de auditoría	Medio	3,0	3,0	Voto Impacto	3,0	3,0	3,0

	Proceso	Líder de proceso	Tipificación del riesgo	Riesgo Evaluado	Observación	Control relacionado (ISO27002)	Criticidad	Vulnerabilidad	Impacto	Voto/Cargos	Calificación Funcionario 1	Calificación Funcionario 2	Calificación Funcionario 3
					organizados para la mejora del SGSI?					Voto Vulnerabilidad	3,0	3,0	3,0
R149	Seguridad	Jean Rodríguez	R149	Modificación de registros de eventos generales	Existe una medida de protección de registros generales de la COOPCCP?	10.10.3. Protección de la información de los registros	Medio	2,0	4,0	Voto Impacto	4,0	4,0	4,0
										Voto Vulnerabilidad	2,0	2,0	2,0
R150	Seguridad	Jean Rodríguez	R150	Falta de notificación de faltas a la seguridad de la información	Existe un registro de fallos físico y digital en la empresa?	10.10.5. Registro de fallos.	Alto	5,0	5,0	Voto Impacto	5,0	5,0	5,0
										Voto Vulnerabilidad	5,0	5,0	5,0
R151	Seguridad	Jean Rodríguez	R151	Errores en redes	Se encuentran sincronizados todos los relojes de la empresa ?	10.10.6 Sincronización de reloj	Medio	1,0	4,0	Voto Impacto	4,0	4,0	4,0
										Voto Vulnerabilidad	1,0	1,0	1,0
R152	Seguridad	Jean Rodríguez	R152	Acceso de personal no autorizado	Existen políticas de control de acceso para todas las áreas organizacionales?	11.1.1. Políticas de control de acceso.	Medio	2,0	4,0	Voto Impacto	4,0	4,0	4,0
										Voto Vulnerabilidad	2,0	2,0	2,0
R153	Seguridad	Jean Rodríguez	R153	Usuarios sin registro de actividad	Se deben registrar todos los usuarios que ingresen a un medio de información físico o lógico	11.2.1. Registro de usuarios	Medio	3,0	4,0	Voto Impacto	4,0	4,0	4,0
										Voto Vulnerabilidad	3,0	3,0	3,0
R154	Seguridad	Jean Rodríguez	R154	Usuarios con accesos no administrados	Se debe contar con una correcta administración de privilegios de las personas dentro de la red	11.2.2. Gestión de privilegios	Medio	3,0	4,0	Voto Impacto	4,0	4,0	4,0
										Voto Vulnerabilidad	3,0	3,0	3,0
R155	Seguridad	Jean Rodríguez	R155	Mala gestión de contraseñas	Se debe controlar la gestión de contraseñas a los usuarios de la red	11.2.3. Gestión de contraseñas	Medio	4,0	3,0	Voto Impacto	3,0	3,0	3,0
										Voto Vulnerabilidad	4,0	4,0	4,0
R156	Seguridad	Jean Rodríguez	R156	Información variada mal organizada, vulnerabilidades en el acceso	Consideran importante una política de puesto de trabajo despejado?	11.3.3. Política de puesto de trabajo despejado y pantalla limpia	Alto	5,0	5,0	Voto Impacto	5,0	5,0	5,0
										Voto Vulnerabilidad	5,0	5,0	5,0
R157	Seguridad	Jean Rodríguez	R157	Accesos no administrados de usuarios	Se deben administrar todas las conexiones de usuarios a la red	11.4.2. Autenticación de usuario para conexiones externas	Medio	3,0	4,0	Voto Impacto	4,0	4,0	4,0
										Voto Vulnerabilidad	3,0	3,0	3,0
R158	Seguridad	Jean Rodríguez	R158	Contraseñas sin esquema de seguridad	Se tiene una manera de generar una contraseña segura para cada persona en la coopccp?	11.5.3. Sistemas de gestión de contraseñas	Medio	4,0	3,0	Voto Impacto	3,0	3,0	3,0
										Voto Vulnerabilidad	4,0	4,0	4,0
R159	Seguridad	Jean Rodríguez	R159	Comunicaciones móviles no administradas	Existen políticas de equipos Wireless?	11.7.1. Ordenadores portátiles y	Medio	1,0	4,0	Voto Impacto	4,0	4,0	4,0

	Proceso	Líder de proceso	Tipificación del riesgo	Riesgo Evaluado	Observación	Control relacionado (ISO27002)	Criticidad	Vulnerabilidad	Impacto	Voto/Cargos	Calificación Funcionario 1	Calificación Funcionario 2	Calificación Funcionario 3
						comunicaciones móviles				Voto Vulnerabilidad	1,0	1,0	1,0
R160	Seguridad	Jean Rodríguez	R160	Adquisiciones erróneas de equipo dedicado	Existe un análisis profesional para los equipos a adquirirse ?	12.1.1 Análisis y especificación de los requisitos de seguridad	Alto	5,0	5,0	Voto Impacto	5,0	5,0	5,0
										Voto Vulnerabilidad	5,0	5,0	5,0
R161	Seguridad	Jean Rodríguez	R161	Información errónea	Se necesita asegurar en todo momento la integridad de los mensajes dentro de la coopccp	12.2.3. Integridad de los mensajes.	Medio	3,0	4,0	Voto Impacto	4,0	4,0	4,0
										Voto Vulnerabilidad	3,0	3,0	3,0
R162	Seguridad	Jean Rodríguez	R162	Información sensible sin tratar	Se cuenta con controles criptográficos en información importante?	12.3.1. Política de controles criptográficos	Alto	5,0	5,0	Voto Impacto	5,0	5,0	5,0
										Voto Vulnerabilidad	5,0	5,0	5,0
R163	Seguridad	Jean Rodríguez	R163	Claves débiles	Existe una manera de gestionar claves de acceso fuertes para todo el personal?	12.3.2. Gestión de claves	Alto	3,0	5,0	Voto Impacto	5,0	5,0	5,0
										Voto Vulnerabilidad	3,0	3,0	3,0
R164	Seguridad	Jean Rodríguez	R164	Posibles fugas de información	Existe un control de software en uso denominado "Core Bancario" ?	12.4.1 Control de software en explotación	Alto	5,0	4,0	Voto Impacto	4,0	4,0	4,0
										Voto Vulnerabilidad	5,0	5,0	5,0
R165	Seguridad	Jean Rodríguez	R165	Infiltración de datos, modificación íntegra de información	Existen controles de acceso administrados por el personal de seguridad para asegurar la integridad del software usado?	12.4.3. Control de acceso al código fuente de los programas	Alto	3,0	5,0	Voto Impacto	5,0	5,0	5,0
										Voto Vulnerabilidad	3,0	3,0	3,0
R166	Seguridad	Jean Rodríguez	R166	Problemas en los procesos	Existen controles técnicos para las diferentes áreas?	12.6.1. Control de las vulnerabilidades técnicas	Medio	1,0	4,0	Voto Impacto	4,0	4,0	4,0
										Voto Vulnerabilidad	1,0	1,0	1,0
R167	Seguridad	Jean Rodríguez	R167	Política de seguridad sin cumplir	Constan de algún medio físico y digital de notar los eventos de seguridad de la información ?	13.1.1. Notificación de los eventos de seguridad de la información.	Alto	5,0	4,0	Voto Impacto	4,0	4,0	4,0
										Voto Vulnerabilidad	5,0	5,0	5,0
R168	Seguridad	Jean Rodríguez	R168	Política de seguridad sin cumplir	Constan de algún medio físico y digital de notar los puntos débiles de la seguridad de la información ?	13.1.2. Notificación de los puntos débiles de seguridad	Alto	5,0	4,0	Voto Impacto	4,0	4,0	4,0
										Voto Vulnerabilidad	5,0	5,0	5,0
R169	Seguridad	Jean Rodríguez	R169	Falta de responsable de cumplimiento	Existen delegados formalmente los responsables sobre los procedimientos en los eventos de seguridad de la información?	13.2.1. Responsables y procedimientos	Alto	4,5	4,5	Voto Impacto	4,5	4,5	4,5
										Voto Vulnerabilidad	4,5	4,5	4,5
R170	Seguridad	Jean Rodríguez	R170	Falta de información para mejora continua		13.2.3. Recopilación de evidencias	Alto	5,0	4,0	Voto Impacto	4,0	4,0	4,0

	Proceso	Líder de proceso	Tipificación del riesgo	Riesgo Evaluado	Observación	Control relacionado (ISO27002)	Criticidad	Vulnerabilidad	Impacto	Voto/Cargos	Calificación Funcionario 1	Calificación Funcionario 2	Calificación Funcionario 3
					Se tiene un método de recopilación de evidencias tras un evento emergente?					Voto Vulnerabilidad	5,0	5,0	5,0
R171	Seguridad	Jean Rodríguez	R171	Política de seguridad estática, sin procesos de mejora	Se cuenta con una herramienta de control de auditoría para evaluaciones constantes?	15.3.1. Controles de auditoría de los sistemas de información	Medio	2,0	5,0	Voto Impacto	5,0	5,0	5,0
										Voto Vulnerabilidad	2,0	2,0	2,0

Figura 10: Análisis de Riesgos Vigente COOPCCP
Elaborado por: Jean P. Rodríguez.

Una vez terminada la tabulación se realizó un diccionario de controles a aplicar incluyendo una topología de red y pasos a implementar según buenas prácticas de seguridad de la información para el cumplimiento normativo y la mejora de nivel de seguridad informática.

3.4.9.3 Servicios transaccionales disponibles y en desarrollo:

Anteriormente la SEPS no contaba con normativas que se encarguen de la regulación sobre el uso y disposición de medidas de seguridad en servicios transaccionales ofrecidos al público, motivo por el cual en noviembre de 2017 dieron plazo de 1 año para regularizar los documentos para la operación de dichos servicios. COOPCCP fue notificada en el mismo mes sobre su ascenso al segmento 1 de Cooperativas y Mutualistas reguladas por la SEPS, por lo que tiene un periodo de 2 años con corte a noviembre de 2019 para realizar dicha regularización. Por tal motivo, los requisitos para el cumplimiento aplican para los servicios ya disponibles y aquellos que se encuentran en desarrollo según la Planificación Estratégica Institucional de la COOPCCP. Dichos servicios son:

- **Tarjeta de débito:** La COOPCCP es miembro secundario de la Cooperativa Policía Nacional quien es miembro principal de la franquicia MASTERCARD y por medio de ellos, las tarjetas emitidas en COOPCCP respaldan su uso en dicha franquicia. Para lograrlo, tecnológicamente la Cooperativa está anclada a CAPTEC S.A. Empresa dedicada únicamente al **procesamiento de las transacciones** efectuadas por compras en dispositivos POS, retiro de cajeros automáticos y compras por Internet. CAPTEC procesa directamente los datos entregados por el POS en compras ya que el organismo autorizador mantiene comunicación directa con MASTERCARD, por otro lado, el servicio del canal de comunicación y enlace en retiros por medio de un ATM es manejado por el canal COONECTA quien entrega la información para ser posteriormente procesada por CAPTEC.

- ***Web Services:*** Se llevó a cabo el proceso de actualización de la plataforma de comunicación con SERVIPAGOS y el BANCO CENTRAL DEL ECUADOR, las comunicaciones desarrolladas con estas instituciones son vitales para continuar ofreciendo el servicio de pagos en ventanillas de extensión Servipagos y el servicio de pagos y cobros interbancarios. El desarrollo se realiza con la empresa CLOUD STUDIO, quienes entregarán los códigos fuentes a COOPCCP para su autogestión.
- **IVR Transaccional:** Desarrollado por la empresa Can&T, la COOPCCP cuenta con el servicio de consulta de saldos y bloqueo de tarjetas vía telefónica, sistema vigente desde el año 2015. Es necesario tomar en cuenta que, para el funcionamiento y actualización de este servicio se requería cambiar algunos puntos de normativa interna y enlaces de comunicación.
- **Cooperativa en Línea:** Montándose a la transformación digital, la COOPCCP inició el proyecto de implementación de un sistema en línea junto al modelo de economía a escala ofertado por FINANCOOP, sistema que permitirá realizar transferencias internas, interbancarias o directas, pago de servicios programados, entre otros.
- **ChatBots Transaccionales:** Uno de los primeros servicios para socios y clientes que permita el intercambio de la información aprovechando el uso de startups como la empresa MENSAJEA.
- **Billetera Móvil:** La COOPCCP se encuentra en vías de adicionar este nuevo proyecto llevado en Ecuador por BANRED. La billetera digital llamada BIMO contará para su lanzamiento con un abanico de instituciones que acepten este nuevo modelo de manejo de dinero en las cuentas bancarias y de cooperativas que van atados a un número de celular y permiten realizar micro transacciones.
- **Servicios 24/7:** Al proporcionar cualquiera de los servicios mencionados anteriormente es necesario contar con un centro de atención y respuestas de

emergencias, que puede ser directamente con funcionarios de la Cooperativa o manejado por terceros, sin embargo, es necesario tener en cuenta que, para efectuar consultas, cambios de estado o posición de fondos, es requerido realizar un proceso de seguridad de la información para cuidar el sigilo financiero.

3.4.3 Revisión de documentos, manuales, informes y auditorías vigentes:

Es importante realizar una recopilación de todos los documentos que se encuentren vigentes en la institución que tenga relación con la matriz de riesgos, que incluye riesgo informático, activos de la información, aplicación de la política de seguridad de la información, cumplimiento de procesos, accesos y permisos por tipos de usuarios, informes y reportes de eventos de riesgos realizados, informes de auditoría interna y externa, prueba de penetración de vulnerabilidades, gestión de proyectos tecnológicos, plan de recuperación de desastres, entre otros que se encuentren relacionados a eventos, cumplimiento y normativas que se encuentren documentadas.

3.4.3.1 Política de seguridad de la información

El siguiente punto fue verificar las políticas de seguridad de la información vigentes, de las cuales se realizó el análisis que permitió desarrollar cambios sugeridos para el área de riesgos sobre dicho documento que contemple el tratamiento sobre eventos de riesgo y controles llevados de manera periódica para el mantenimiento y gestión de los servicios transaccionales que se encuentran en desarrollo y producción dentro de la Cooperativa. A continuación se muestra un extracto de la política de los puntos destacados:

OBJETIVO

El objetivo de este documento es establecer las normas en seguridad de la información de la COOPCCP, con el fin de regular la gestión de la seguridad de la información al interior de la Entidad.

ALCANCE

Las normas de seguridad de la información cubren todos los aspectos administrativos y de control que deben ser cumplidos por los directivos, funcionarios y terceros que tengan relación con la COOPCCP, para conseguir un adecuado nivel de protección de las características de seguridad de la información.

NORMATIVA LEGAL

Este documento describe las normas de seguridad de la información definidas por la COOPCCP. Para la elaboración del mismo, se toman como base las leyes y demás regulaciones aplicables en la resolución No JB-2005-834 SECCIÓN VII.- SEGURIDAD DE LA INFORMACIÓN (incluida con resolución No. JB-2014-3066, la norma ISO 27001:2013 y las recomendaciones del estándar ISO 27002:2013.
Se incluye también las disposiciones contenidas en el Artículo 225 del Código Orgánico Monetario y Financiero.

RESPONSABILIDADES DE LOS FUNCIONARIOS Y USUARIOS FINALES

1. Manejar la información de la institución con responsabilidad mientras que este bajo su custodia.
2. Proteger la información a la cual accedan y procesen, para evitar su pérdida, alteración, destrucción o uso indebido mientras que este bajo su custodia.
3. Evitar la divulgación no autorizada o el uso indebido de la información.
4. Cumplir con todos los controles y políticas establecidos por la COOPCCP.
5. Informar a sus superiores sobre la violación de estas políticas o si conocen de alguna falta a alguna de ellas.
6. Proteger los datos almacenados en los equipos de cómputo y sistemas de información a su disposición de la destrucción o alteración intencional o no justificada y de la divulgación no autorizada.
7. Reportar los Incidentes de seguridad, eventos sospechosos y el mal uso de los recursos que se identifique.
8. Proteger los equipos de cómputo, de comunicaciones y demás dispositivos tecnológicos designados para el desarrollo de sus funciones.
9. No está permitida la conexión de equipos de cómputo y de comunicaciones ajenos al instituto al a red Institucional.
10. No está permitida el uso de dispositivos de acceso externo a Internet o de difusión de señales de red que no hayan sido previamente autorizadas por la Oficina de Seguridades de la Información.
11. Usar software autorizado que haya sido adquirido legalmente por la Institución. No está permitido la instalación ni uso de software diferente al Institucional sin el consentimiento del Oficial de Seguridad de la Información.
12. Proteger y resguardar su información personal que no esté relacionada con sus funciones en la Institución. La COOPCCP no es responsable por la pérdida de información, desfalco o daño que pueda tener un usuario al brindar y hacer uso de la información personal dentro de las instalaciones de institución.

POLÍTICAS

POLÍTICAS GENERALES

13. El Comité de Riesgos tendrá a cargo el mantenimiento y la presentación para la aprobación de la Política de Seguridad de la Información ante el Consejo de Administración.
14. El Oficial de Seguridad de la Información se encargará de: análisis de riesgos, monitoreo de incidentes, implementación de controles y actividades de concientización.
15. El Comité de Riesgos se encargará del seguimiento trimestral de las actividades relativas a la seguridad de la información.
16. Cualquier acción que comprometa la información o cualquiera de sus activos de la información, se considerará como falta grave y se aplicará la sanción respectiva en base al reglamento interno de trabajo.
17. La Oficina de Riesgos debe liderar la generación de lineamientos para gestionar la seguridad de la información de COOPCCP y establecer controles técnicos, físicos y administrativos derivados de análisis de riesgos de seguridad.
18. La Oficina de Riesgos debe validar y monitorear de manera periódica la implantación de los controles de seguridad establecidos.
19. El oficial de Seguridad de la Información debe analizar los incidentes de seguridad que le son escalados y activar el procedimiento de control y mitigación, cuando lo estime necesario.
20. El Comité de Riesgos de debe verificar el cumplimiento de las políticas de seguridad de la información aquí mencionadas
21. El área de Talento Humano debe certificar que los funcionarios de la cooperativa firmen un acuerdo y/o cláusula de Confidencialidad, así un documento de creación de usuario y permiso acceso a los sistemas.
22. El Oficial de Seguridad de la información debe revisar mensualmente la documentación para la creación, actualización y eliminación de usuarios.
23. El Oficial de Seguridad de la información debe revisar trimestralmente las políticas vigentes del Firewall y de ser necesario o según lo amerite establecerá nuevas políticas.
24. El Oficial de Seguridad de la Información realizará semestralmente un control y depuración de los usuarios en los aplicativos de la institución.

POLÍTICAS DE CONTROL DE ACCESO A LA INFORMACIÓN

1. El Oficial de Seguridad de la Información debe establecer los requerimientos y criterios para la clasificación de los activos de información.
2. Los Responsables de los Procesos son los propietarios de la información física y electrónica del área a su cargo, ejerciendo así la facultad de aprobar o revocar el acceso a la información con los perfiles adecuados para tal fin.
3. Los Responsables de los Procesos deben generar un inventario de dichos activos para las áreas o procesos que lideran, acogiendo las indicaciones de las guías de clasificación de la información; así mismo, deben mantener actualizado el inventario de sus activos de información.
4. Los Responsables de los Procesos deben monitorear anualmente la validez de los usuarios y sus perfiles de acceso a la información.
5. Los Responsables de los Procesos deben recibir los recursos tecnológicos asignados a sus colaboradores cuando estos se retiran de la Entidad o son trasladados de área., en base a lo estipulado en el manual de Talento Humano.

Figura 11: Extracto de la política de seguridad de la información vigente
Elaborado por COOPCCP (2019).

3.4.3.2 Aplicaciones informáticas del negocio y acceso de usuario

La Cooperativa tiene a su disposición tres (3) tipos de software importantes sobre los cuales se realiza la gestión y operatividad de los servicios transaccionales vigentes y estos corresponden a CORE financiero, herramientas de gestión de tarjetas y herramienta de gestor documental.

El Core financiero de la COOPCCP se puso en marcha el 12 de marzo de 2018, fecha en la cual, para la definición de controles de acceso se realizaron reuniones con el proveedor y según la política de seguridad se realizó la prueba de los controles iniciales de la pantalla de inicio para cumplir con las políticas de acceso y para la definición de perfiles, se realizaron reuniones con los jefes de procesos y jefes de área. El levantamiento preliminar fue vigente hasta finalizar el periodo de estabilidad del Core en septiembre de 2018 sin embargo, el plazo se vio extendido hasta que el sistema cubra todas las necesidades de negocio, encontrándose abierto hasta la presentación del proyecto. A continuación, se presenta la pantalla inicial de definición de perfiles para el Core Financiero. Para esto se realizó un barrido de todas las opciones disponibles en el Core y se cotejó con respecto a las funciones que realizan según el manual de funciones. Se presenta un extracto del índice y los perfiles definidos para el área de Seguridad, Auditoría, Operaciones.

Descripción:	Resumen de Usuarios creados con perfiles			
Fecha Corte:	10 de Marzo 2018			
Jefes de Oficina				
perfil	**oficina**	**login**	**usuario**	**cargo**
JEFE DE OFICINA	AGENCIA - B DE CARAQUEZ	##########	##########	JEFE DE OFICINA
JEFE DE OFICINA	AGENCIA - ISABELA	##########	##########	JEFE DE OFICINA
JEFE DE OFICINA	AGENCIA - LAGO AGRIO	##########	##########	JEFE DE OFICINA
JEFE DE OFICINA	AGENCIA - LOJA	##########	##########	JEFE DE OFICINA

JEFE DE OFICINA	AGENCIA - MANTA	##########	##########	JEFE DE OFICINA
JEFE DE OFICINA	AGENCIA - MILAGRO	##########	##########	JEFE DE OFICINA
JEFE DE OFICINA	AGENCIA - GUAYAQUIL	##########	##########	JEFE DE OFICINA
JEFE DE OFICINA	AGENCIA - PEDERNALES	##########	##########	JEFE DE OFICINA
JEFE DE OFICINA	AGENCIA - SAN CRISTOBAL	##########	##########	JEFE DE OFICINA
JEFE DE OFICINA	AGENCIA - STA. CRUZ	##########	##########	JEFE DE OFICINA
JEFE DE OFICINA	AGENCIA - TULCAN	##########	##########	JEFE DE OFICINA
JEFE DE OFICINA	AGENCIA - UIO NORTE	##########	##########	JEFE DE OFICINA
JEFE DE OFICINA	AGENCIA - UIO SUR	##########	##########	JEFE DE OFICINA
JEFE DE OFICINA	AGENCIA . UIO CENTRO	##########	##########	JEFE DE OFICINA
JEFE DE OFICINA	SUCURSAL MATRIZ - QUITO	##########	##########	JEFE DE OFICINA
Asistentes de Oficina				
ASISTENTE DE OFICINA	AGENCIA - B DE CARAQUEZ	##########	##########	RECIBIDOR PAGADOR
ASISTENTE DE OFICINA	AGENCIA - GUAYAQUIL	##########	##########	ASISTENTE DE OFICINA
ASISTENTE DE OFICINA	AGENCIA - ISABELA	##########	##########	ASISTENTE DE OFICINA
ASISTENTE DE OFICINA	AGENCIA - LAGO AGRIO	##########	##########	ASISTENTE DE OFICINA
ASISTENTE DE OFICINA	AGENCIA - LOJA	##########	##########	ASISTENTE DE OFICINA
ASISTENTE DE OFICINA	AGENCIA - MANTA	##########	##########	ASISTENTE DE OFICINA
ASISTENTE DE OFICINA	AGENCIA - MILAGRO	##########	##########	ASISTENTE DE OFICINA
ASISTENTE DE OFICINA	AGENCIA - PEDERNALES	##########	##########	ASISTENTE DE OFICINA
ASISTENTE DE OFICINA	AGENCIA - SAN CRISTOBAL	##########	##########	ASISTENTE DE OFICINA
ASISTENTE DE OFICINA	AGENCIA - STA. CRUZ	##########	##########	ASISTENTE DE OFICINA
ASISTENTE DE OFICINA	AGENCIA - TULCAN	##########	##########	ASISTENTE DE OFICINA
ASISTENTE DE OFICINA	AGENCIA - UIO NORTE	##########	##########	ASISTENTE DE OFICINA
ASISTENTE DE OFICINA	AGENCIA - UIO SUR	##########	##########	ASISTENTE DE OFICINA
ASISTENTE DE OFICINA	AGENCIA . UIO CENTRO	##########	##########	ASISTENTE DE OFICINA
ASISTENTE DE OFICINA	SUCURSAL MATRIZ - QUITO	##########	##########	ASISTENTE DE OFICINA
Administradores de Bóveda				
BOVEDA ADMINISTRACION	AGENCIA - B DE CARAQUEZ	##########	##########	SUPERVISORA DE CAJAS
BOVEDA ADMINISTRACION	AGENCIA - GUAYAQUIL	##########	##########	ASISTENTE DE OFICINA
BOVEDA ADMINISTRACION	AGENCIA – ISABELA	##########	##########	ASISTENTE DE OFICINA
BOVEDA ADMINISTRACION	AGENCIA - LAGO AGRIO	##########	##########	ASISTENTE DE OFICINA
BOVEDA ADMINISTRACION	AGENCIA - LOJA	##########	##########	ASISTENTE DE OFICINA
BOVEDA ADMINISTRACION	AGENCIA – MANTA	##########	##########	ASISTENTE DE OFICINA
BOVEDA ADMINISTRACION	AGENCIA – MILAGRO	##########	##########	ASISTENTE DE OFICINA

BOVEDA ADMINISTRACION	AGENCIA - PEDERNALES	##########	##########	ASISTENTE DE OFICINA
BOVEDA ADMINISTRACION	AGENCIA - SAN CRISTOBAL	##########	##########	ASISTENTE DE OFICINA
BOVEDA ADMINISTRACION	AGENCIA - STA. CRUZ	##########	##########	ASISTENTE DE OFICINA
BOVEDA ADMINISTRACION	AGENCIA – TULCAN	##########	##########	ASISTENTE DE OFICINA
BOVEDA ADMINISTRACION	AGENCIA - UIO NORTE	##########	##########	ASISTENTE DE OFICINA
BOVEDA ADMINISTRACION	AGENCIA - UIO SUR	##########	##########	ASISTENTE DE OFICINA
BOVEDA ADMINISTRACION	AGENCIA . UIO CENTRO	##########	##########	ASISTENTE DE OFICINA
BOVEDA ADMINISTRACION	SUCURSAL MATRIZ - QUITO	##########	##########	ASISTENTE DE OFICINA
BOVEDA ADMINISTRACION	VENT. EXT UIO GUAMANI	##########	##########	SUPERVISORA DE CAJAS
Oficiales de Negocio				
OFICIAL DE NEGOCIOS	AGENCIA - B DE CARAQUEZ	##########	##########	JEFE DE OFICINA
OFICIAL DE NEGOCIOS	AGENCIA - B DE CARAQUEZ	##########	##########	OFICIAL DE NEGOCIOS
OFICIAL DE NEGOCIOS	AGENCIA - GUAYAQUIL	##########	##########	OFICIAL DE NEGOCIOS
OFICIAL DE NEGOCIOS	AGENCIA - GUAYAQUIL	##########	##########	OFICIAL DE NEGOCIOS
OFICIAL DE NEGOCIOS	AGENCIA – ISABELA	##########	##########	OFICIAL DE NEGOCIOS
OFICIAL DE NEGOCIOS	AGENCIA - LAGO AGRIO	##########	##########	OFICIAL DE NEGOCIOS
OFICIAL DE NEGOCIOS	AGENCIA - LOJA	##########	##########	OFICIAL DE NEGOCIOS
OFICIAL DE NEGOCIOS	AGENCIA - LOJA	##########	##########	OFICIAL DE NEGOCIOS
OFICIAL DE NEGOCIOS	AGENCIA - LOJA	##########	##########	ASISTENTE DE INVERSIONES Y SERVICIO AL CLIENTE
OFICIAL DE NEGOCIOS	AGENCIA - LOJA	##########	##########	OFICIAL DE NEGOCIOS
OFICIAL DE NEGOCIOS	AGENCIA – MANTA	##########	##########	OFICIAL DE NEGOCIOS
OFICIAL DE NEGOCIOS	AGENCIA – MANTA	##########	##########	OFICIAL DE NEGOCIOS
OFICIAL DE NEGOCIOS	AGENCIA - PEDERNALES	##########	##########	OFICIAL DE NEGOCIOS
OFICIAL DE NEGOCIOS	AGENCIA - PEDERNALES	##########	##########	OFICIAL DE NEGOCIOS
OFICIAL DE NEGOCIOS	AGENCIA - SAN CRISTOBAL	##########	##########	JEFE DE OFICINA
OFICIAL DE NEGOCIOS	AGENCIA - SAN CRISTOBAL	##########	##########	OFICIAL DE NEGOCIOS
OFICIAL DE NEGOCIOS	AGENCIA - STA. CRUZ	##########	##########	OFICIAL DE NEGOCIOS
OFICIAL DE NEGOCIOS	AGENCIA - STA. CRUZ	##########	##########	OFICIAL DE NEGOCIOS
OFICIAL DE NEGOCIOS	AGENCIA – TULCAN	##########	##########	OFICIAL DE NEGOCIOS
OFICIAL DE NEGOCIOS	AGENCIA - UIO NORTE	##########	##########	OFICIAL DE NEGOCIOS (ROTATIVA)
OFICIAL DE NEGOCIOS	AGENCIA - UIO NORTE	##########	##########	OFICIAL DE NEGOCIOS
OFICIAL DE NEGOCIOS	AGENCIA - UIO SUR	##########	##########	OFICIAL DE NEGOCIOS
OFICIAL DE NEGOCIOS	AGENCIA - UIO SUR	##########	##########	OFICIAL DE NEGOCIOS
OFICIAL DE NEGOCIOS	AGENCIA - UIO SUR	##########	##########	OFICIAL DE NEGOCIOS
OFICIAL DE NEGOCIOS	AGENCIA . UIO CENTRO	##########	##########	OFICIAL DE NEGOCIOS

OFICIAL DE NEGOCIOS	SUCURSAL MATRIZ - QUITO	##########	##########	OFICIAL DE NEGOCIOS
OFICIAL DE NEGOCIOS	SUCURSAL MATRIZ - QUITO	##########	##########	OFICIAL DE NEGOCIOS
OFICIAL DE NEGOCIOS	SUCURSAL MATRIZ - QUITO	##########	##########	OFICIAL DE NEGOCIOS
OFICIAL DE NEGOCIOS	SUCURSAL MATRIZ - QUITO	##########	##########	OFICIAL DE INVERSIONES
Oficiales de Inversiones				
OFICIAL DE INVERSIONES	AGENCIA - LOJA	##########	##########	ASISTENTE DE INVERSIONES Y SERVICIO AL CLIENTE
Recibidor - Pagador				
RECIBIDOR - PAGADOR	AGENCIA - B DE CARAQUEZ	##########	##########	RECIBIDOR PAGADOR
RECIBIDOR - PAGADOR	AGENCIA - B DE CARAQUEZ	##########	##########	RECIBIDOR PAGADOR
RECIBIDOR - PAGADOR	AGENCIA - GUAYAQUIL	##########	##########	RECIBIDOR PAGADOR
RECIBIDOR - PAGADOR	AGENCIA - GUAYAQUIL	##########	##########	ASISTENTE DE OFICINA
RECIBIDOR - PAGADOR	AGENCIA - ISABELA	##########	##########	ASISTENTE DE OFICINA
RECIBIDOR - PAGADOR	AGENCIA - ISABELA	##########	##########	RECIBIDOR PAGADOR
RECIBIDOR - PAGADOR	AGENCIA - ISABELA	##########	##########	RECIBIDOR PAGADOR
RECIBIDOR - PAGADOR	AGENCIA - LAGO AGRIO	##########	##########	RECIBIDOR PAGADOR
RECIBIDOR - PAGADOR	AGENCIA - LAGO AGRIO	##########	##########	ASISTENTE DE OFICINA
RECIBIDOR - PAGADOR	AGENCIA - LOJA	##########	##########	ASISTENTE DE OFICINA
RECIBIDOR - PAGADOR	AGENCIA - LOJA	##########	##########	RECIBIDOR PAGADOR
RECIBIDOR - PAGADOR	AGENCIA - MANTA	##########	##########	ASISTENTE DE OFICINA
RECIBIDOR - PAGADOR	AGENCIA - MANTA	##########	##########	RECIBIDOR PAGADOR
RECIBIDOR - PAGADOR	AGENCIA - MILAGRO	##########	##########	RECIBIDOR PAGADOR
RECIBIDOR - PAGADOR	AGENCIA - PEDERNALES	##########	##########	RECIBIDOR PAGADOR
RECIBIDOR - PAGADOR	AGENCIA - SAN CRISTOBAL	##########	##########	RECIBIDOR PAGADOR
RECIBIDOR - PAGADOR	AGENCIA - STA. CRUZ	##########	##########	RECIBIDOR PAGADOR
RECIBIDOR - PAGADOR	AGENCIA - STA. CRUZ	##########	##########	RECIBIDOR PAGADOR
RECIBIDOR - PAGADOR	AGENCIA - STA. CRUZ	##########	##########	ASISTENTE DE OFICINA
RECIBIDOR - PAGADOR	AGENCIA - TULCAN	##########	##########	RECIBIDOR PAGADOR
RECIBIDOR - PAGADOR	AGENCIA - UIO NORTE	##########	##########	RECIBIDOR PAGADOR
RECIBIDOR - PAGADOR	AGENCIA - UIO SUR	##########	##########	RECIBIDOR PAGADOR
RECIBIDOR - PAGADOR	AGENCIA . UIO CENTRO	##########	##########	RECIBIDOR PAGADOR
RECIBIDOR - PAGADOR	SUCURSAL MATRIZ - QUITO	##########	##########	RECIBIDOR PAGADOR
RECIBIDOR - PAGADOR	SUCURSAL MATRIZ - QUITO	##########	##########	ADMIN
RECIBIDOR - PAGADOR	SUCURSAL MATRIZ - QUITO	##########	##########	ASISTENTE DE OFICINA
RECIBIDOR - PAGADOR	VENT. EXT UIO GUAMANI	##########	##########	RECIBIDOR PAGADOR
Asesor Legal				
ASESOR LEGAL	SUCURSAL MATRIZ - QUITO	##########	##########	ASESOR LEGAL

Abogado de Cobranzas				
		##########	##########	
Asistente Legal				
ASISTENTE LEGAL	SUCURSAL MATRIZ - QUITO	##########	##########	ASISTENTE LEGAL
Auxiliar Legal				
AUXILIAR LEGAL	SUCURSAL MATRIZ - QUITO	##########	##########	AUXILIAR LEGAL
Coordinador de la Unidad de Procesamiento de Crédito				
COORDINADOR UNIDAD PROCESAMIENTO DE CRÉDITO	SUCURSAL MATRIZ - QUITO	##########	##########	COORDINADOR UNIDAD PROCESAMIENTO DE CREDITOS
Verificador - Digitador				
		##########	##########	
Verificador Telefónico				
VERIFICADOR TELEFONICO	SUCURSAL MATRIZ - QUITO	##########	##########	VERIFICADOR-DIGITADOR
VERIFICADOR TELEFONICO	SUCURSAL MATRIZ - QUITO	##########	##########	VERIFICADOR-DIGITADOR
Coordinador de Cobranza				
COORDINADOR DE COBRANZAS	SUCURSAL MATRIZ - QUITO	##########	##########	COORDINADOR DE COBRANZAS
Jefe Comercial				
JEFE COMERCIAL	SUCURSAL MATRIZ - QUITO	##########	##########	JEFE COMERCIAL
Oficial de Marketing				
OFICIAL DE MARKETING	SUCURSAL MATRIZ - QUITO	##########	##########	OFICIAL DE MARKETING
Oficial de Seguridades físicas				
OFICIAL DE SEGURIDADES FISICAS	SUCURSAL MATRIZ - QUITO	##########	##########	JEFE DE OPERACIONES
Jefe de Operaciones				
OFICIAL DE SEGURIDADES FISICAS	SUCURSAL MATRIZ - QUITO	##########	##########	JEFE DE OPERACIONES
JEFE DE OPERACIONES	SUCURSAL MATRIZ - QUITO	##########	##########	ADMIN
Asistente de Operaciones				
ASISTENTE DE OPERACIONES	SUCURSAL MATRIZ - QUITO	##########	##########	ASISTENTE DE OPERACIONES

Tabla 8: Definición General de Perfiles COOPCCP
Elaborado por: (COOPCCP, 2018)

PERFIL AUTORIZADO DEL PERFIL "OFICIAL DE SEGURIDAD DE LA INFORMACIÓN" OSI		
Creado:	Oficial de Seguridad de la Información	
Modificado:	N/A	
Levantado con:	Oficial de Seguridad de la Información	
Revisado por:	Jefe de Riesgos	
Menú	Sub-Menú	Módulo
CAJA	Reporte	##########
CAJA	Parámetros	##########
CAJA	Parámetros	##########
CREDITOS	Parámetros	##########
CAPTACIONES	Parámetros	##########
PARAMETROS	Comunes	##########

PERFIL AUTORIZADO DEL PERFIL "OFICIAL DE SEGURIDAD DE LA INFORMACIÓN" OSI

Creado:	Oficial de Seguridad de la Información	
Modificado:	N/A	
Levantado con:	Oficial de Seguridad de la Información	
Revisado por:	Jefe de Riesgos	
Menú	Sub-Menú	Módulo
PARAMETROS	Comunes	############################
PARAMETROS	Comunes	############################
PARAMETROS	Organización de menú	############################
SEGURIDADES	Sucursales y Oficinas	############################
SEGURIDADES	Sucursales y Oficinas	############################
SEGURIDADES	Sucursales y Oficinas	############################
SEGURIDADES	Sucursales y Oficinas	############################
SEGURIDADES	Usuarios y perfiles	############################
SEGURIDADES	Usuarios y perfiles	############################
SEGURIDADES	Usuarios y perfiles	############################
SEGURIDADES	Usuarios y perfiles	############################
SEGURIDADES	Usuarios y perfiles	############################
SEGURIDADES	Usuarios y perfiles	############################
SEGURIDADES	Usuarios y perfiles	############################
SEGURIDADES	Usuarios y perfiles	############################
SEGURIDADES	Usuarios y perfiles	############################
SEGURIDADES	Dispositivos	############################
SEGURIDADES	Dispositivos	############################
SEGURIDADES	Dispositivos	############################
SEGURIDADES	Permisos	############################
SEGURIDADES	Permisos	############################
SEGURIDADES	Permisos	############################
SEGURIDADES	Auditoria	############################
SEGURIDADES	Auditoria	############################
SEGURIDADES	Auditoria	############################
SEGURIDADES	Auditoria	############################
SEGURIDADES	Inicios de Sesion	############################

PERFIL AUTORIZADO DEL PERFIL "JEFE DE OPERACIONES" JOP

Creado:	Oficial de Seguridad de la Información	
Modificado:	N/A	
Levantado con:	Asistente de Operaciones	
Revisado por:	Alberto Llive	
Menú	Sub-Menú	Módulo
CLIENTES	Mantenimiento	################################
CLIENTES	Mantenimiento	################################
CLIENTES	Mantenimiento	################################
CLIENTES	Mantenimiento	################################
CLIENTES	Mantenimiento	################################
CLIENTES	Mantenimiento	################################
CLIENTES	Mantenimiento	################################
CLIENTES	Mantenimiento	################################
CLIENTES	Documentos Digitales	################################
CLIENTES	Documentos Digitales	################################
CLIENTES	Documentos Digitales	################################
CLIENTES	Documentos Digitales	################################
CLIENTES	Fondo Mortuosio	################################
CLIENTES	Fondo Mortuosio	################################

PERFIL AUTORIZADO DEL PERFIL "JEFE DE OPERACIONES" JOP

Creado:	Oficial de Seguridad de la Información	
Modificado:	N/A	
Levantado con:	Asistente de Operaciones	
Revisado por:	Alberto Llive	
Menú	Sub-Menú	Módulo
CLIENTES	Consultas y Reportes	################################
CLIENTES	Consultas y Reportes	################################
CLIENTES	Consultas y Reportes	################################
CLIENTES	Consultas y Reportes	################################
CLIENTES	Consultas y Reportes	################################
CLIENTES	Consultas y Reportes	################################
CLIENTES	Consultas y Reportes	################################
CLIENTES	Parámetros > Estado Financiero	################################
CLIENTES	Parámetros > Estado Financiero	################################
CLIENTES	Parámetros > Estado Financiero	################################
CLIENTES	Parámetros > Estado Financiero	################################
CLIENTES	Parámetros > Estado Financiero	################################
CLIENTES	Parámetros > Estado Financiero	################################
CLIENTES	Parámetros > Estado Financiero	################################
CLIENTES	Parámetros > Grupos	################################
CLIENTES	Parámetros > Grupos	################################
CLIENTES	Parámetros > Datos Adicionales	################################
CLIENTES	Parámetros > Datos Adicionales	################################
CLIENTES	Parámetros > Datos Adicionales	################################
CLIENTES	Parámetros > Ubicación Geográfica	################################
CLIENTES	Parámetros > Ubicación Geográfica	################################
CLIENTES	Parámetros > Ubicación Geográfica	################################
CLIENTES	Parámetros > Ubicación Geográfica	################################
CLIENTES	Parámetros > Ubicación Geográfica	################################
CLIENTES	Parámetros > Fondo Mortuorio	################################
CLIENTES	Parámetros > Fondo Mortuorio	################################
CLIENTES	Parámetros	################################
CLIENTES	Parámetros	################################
CLIENTES	Parámetros	################################
CLIENTES	Parámetros	################################
CLIENTES	Parámetros	################################
CLIENTES	Parámetros	################################
CLIENTES	Parámetros	################################
CLIENTES	Parámetros	################################
CLIENTES	Parámetros	################################
CLIENTES	Parámetros	################################
CLIENTES	Parámetros	################################
CLIENTES	Parámetros	################################
CLIENTES	Parámetros	################################
CLIENTES	Parámetros	################################

PERFIL AUTORIZADO DEL PERFIL "AUDITOR INTERNO" AUD		
Creado:	Oficial de Seguridad de la Información	
Modificado:	N/A	
Levantado con:	UAI	
Revisado por:	UAI	
Menú	Sub-Menú	Módulo
CLIENTES	Consultas y Reportes	##############################
CLIENTES	Consultas y Reportes	##############################
CLIENTES	Consultas y Reportes	##############################
CLIENTES	Consultas y Reportes	##############################
CLIENTES	Consultas y Reportes	##############################
CLIENTES	Consultas y Reportes	##############################
CLIENTES	Consultas y Reportes	##############################
CLIENTES	Consultas y Reportes	##############################
CLIENTES	Consultas y Reportes	##############################
CAJA	Reportes	##############################
CAJA	Reportes	##############################
CAJA	Reportes	##############################
CAJA	Reportes	##############################
CAJA	Reportes	##############################
CAJA	Reportes	##############################
CAJA	Reportes	##############################
CAJA	Reportes	##############################
CAJA	Reportes	##############################
CAJA	Reportes	##############################
CAJA	Reportes	##############################
CAJA	Reportes	##############################
CAJA	Reportes	##############################
CAJA	Reportes	##############################
CREDITO	Consultas y Reportes	##############################
CREDITO	Consultas y Reportes	##############################
CREDITO	Consultas y Reportes	##############################
CREDITO	Consultas y Reportes	##############################
CREDITO	Consultas y Reportes	##############################
CREDITO	Consultas y Reportes	##############################
CREDITO	Consultas y Reportes	##############################
CREDITO	Consultas y Reportes	##############################
CREDITO	Consultas y Reportes	##############################
CREDITO	Consultas y Reportes	##############################
CREDITO	Consultas y Reportes	##############################
CREDITO	Consultas y Reportes	##############################
CREDITO	Consultas y Reportes	##############################
CREDITO	Consultas y Reportes	##############################
CREDITO	Consultas y Reportes	##############################
CREDITO	Consultas y Reportes	##############################
CREDITO	Consultas y Reportes	##############################

Figura 12: Definición de perfiles específicos Core Financiero COOPCCP
Elaborado por: (COOPCCP, 2018)

La herramienta para gestión de tarjeta fue proporcionada por CAPTEC, la institución encargada de llevar a cabo el procesamiento de las tarjetas de débito y así mismo, la definición

de perfiles de usuario fue realizada por la misma empresa y no existe una persona encargada directamente de administrar dicho sistema ya que, no existieron definiciones sobre los dueños de proceso al momento de acceder al sistema sin embargo, al ser este considerado como un producto transaccional, lo idóneo es manejarlo con el área especializada de los procesos que lleva a cabo. Actualmente, el sistema es utilizado para dos áreas diferentes de la COOPCCP, el área de Operaciones se encarga de realizar la impresión de tarjetas y envío de especies a agencias, el área de Operaciones tiene dos roles, los jefes de agencias son aquellos que requieren realizar la entrega de tarjetas por medio de este sistema, por lo que cuentan con un perfil básico de activación y reseteo de contraseñas, mientras que por otro lado existe un perfil de monitoreo, análisis y control del funcionamiento de las transacciones y reportes encontrados por el uso de las tarjetas así también como los problemas suscitados. A continuación, se muestra un extracto de la pantalla de la gestión de perfiles de usuario

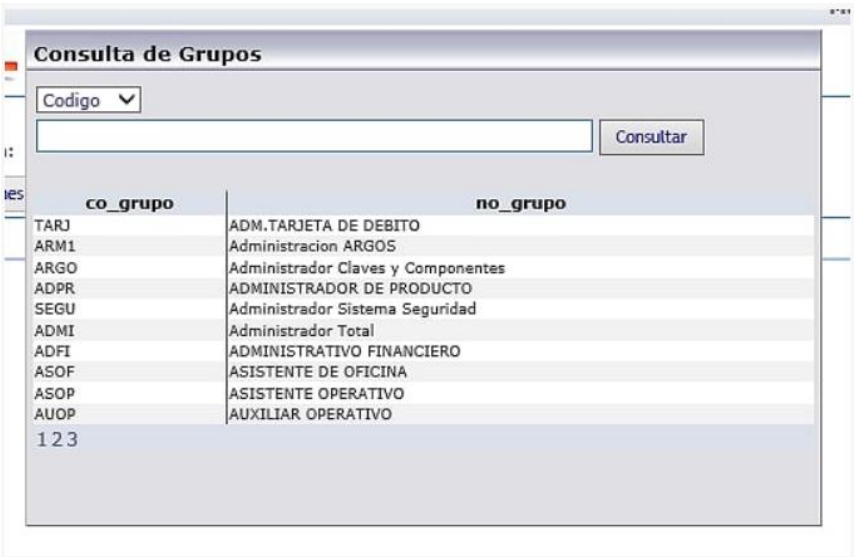


Figura 13: Perfiles de usuarios Sistema ExtremeWebFX
Elaborado por: COOPCCP

Hoy en día los gestores documentales son cada vez más importantes ya que el objetivo y futuro de las instituciones financieras es ofrecer más canales mediante los cuales sus socios o clientes puedan disponer de sus fondos, monitorear sus inversiones o realizar solicitudes de

crédito utilizando el intercambio de documentación entre el cliente o socio y la institución financiera. Por tal motivo, es importante mencionar que, actualmente el sistema gestor de archivos consta de perfiles para oficiales de negocios y procesos, sin poder contar con pantallas de visualización, esta versión es antigua y no consta de configuraciones adicionales.

Software complementario para tomar en cuenta: Existen otros sistemas que directamente no se encuentran relacionados con los servicios transaccionales que actualmente se ofrecen sin embargo, se encuentran planificadas las integraciones para poder permitir el uso de diferentes canales de atención para ofrecer productos automatizados que permitan realizar toda la gestión de cuentas directamente desde plataformas virtuales con el uso de asistentes que puedan manejar la información de los socios sin incurrir en problemas de sigilo bancario y se encuentre aprobada por los organismos de control. Estos programas son:

- Buró de crédito – Equifax. – sistema al que tiene acceso el área de negocios y crédito para revisar el score de crédito definido por la COOPCCP. Todas las aplicaciones de Fintech deben contemplar la integración de este sistema para poder automatizar el proceso de solicitud y aprobaciones de crédito. Es importante tomar en cuenta que este sistema funciona con una heurística de modelo predictivo sobre el comportamiento de pago de los socios y clientes que apliquen a la institución.
- Administrador de relaciones con el cliente – CRM. – Actualmente es importante considerar soluciones de big data que permitan el análisis y tratamiento de la información de los socios y posibles clientes de la institución.
- Línea 1800 COOPCCP. – La gestión de incidentes es requerimiento normativo que debe estar incluido y automatizado para el tratamiento de emergencias relacionadas a los servicios transaccionales, motivo por el cual debe buscarse la

manera de realizar integraciones necesarias y definir el personal que se encargará de atender estas líneas de contacto que podrán ser usadas tanto como para atención, consultas, quejas o ventas.

Los controles de acceso así también con la definición de perfiles de usuarios son necesarios para el correcto desarrollo de la institución y deben ser aplicados a todos los proyectos considerados dentro del Plan Operativo Anual.

3.4.3.3 Reportes de eventos de riesgo realizados

Los informes de seguridad de la información se realizaron en base a los reportes de la herramienta de control 619.49 firewall Fortinet con su software Fortigate y análisis de tráfico de las conexiones a puertos abiertos vulnerables encontrados con la consola de escaneo de puertos y vulnerabilidades NESUS. Durante todo el año 2018 se registraron un total de 8 ataques persistentes y 178 intentos de intrusiones a distintos segmentos de la red, entre ellos la página web, el servidor de correos y el servidor de aplicaciones. Resumido en la siguiente gráfica

Tipo de intrusión	Número de eventos	IP de destino	Explotación encontrada
Vulnerabilidades en puertos	17	Servidor de correos	SMBv1,2,3
XSS	27	Servidor de BDD	TCP 49152 - 49160
Command & Control	8	Servidor de Aplicaciones	TCP 990 -1433-135
DDoS	121	Servidor de aplicaciones	TCP2266 (rpc)
DoS	13	Servidor Web	TCP 80 – 135

Tabla 9: Resumen de intrusiones y eventos de riesgo COOPCCP
Elaborado por: Jean P. Rodríguez.

De los reportes encontrados, únicamente existió un evento de riesgo que tuvo como resultado la falla e inoperatividad de uno de los puntos de comunicaciones encontrados en el segmento de red perteneciente a la comunicación del servidor del core financiero con el servidor del

switch que se encarga de procesar las transacciones de compra con la tarjeta de débito. Por lo que, en este caso el afectado fue directamente un servicio transaccional. Para este evento y los demás se realizó la contingencia necesaria y se procedieron a reiniciar los servicios caídos.

3.4.3.4 Gestión de Auditoría interna y externa:

El área de auditoría interna de la COOPCCP se permitió levantar hallazgos que paulatinamente se han ido subsanando a medida que pasa el tiempo sin embargo, no cuentan con un auditor informático que realice el seguimiento adecuado a todos los servicios que el departamento de tecnología pone a disposición tanto de los usuarios internos (colaboradores de la COOPCCP) como externos (socios y clientes). Se presenta la matriz de hallazgos correspondientes a corte diciembre 2017 y Marzo de 2018:

REPORTE DE AVANCES

Nro Estrategia	Estrategia	Responsable de la estrategia	Fecha inicio	Fecha fin	Porcentaje Avance	Estado Cumplimiento	Entregable	Evidencia de avances
3	el oficial de SI procedera a efectaur un cronograma para aplicar el control de escritorios limpios (fisicos y pantallas) para todas las agencias a nivel nacional, junto con el area de Procesos en caso necesario	Responsable de Seguridad de Información	09/08/2017	31/12/2018	75%	INICIADO	Cronograma de visitas a las agencias y aplicar procesos de control mencionado en hallazgo por parte de la UAI	Se adjunta el Cronograma tentativo de aplicación del control de "Escritorios Limpios" que incluye: Estaciones de trabajo lógicas, Estaciones de trabajo físicas, Capacitaciones y Visitas para constatación de aplicación de políticas
4	el oficial de SI coordinara con el area de procesos para validar dicho control y modificar en caso necesario el manual indicado en el hallazgo por la UAI	Responsable de Seguridad de Información	09/08/2017	30/11/2017	35%	INICIADO	Manual de seguridad de informacion actualizado y aprobado por el CAD	Actualmente el manual de seguridad de la información se encuentra en proceso de revisión y modificación en varios puntos, dentro de los cuales se contempla lo relativo a este punto en "Políticas de escritorios limpios" para poder entregarlo posteriormente a CAD para su revisión y aprobación

REPORTE DE AVANCES

Nro Estrategia	Estrategia	Responsable de la estrategia	Fecha inicio	Fecha fin	Porcentaje Avance	Estado Cumplimiento	Entregable	Evidencia de avances
2	el oficial de SI coordinara con el area de Procesos para actualizar este procedimiento y su posterior validacion de acuerdo al hallazgo de la UAI	Responsable de Seguridad de Información	09/08/2017	30/11/2017	100%	FINALIZADO	procedimiento PGTI13 actualizado y aprobado por el CAD	El proceso PGTI13 se está actualizado y se encuentra en la plataforma ISOTOOLS en la ruta: IsoTools -> Gestión de TI -> Seguridad y control de la información de hardware y software -> Modificación directa a la BDD.
1	El responsable de SI junto con el area de procesos analizaran el procedimiento PGTI11 y en caso necesario actualizaran de acuerdo a la necesidad de la entidad para que, el CAD en forma posterior lo apruebe y se socialice en la cooperativa	Responsable de Seguridad de Información	09/08/2017	29/12/2017	100%	FINALIZADO	proceso PGTI11 aprobado por el Consejo de Administracion	El proceso PFTI11 fue removido y actualizado al proceso UAIR12. Mismo que se encuentra aceptado, actualizado y socializado.
1	OFIC DE SEGURIDAD DE INFORMACION determina .- Revisara los criterios de creacion de los grupos de internet y determinara que requieran entrar a diferentes paginas, aplicando heramientas estandares .-Actualizara manual de seguridad de informacion previo conocimeinto del CAD para su aprobacion .- Aplicara politicas y controles sobe comunicacion de archivos para el uso del correo institucional	RESPONSABLE DE SEGURIDAD DE INFORMACIÓN	13/12/2017	27/04/2018	0	NO INICIADA	.- listado de empleados con acceso a redes .- Manual de Segur, de Informac aprobado por CAD	Listado de empleados con acceso a redes

Figura 14: Matriz de hallazgos Auditoría interna COOPCCP
Elaborado por: COOPCCP

Adicionalmente, por normativa la COOPCCP debe realizar un análisis de auditoría externa y calificadora de riesgos anualmente, que se encargan de poner en consideración los cambios necesarios para asegurar una buena operatividad. Cada compañía auditora tiene su esquema de

trabajo e igualmente presentan hallazgos que deben ser modificados en un periodo de tiempo no mayor a 1 año. A continuación, un extracto de la matriz.

Hallazgos de auditoría externa

1. *En la revisión se observó que no todos los sistemas están siendo monitoreados y controlados por Seguridad de la Información, puesto que se evidenció la falta de monitoreo en los procesos de creación, eliminación y modificación de usuarios, perfiles y permisos a las bases de datos del Core Financiero, directorio activo y firewall.*
2. *ORION*

   ✓ *Falta de alineación de las configuraciones de contraseñas del sistema ORION, en comparación con el documento: "M.GTI02 Manual de Seguridades de la Información v4", en características como:*

Nombre parámetro	***Sistema***	***Manual***	***Cumple Manual***
Historial de contraseña	*No tiene*	*5*	*NO*
Vigencia máxima de contraseña	*30*	*120*	*NO*
Longitud mínima de la contraseña	*6*	*8*	*NO*
Bloqueo ante intentos fallidos	*3*	*No tiene*	*NO*

3. *SPYRAL*

   ✓ *Falta de alineación de las configuraciones de contraseñas del sistema SPYRAL, en comparación con el documento: "M.GT02 Manual de Seguridades de la Información v4", en características como:*

Nombre parámetro	***Sistema***	***Manual***	***Cumple Manual***
Historial de contraseña	*No tiene*	*5*	*NO*
Longitud mínima de la contraseña	*5*	*8*	*NO*
Bloqueo ante intentos fallidos	*3*	*No tiene*	*NO*

4. *Se observó en el sistema ORION la presencia de una persona activa a pesar que dejó de laborar en el año 2018 hasta la fecha de revisión. El ex funcionario es: XXXXXXXXXXXXXXXXXXXXXXXXX.*

5. *Se observó la presencia de 84 usuarios de sistema que tienen configurado en el Directorio Activo la opción de que nunca expire su contraseña, y no se evidenció ningún documento que justifique la parametrización dada.*

Figura 15: Hallazgos Auditoría Externa COOPCCP
Elaborado por: Consultora externa.

Dentro de los hallazgos presentados en ambas auditorías, se encuentran puntos relevantes para la seguridad en servicios transaccionales que deben ser tratados de tal manera que no sean representativas para el desarrollo de los futuros proyectos.

3.4.3.5 Pruebas de penetración de vulnerabilidades

Para las instituciones reguladas por la SEPS, la normativa indica que se debe realizar una prueba de penetración o "*Ethical Hacking*" al menos 1 vez al año, sin embargo, no menciona descripción alguna sobre el alcance al cual debe realizarse o con respecto a los vectores de ataque existentes. Lo que ocasiona que únicamente reflejen resultados sobre un tramo de la red. En COOPCCP se realizó un *pentest* enfocado a cubrir dos aristas importantes, fallos de la red en configuraciones y comunicaciones entre enlaces internos y externos; uso de métodos de ingeniería social utilizando a usuarios de la red interna como foco de infección. De los resultados se pueden expresar algunas consideraciones:

- **Ingeniería social:** Se desplegaron ataques controlados para poder evidenciar la probabilidad de infección de tipo Ransomware dentro de la institución, utilizando el método de phishing a una muestra de 25 colaboradores de la COOPCCP. El ataque controlado consistió en utilizar la figura de citación por la ANT y citación a una causa judicial en el que el objetivo fue evidenciar si el colaborador con figura de víctima dio clic al ejecutable y links que contenía dicho correo. El resultado de esta prueba es preocupante ya que en promedio el 70% y 80% respectivamente dieron positivo a la infección, lo que quiere decir que no existe información relevante

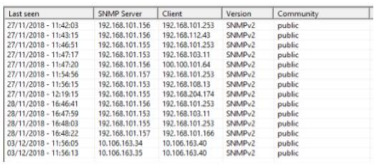
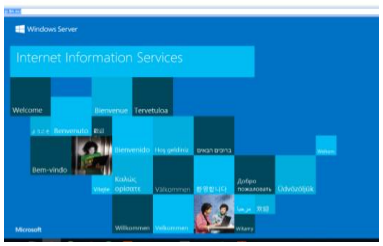
COOPCCP - Resumen test de ingeniería social	
Fecha:	18 de Octubre de 2018
Área:	Riesgos - Seguridad de la Información
Descripción:	Los ataques fueron dirigidos con asuntos diferentes con contenido diferente a 50 colaboradores de la COOPCCP, en el que se entregaba un link, cuyo objetjivo es simular la ejecución de código auto ejecutable de tipo ransomware y ataques de día ceto.
Muestra:	

Resultados

Ataque 1: 25 Usuarios - Multa de tránsito				Ataque 2: 25 usuarios - Citación			
Total infectados	17			Total infectados	17		
Efectividad	68%			Efectividad	68%		
Hombres	5			Hombres	4		
Mujeres	12			Mujeres	13		
Áreas de infección				Áreas de infección			
Departamento	Fallido	Exitoso	% Victimas	Auditoría	Fallido	Exitoso	% Victimas
Contabilidad		1	100,00%	Call Center		2	100,00%
Cobranzas	1		0,00%	Comercial		1	100,00%
Fábrica		1	100,00%	Contabilidad		1	100,00%
Gerencia	1	1	50,00%	Cumplimiento		1	100,00%
Legal		1	100,00%	Agencias	6	7	53,84%
Agencias	5	11	64,70%	Operaciones	2	1	33,33%
Talento Humano		1	100,00%	Talento Humano		1	100,00%
Tecnología	1	1	50,00%	Riesgos		1	100,00%
				Tecnología		1	100,00%
Total/promedio	8	17	70,59%	Total/promedio	8	17	87,46%

Tabla 10: Resultado Ingeniería social COOPCCP
Elaborado por: Jean P. Rodríguez.

- Prueba de penetración a los sistemas: Para realizar el *pentest* se realizó una prueba a 27 IP´s, 17 de ellas realizadas a máquinas de usuario final, 4 para servidores de bases de datos, 4 para servidores de aplicaciones y 2 equipos de seguridad, de las cuales se detalla la siguiente información:

<table>
<tr><th colspan="2">COOPCCP - Resumen test de ingeniería social</th></tr>
<tr><td>Fecha:</td><td>19 de septiembre de 2018</td></tr>
<tr><td>Área:</td><td>Riesgos - Seguridad de la Información</td></tr>
<tr><td>Descripción:</td><td>El equipo de especialistas responsable del servicio de análisis de vulnerabilidades de GMS ha
ejecutado tareas de búsqueda de vulnerabilidades en veinticinco (27) IP’s internas y dos (2)
aplicaciones Web.
Las técnicas, tácticas y destrezas administradas por el equipo de especialistas permiten presentar
en este documento una situación real en términos de niveles de exposición a riesgos y amenazas
tecnológicas, además se plantea el compromiso que debe asumir la COOPCCP, si alguna de estas
brechas de seguridad es utilizadas por actores mal intencionados e inclusive por elementos internos
de la organización.</td></tr>
<tr><td>Muestra:</td><td>
<table>
<tr><th>IP's</th><th>Crítica</th><th>Alta</th><th>Media</th><th>Baja</th><th>Informativas</th><th>Total general</th></tr>
<tr><td>192.168.204.128</td><td>0</td><td>0</td><td>3</td><td>1</td><td>26</td><td>30</td></tr>
<tr><td>192.168.204.178</td><td>0</td><td>0</td><td>0</td><td>0</td><td>16</td><td>16</td></tr>
<tr><td>192.168.204.151</td><td>0</td><td>0</td><td>3</td><td>0</td><td>21</td><td>24</td></tr>
<tr><td>192.168.204.165</td><td>0</td><td>0</td><td>3</td><td>1</td><td>23</td><td>27</td></tr>
<tr><td>192.168.204.174</td><td>0</td><td>0</td><td>3</td><td>0</td><td>24</td><td>27</td></tr>
<tr><td>192.168.204.177</td><td>1</td><td>5</td><td>0</td><td>1</td><td>49</td><td>56</td></tr>
<tr><td>192.168.204.182</td><td>0</td><td>0</td><td>3</td><td>0</td><td>21</td><td>24</td></tr>
<tr><td>192.168.204.189</td><td>0</td><td>0</td><td>3</td><td>1</td><td>25</td><td>29</td></tr>
<tr><td>192.168.101.194</td><td>0</td><td>0</td><td>0</td><td>0</td><td>6</td><td>6</td></tr>
<tr><td>192.168.204.100</td><td>0</td><td>0</td><td>3</td><td>0</td><td>26</td><td>29</td></tr>
<tr><td>192.168.204.122</td><td>0</td><td>0</td><td>3</td><td>1</td><td>23</td><td>27</td></tr>
<tr><td>100.100.101.104</td><td>0</td><td>0</td><td>0</td><td>0</td><td>45</td><td>45</td></tr>
<tr><td>192.168.204.6</td><td>0</td><td>0</td><td>3</td><td>0</td><td>20</td><td>23</td></tr>
<tr><td>192.168.101.81</td><td>0</td><td>0</td><td>0</td><td>0</td><td>6</td><td>6</td></tr>
<tr><td>192.168.116.10</td><td>0</td><td>0</td><td>0</td><td>0</td><td>25</td><td>25</td></tr>
<tr><td>192.168.114.10</td><td>0</td><td>0</td><td>0</td><td>0</td><td>6</td><td>6</td></tr>
<tr><td>192.168.115.10</td><td>0</td><td>0</td><td>0</td><td>0</td><td>7</td><td>7</td></tr>
<tr><td>100.100.101.52</td><td>0</td><td>0</td><td>0</td><td>0</td><td>39</td><td>39</td></tr>
<tr><td>100.100.101.253</td><td>0</td><td>0</td><td>5</td><td>3</td><td>29</td><td>37</td></tr>
<tr><td>100.100.101.79</td><td>0</td><td>0</td><td>0</td><td>0</td><td>36</td><td>36</td></tr>
<tr><td>100.100.101.54</td><td>0</td><td>0</td><td>1</td><td>0</td><td>35</td><td>36</td></tr>
<tr><td>100.100.101.110</td><td>0</td><td>0</td><td>0</td><td>0</td><td>7</td><td>7</td></tr>
<tr><td>100.100.101.84</td><td>0</td><td>0</td><td>0</td><td>0</td><td>32</td><td>32</td></tr>
<tr><td>100.100.101.123</td><td>0</td><td>0</td><td>0</td><td>0</td><td>31</td><td>31</td></tr>
<tr><td>192.168.201.229</td><td>4</td><td>1</td><td>13</td><td>3</td><td>49</td><td>70</td></tr>
<tr><td>100.100.101.120</td><td>0</td><td>0</td><td>0</td><td>0</td><td>11</td><td>11</td></tr>
<tr><td>Total general</td><td>5</td><td>6</td><td>46</td><td>11</td><td>638</td><td>706</td></tr>
</table>



</td></tr>
</table>

Tabla 11: Descripción PenTest – Ingeniería Social
Elaborado por: COOPCCP

Resultados	
Severidad	**Detalle**
Alta	SSL Versión 2 & 3 Protocol detection
Crítica	Update SMB Server - Ransomware Risk
Crítica	Update SMB Server - Ransomware Risk
Crítica	Update SMB Server - Ransomware Risk
Crítica	Unsuported windows OS
Crítica	Windows Server 2003 Unsuported instalation found
Alta	Captura de tráfico
Alta	Visualización de contraseñas de Correo
Crítica	Enumeración del directorio de IIS "orion"
Baja	Revelación de versión de ASP.NET
Baja	ClickJacking : Falta el encabezado de X-FRAME-OPT
Baja	Método http - Option está habilitado
Baja	Posible directorio sensible
Informativa	Revelación de versión de IIS

Severidad	Total
Crítica	5
Alta	17
Media	288
Baja	95
Informativas	1673
Total General	2078

Figura 16: Resultado de Pentest COOPCCP
Elaborado por: COOPCCP

3.4.3.6 Clasificación de activos de información

En la COOPCCP se encuentra definida una metodología para la clasificación de activos de la información que es aplicada por el área de Tecnología y sobre el que se rige los siguientes análisis, a continuación se muestra un extracto del manual:

INTRODUCCION

La presente metodología de Riesgos para la Seguridad de la Información establece los lineamientos básicos, para administrar el riesgo para la Seguridad de la Información en todos sus medios, ofreciendo un método sistemático para analizar los riesgos derivados del uso de las tecnologías de la información y comunicaciones (TIC).

Esta metodología pretende brindar la capacidad para que las redes o de los sistemas de información provean un determinado nivel de confianza frente a los accidentes, acciones ilícitas o malintencionadas que comprometan la disponibilidad, integridad y confidencialidad de los datos físicos, almacenados, transmitidos y de los servicios.

OBJETIVO

Definir y establecer directrices para la administración del riesgo de seguridad de la información a nivel de todos los procesos de la Institución.

DEFINICIONES

3.1. Administración de riesgos. - Es el proceso mediante el cual las entidades identifican, miden, priorizan, controlan, mitigan, monitorean, y comunican los riesgos a los cuales se encuentran expuestas.

3.2. Riesgo. - Es la posibilidad de que se produzca un hecho generador de pérdidas que afecten el valor económico de las instituciones.

3.3. Riesgo operativo. - Es la posibilidad de que se produzcan pérdidas debido a eventos originados en fallas o insuficiencia de procesos, personas, sistemas internos, tecnología, y en la presencia de eventos externos.

3.4. Declaración de aplicabilidad. - Para un conjunto de salvaguardas, se indica sin son de aplicación en el sistema de información bajo estudio o si, por el contrario, carecen de sentido.

3.5. Comité de administración integral de riesgos (CAIR). - Es el órgano creado por el directorio u organismo que haga sus veces de la institución del sistema financiero, responsable del diseño de las políticas, sistemas, metodologías, modelos y procedimientos, para la eficiente gestión integral de los riesgos y de manera específica en los identificados en la actividad que efectúa la entidad; y, de proponer los límites de exposición a éstos.

3.6. Disponibilidad. - Disposición de los servicios a ser usados cuando sea necesario. La carencia de disponibilidad supone una interrupción del servicio. La disponibilidad afecta directamente a la productividad de la cooperativa.

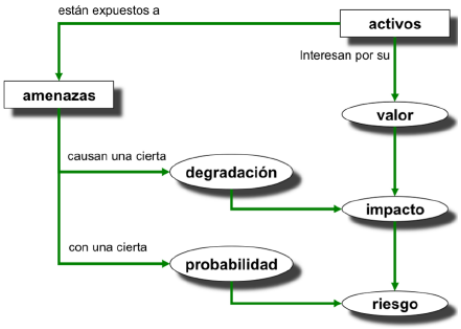
3.7. Integridad. - Mantenimiento de las características de completitud y corrección de los datos. Contra la integridad, la información puede aparecer manipulada, corrupta o incompleta. La integridad afecta directamente al correcto desempeño de las funciones de la cooperativa.

METODOLOGIA PARA EL ANALISIS DEL RIESGO DE SEGURIDAD DE LA INFORMACION.

El análisis de riesgos de seguridad de la información es una aproximación metódica para determinar el riesgo siguiendo unos pasos pautados:

1. Determinar los activos relevantes para la COOPCCP, su interrelación y su valor, en el sentido de qué perjuicio (coste) supondría su degradación
2. Determinar a qué amenazas están expuestos aquellos activos
3. Determinar qué controles existen y cuán eficaces son frente al riesgo
4. Estimar el impacto, definido como el daño sobre el activo derivado de la materialización de la amenaza
5. Estimar el riesgo.

La siguiente figura recoge este primer recorrido, cuyos pasos se detallan en las siguientes secciones:



Identificación de Activos de Información

Se define un activo como Componente o funcionalidad de un sistema de información susceptible de ser atacado deliberada o accidentalmente con consecuencias para la COOPCCP. Incluye: información, datos, servicios, aplicaciones (software), equipos (hardware), comunicaciones y recursos físicos.

Figura 17:Manual de Clasificación de activos de información
Elaborado por: *(COOPCCP, 2017)*

3.4.4 Revisión de equipos y estructura de tecnología:

Este es un pilar fundamental en el que se basará la metodología para plantear alternativas de acuerdo con los tipos de equipos e infraestructura con la que cuente la institución, ya que, dependiendo del desarrollo tecnológico se podrá realizar propuestas que ayuden a adquirir nuevos terminales o realizar un proceso de robustecimiento de servidores con herramientas

nativas de distintos sistemas operativos. Además de los equipos y estructura de red, se debe revisar las configuraciones de los distintos puntos de control que existen para responder ante el tráfico entrante y saliente y sobre todo las conexiones a la base de datos.

Motivo por el cual se presenta a continuación la topología de la COOPCCP que se encuentra implementada.

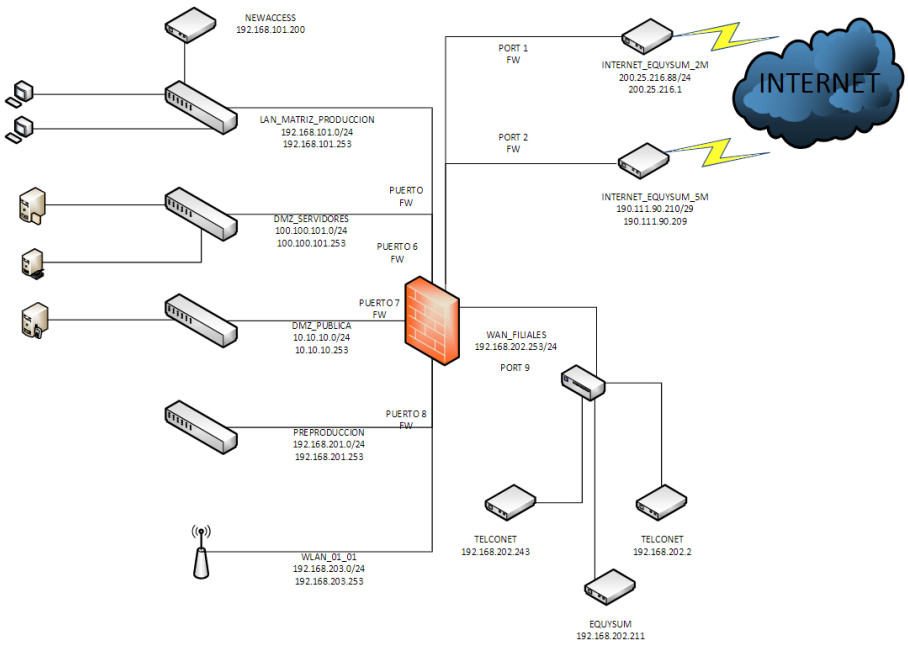


Figura 18: Topología de red COOPCCP
Elaborado por: Jean Rodríguez.

En la topología presentada no se encontró factores de configuración o equipos que realicen una adecuada gestión de seguridad informática y aunque es funcional, se encuentran varios fallos de seguridad ya que aún con una excelente configuración de Firewall, la carga que tendrá, resultado de la aplicación de las reglas, puede saturarlo y al no tener equipos que gestionen el tráfico o lo filtren previamente, se ocasionaría una baja de los servicios.

Correspondiendo a la topología vigente, el departamento de tecnología cuenta con los equipos listados a continuación:

Inventario de activos de la información

		REQUERIMIENTOS DE SEGURIDAD			
ID ACTIVO	HOSTNAME	INTEGRIDAD	CONFIDENCIALIDAD	DISPONIBILIDAD	CLASIFICACION
EAR0001	Router TELCONET ET	3	3	3	ALTAMENTE RESTRINGIDA
EAR0002	Router TELCONET Agencias	3	3	3	ALTAMENTE RESTRINGIDA
EAR0003	Router T1	3	3	2	ALTAMENTE RESTRINGIDA
EAR0004	Router Accesat	3	3	2	ALTAMENTE RESTRINGIDA
EAR0005	Router Eqysum ED	3	3	3	ALTAMENTE RESTRINGIDA
EAR0006	Modem Eqysum	3	3	3	ALTAMENTE RESTRINGIDA
EAR0007	Modem Eqysum Internet	3	3	3	ALTAMENTE RESTRINGIDA
EAR0008	DLINK_DMZ	3	3	3	ALTAMENTE RESTRINGIDA
EAR0009	DLINK_SERVIDORES	3	3	3	ALTAMENTE RESTRINGIDA
EAR0010	DLINK_LAN	3	3	3	ALTAMENTE RESTRINGIDA
EAR0011	DLINK_PREPRODUCCION	3	3	2	ALTAMENTE RESTRINGIDA
EAR0012	DLINK_FILIALES	3	3	3	ALTAMENTE RESTRINGIDA
EAR0013	DLINK_WIRELESS	3	3	2	ALTAMENTE RESTRINGIDA
EAR0014	FWPRINCIPAL	3	3	3	ALTAMENTE RESTRINGIDA
EAR0015	FWALTERNO	3	3	2	ALTAMENTE RESTRINGIDA
EAR0016	FW-1008-Quito-Prensa	3	3	3	ALTAMENTE RESTRINGIDA
EAR0017	FW-1002-Quito-Centro	3	3	3	ALTAMENTE RESTRINGIDA
EAR0018	FW-1003-Quito-Sur	3	3	3	ALTAMENTE RESTRINGIDA
EAR0019	FW-1011-LOJA-LOJA	3	3	3	ALTAMENTE RESTRINGIDA
EAR0020	FW-1005-BAHIA	3	3	3	ALTAMENTE RESTRINGIDA
EAR0021	FW-1006-PEDERNALES	3	3	3	ALTAMENTE RESTRINGIDA
EAR0022	FW-1013-MANTA	3	3	3	ALTAMENTE RESTRINGIDA
EAR0023	FWANALYZER	3	3	1	USO INTERNO
EAR0024	FAP_1001_01	3	3	1	USO INTERNO
EAR0025	FAP_1001_02	3	3	1	USO INTERNO
EAR0026	FAP_1001_03	3	3	1	USO INTERNO
EAR0027	FAP_1001_04	3	3	1	USO INTERNO

Tabla 12: Inventario de Activos de Información
Elaborado por: COOPCCP

	SERVIDORES FÍSICOS		
Nombre de computador	**Detalles**	**Aplicación**	**Ubicación**
SRVDOCUME	Dual-Core AMD Opteron(tm) Processor 1210 1.79 GHz	Gestion Documental	Servidor Físico
APPSERCCP	Pentium ® Core ™ I5-3330 CPU @ 3.00 Ghz	Delgado Travel	Servidor Físico
SRV3003	Pentium ® Core ™ 2 CPU E7400 @ 2.8Ghz 2.67 Ghz	Callcenter llamadas salientes	Servidor Físico
SRV_EXTREME	Intel(R) Xeon(R) CPU E5-2620 v3 @ 2.40GHz	tarjeta de debito	Servidor Físico

Tabla 13:Inventario de Servidores Físicos
Elaborado por: COOPCCP

	SERVIDORES VIRTUALES		
Nombre de computador	**Detalles**	**Aplicación**	**Ubicación**
SRV0011	NEGOCIOP	Servidor Virtual	CRONOS
SRV0012	PNEGOCIOL	Servidor Virtual	CRONOS
SRV0013	PSRV1001	Servidor Virtual	CRONOS Pre-Producción
SRV0014	PSRV1002	Servidor Virtual	CRONOS Pre-Producción
SRV0015	PSRV1003	Servidor Virtual	CRONOS Pre-Producción
SRV0016	PSRV1005	Servidor Virtual	CRONOS Pre-Producción
SRV0017	PSRV1013	Servidor Virtual	CRONOS Pre-Producción
SRV0018	PSRV1021	Servidor Virtual	CRONOS Pre-Producción
SRV0019	SERVERLOC	Servidor Virtual	CRONOS Producción
SRV0020	SRV1001	Servidor Virtual	AD Secuadario
SRV0022	SRV1004	Servidor Virtual	Equifax
SRV0023	SRV1006	Servidor Virtual	Web CRONOS
SRV0024	SRV1007	Servidor Virtual	Pagina Web CRONOS
SRV0025	SRV1008	Servidor Virtual	-
SRV0026	SRV1009	Servidor Virtual	Web Service BCE
SRV0027	SRV1010	Servidor Virtual	Servipagos
SRV0028	SRV1012	Servidor Virtual	Biometrico
SRV0029	SRV1013	Servidor Virtual	Spyral / Grupo TEA
SRV0031	SRV1022	Servidor Virtual	CRONOS
SRV0032	SRV1023	Servidor Virtual	CRONOS
SRV0033	SRV2001	Servidor Virtual	Tranferencia Datos Cronos
SRV0034	SRV2002	Servidor Virtual	Gestión BDD
SRV0035	SRV2003	Servidor Virtual	Historicos
SRV0036	SRV3002	Servidor Virtual	Whatsup
SRV0042	SRV3018	Servidor Virtual	Encripción de Discos
SRV0043	SRV3021	Servidor Virtual	Aplicación MFILES
SRV0044	SRV3022	Servidor Virtual	SysAid
SRV0045	SRV3023	Servidor Virtual	Base de Datos MFILES
SRV0046	SRV3Z01	Servidor Virtual	Pagina Web
SRV0047	SRV3Z02	Servidor Virtual	COSEDE
SRV0048	SRVDBMS	Servidor Virtual	POINTEC
SRV0049	SRVPOINTEC	Servidor Virtual	POINTEC
SRV0050	SRV_EXTREME2	Servidor Virtual	EXTREME PRUEBAS
SRV0051	TESTSRV002	Servidor Virtual	-
SRV0052	mail.coopccp.fin.ec	Servidor Virtual	-
SRV0053	encuestas.coopccp.fin.ec	Servidor Virtual	-
SRV0054	webTitan.coopccp.fin.ec	Servidor Virtual	Web Titan
SRV0055	spamTitan.coopccp.fin.ec	Servidor Virtual	Spam Titan

SRV0056	inventory.coopccp.fin.ec	Servidor Virtual	Inventory entory
SRV0057	owncloud.coopccp.fin.ec	Servidor Virtual	Owncloud cloud
SRV0058	antispambck	Servidor Virtual	Antispambck ispambck
SRV0059	webtitanbck	Servidor Virtual	Webtitanbck titanbck
SRV0061	SRV1026	Servidor Virtual	Activos Fijos
SRV0062	SRV_0101	Servidor Virtual	Carpetas Compartidas
SRV0063	SRV_0202	Servidor Virtual	Bases de Datos
SRV0064	SRV3020	Servidor Virtual	EndPoint Protector
SRV0065	SRV3001	Servidor Virtual	Active Directory
SRV0066	SRV3025	Servidor Virtual	Guardium
SRV0067	SRV3027	Servidor Virtual	Orion Riesgo Operativo
SRV0068	SRV_0301	Servidor Virtual	WSUS
SRV0069	SRV_0304	Servidor Virtual	Entidad Certificadora
SRV0070	SRV_0305	Servidor Virtual	Anti-Malware ATM
SRV0071	SRV_0308	Servidor Virtual	BitDefender
SRV0072	SRV_0309	Servidor Virtual	Zimbra
SRV0073	SRV_0312	Servidor Virtual	Orion Jefaturas
SRV0074	SRV_0312	Servidor Virtual	GRUPO TEA
SRV0075	SRV_1023	Servidor Virtual	Businness Ware
SRV0076	SRV_0401	Servidor Virtual	Aplicación Orion
SRV0077	SRV_0402	Servidor Virtual	Base de Datos Orion

Tabla 14: Servidores Virtuales COOPCCP
Elaborado por: Jean P. Rodríguez.

	BASES DE DATOS		
Identificador	**Nombre BDD**	**Respaldo**	**Almacenamiento**
BDD00001	BD Business Ware	Mensual	Disco Servidor
BDD00002	BD Spyral	Diario	Disco Servidor
BDD00003	BD Cronos	Diario	Disco Servidor
BDD00004	BD Contact Manager	Mensual	Disco Servidor
BDD00005	BD Mfiles	Mensual	Disco Servidor
BDD00006	BD Local EXTREME	Diario	Disco Servidor
BDD00007	BDD POINTEC - Captaciones	Diario	Disco Servidor
BDD00008	BDD POINTEC - Garantias	Diario	Disco Servidor
BDD00009	BDD POINTEC - Activos Fijos	Diario	Disco Servidor
BDD00010	BDD POINTEC - Clientes	Diario	Disco Servidor
BDD00011	BDD POINTEC - Tesoreria	Diario	Disco Servidor
BDD00012	BDD POINTEC - Work Flow	Diario	Disco Servidor
BDD00013	BDD POINTEC - Contabilidad	Diario	Disco Servidor
BDD00014	BDD POINTEC - Credito	Diario	Disco Servidor
BDD00015	BDD POINTEC - Seguridades	Diario	Disco Servidor
BDD00016	BDD POINTEC - Proveedores	Diario	Disco Servidor
BDD00017	BDD POINTEC - Proveeduria	Diario	Disco Servidor
BDD00018	BDD POINTEC - Call Center	Diario	Disco Servidor
BDD00019	BDD IDCE - Mercado y Liquidez	Mensual	Disco Servidor
BDD00020	BDD SysAid	Mensual	Disco Servidor
BDD00021	BDD Orion RO	Mensual	Disco Servidor

Tabla 15: Bases de datos COOPCCP
Elaborado por: Jean P. Rodríguez.

3.4.5 Proveedores de servicios

La COOPCCP cuenta con diferentes proveedores que brindan sus servicios a nivel de mantenimiento y gestión de enlaces de red, ISP, Intermediarios de compensación y tecnologías

de negocios. Por tal motivo se menciona a los proveedores más importantes que intervienen en la gestión y aplicación de los servicios transaccionales, entre ellos se encuentra:

- **Captec:** Se encarga de realizar el procesamiento de las tarjetas de débito de la COOPCCP, de igual manera brindan soporte sobre los inconvenientes dados en el Switch transaccional.
- **AlexSoft:** Empresa proveedora del Switch que se encarga de comunicar las transacciones realizadas por medio del ATM de la COOPCCP.
- **Diebolt:** Se encarga del mantenimiento del ATM encontrado en Galápagos – Isabela.
- **Coonecta:** Red de gestión de enlace y salida de servicio transaccional, por medio de una licencia, permite a los sistemas de la COOPCCP y puntualmente tarjeta de débito, tener salida con todos los cajeros de esta red transaccional así también como en BANRED.
- **Telconet:** Empresa dedicada a prestar el servicio de Internet seleccionado como enlace principal
- **T1:** Encargada de las comunicaciones, un ISP seleccionado para el manejo de los enlaces s
- **FinanCoop:** La caja central FinanCoop es una cooperativa de segundo piso, es decir, que presta sus servicios únicamente a instituciones de intermediación financiera de primer piso como lo son las cooperativas.
- **Red Facilito:** Una red de compensación pequeña que se encarga de realizar la recaudación de distintos GAD´s y servicios básicos en sectores rurales. Cuenta con una malla de compensación única.
- **Pago Ágil:** El servicio por excelencia utilizado en el Ecuador para la recaudación de valores de diferentes instituciones, compensado por Produbanco, es un sistema mediante el cual se pueden realizar varios pagos a diferentes instituciones.

- **Banco Central del Ecuador:** El rol del BCE es muy importante ya que se encarga de compensar el sistema de pagos/cobros interbancarios, para ello, se levantó un esquema de comunicación seguro con Web Service y enlaces de contingencia que actúan con una cámara de compensación.
- **Wester Union:** Manejo de remesas y dinero enviado desde y hacia el exterior, actualmente el sistema se encuentra levantado como un servicio en caja nivel nacional que se encarga de realizar compensaciones por medio de un saldo manejado por la COOPCCP.

A sumarse entre estos proveedores se encuentran otras instituciones que ofrecen la adhesión a sus servicios para realizar gestión operativa de negocios, gestión de cobranzas, fidelización del cliente, red de servicios y beneficios, tipos de seguros, billetera móvil, entre otros. Estos servicios serán adheridos al CORE de la COOPCCP mediante enlaces de comunicación con tecnología *web service* a cargo del personal de desarrollo del área de tecnología.

3.4.6 Análisis de la normativa PCI DSS:

La COOPCCP así también como otras instituciones financieras manejan políticas basadas en las buenas prácticas y controles de la ISO27000 para la gestión y tratamiento de los eventos de riesgo enfocados de manera integral a la institución, sin embargo, al momento de implementar nuevos sistemas que involucren temas de botones de pago y afectaciones de los saldos de las cuentas mediante transferencias directas o recepción de documentos, es importante contar con un esquema especializado para el manejo de la información. Es por eso que en el presente trabajo se tomaron como pilares los requisitos de la PCI DSS que corresponden a los 12 dominios a ser utilizados

Norma de seguridad de datos de la PCI: descripción general de alto nivel.	
Desarrolle y Mantenga redes y sistemas seguros	1. Instalar y mantener una configuración de firewall para proyeger los datos del titular de la tarjeta. 2. No utilizar contraseñas de sistemas y otros parámetros de seguridad provistos por los proveedores.
Proteger los datos del titular de la tarjeta	3. Proteja los datos del titular de la tarjeta que fueron almacenados. 4. Cifrar la transmisión de los datos del titular de la tarjeta en las redes públicas abiertas.
Mantener un programa de administración de vulnerabilidad	5. Utilizar y actualizar con regularidad los programas o software antivirus 6. Desarrolle y mantenga sistemas y aplicaciones seguras.
Implementar medidas sólidas de control de acceso	7. Restrinja el acceso a los datos del titular de la tarjeta según la necesidad de saber que tenga la empresa. 8. Identifique y autentique el acceso a los componentes del sistema. 9. Restringir el acceso físico a los datos del titular de la tarjeta.
Supervisar y evaluar las redes con regularidad	10. Rastree y supervise todos los accesos a los recursos de red y a los datos de los titulares de las tarjetas 11. Compruebe con regularidad los sistemas y procesos de seguridad.
Mantener una política de seguridad de la información	12. Mantenga una política que aborde la seguridad de la información para todo el personal

Figura 19: Requisitos generales PCI DSS
Extraído de: PCI DSS – Requisitos y procedimientos de evaluación de seguridad

A continuación, se presentan dos puntos importantes de cada requisito tomados como controles que fueron concatenados con la matriz de riesgos presentada:

Controles de la Norma PCI DSS

Requisito 1: Instale y mantenga una configuración de firewall para proteger los datos

- Prohíba el acceso directo público entre Internet y todo componente del sistema en el entorno de datos de los socios
- Asegúrese de que las políticas de seguridad y los procedimientos operativos para administrar los firewalls estén documentados, implementados y que sean de conocimiento para las partes afectadas.

Requisito 2: No utilizar contraseñas de sistemas y otros parámetros de seguridad provistos por los proveedores

- Desarrolle normas de configuración para todos los componentes de sistemas. Asegúrese de que estas normas contemplen todas las vulnerabilidades de seguridad conocidas que concuerden con las normas de alta seguridad de sistema aceptadas en la industria. (ISO-ANSI-NIST)

- Cifre todo el acceso administrativo que no sea de consola utilizando un cifrado sólido. Utilice tecnologías como SSH, VPN o SSL/TLS para la administración basada en la web y otros tipos de acceso administrativo que no sea de consola

Requisito 3: Proteger los datos del socio que ya fueron almacenados.

- No almacene datos confidenciales de autenticación después de recibir la autorización. Si se reciben datos de autenticación confidenciales convierta todos los datos en irrecuperables al finalizar el proceso de autorización.
- Documente por completo e implemente todos los procesos y procedimientos de administración de claves de las claves criptográficas que se utilizan para el cifrado de datos del socio

Requisito 4: Cifrar la transmisión de los datos del socio en las redes públicas abiertas

- Utilice cifrado sólido y protocolos de seguridad (SSL/TLC, IPSEC, SSH, etc) para proteger los datos confidenciales del socio durante la transmisión por redes públicas abiertas, por ejemplo: (Solo se aceptan claves y certificados de confianza, el protocolo implementado solo admite configuraciones o versiones seguras, la solidez del cifrado es la adecuada para la metodología de cifrado que se utiliza. (redes públicas son: la Internet, tecnologías 802,11 y bluetooth, tecnología celular CDMA y GSM, GPRS, comunicación satelital
- Nunca se debe enviar PAN no cifrados por medio de tecnologías de mensajería de usuario final (correo electrónico, mensajería instantánea, chat)

Requisito 5: Proteger todos los sistemas contra malware y actualizar los programas o software de antivirus regularmente

- Implemente un software antivirus en todos los sistemas que, generalmente, se ven afectados por SW malicioso (pc y servidores)
- Asegúrese de que los mecanismos de antivirus funcionen activamente y que los usuarios no puedan deshabilitarlos ni alterarlos, salvo que estén específicamente autorizados por la gerencia en casos particulares y durante un periodo limitado

Requisito 6: Desarrolle y mantenga sistemas y aplicaciones seguras

- Asegúrese de que todos los SW y componentes del sistema tengan instalados parches de seguridad proporcionados por los proveedores que ofrecen protección contra vulnerabilidades conocidas. Instale los parches importantes dentro de un plazo de un mes desde su lanzamiento.
- Siga los procesos y procedimientos de control de todos los cambios en los componentes del sistema

Requisito 7: Restrinja el acceso a los datos del socio según la necesidad de saber que tenga la empresa

- Limite el acceso a los componentes del sistema y a los datos del titular de la tarjeta a aquellos individuos cuyas tareas necesitan de ese acceso.
- Establezca un sistema de control de acceso para los componentes del sistema que restrinja el acceso según la necesidad del usuario de conocer y que se configure para

"negar todo", salvo que se permita específicamente. Este sistema de control de acceso debe incluir lo siguiente:

Requisito 8: Identificar y autenticar el acceso a los componentes del sistema.

- Defina e implemente políticas y procedimientos para garantizar la correcta administración de la identificación de usuarios para usuarios no consumidores y administradores en todos los componentes del sistema de la siguiente manera:
- Incorpore la autenticación de dos factores para el acceso remoto a la red desde fuera de la red por parte del personal (incluso usuarios y administradores) y todas las partes externas involucradas (que incluye acceso del proveedor para soporte o mantenimiento).

Requisito 9: Restringir el acceso físico a los datos del titular de la tarjeta

- Utilice controles de entrada a la empresa apropiados para limitar y supervisar el acceso físico a los sistemas en el entorno de datos del titular de la tarjeta.
- Proteja físicamente todos los medios.

Requisito 10: Rastree y supervise todos los accesos a los recursos de red y a los datos de los titulares de las tarjetas

- Implemente pistas de auditoría para vincular todo acceso a componentes del sistema con usuarios específicos.
- Utilizando tecnología de sincronización, sincronice todos tiempos y relojes críticos y asegúrese de que lo siguiente sea implementado para adquirir, distribuir y almacenar tiempos.

Requisito 11: Pruebe con regularidad los sistemas y procesos de seguridad.

- Implemente procesos para determinar la presencia de puntos de acceso inalámbrico (802.11), detecte e identifique, trimestralmente, todos los puntos de acceso inalámbricos autorizados y no autorizados.
- Implemente un mecanismo de detección de cambios (por ejemplo, herramientas de monitorización de integridad de archivos) para alertar al personal sobre modificaciones no autorizadas de archivos críticos del sistema, de archivos de configuración o de contenido, y configure el software para realizar comparaciones de archivos críticos, al menos, una vez por semana.

Requisito 12: Mantener una política que aborde la seguridad de la información de todo el personal

- Establezca, publique, mantenga y distribuya una política de seguridad.
- Asegúrese de que las políticas y los procedimientos de seguridad definan, claramente, las responsabilidades de seguridad de la información de todo el personal.

Figura 20: Extracto de Requisitos (Controles) PCI DSS
Elaborado por: PCI DSS - Jean P. Rodríguez.

La normativa PCI consta de 253 Controles que se encuentran orientados a la configuración, protección y modelos de seguridad de las telecomunicaciones para salvaguardar los datos de los socios y clientes.

Adicionalmente, en la metodología es necesario aplicar las mejores prácticas para implementar las PCI DSS en los procesos habituales, esto con el fin de asegurar que los controles de seguridad se sigan implementando correctamente. Estas revisiones deberán realizarse de manera mensual:

1. Monitorear los controles de seguridad, tales como firewalls, IDS/IPS (sistemas de intrusión-detección o de intrusión-prevención), FIM (monitorización de la integridad de archivos), antivirus, controles de acceso, entre otros.
2. Garantizar la detección de todas las fallas en los controles de seguridad y solucionarlas oportunamente.
3. Revisar los cambios implementados en el entorno (por ejemplo, incorporación de nuevos sistemas, cambios en las configuraciones del sistema o la red) antes de finalizar el cambio
4. Si se implementan cambios en la estructura organizativa (por ejemplo, la adquisición o fusión de una empresa), se debe realizar una revisión formal del impacto en el alcance y en los requisitos de las PCI DSS.
5. Se deben realizar revisiones y comunicados periódicos para confirmar que los requisitos de las PCI DSS se siguen implementando y que el personal cumple con los procesos de seguridad.

6. Estas revisiones también se pueden usar para verificar que se mantiene la evidencia correspondiente, por ejemplo, registros de auditorías, informes de análisis de vulnerabilidades, revisiones de firewall, etc.

CAPITULO IV

PROPUESTA

Desarrollo de la metodología para la implementación y gestión de un sistema de seguridad para servicios transaccionales.

1. INTRODUCCIÓN

El presente trabajo fue realizado con el objetivo de reforzar los distintos nodos de las plataformas tecnológicas en las que se almacena la información administrativa, contable y operativa existentes en la institución relacionadas a los servicios transaccionales vigentes y futuros. Enfocados en resguardar la seguridad de la información en las telecomunicaciones, redes internas, aplicaciones, canales web y enlaces de datos, se realiza el levantamiento de información preliminar para determinar el punto en el que inicia la aplicación de la metodología. Por lo tanto, de acuerdo con lo expuesto, se planteó trabajar sobre la base de distintas normativas para cada una de estas áreas. Para el control de infraestructura, gestión de seguridad y control de configuraciones avanzadas de equipos de seguridad en la red se tomaron en cuenta los siguientes estándares:

- **ANSI/TIA 942:** Estándar utilizado para la instalación de infraestructura de los centros de datos, proporciona una capa de seguridad física de equipos y minimiza el riesgo de inoperatividad resultado de fallas en sistemas eléctricos, mecánicos u otros problemas ocasionados por mala gestión de la red. Se tomó en cuenta por su distribución en capas definidas como TIER I, II, III y IV.

- **ANSI/EIA-568:** Estándar del cableado estructurado para productos y servicios de telecomunicaciones que proporciona una mejor velocidad, y añade una capa adicional de seguridad en los centros de distribución como *racks* y *switch´s*. Se tomó en cuenta por el blindaje y seguridad a nivel de enrutamiento desde el punto físico conectado a los equipos de la red.
- **ISO270001:** Estándar de buenas prácticas para mantener un sistema de gestión de seguridad de la información que incluye 114 controles de seguridad. Se toma en cuenta debido a su gran influencia en el sector financiero y su aplicación en la normativa interna de la institución.
- **PCI DSS:** Es el estándar de seguridad de datos para la industria en tarjetas de pago que trabaja en los puntos de configuración y auditoría en los sistemas de información del usuario final del sistema. Su uso se desarrolló para el servicio transaccional de tarjetas de débito y crédito y hoy en día, son un referente sobre la configuración de equipos y segmentación de la red para salvaguardar la información utilizada en las nuevas tecnologías denominadas *Fintech*,

Además de la normativa nacional establecida por los entes de control, las resoluciones de la SEPS en vigencia:

- **Resolución No. SEPS-IGT-IR-ISF-ITIC-IGJ-2017-103:** Habla sobre la gestión de los procesos de seguridad informática y requerimientos mínimos de inclusión. El cumplimiento de esta normativa es indispensable para la adhesión y funcionamiento de servicios transaccionales.
- **Resolución No. SEPS-IGT-IR-IGJ-2018-0279:** Habla sobre la gestión del riesgo operativo para las instituciones controladas por la SEPS en los puntos de administración del riesgo, factores del riesgo, procedimientos y políticas de gestión

de tecnología de la información y para la gestión del riesgo legal. Esta normativa habla en ámbitos más generales sobre las responsabilidades de la gestión de los eventos de riesgo operativo informático.

- **Resolución No. JB-2005-834:** Normativa de la SBS que habla sobre la gestión del riesgo operativo y administración del riesgo informático de manera general en instituciones de la banca. Se toma como puntos de referencia ya que habla sobre puntos importantes de la administración de la seguridad de la información en los servicios provistos por terceros.

2. DISEÑO DE LA METODOLOGÍA

La presente metodología tiene como objetivo identificar los diferentes estados de desarrollo en los que una institución financiera de la Economía Popular y Solidaria se encuentra a nivel de seguridad tecnológica tomando en cuenta los siguientes hitos:

- Estado de madurez tecnológica institucional
- Definición de alcance normativo institucional
- Gobierno de TI - Directrices PETI
- Gestión del Proyecto
- Implementando la solución
- Pruebas funcionales de desarrollo.

El trabajo realizado se basó en la información presentada en las entrevistas con las áreas de Riesgos, Operaciones y Tecnología, y su alcance se definió con miras a cumplir con el Plan Operativo Anual de la Cooperativa tomando en cuenta el presupuesto asignado para la

implementación de soluciones de seguridad informática así también como el manual de funciones de la institución. Debido a la sensibilidad de la información, la metodología presentada no contendrá datos específicos sobre el giro del negocio, pero sí funcionales sobre los pasos a implementar en el caso práctico COOPCCP.

CONTENIDO DE LA METODOLOGÍA

El diseño de la metodología para la implementación y gestión de un sistema de seguridad para servicios transaccionales fue desarrollado conteniendo los siguientes puntos:

1. Parámetros de la metodología
2. Definición de controles bases a aplicar
3. Situación actual de la Cooperativa en relación a la metodología
    - 3.1 Análisis de Riesgos
    - 3.2 Diccionario de Controles
    - 3.3 Definición de roles de usuarios
    - 3.4 Requerimientos de infraestructura
    - 3.5 Requerimientos de Procesos
    - 3.6 Requerimientos de Riesgos
    - 3.7 Requerimientos de administración y control
4. Cosas a cambiar en la cooperativa según metodología
    - 4.1 Creación y actualización de procesos
    - 4.2 Actualización de manuales
    - 4.3 Topología de la red propuesta
    - 4.4 Adquisición de equipos de la red
    - 4.5 Configuración de equipos de red según repositorios de *exploits* diarios
    - 4.6 Descripción de pruebas de seguridad de *pentest* necesarias
    - 4.7 Plan de capacitación de seguridad
    - 4.8 Pasos a seguir por el responsable de la seguridad de la información.

A continuación, se muestran los diagramas de estado que ilustran el proceso de levantamiento de la información, análisis de riesgo y la creación del diccionario de datos:

Levantamiento de la información – Diagrama de estado

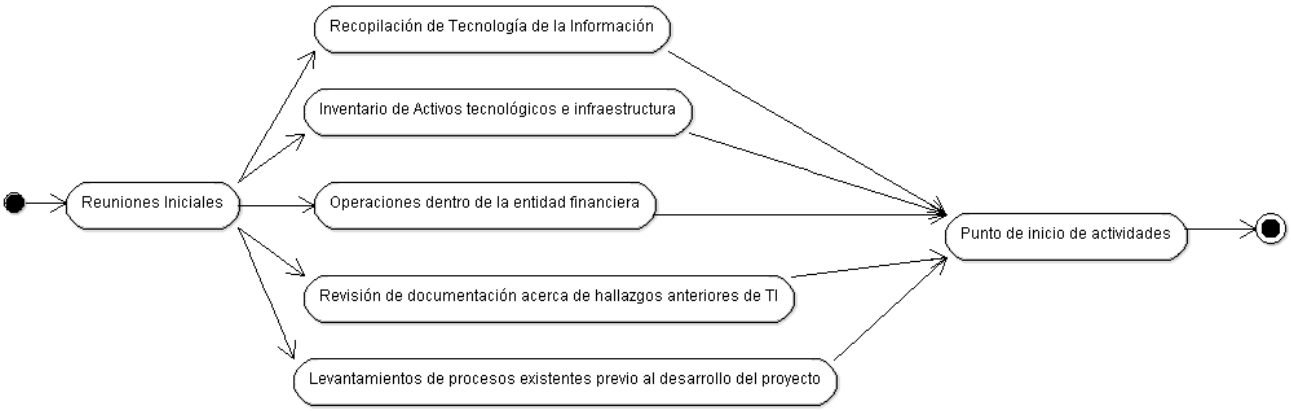


Figura 21: Levantamiento de la información – Diagrama de estado.
Elaborado por: Jean P. Rodríguez.

Análisis de Riesgo – Diagrama de estado

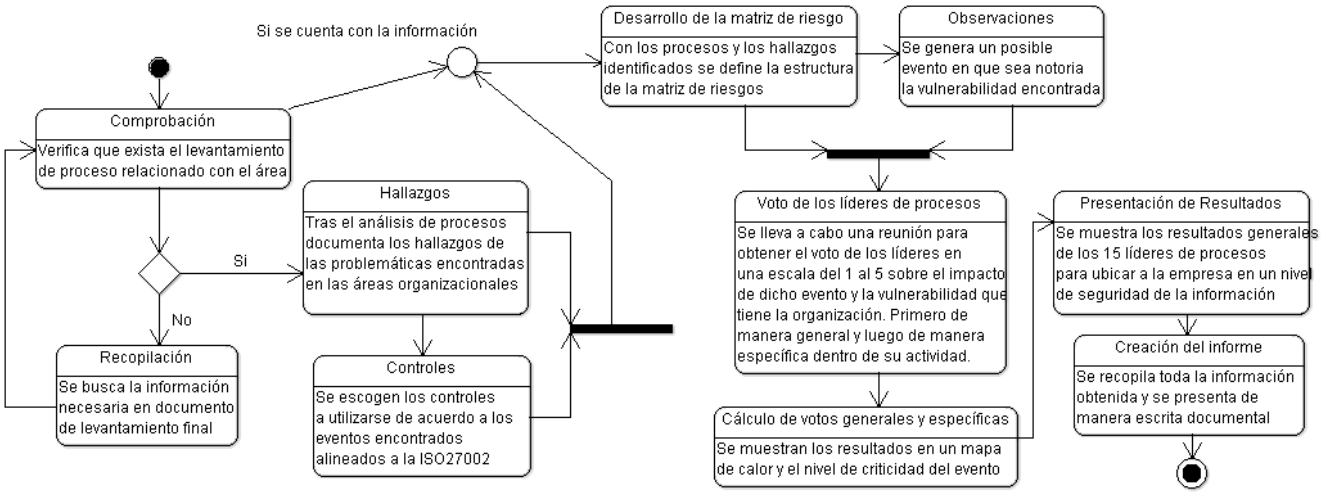


Figura 22: Análisis de Riesgo – Diagrama de Estado
Elaborado por: Jean P. Rodríguez.

Creación del diccionario de datos – Diagrama de estado

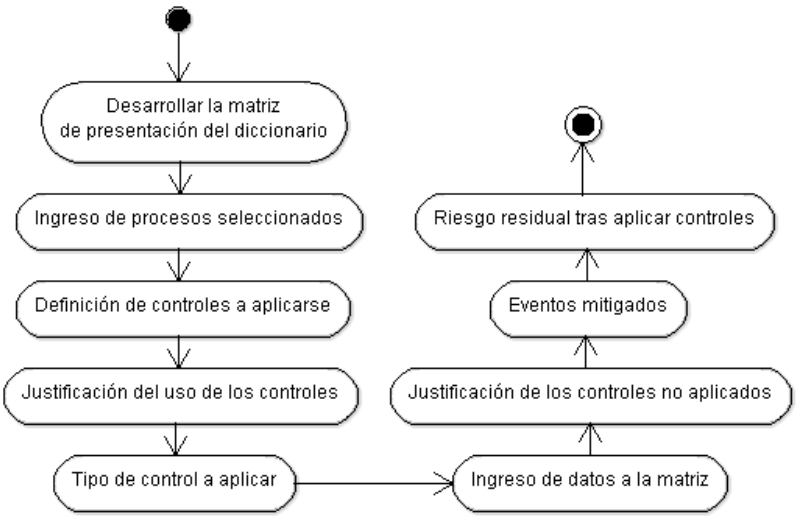


Figura 23: Creación del diccionario de datos – Diagrama de Estado.
Elaborado por: Jean P. Rodríguez.

3. OBJETIVO

Establecer los controles de seguridad de la información para fortalecer los sistemas de seguridad que permitan realizar la implementación de servicios transaccionales de acuerdo con la normativa vigente y legal en instituciones financieras pertenecientes a la economía popular y solidaria.

4. ALCANCE

La presente metodología se aplica para todos los sistemas informáticos existentes en la institución, para los colaboradores de la COOPCCP y sus clientes, quienes participan en los procesos, procedimientos y actividades ligadas a los servicios transaccionales disponibles por la institución, de acuerdo con lo establecido en las normativas internas, normativas impuestas por los entes reguladores externos y las buenas prácticas de seguridad.

5. NORMATIVA LEGAL

El presente documento sirve como guía para la definición del SGSI que describa los requisitos mínimos de seguridad informática. Para su elaboración se tomó en cuenta las regulaciones aplicables en la resolución No JB-2005-834 SECCIÓN VII.- SEGURIDAD DE LA INFORMACIÓN, las recomendaciones del estándar ISO 27002:2013; PCI DSS. Además de la normativa Nº SEPS-IGT-IR-ISF-ITIC-IGJ-2017-103 y SEPS-IGT-IR-IGJ-2018-0279.

6. GLOSARIO DE TÉRMINOS. -

- **Activo de la información:** Toda información que resulta fundamental para la institución, así como para la continuidad del negocio en el desempeño de las funciones de los usuarios, por ende, comprende de un valor significativo.
- **ADS:** *Anomaly Detection system* o Sistema detector de anomalías. Software que identifica el uso normal de una red especificando movimientos anómalos y notificándolos automáticamente. Éste puede ser basado en "ruido" o tipo de comunicación con los servidores. (Scarfone & Mell, 2007)
- **ATM:** Término en inglés, *Automated Teller Machine* o en español, cajero automático, mecanismo que permite al usuario realizar ciertas operaciones bancarias mediante el uso de una tarjeta magnética o chip.
- **Confidencialidad:** Es la garantía de que sólo el personal autorizado accede a la información preestablecida. (ISOTOOLS, 2017)
- **Controles:** Medidas de seguridad tomadas en cuenta para minimizar el riesgo por una actividad inherente al trabajo desempeñado dentro de la institución que ayuden al desarrollo de las actividades sin perjudicar la productividad. (ISOTOOLS, 2017)

- **Disponibilidad:** Característica de la información que refiere al tipo de acceso y las veces que la información está disponible para su consulta en cada vez que sea requerida. Es la garantía de que los usuarios autorizados tienen acceso a la información cada vez que lo requieran a través de los medios adecuados que satisfagan sus necesidades. (ISOTOOLS, 2017)
- **Evento de seguridad de la información:** Un evento de seguridad es cualquier ocurrencia observable en un sistema o una red. (NIST, 2007).
- **Firewall:** Dispositivo de seguridad de la red que monitorea el tráfico de red -entrante y saliente- y decide si permite o bloquea tráfico específico en función de un conjunto definido de reglas de seguridad. (OWASP, 2016)
- **Incidente de seguridad de la información:** Evento asociado a posibles fallas en la seguridad de la información, o una situación con probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.
- **Información:** Es cualquier forma de registro electrónico, óptico, magnético o en otros medios, previamente procesado a partir de datos, que puede ser almacenado, distribuido y sirve para análisis, estudios, toma de decisiones, ejecución de una transacción o entrega de un servicio
- **Información confidencial:** Es toda información considerada vital para el desarrollo de las actividades de la institución que puede involucrar temas sensibles como información personal del cliente, de cuentas de dinero, etc.
- **Información crítica:** Es la información considerada esencial para la continuidad del negocio y para la adecuada toma de decisiones.
- **Integridad:** Es la garantía de mantener la totalidad y exactitud de la información y de los métodos de procesamiento. (ISOTOOLS, 2017)

- **IPS:** *Intrusion Prevention system* o Sistema de prevención de intrusos, son dispositivos que generan alertas en base a la interacción de eventos en la red, se segrega en 4 tipos; según su función en IPS por firmas y anomalías y por su implementación en IPS de red o de host (comúnmente IDS). (NIST, 2007).
- **Logs:** Registros o pistas de modificación de archivos o comportamientos sobre un sistema (incluyendo Sistema Operativo) en base a todos los eventos que afectan un proceso en particular. (OWASP, 2016)
- **Seguridades lógicas:** Se refieren a la seguridad en el uso del software, la protección de los datos, procesos y programas, así como la del acceso ordenado y autorizado de los usuarios a la información. (ISOTOOLS, 2017)
- **Seguridad de la información:** Son los mecanismos implantados que garantizan la confidencialidad, integridad y disponibilidad de la información y los recursos relacionados con ella. (ISOTOOLS, 2017)

7. PARÁMETROS DE LA METODOLOGÍA

A continuación, se definen los parámetros con los que se concatenarán el resultado del análisis previo, exponiendo el estándar que la metodología ha tomado en cuenta para desarrollar las sugerencias a cambios y planificación de pasos para la aplicación de servicios transaccionales.

7.1 MADUREZ INSTITUCIONAL:

Como punto inicial es necesario definir el estado de madurez de la empresa en base a infraestructura, procesos y documentación de seguridad informática, lo que dará un punto de partida sobre el cuál trabajar dentro de la institución. Para estandarización dentro del documento, se definió 4 niveles de madurez:

IDENTIFICATIVO	DEBE CUMPLIR AL MENOS CON
Nivel 1	Infraestructura con enlaces redundantes, procesos de seguridad definidos.
Nivel 2	Infraestructura con enlaces redundantes, centro de datos alterno, políticas, procesos y procedimientos de seguridad de la información definidos, tómese como referencia un Data Center nivel 1.
Nivel 3	Infraestructura con alta disponibilidad (HA) en sus enlaces y equipos de gestión de red en su centro de datos principal, tómese como referencia un Data Center Tier 2, cableado estructurado, sistema de gestión de la seguridad de la información (SGSI) definido y aplicado.
Nivel 4	Infraestructura robusta con alta disponibilidad (HA) tanto en enlaces de comunicación como equipos de gestión de red en su centro de datos principal y alterno, tómese en cuenta un Data Center Tier 3 o superior, cableado estructurado, procesos y políticas de seguridad definidos que además cuente con un Sistema de Gestión Integral (SGI) homologado a normas y buenas prácticas nacionales e internacionales. Segregación de funciones y capacitación o certificación de calidad en sus productos (procesos) departamentales.

Tabla 16: Descripción estados de madurez
Elaborado por: Jean P. Rodríguez.

Dicha matriz toma como punto central la infraestructura de red con la que se cuenta para el desarrollo e inclusión de servicios transaccionales, mismos que pueden variar según los estados de maduración de los proyectos que se lleven a cabo en la institución siempre y cuando se cuente con un cronograma y se evidencien actas de constitución y avance de este.

7.2 ESQUEMA GENERAL ADMINISTRATIVO, HUMANO Y TECNOLÓGICO:

Cada institución es diferente de acuerdo con sus esquemas y propias estructuras organizacionales, sin embargo, indistintamente de sus puestos y definición de funciones, para llevar a cabo las actividades inherentes a la línea de negocio se requiere lo siguiente:

Esquema para estado de madurez nivel 1

Esquema para estado de madurez 1	
Requerimientos mínimos: Infraestructura con enlaces redundantes, procesos de seguridad definidos.	
Administrativos	**Detalle**
Procesos de seguridad	Debe incluir procesos de gestión para accesos a los aplicativos, definición de perfiles administrativos
Respuesta a incidentes	Debe contener planes de acción para escenarios a eventos informáticos como ataques DDoS.
Procesos de auditorías a sistemas	Debe existir al menos 1 ethical hacking al año a los sistemas de información
Políticas internas	Incluye procesos de seguridad definidos para la gestión de contraseñas y controles definidos por los proveedores de tecnología
Talento humano y funciones	Debe contar al menos con una persona que se encargue de la gestión de infraestructura y normas de seguridad
Administrador de base de datos	Se debe contar con un profesional con conocimientos
Equipos de infraestructura	Debe contar con enrutamiento de paquetes
Equipos de seguridad	Configuración de firewall
Servicios de seguridad	N/A

Tabla 17: Esquema para estado de madurez 1
Elaborado por: Jean P. Rodríguez.

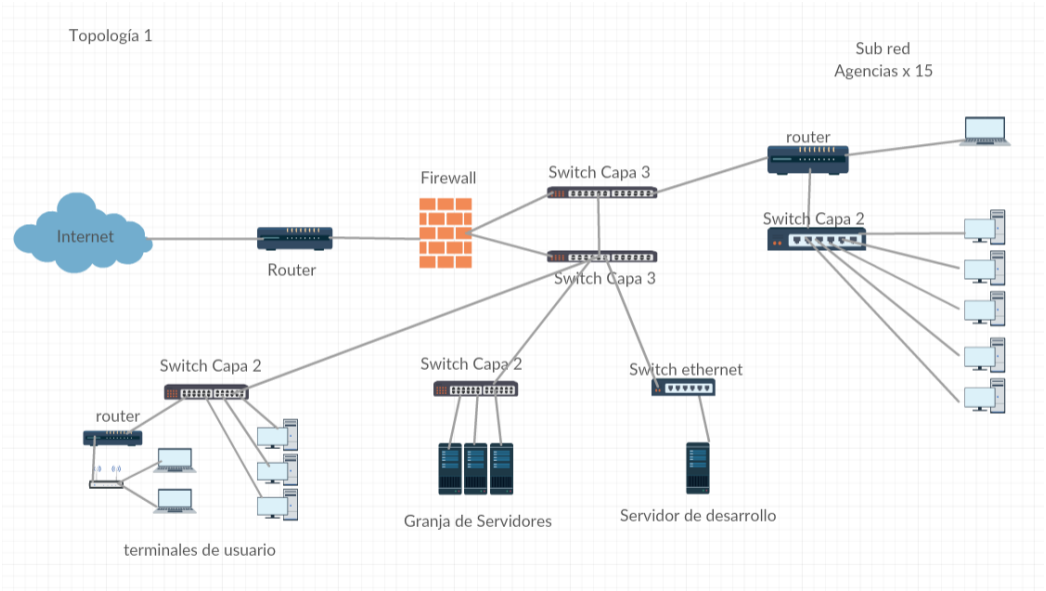


Figura 24: Topología de red para el estado de madurez 1.
Elaborado por: Jean P. Rodríguez.

Esquema para estado de madurez nivel 2

Esquema para estado de madurez 2	
Detalle: Infraestructura con enlaces redundantes, centro de datos alterno, políticas, procesos y procedimientos de seguridad de la información definidos, tómese como referencia un Data Center nivel 1.	
Administrativos	**Detalle**
Procesos de seguridad	Debe contar con procesos de aprobación de cambios, control de perfiles de usuario y niveles de acceso a recursos tecnológicos
Respuesta a incidentes	Debe estar preparado para responder ante ataques volumétricos, bloquear comunicaciones de puertos
Procesos de auditorías a sistemas	Debe planificar pruebas de penetración sobre los servicios, puertos y servicios vigentes
Políticas internas	Debe contar con normativas generales para el trato de la información y gestión de acciones correctivas
Talento humano y funciones	Debe contar con 2 personas dedicadas a administrar la red y 1 persona dedicada a la seguridad de la información
Administrador de base de datos	Se debe contar con un DBA
Equipos de infraestructura	Cluster de energía, VLANS,
Equipos de seguridad	anti spam y bloqueo físico de conexiones a puertos
Servicios de seguridad	N/A

Tabla 18:Esquema para estado de madurez 2
Elaborado por: Jean P. Rodríguez.

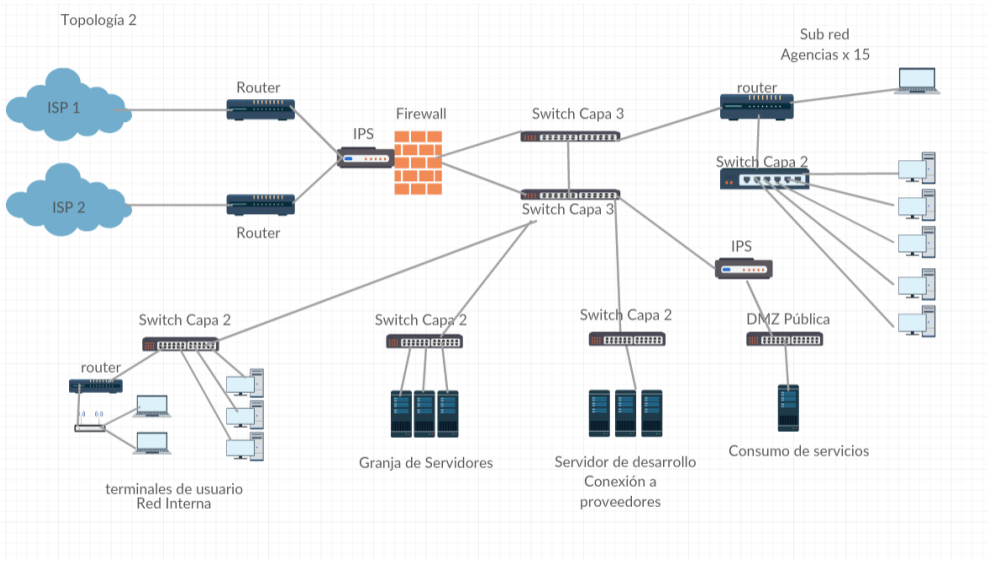


Figura 25: Topología para estado de madurez 2.
Elaborado por: Jean P. Rodríguez.

Esquema para estado de madurez nivel 3

Esquema para estado de madurez 3	
Detalle: Infraestructura con alta disponibilidad (HA) en sus enlaces y equipos de gestión de red en su centro de datos principal, tómese como referencia un Data Center Tier 2, cableado estructurado, sistema de gestión de la seguridad de la información (SGSI) definido y aplicado.	
Administrativos	**Detalle**
Procesos de seguridad	Debe tener procesos definidos para revisar los controles de las normativas aplicadas
Respuesta a incidentes	Debe tener un esquema automático de comunicación y gestión de incidentes con un sistema de cuarentena
Procesos de auditorías a sistemas	Debe existir un profesional dedicado a levantar las pistas de auditoría en cada uno de los sistemas que aseguren el rastro de cada transacción efectuada controlando el storage interno
Políticas internas	Debe contar con la vigencia, monitoreo y control de un SGSI dentro de la institución adicionalmente de documentación y segmentación de la red por el área de TI.
Talento humano y funciones	Debe contar con al menos 4 personas dedicadas a tecnología y 3 personas en seguridad de la información
Administrador de base de datos	Se debe contar con analistas de desarrollo que se encargue clasificar la información en la base de manera estructurada
Equipos de infraestructura	Balanceo de carga, segmentación de topología Redundancia en equipos de direccionamiento de tráfico; IPS, ADS tipo SAS
Equipos de seguridad	WAF, DB FIREWALLS, Redundancia
Servicios de seguridad	Anti Black Seo, SaS de seguridad

Tabla 19: Esquema para estado de madurez 3
Elaborado por: Jean P. Rodríguez.

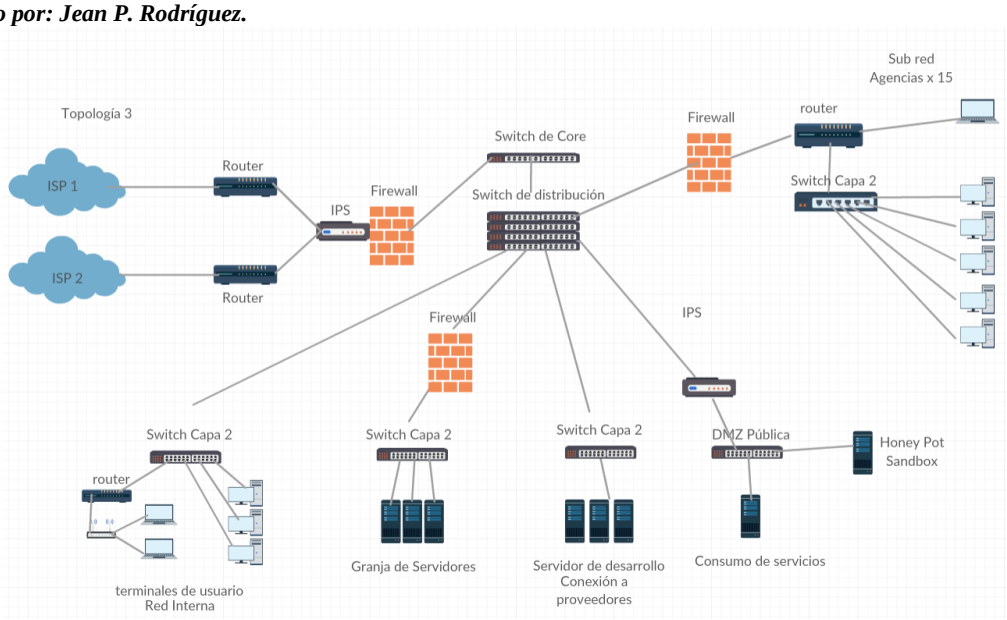


Figura 26: Topología propuesta para estado de madurez 3
Elaborado por: Jean P. Rodríguez.

Esquema para estado de madurez nivel 4

Esquema para estado de madurez 4	
Detalle: Infraestructura robusta con alta disponibilidad (HA) tanto en enlaces de comunicación como equipos de gestión de red en su centro de datos principal y alterno, tómese en cuenta un Data Center Tier 3 o superior, cableado estructurado, procesos y políticas de seguridad definidos que además cuente con un Sistema de Gestión Integral (SGI) homologado a normas y buenas prácticas nacionales e internacionales. Segregación de funciones y capacitación o certificación de calidad en sus productos (procesos) departamentales.	
Administrativos	**Detalle**
Procesos de seguridad	Debe incluir un proceso a detalle sobre las pruebas de penetración con al menos el desarrollo de caja gris
Respuesta a incidentes	Debe contar con un sistema de bloqueo dinámico y cuarentena en el terminal infectado, correlacionar los eventos y permitir al Oficial de seguridad de la información sobre el evento mientras la pantalla se encuentra
Procesos de auditorías a sistemas	Debe considerar ataques de movimientos horizontales y scripts con payloads de botnets autoejecutables en distintos segmentos de la red
Políticas internas	Debe constar con políticas basadas en Inteligencia Artificial que puedan correlacionar los eventos y responder de acuerdo a un nivel de criticidad establecido por un CSIRT
Talento humano y funciones	Debe contar con al menos 6 personas dedicadas a seguridad de la información y un equipo de 7 personas en tecnología
Administrador de base de datos	Debe existir personal que permita aplicar controles criptográficos propios
Equipos de infraestructura	WAF IPS Y ADS TIPO APLIANCE
Equipos de seguridad	SIEM, IPS, ADS, ENDPOINT PROTECTORS, WAF, DBAFIREWALLS,
Servicios de seguridad	CSIRT - ESET LAB

Tabla 20:Esquema para estado de madurez 4.
Elaborado por: Jean P. Rodríguez.

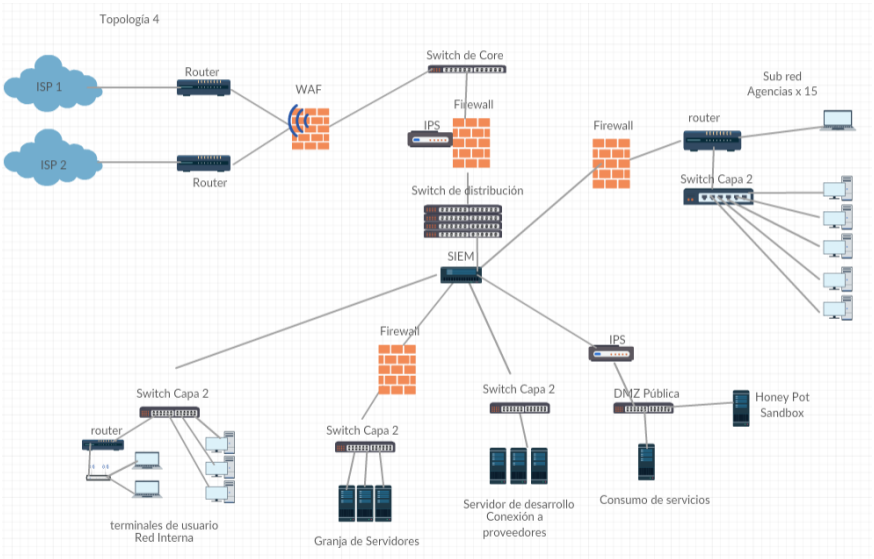


Figura 27: Topología para estado de madurez 4
Elaborado por: Jean P. Rodríguez.

7.3 MATRIZ DE RIESGOS Y CONTROLES DE APLICACIÓN CON PCI

Matriz de análisis de riesgos informáticos para el desarrollo y aplicación de servicios transaccionales en la COOPCCP

Descripción:

La matriz presentada está realizada en base a los eventos de riesgo encontrados en la Cooperativa que se encuentran de acuerdo a la normativa PCI DSS encargada del manejo de información de manera segura en componentes de la red y temas administrativos sobre la seguridad de la información.

COD	Proceso	Líder de proceso	Tipificación del riesgo	Riesgo Evaluado	Observación	Control relacionado (PCI DSS / ISO27002)	Criticidad	Vulnerabilidad	Impacto	Voto/Cargos	Calificación Funcionario 1	Calificación Funcionario 2	Calificación Funcionario 3
G01	General	CPSE	RG01	No existencia / desconocimiento del documento de la política de seguridad de la información	Existe conocimiento / aplicación de alguna norma de la política de seguridad vigente	5.1.1 Documento de SGSI / 5.1.2. Revisión	Medio	1,0	4,5	Voto Impacto	4,5	4,5	4,5
										Voto Vulnerabilidad	1,0	1,0	1,0
G02	General	CPSE	RG02	Falta de conocimiento de coordinación de la seguridad de la información	Conoce algún tipo de organización o responsables de la empresa sobre el tema	6.1.2. Coordinación de la seguridad de la información	Bajo	1,0	2,0	Voto Impacto	2,0	2,0	2,0
										Voto Vulnerabilidad	1,0	1,0	1,0
G03	General	CPSE	RG03	Personas no designadas a resguardar la Seguridad de la información	Conoce alguna persona encargada de regular esto dentro de la empresa	6.1.3. Asignación de responsabilidades relativas a la seguridad de la información	Bajo	0,0	3,0	Voto Impacto	3,0	3,0	3,0
										Voto Vulnerabilidad	0,0	0,0	0,0
G04	General	CPSE	RG04	Falta de personal para la asignación de recursos	Existe alguien a quién se le deba buscar por motivos de seguridad de la información	6.1.4. Proceso de autorización de recursos para el tratamiento de seguridad de la información	Bajo	1,0	3,0	Voto Impacto	3,0	3,0	3,0
										Voto Vulnerabilidad	1,0	1,0	1,0
G05	General	CPSE	RG05	Carencia de acuerdos de confidencialidad para la información sensible	Maneja acuerdos de confidencialidad con las personas que trabaja	6.1.5. Acuerdos de confidencialidad	Bajo	0,0	2,0	Voto Impacto	2,0	2,0	2,0
										Voto Vulnerabilidad	0,0	0,0	0,0
G06	General	CPSE	RG06	Falta de conocimiento del funcionamiento del SGSI	Revisa independiente de las capacitaciones los manuales o políticas de seguridad de la información	6.1.8. Revisión independiente de la seguridad de la información.	Medio	1,0	4,5	Voto Impacto	4,5	4,5	4,5
										Voto Vulnerabilidad	1,0	1,0	1,0
G07	General	CPSE	RG07	No clasificar la información de acuerdo a políticas de la empresa	Maneja algún método para clasificar la sensibilidad de su	7.2.1.Directrices de clasificación de la información	Alto	4,0	4,8	Voto Impacto	4,8	4,8	4,8
										Voto Vulnerabilidad	4,0	4,0	4,0

COD	Proceso	Líder de proceso	Tipificación del riesgo	Riesgo Evaluado	Observación	Control relacionado (PCI DSS / ISO27002)	Criticidad	Vulnerabilidad	Impacto	Voto/Cargos	Calificación Funcionario 1	Calificación Funcionario 2	Calificación Funcionario 3
					información. Sea personal u organizacional								
G08	General	CPSE	RG08	Mal manejo de la información	Existe un debido etiquetado de la información y manipulación del mismo	7.2.2. Etiquetado y manipulado de la información	Medio	1,0	3,8	Voto Impacto	3,8	3,8	3,8
										Voto Vulnerabilidad	1,0	1,0	1,0
G09	General	CPSE	RG09	Falta de controles de acceso físicos	Facilidad para ingresar a diferentes áreas físicas de la organización	9.1.2. Control físico de entradas	Medio	1,0	4,7	Voto Impacto	4,7	4,7	4,7
										Voto Vulnerabilidad	1,0	1,0	1,0
G10	General	CPSE	RG10	Seguridad en el ambiente de trabajo	Seguridad física, de la información dentro de la empresa	9.1.3. Seguridad de oficinas, despachos e instalaciones	Medio	1,0	4,5	Voto Impacto	4,5	4,5	4,5
										Voto Vulnerabilidad	1,0	1,0	1,0
G11	General	CPSE	RG11	No existencia de un procesos para realizar copias de seguridad	Realiza respaldos de su información etiquetada y clasificada debidamente con algún protocolo, explique frecuencia	10.5.1 Copias de seguridad de la información	Alto	5,0	3,8	Voto Impacto	3,8	3,8	3,8
										Voto Vulnerabilidad	5,0	5,0	5,0
G12	General	CPSE	RG12	Falta de controles para el uso de medios extraíbles	Conoce de alguna política de medios extraíbles vigente	10.7.1. Gestión de soportes extraíbles	Bajo	0,0	3,0	Voto Impacto	3,0	3,0	3,0
										Voto Vulnerabilidad	0,0	0,0	0,0
G13	General	CPSE	RG13	Falta de ayuda técnica para generar una contraseña adecuada	Cuál es la manera que usa para asignar sus contraseñas en equipos personales y plataformas web	11.3.1. Uso de contraseñas	Medio	3,3	4,0	Voto Impacto	4,0	4,0	4,0
										Voto Vulnerabilidad	3,3	3,3	3,3
G14	General	CPSE	RG14	Ambiente de trabajo no debidamente manejado	Conoce cuales son los riesgos de tener un puesto de trabajo limpio, qué políticas lleva al respecto	11.3.3. Política de puesto de trabajo despejado y pantalla limpia.	Bajo	0,0	3,0	Voto Impacto	3,0	3,0	3,0
										Voto Vulnerabilidad	0,0	0,0	0,0
G15	General	CPSE	RG15	Falta de seguridad dentro de los pc´s de la empresa	Tiene controles seguros para el acceso a los sistemas operativos de su pc, qué otros accesos utiliza	11.5.1. Procedimientos seguros de inicio de sesión (SO)	Alto	4,5	4,6	Voto Impacto	4,6	4,6	4,6
										Voto Vulnerabilidad	4,5	4,5	4,5
G16	General	CPSE	RG16	Libertad de manejo, compartición de la información	Tienes alguna restricción a páginas web, red interna de la empresa, web mail	11.6.1. Restricción del acceso a la información	Bajo	0,0	2,0	Voto Impacto	2,0	2,0	2,0
										Voto Vulnerabilidad	0,0	0,0	0,0
G17	General	CPSE	RG17			11.7.2. Teletrabajo	Medio	3,0	4,6	Voto Impacto	4,6	4,6	4,6

COD	Proceso	Líder de proceso	Tipificación del riesgo	Riesgo Evaluado	Observación	Control relacionado (PCI DSS / ISO27002)	Criticidad	Vulnerabilidad	Impacto	Voto/Cargos	Calificación Funcionario 1	Calificación Funcionario 2	Calificación Funcionario 3
				Falta de normalización en el teletrabajo	Cuáles son las políticas del teletrabajo conocidas y mantenidas por el usuario					Voto Vulnerabilidad	3,0	3,0	3,0
G18	General	CPSE	RG18	No uso de controles criptográficos	Maneja algún tipo de control criptográfico para la información sensible	12.3.1. Política de uso de los controles criptográficos	Alto	5,0	4,6	Voto Impacto	4,6	4,6	4,6
										Voto Vulnerabilidad	5,0	5,0	5,0
G19	General	CPSE	RG19	Falta de conocimiento en caso de eventos emergentes	A quién y de qué manera notifica los eventos de seguridad que no sean ajustados a sus niveles de acceso	11.3.1. Notificación de los eventos de la seguridad de la información	Bajo	0,0	2,0	Voto Impacto	2,0	2,0	2,0
										Voto Vulnerabilidad	0,0	0,0	0,0
G20	General	CPSE	RG20	Falta de regulación en el cumplimiento del SGSI	Dentro del departamento, existe el encargado de hacer cumplir las normas y políticas de seguridad	15.2.1. Cumplimiento de las normas y políticas de seguridad	Medio	3,0	4,7	Voto Impacto	4,7	4,7	4,7
										Voto Vulnerabilidad	3,0	3,0	3,0
SE01	Servicios Electrónicos	CPSE	SE01	Capacidad para detección	No Existen normas para realizar las configuraciones de firewall y routers	1,1 Normas de configuración para firewalls y routers	Medio	2,0	4,0	Voto Impacto	4,0	4,0	4,0
										Voto Vulnerabilidad	2,0	2,0	2,0
SE02	Servicios Electrónicos	CPSE	SE02	Vulnerabilidades a nivel de puertos	Existe un protocolo de uso de puertos para los dispositivos de red como Firewalls, Routers, Switch	1,1,6 Documentación y justificación de negocio para el uso de todos los servicios, protocolos y puertos permitidos	Medio	4,0	1,0	Voto Impacto	1,0	1,0	1,0
										Voto Vulnerabilidad	4,0	4,0	4,0
SE03	Servicios Electrónicos	CPSE	SE03	Desactualización de políticas de firewall	No existe un monitoreo de las políticas establecidas	1,1,7 Requisito de la revisión de las normas de firewalls y routers cada 6 meses	Alto	4,0	5,0	Voto Impacto	5,0	5,0	5,0
										Voto Vulnerabilidad	4,0	4,0	4,0
SE04	Servicios Electrónicos	CPSE	SE04	Prevención de ataques para escuchar segmentos de la red	Existen reglas de control sobre las comunicaciones a puertos de enlace	1,2 Desarrollar configuraciones para FW y Routers que restrinjan conexiones no confiables	Medio	2,0	3,0	Voto Impacto	3,0	3,0	3,0
										Voto Vulnerabilidad	2,0	2,0	2,0

COD	Proceso	Líder de proceso	Tipificación del riesgo	Riesgo Evaluado	Observación	Control relacionado (PCI DSS / ISO27002)	Criticidad	Vulnerabilidad	Impacto	Voto/Cargos	Calificación Funcionario 1	Calificación Funcionario 2	Calificación Funcionario 3
SE05	Servicios Electrónicos	CPSE	SE05	Exploración no autorizada de la red con tramas de payloads muy altas	Tiene conocimiento de la cantidad de información debe recibir como máximo cada transacción realizada por cada servicio transaccional?	1,2,1 Restringir el tráfico entrante y saliente a cantidades estrictamente necesarias	Medio	3,0	4,0	Voto Impacto	4,0	4,0	4,0
										Voto Vulnerabilidad	3,0	3,0	3,0
SE06	Servicios Electrónicos	CPSE	SE06	Suplantación de identidad en tablas de enrutamiento	Existe filtrado de información que protejan los AP contra un reseteo forzado ?	1,2,2 Asegure y sincronice los archivos de configuración de Routers	Alto	3,0	5,0	Voto Impacto	5,0	5,0	5,0
										Voto Vulnerabilidad	3,0	3,0	3,0
SE07	Servicios Electrónicos	CPSE	SE07	No existencia de primera línea de defensa	No dispone de equipos de seguridad perimetral específicos para los servicios transaccionales	1,2,3 Instale firewalls de perímetro entre las redes inalámbricas	Alto	3,0	5,0	Voto Impacto	5,0	5,0	5,0
										Voto Vulnerabilidad	3,0	3,0	3,0
	Servicios Electrónicos	CPSE	SE08	Alteración no consentida de BDD	Existen mecanismos que permitan prohibir las afectaciones de bases de datos?	1,3 Prohibi} el acceso directo público entre internet y todo componente del sistema de datos	Alto	4,0	4,0		4,0	4,0	4,0
											4,0	4,0	4,0
SE09	Servicios Electrónicos	CPSE	SE09	Acceso no censado a modificaciones en base de datos	No dispone de bloqueo de puertos en servidores de comunicación pública	1,3,1 Restricciones de acceso a la base de datos del acceso por puerto 80	Medio	3,0	4,0	Voto Impacto	4,0	4,0	4,0
										Voto Vulnerabilidad	3,0	3,0	3,0
SE10	Servicios Electrónicos	CPSE	SE10	Movimientos laterales no autorizados	Los equipos de seguridad vigente no realizan doble verificación del tráfico en la red interna	1,3,4 Implementar medidas anti suplantación para detectar y bloquear direcciones IP manipuladas	Medio	3,0	4,0	Voto Impacto	4,0	4,0	4,0
										Voto Vulnerabilidad	3,0	3,0	3,0
SE11	Servicios Electrónicos	CPSE	SE11	Permite realizar nuevas concesiones en equipos de seguridad	No constan con una configuración estática y es susceptible a cambios no autorizados	1,3,6 Filtrado dinámico de paquetes	Alto	4,0	5,0	Voto Impacto	5,0	5,0	5,0
										Voto Vulnerabilidad	4,0	4,0	4,0
SE12	Servicios Electrónicos	CPSE	SE12	Conocimiento de la información privada de la Cooperativa	No realizan enmascaramiento de las direcciones que se manejan para las aplicaciones web	1,3,8 No divulgación de direcciones IP a sectores no autorizados	Alto	4,0	4,0	Voto Impacto	4,0	4,0	4,0
										Voto Vulnerabilidad	4,0	4,0	4,0
		CPSE	SE13			1,4 Firewalls móviles	Medio	2,0	3,0	Voto Impacto	3,0	3,0	3,0

COD	Proceso	Líder de proceso	Tipificación del riesgo	Riesgo Evaluado	Observación	Control relacionado (PCI DSS / ISO27002)	Criticidad	Vulnerabilidad	Impacto	Voto/Cargos	Calificación Funcionario 1	Calificación Funcionario 2	Calificación Funcionario 3
SE13	Servicios Electrónicos			Foco de infección móvil por concesiones permitidas	No se realiza instalación de proxys o firewalls de redes móviles en los dispositivos para gestión comercial					Voto Vulnerabilidad	2,0	2,0	2,0
SE14	Servicios Electrónicos	CPSE	SE14	No personalización de usuarios y accesos a sistemas	Existen sistemas a los cuales no se han realizado un cambios desde la implementación del sistema para usuarios y administradores	2,1 Cambio de valores predeterminados por proveedor	Alto	5,0	3,0	Voto Impacto	3,0	3,0	3,0
										Voto Vulnerabilidad	5,0	5,0	5,0
SE15	Servicios Electrónicos	CPSE	SE15	Falta de configuraciones de seguridad para los equipos de la topología	No se encuentra una metodología ni base técnica para realizar las configuraciones de los equipos de red	2,2 Desarrollo de normas de configuración para todos los componentes del sistema	Bajo	3,0	1,0	Voto Impacto	1,0	1,0	1,0
										Voto Vulnerabilidad	3,0	3,0	3,0
SE16	Servicios Electrónicos	CPSE	SE16	Acceso sobredimensionado de servidores	Existen aplicaciones que comparten servidor, lo que ocasiona que tengan accesos superiores a los requeridos y por ende, se identifica un nuevo vector de ataque	2,2,1 Segregación de servidores para evitar que coexistan servidores que necesiten diferentes niveles de seguridad	Medio	3,0	4,0	Voto Impacto	4,0	4,0	4,0
										Voto Vulnerabilidad	3,0	3,0	3,0
SE17	Servicios Electrónicos	CPSE	SE17	Uso de protocolos y servicios innecesarios en servidores	No se encuentra un registro de los protocolos necesarios por aplicación y servidor	2,2,2 Seguridad en Servicios, protocolos y daemons necesarios	Alto	4,0	5,0	Voto Impacto	5,0	5,0	5,0
										Voto Vulnerabilidad	4,0	4,0	4,0
SE18	Servicios Electrónicos	CPSE	SE18	Comunicaciones P2P no controladas	No implementan protocolos de comunicación seguros como SSH para la conexión remota en sus agencias	2,2,3 Funciones de seguridad adicionales para servicios requeridos que no se consideren seguros	Medio	3,0	2,0	Voto Impacto	2,0	2,0	2,0
										Voto Vulnerabilidad	3,0	3,0	3,0

COD	Proceso	Líder de proceso	Tipificación del riesgo	Riesgo Evaluado	Observación	Control relacionado (PCI DSS / ISO27002)	Criticidad	Vulnerabilidad	Impacto	Voto/Cargos	Calificación Funcionario 1	Calificación Funcionario 2	Calificación Funcionario 3
SE19	Servicios Electrónicos	CPSE	SE19	Componentes por default en direcciones públicas y conocimiento de versiones de software utilizados	Se evidenció que las pantallas de error y ficheros de instalación se encuentran aún en los servidores públicos	2,2,5 Eliminar las funciones innecesarias de ejecución de sistemas de archivos, instalación o drivers de servidores públicos	Medio	4,0	3,0	Voto Impacto	3,0	3,0	3,0
										Voto Vulnerabilidad	4,0	4,0	4,0
SE20	Servicios Electrónicos	CPSE	SE20	Accesos administradores de sistemas sin cifrar	No se evidencia una cultura de cifrado de los datos para contraseñas ni bases de datos	2,3 Cifrado de acceso administrativo	Medio	3,0	4,0	Voto Impacto	4,0	4,0	4,0
										Voto Vulnerabilidad	3,0	3,0	3,0
SE21	Servicios Electrónicos	CPSE	SE21	Tramos de comunicación de terceros desprotegido	Todas las comunicaciones de red deben ser certificadas con un aval de seguridad	2,6 Los proveedores hosting compartido deben proteger el entorno y los datos que viajan a través de sus sistemas	Medio	1,0	5,0	Voto Impacto	5,0	5,0	5,0
										Voto Vulnerabilidad	1,0	1,0	1,0
SE22	Servicios Electrónicos	CPSE	SE22	Sustracción de OTPs quemadas	No se deben guardar las OTPs una vez utilizadas por el usuario	3,2 No almacenar datos confidenciales de autenticación después de recibir autorización	Medio	3,0	3,0	Voto Impacto	3,0	3,0	3,0
										Voto Vulnerabilidad	3,0	3,0	3,0
SE23	Servicios Electrónicos	CPSE	SE23	Pérdida de sigilo bancario	No se debe enviar datos de números de cuentas principales por servicios transaccionales con tecnologías emergentes	3,3 Ocultar el PAM	Medio	5,0	2,0	Voto Impacto	2,0	2,0	2,0
										Voto Vulnerabilidad	5,0	5,0	5,0
SE24	Servicios Electrónicos	CPSE	SE24	Visualización de contraseñas en texto plano	No se utiliza cifrado de bases de datos por medio de componentes de seguridad ni en discos físicos	3,4,1 Tipo de cifrado de la información del socio	Medio	3,0	4,0	Voto Impacto	4,0	4,0	4,0
										Voto Vulnerabilidad	3,0	3,0	3,0
SE25	Servicios Electrónicos	CPSE	SE25	Conocimiento de las claves de encriptación para enlaces de comunicaciones	Deben guardarse las llaves de encriptación de las tarjetas en medios físicos y digitales siempre y cuando exista un cifrado del archivo	3,5,1 Reducción de custodios de acceso a las claves criptográficas	Alto	4,0	5,0	Voto Impacto	5,0	5,0	5,0
										Voto Vulnerabilidad	4,0	4,0	4,0
SE26	Servicios Electrónicos	CPSE	SE26	Pérdida de contraseñas	No se evidencia cumplimiento de cambio de contraseñas de servidores	3,6,6 Operaciones manuales de administración de claves	Medio	2,0	3,0	Voto Impacto	3,0	3,0	3,0
										Voto Vulnerabilidad	2,0	2,0	2,0

COD	Proceso	Líder de proceso	Tipificación del riesgo	Riesgo Evaluado	Observación	Control relacionado (PCI DSS / ISO27002)	Criticidad	Vulnerabilidad	Impacto	Voto/Cargos	Calificación Funcionario 1	Calificación Funcionario 2	Calificación Funcionario 3
SE27	Servicios Electrónicos	CPSE	SE27	Robo de contraseña	No se realiza un seguimiento activo sobre el cambio de contraseñas en el área de Tecnología o para los sistemas administrativos	3,6,7 Políticas documentadas, probadas e implementadas	Alto	4,0	4,0	Voto Impacto	4,0	4,0	4,0
										Voto Vulnerabilidad	4,0	4,0	4,0
SE28	Servicios Electrónicos	CPSE	SE28	Visualización de todo el tráfico de red	La Cooperativa no tiene implementado ningún certificado de seguridad en sus comunicaciones	4,1 Uso de cifrado en el traspaso de información	Medio	3,0	4,0	Voto Impacto	4,0	4,0	4,0
										Voto Vulnerabilidad	3,0	3,0	3,0
SE29	Servicios Electrónicos	CPSE	SE29	Infección de equipos	No se realizan reportes del uso de los antivirus	5,1 Implementación de Antivirus	Medio	1,0	5,0	Voto Impacto	5,0	5,0	5,0
										Voto Vulnerabilidad	1,0	1,0	1,0
SE30	Servicios Electrónicos	CPSE	SE30	Capacidad de respuesta de antivirus	Se deben probar periódicamente los antivirus para certificar su funcionamiento.	5,1,1 Probar la funcionabilidad de los antivirus	Medio	3,0	4,0	Voto Impacto	4,0	4,0	4,0
										Voto Vulnerabilidad	3,0	3,0	3,0
SE31	Servicios Electrónicos	CPSE	SE31	Funcionalidad del antivirus	No se encuentra un sistema de evaluación del funcionamiento de la herramienta por parte del área de Riesgos	5,2 Evaluación de Antivirus	Medio	2,0	5,0	Voto Impacto	5,0	5,0	5,0
										Voto Vulnerabilidad	2,0	2,0	2,0
SE32	Servicios Electrónicos	CPSE	SE32	Baja de protección temporal	Existen equipos en los que se puede acceder a la modificación de las preferencias de los antivirus	5,3 Proteger contra alteraciones a los antivirus	Medio	3,0	3,0	Voto Impacto	3,0	3,0	3,0
										Voto Vulnerabilidad	3,0	3,0	3,0
SE33	Servicios Electrónicos	CPSE	SE33	Desconocimiento de la capacidad de respuesta ante incidentes de la red	El pentest debe ser llevado a los servicios vigentes de la COOPCCP	6,1 Proceso de identificación de vulnerabilidades	Medio	2,0	5,0	Voto Impacto	5,0	5,0	5,0
										Voto Vulnerabilidad	2,0	2,0	2,0
SE34	Servicios Electrónicos	CPSE	SE34	Infección de equipos por servicios legítimos de Windows	No existe una actualización periódica de los parches de seguridad	6,2 Parches de seguridad	Alto	4,0	5,0	Voto Impacto	5,0	5,0	5,0
										Voto Vulnerabilidad	4,0	4,0	4,0
SE35	Servicios Electrónicos	CPSE	SE35	Software vulnerable	Diseño de código seguir	6,3Desarrollo de software	Medio	3,0	4,0	Voto Impacto	4,0	4,0	4,0
										Voto Vulnerabilidad	3,0	3,0	3,0

COD	Proceso	Líder de proceso	Tipificación del riesgo	Riesgo Evaluado	Observación	Control relacionado (PCI DSS / ISO27002)	Criticidad	Vulnerabilidad	Impacto	Voto/Cargos	Calificación Funcionario 1	Calificación Funcionario 2	Calificación Funcionario 3
SE36	Servicios Electrónicos	CPSE	SE36	Escalabilidad de infección	Se debe realizar una DMZ que esté controlada por un IPS como contingencia	6,4,1 Separación de los ambientes de desarrollo y producción	Medio	1,0	5,0	Voto Impacto	5,0	5,0	5,0
										Voto Vulnerabilidad	1,0	1,0	1,0
SE37	Servicios Electrónicos	CPSE	SE37	Perdida de sigilo bancario	Filtrado de datos de socios	6,4,3 Datos de producción	Alto	4,0	4,0	Voto Impacto	4,0	4,0	4,0
										Voto Vulnerabilidad	4,0	4,0	4,0
SE38	Servicios Electrónicos	CPSE	SE38	Base de datos corrompida	Los perfiles de prueba y desarrollo deben ser eliminados para asegurar una instalación limpia	6,4,4 Eliminación de datos y cuentas de prueba	Medio	4,0	3,0	Voto Impacto	3,0	3,0	3,0
										Voto Vulnerabilidad	4,0	4,0	4,0
SE39	Servicios Electrónicos	CPSE	SE39	Desconocimiento de vectores de ataque en BDD	El personal técnico debe capacitarse sobre la respuesta a nuevos tipos de incidentes en las bases de datos	6,5 Conocimiento técnico de vulnerabilidades en el desarrollo de código	Alto	5,0	3,0	Voto Impacto	3,0	3,0	3,0
										Voto Vulnerabilidad	5,0	5,0	5,0
SE40	Servicios Electrónicos	CPSE	SE40	Acción en eventos de riesgo	Se debe realizar talleres de acción sobre los eventos de seguridad	6,5,1 Talleres de tipos de vulnerabilidades y métodos	Alto	4,0	5,0	Voto Impacto	5,0	5,0	5,0
										Voto Vulnerabilidad	4,0	4,0	4,0
SE41	Servicios Electrónicos	CPSE	SE41	Pérdida de claves cifradas	El personal técnico debe realizar el almacenamiento correcto de las claves y su encriptación	6,5,3 Almacenamiento cifrado inseguro	Alto	4,0	4,0	Voto Impacto	4,0	4,0	4,0
										Voto Vulnerabilidad	4,0	4,0	4,0
SE42	Servicios Electrónicos	CPSE	SE42	Red vulnerable	No existen controles de acceso apropiado para las bases de datos ni para los sistemas web administrables	6,5,8 Control de accesos inapropiados a BDD y HTTP	Alto	4,0	5,0	Voto Impacto	5,0	5,0	5,0
										Voto Vulnerabilidad	4,0	4,0	4,0
SE43	Servicios Electrónicos	CPSE	SE43	Aceptación de concesiones sin verificar	es importante deshabilitar la aceptación automática de certificados de seguridad cuando se pierde la concesión y	6,5,9 Falsificación de solicitudes entre sitios	Medio	3,0	4,0	Voto Impacto	4,0	4,0	4,0
										Voto Vulnerabilidad	3,0	3,0	3,0

COD	Proceso	Líder de proceso	Tipificación del riesgo	Riesgo Evaluado	Observación	Control relacionado (PCI DSS / ISO27002)	Criticidad	Vulnerabilidad	Impacto	Voto/Cargos	Calificación Funcionario 1	Calificación Funcionario 2	Calificación Funcionario 3
					relación de confianza entre redes								
SE44	Servicios Electrónicos	CPSE	SE44	Control de inicio de sesión	Se debe homologar a la política de seguridad los controles de sesión para los usuarios de los sistemas transaccionales	6,5,10 Autenticación y administración de sesión interrumpida	Medio	3,0	2,0	Voto Impacto	2,0	2,0	2,0
										Voto Vulnerabilidad	3,0	3,0	3,0
SE45	Servicios Electrónicos	CPSE	SE45	Falta de control de primera línea	Es necesario un WAF para poder denegar las solicitudes directas a los sistemas transaccionales sin siquiera pasar por la red interna	6,6 Seguridad en aplicaciones Web -	Alto	4,0	4,0	Voto Impacto	4,0	4,0	4,0
										Voto Vulnerabilidad	4,0	4,0	4,0
SE46	Servicios Electrónicos	CPSE	SE46	Pérdida de sigilo bancario	Exceso de conocimiento del personal	7,2 Sistema de control que restringa el acceso a información del socio dentro de sistemas internos no autorizados	Medio	4,0	3,0	Voto Impacto	3,0	3,0	3,0
										Voto Vulnerabilidad	4,0	4,0	4,0
SE47	Servicios Electrónicos	CPSE	SE47	falta de pistas de auditoría	Cada sistema transaccional debe tener definidas las pistas de auditoría y estar en capacidad de ajustarse según requerimiento	8,1 Generar controles de auditoría para personal con perfil administrativo sobre los servicios	Alto	4,0	5,0	Voto Impacto	5,0	5,0	5,0
										Voto Vulnerabilidad	4,0	4,0	4,0
SE48	Servicios Electrónicos	CPSE	SE48	Control de inicio de sesión	Se debe homologar a la política de seguridad los controles de sesión para los usuarios de los sistemas transaccionales	8,1,8 Control de accesos a los sistemas	Medio	3,0	4,0	Voto Impacto	4,0	4,0	4,0
										Voto Vulnerabilidad	3,0	3,0	3,0
SE49	Servicios Electrónicos	CPSE	SE49	Inicio no autorizado	Es necesario implementar claves de doble factor para los sistemas administrativos que generen cambios directos al negocio	8,2 Autenticación de doble factor para servicios sensibles	Medio	3,0	3,0	Voto Impacto	3,0	3,0	3,0
										Voto Vulnerabilidad	3,0	3,0	3,0

COD	Proceso	Líder de proceso	Tipificación del riesgo	Riesgo Evaluado	Observación	Control relacionado (PCI DSS / ISO27002)	Criticidad	Vulnerabilidad	Impacto	Voto/Cargos	Calificación Funcionario 1	Calificación Funcionario 2	Calificación Funcionario 3
SE50	Servicios Electrónicos	CPSE	SE50	Cambio de contraseñas no consentidas	Es necesario implementar claves de doble factor para los sistemas administrativos que generen cambios directos al negocio	8,2,2 Generación de nuevas claves para los cambios y modificaciones del sistema	Alto	3,0	5,0	Voto Impacto	5,0	5,0	5,0
										Voto Vulnerabilidad	3,0	3,0	3,0
SE51	Servicios Electrónicos	CPSE	SE51	Teletrabajo no autorizados	Para el acceso a la red por medio de una ip pública es necesario realizar una doble autenticación	8,3 Autenticación de doble factor para conexiones remotas permitidas	Medio	3,0	4,0	Voto Impacto	4,0	4,0	4,0
										Voto Vulnerabilidad	3,0	3,0	3,0
SE52	Servicios Electrónicos	CPSE	SE52	Falta de documentación para procesos de seguridad	No se encuentran identificados los informes de funcionamiento y aplicación de la política de seguridad	8,4 Documentación e identificación de procesos	Medio	2,0	3,0	Voto Impacto	3,0	3,0	3,0
										Voto Vulnerabilidad	2,0	2,0	2,0
SE53	Servicios Electrónicos	CPSE	SE53	Suplantación de identidad en tablas de enrutamiento	Se debe llevar un registro de usuarios distintos a los patrones ya conocidos para evitar suplantación	8,5 Gestión de contraseñas genéricas	Medio	2,0	4,0	Voto Impacto	4,0	4,0	4,0
										Voto Vulnerabilidad	2,0	2,0	2,0
SE54	Servicios Electrónicos	CPSE	SE54	Afectaciones a bases de datos no autorizadas	Ningún sistema de administración tendrá acceso a modificar directamente la base de datos	8,7 Los usuarios administradores tendrán acceso restringido a cualquier base de datos que contenga información de tarjetas o instrumentos requeridos para efectuar una transacción.	Medio	2,0	3,0	Voto Impacto	3,0	3,0	3,0
										Voto Vulnerabilidad	2,0	2,0	2,0
SE55	Servicios Electrónicos	CPSE	SE55	acceso físico no autorizado	Es importante resguardar el acceso al área de procesamiento de datos	9 Restricción del acceso físico a los datos del socio	Medio	2,0	5,0	Voto Impacto	5,0	5,0	5,0
										Voto Vulnerabilidad	2,0	2,0	2,0
SE56	Servicios Electrónicos	CPSE	SE56	Pérdida de información	No se evidencia un procedimiento de etiquetado de la información	9,6 Clasificación de la información	Medio	3,0	3,0	Voto Impacto	3,0	3,0	3,0
										Voto Vulnerabilidad	3,0	3,0	3,0
SE57	Servicios Electrónicos	CPSE	SE57	Recuperación de información sensible no autorizada	Se deben aplicar métodos que aseguren la destrucción de información crítica para el negocio	9,8 Destrucción de medios	Medio	2,0	3,0	Voto Impacto	3,0	3,0	3,0
										Voto Vulnerabilidad	2,0	2,0	2,0

COD	Proceso	Líder de proceso	Tipificación del riesgo	Riesgo Evaluado	Observación	Control relacionado (PCI DSS / ISO27002)	Criticidad	Vulnerabilidad	Impacto	Voto/Cargos	Calificación Funcionario 1	Calificación Funcionario 2	Calificación Funcionario 3
SE58	Servicios Electrónicos	CPSE	SE58	Incapacidad de rastreo	Todos los sistemas deben contener sus pistas de auditoría	10,1 Implementación de pistas de auditoría	Alto	4,0	5,0	Voto Impacto	5,0	5,0	5,0
										Voto Vulnerabilidad	4,0	4,0	4,0
SE59	Servicios Electrónicos	CPSE	SE59	Transacciones sin responsable	Toda pista de auditoría debe estar atada a un usuario	10,3 Registrar pistas por evento	Alto	4,0	5,0	Voto Impacto	5,0	5,0	5,0
										Voto Vulnerabilidad	4,0	4,0	4,0
SE60	Servicios Electrónicos	CPSE	SE60	Vulnerabilidades de sincronización	Es necesario homologar el reloj de todos los sistemas para poder correlacionar eventos	10,4 Actualización de relojes del sistema	Alto	4,0	4,0	Voto Impacto	4,0	4,0	4,0
										Voto Vulnerabilidad	4,0	4,0	4,0
SE61	Servicios Electrónicos	CPSE	SE61	Alteración de pistas de auditoría	Las pistas de auditoría deben estar configuradas como solo lectura dentro de bases de datos y no deben permitirse cambiar desde perfiles administrativos	10,5 Protección de pistas de auditoría	Alto	5,0	5,0	Voto Impacto	5,0	5,0	5,0
										Voto Vulnerabilidad	5,0	5,0	5,0
SE62	Servicios Electrónicos	CPSE	SE62	Comportamiento sospechoso	Es importante rastrear toda actividad atípica llevada a cabo en las instituciones	10,6 Anomalías en el sistema	Medio	3,0	4,0	Voto Impacto	4,0	4,0	4,0
										Voto Vulnerabilidad	3,0	3,0	3,0
SE63	Servicios Electrónicos	CPSE	SE63	Pérdida de información normativa	Se debe llevar un registro de todas las pistas de auditoría y tenerlas disponibles para cuando el ente regulador la requiera	10,7 Conservar el historial de auditoría al menos 1 año y 3 meses para revisión inmediata	Alto	3,0	5,0	Voto Impacto	5,0	5,0	5,0
										Voto Vulnerabilidad	3,0	3,0	3,0
SE64	Servicios Electrónicos	CPSE	SE64	Adhesión de equipos no autorizados	No se encuentra informes de monitoreo de tráfico o seguimiento de tramas que cuenten los saltos de dispositivos	11,1 Implementación de sistema que detecten puntos de acceso con tecnología 802,11	Medio	3,0	4,0	Voto Impacto	4,0	4,0	4,0
										Voto Vulnerabilidad	3,0	3,0	3,0
SE65	Servicios Electrónicos	CPSE	SE65	Adhesión de equipos no autorizados	Es importante llevar actualizado los puntos de accesos	11,1,1 Inventario de puntos de acceso	Alto	4,0	4,0	Voto Impacto	4,0	4,0	4,0
										Voto Vulnerabilidad	4,0	4,0	4,0
SE66	Servicios Electrónicos	CPSE	SE66	Adhesión de equipos no autorizados	No se encuentran planes de acción contra este tipo de vulnerabilidades	11,1,2 Plan de acción contra equipos no autorizados	Medio	3,0	4,0	Voto Impacto	4,0	4,0	4,0
										Voto Vulnerabilidad	3,0	3,0	3,0
SE67	Servicios Electrónicos	CPSE	SE67		Es importante realizar una revisión interna y externa		Alto	4,0	5,0	Voto Impacto	5,0	5,0	5,0

COD	Proceso	Líder de proceso	Tipificación del riesgo	Riesgo Evaluado	Observación	Control relacionado (PCI DSS / ISO27002)	Criticidad	Vulnerabilidad	Impacto	Voto/Cargos	Calificación Funcionario 1	Calificación Funcionario 2	Calificación Funcionario 3
				Debilidades de los sistemas de seguridad implementados	de los componentes de la red	11,2 Análisis interno y externo de las vulnerabilidades de la red				Voto Vulnerabilidad	4,0	4,0	4,0
SE68	Servicios Electrónicos	CPSE	SE68	Seguridad no debidamente administrada	Un proveedor externo debe realizar un pentest cada 3 meses	11,2,2 Pentest Externo	Alto	5,0	5,0	Voto Impacto	5,0	5,0	5,0
										Voto Vulnerabilidad	5,0	5,0	5,0
SE69	Servicios Electrónicos	CPSE	SE69	Pentest sin valor real	No se encuentra una directriz clara sobre las solicitudes a los pentest realizados a la institución por proveedores externos	11,3 las metodologías de pruebas de penetración	Medio	3,0	4,0	Voto Impacto	4,0	4,0	4,0
										Voto Vulnerabilidad	3,0	3,0	3,0
SE70	Servicios Electrónicos	CPSE	SE70	Intentos de intrusión efectivos	No existe una persona dedicada a realizar la expertiz técnica sobre los controles y tráfico de la red	11,4 Monitoreo Activo	Medio	3,0	4,0	Voto Impacto	4,0	4,0	4,0
										Voto Vulnerabilidad	3,0	3,0	3,0
SE71	Servicios Electrónicos	CPSE	SE71	Infecciones y pérdida de la información	Si no se cumple los lineamientos de la metodología no se puede asegurar la integridad, disponibilidad y confidencialidad de los datos	12,1 Mantenimiento de la política de seguridad	Alto	3,0	5,0	Voto Impacto	5,0	5,0	5,0
										Voto Vulnerabilidad	3,0	3,0	3,0

Tabla 21: Matriz de riesgos PCI DSS - COOPCCP
Elaborado por: Jean P. Rodríguez.

Matriz de control en relación para el desarrollo y aplicación de servicios transaccionales en la COOPCCP

Descripción:

La matriz presentada está realizada en base a los eventos de riesgo encontrados en la Cooperativa que se encuentran de acuerdo a la normativa PCI DSS encargada del manejo de información de manera segura en componentes de la red y temas administrativos sobre la seguridad de la información.

# Control	Tipo de control	Área	Problema	Descripción	Definición del Control	Aplicación
1	Correctivo	General	Falta de conocimiento de coordinación de la seguridad de la información	No existe coordinación de seguridad de la información a nivel general	6.1.2. Coordinación de la seguridad de la información	coordinar la información de acuerdo a las protocolos del nuevo manual
2	Preventivo	General	Personas no designadas a resguardar la Seguridad de la información	Falta de coordinación para delegar responsables sobre la seguridad de información	6.1.3. Asignación de responsabilidades relativas a la seguridad de la información	Asignación formal de los responsables del cumplimiento de la seguridad de la información dentro de La Compañía
3	Correctivo	General	Falta de personal para la asignación de recursos	No existe personal que se dedique a la asignación de recursos	6.1.4. Proceso de autorización de recursos para el tratamiento de seguridad de la información	Asignación de los responsables de manejar las herramientas que ayuden a resguardar la seguridad de la información
4	Correctivo	General	Carencia de acuerdos de confidencialidad para la información sensible	No poseen acuerdos de confidencialidad para el manejo de filtración de información	6.1.5. Acuerdos de confidencialidad	Generar documentos de acuerdos de confidencialidad que se manejen a diferentes niveles según sean requeridos por los empleados, consultores, etc.
5	Preventivo	General	Falta de conocimiento del funcionamiento del SGSI	No existe una cultura sobre el sistema de gestión de seguridad integrada	6.1.8. Revisión independiente de la seguridad de la información.	Generar capacitaciones acerca de la seguridad de la información para cada Perona dentro de la COOPCCP de acuerdo a su nivel de acceso
6	Correctivo	General	Falta de controles de acceso físicos	No hay un control de los accesos físicos a la información de la empresa	9.1.2. Control físico de entradas	Establecer el uso en toda la empresa de controles de accesos apropiados tomando como referencia el tipo de área al que se requiere ingresar
7	Correctivo	General	Seguridad en el ambiente de trabajo	Las oficinas, despachos e instalaciones no dan la seguridad física de la información	9.1.3. Seguridad de oficinas, despachos e instalaciones	Desarrollar proyectos de implementación de sitios seguros que tengan como principal objetivo el resguardo de los bienes que se almacenen, sean físicos o virtuales

# Control	Tipo de control	Área	Problema	Descripción	Definición del Control	Aplicación
8	Preventivo	General	No existencia de un procesos para realizar copias de seguridad	No se realizan copias de la información a nivel general	10.5.1 Copias de seguridad de la información	Establecer un protocolo que hable del proceso a seguir para respaldar información de todos los equipos de la empresa.
9	Correctivo	General	Falta de ayuda técnica para generar una contraseña adecuada	Carencia de personal que ayude a la generación de contraseñas según el tipo de información	11.3.1. Uso de contraseñas	Desarrollar una política de gestiona miento de contraseñas que cuenten con el apoyo de herramientas que ayuden a los usuarios de dicha política gestionar sus claves.
10	Correctivo	General	Libertad de manejo, compartición de la información	La información se comparte de forma libre dentro de la empresa	11.6.1. Restricción del acceso a la información	Normalizar los métodos de restricción a la información para empleados con sanciones, incurrencias en eventos de riesgo o alguna otra medida especial.. Mediante el uso de herramientas o controles de cualquier tipo.
11	Correctivo	General	Falta de normalización en el teletrabajo	El trabajo que se realiza fuera de la empresa no posee regularizaciones ni normativas	11.7.2. Teletrabajo	Normalizar el procedimiento de salida de activos e información de alta sensibilidad de la empresa con el uso de herramientas y documentación que respalde la toma de responsabilidades en caso de pérdida, robo o intervención del equipo que viole la política de seguridad
12	Preventivo	General	No uso de controles criptográficos	No poseen controles sobre la protección de seguridad es decir contraseñas especiales	12.3.1. Política de uso de los controles criptográficos	Desarrollar una política de uso de los controles criptográficos adecuados dentro de la empresa para las personas que lo requieran y manejen directamente información de más alto nivel
13	Preventivo	General	Falta de conocimiento en caso de eventos emergentes	No poseen un plan de seguridad de información en casos de emergencia	11.3.1. Notificación de los eventos de la seguridad de la información	Desarrollar un protocolo KISS para aplicarlo en todos los niveles de la COOPCCP y así exista un correcto mantenimiento continuo de la política.
14	Correctivo	General	Falta de regulaciones el cumplimiento del SGSI	No se posee regulaciones de cumplimiento de las normas y políticas de seguridad	15.2.1. Cumplimiento de las normas y políticas de seguridad	Se deben efectuar supervisiones y enviar comunicados periódicamente de acuerdo a temas que se relacionen con la seguridad de la información.
15	Correctivo	Tecnología Seguridad Información	Capacidad para detección	No Existen normas para realizar las configuraciones de firewall y routers	1,1 Normas de configuración para firewalls y routers	Crear un proceso de cambios, registro y actualización de las configuraciones de Firewalls

# Control	Tipo de control	Área	Problema	Descripción	Definición del Control	Aplicación
16	Correctivo	Tecnología Seguridad Infor.	Vulnerabilidades a nivel de puertos	Existe un protocolo de uso de puertos para los dispositivos de red como Firewalls, Routers, Switch	1,1,6 Documentación y justificación de negocio para el uso de todos los servicios, protocolos y puertos permitidos	Todos los dispositivos deben incluir una lista de los servicios, protocolos y puertos, dicho documento debe ser anexado a las revisiones trimestrales del Switch
17	Correctivo	Tecnología Seguridad Información	Desactualización de políticas de firewall	No existe un monitoreo de las políticas establecidas	1,1,7 Requisito de la revisión de las normas de firewalls y routers cada 6 meses	Todas las reglas deben ser revisadas y validadas al menos con una periodicidad de cada 6 meses
18	Correctivo	Tecnología Seguridad Información	Prevención de ataques para escuchar segmentos de la red	Existen reglas de control sobre las comunicaciones a puertos de enlace	1,2 Desarrollar configuraciones para FW y Routers que restrinjan conexiones no confiables	Desarrollar políticas de FW que permitan bloquear la comunicación de manera adecuada
19	Correctivo	Tecnología Seguridad Información	Exploración no autorizada de la red con tramas de payloads muy altas	Tiene conocimiento de la cantidad de información debe recibir como máximo cada transacción realizada por cada servicio transaccional?	1,2,1 Restringir el tráfico entrante y saliente a cantidades estrictamente necesarias	Definir el tráfico que existe en cada comunicación por cada servicios transaccional y documentarlo para negar todo tráfico que sobrepase el permitido en la trama
20	Correctivo	Tecnología Seguridad Información	Suplantación de identidad en tablas de enrutamiento	Existe filtrado de información que protejan los AP contra un reseteo forzado ?	1,2,2 Asegure y sincronice los archivos de configuración de Routers	Certificar que los archivos de configuración de todos los routers estén protegidos contra el acceso no autorizado
21	Correctivo	Tecnología Seguridad Información	No existencia de primera línea de defensa	No dispone de equipos de seguridad perimetral específicos para los servicios transaccionales	1,2,3 Instale firewalls de perímetro entre las redes inalámbricas	Gestionar el uso de un firewall perimetral o Web Aplication Firewall que permita controlar las conexiones establecidas para cada sesión
22	Correctivo	Tecnología Seguridad Información	Alteración no consentida de BDD	Existen mecanismos que permitan prohibir las afectaciones de bases de datos?	1,3 Prohibir el acceso directo público entre internet y todo componente del sistema de datos	Utilizar SP´S de conexión entre la base de datos y el servidor de aplicaciones para que, ninguna consulta o segmento de red alcance directamente las bases de datos
23	Correctivo	Tecnología Seguridad Información	Acceso no censado a modificaciones en base de datos	No dispone de bloqueo de puertos en servidores de comunicación pública	1,3,1 Restricciones de acceso a la base de datos del acceso por puerto 80	Segmentar la red para la inclusión de una DMZ que limite el tráfico entrante únicamente para los componentes del sistema que proporcionen servicios
24	Correctivo		Movimientos laterales no autorizados			

# Control	Tipo de control	Área	Problema	Descripción	Definición del Control	Aplicación
		Tecnología Seguridad Información		Los equipos de seguridad vigente no realizan doble verificación del tráfico en la red interna	1,3,4 Implementar medidas anti suplantación para detectar y bloquear direcciones IP manipuladas	Realizar las configuraciones necesarias para no permitir tráfico proveniente de internet con una dirección de fuente interna
25	Correctivo	Tecnología Seguridad Información	Permite realizar nuevas concesiones en equipos de seguridad	No constan con una configuración estática y es susceptible a cambios no autorizados	1,3,6 Filtrado dinámico de paquetes	Segregar los componentes de la red y permitir únicamente conexiones para equipos previamente registrados bajo un esquema inicial
26	Correctivo	Tecnología Seguridad Información	Conocimiento de la información privada de la Cooperativa	No realizan enmascaramiento de las direcciones que se manejan para las aplicaciones web	1,3,8 No divulgación de direcciones IP a sectores no autorizados	Desarrollar métodos para ocultar direcciones IP NAT, Proxys, filtrado de anuncios de enrutamiento o uso de direcciones RFC1918
27	Correctivo	Tecnología Seguridad Información	Foco de infección móvil por concesiones permitidas	No se realiza instalación de proxys o firewalls de redes móviles en los dispositivos para gestión comercial	1,4 Firewalls móviles	Implementar políticas de instalación de firewalls personal en los dispositivos móviles propiedad de la COOPCCP
28	Correctivo	Tecnología Seguridad Información	No personalización de usuarios y accesos a sistemas	Existen sistemas a los cuales no se han realizado un cambios desde la implementación del sistema para usuarios y administradores	2,1 Cambio de valores predeterminados por proveedor	Llevar una bitácora de cambio de contraseñas de los sistemas configurados con la ayuda del proveedor, restringiendo todos los accesos con una periodicidad de 3 meses
29	Correctivo	Tecnología Seguridad Información	Falta de configuraciones de seguridad para los equipos de la topología	No se encuentra una metodología ni base técnica para realizar las configuraciones de los equipos de red	2,2 Desarrollo de normas de configuración para todos los componentes del sistema	Desarrollar un manual de configuraciones del sistema homologado a normas de seguridad como CIS, NIST, SANS
30	Correctivo	Tecnología Seguridad Información	Acceso sobredimensionado de servidores	Existen aplicaciones que comparten servidor, lo que ocasiona que tengan accesos superiores a los requeridos y por ende, se identifica un nuevo vector de ataque	2,2,1 Segregación de servidores para evitar que coexistan servidores que necesiten diferentes niveles de seguridad	Segregar la red cuantas veces sea necesaria para asignar niveles de seguridad con autonomía
31	Correctivo	Tecnología Seguridad Información	Uso de protocolos y servicios innecesarios en servidores	No se encuentra un registro de los protocolos necesarios por aplicación y servidor	2,2,2 Seguridad en Servicios, protocolos y daemons necesarios	llevar un registro de los servicios y protocolos utilizados por cada servidor y negar las conexiones que no sean necesarias

# Control	Tipo de control	Área	Problema	Descripción	Definición del Control	Aplicación
32	Correctivo	Tecnología Seguridad Información	Comunicaciones P2P no controladas	No implementan protocolos de comunicación seguros como SSH para la conexión remota en sus agencias	2,2,3 Funciones de seguridad adicionales para servicios requeridos que no se consideren seguros	Definir tecnologías seguras como SSH, SFTP, SSL, IPSec VPN
33	Correctivo	Tecnología Seguridad Información	Componentes por default en direcciones públicas y conocimiento de versiones de software utilizados	Se evidenció que las pantallas de error y ficheros de instalación se encuentran aún en los servidores públicos	2,2,5 Eliminar las funciones innecesarias de ejecución de sistemas de archivos, instalación o drivers de servidores públicos	Realizar pentest internos enfocados a encontrar vulnerabilidades por ficheros de instalación no eliminados de manera segura
34	Correctivo	Tecnología Seguridad Información	Accesos administradores de sistemas sin cifrar	No se evidencia una cultura de cifrado de los datos para contraseñas ni bases de datos	2,3 Cifrado de acceso administrativo	Utilizar tecnologías de cifrado para el acceso administrativo para administraciones basadas en la web y otros tipos de acceso administrativo como SSH, VPN, SSL/TLS
35	Correctivo	Tecnología Seguridad Información	Tramos de comunicación de terceros desprotegido	Todas las comunicaciones de red deben ser certificadas con un aval de seguridad	2,6 Los proveedores hosting compartido deben proteger el entorno y los datos que viajan a través de sus sistemas	Solicitar y llevar un registro de las certificaciones PCI, ISO 270002 así también como de su vigencia
36	Correctivo	Tecnología Seguridad Información	Sustracción de OTPs quemadas	No se deben guardar las OTPs una vez utilizadas por el usuario	3,2 No almacenar datos confidenciales de autenticación después de recibir autorización	Generar métodos de encriptación para las OTP+s generadas volviéndolas ilegibles al momento de realizar revisiones de auditoría
37	Correctivo	Tecnología Seguridad Información	Pérdida de sigilo bancario	No se debe enviar datos de números de cuentas principales por servicios transaccionales con tecnologías emergentes	3,3 Ocultar el PAN	De las transacciones enviadas por servicios financieros no ligados a la infraestructura de la institución, no enviar valores con el número de cuenta principal asociado
38	Correctivo	Tecnología Seguridad Información	Visualización de contraseñas en texto plano	No se utiliza cifrado de bases de datos por medio de componentes de seguridad ni en discos físicos	3,4,1 Tipo de cifrado de la información del socio	Utilizar cifrado de base de datos o de disco, en caso de ser de disco, definir distintos acceso a la información.
39	Correctivo	Tecnología Seguridad Información	Conocimiento de las claves de encriptación para enlaces de comunicaciones	Deben guardarse las llaves de encriptación de las tarjetas en medios físicos y digitales siempre y cuando exista un cifrado del archivo	3,5,1 Reducción de custodios de acceso a las claves criptográficas	Definir el procedimiento para cambio de claves criptográficas y realizarlo con una periodicidad de al menos semestral

# Control	Tipo de control	Área	Problema	Descripción	Definición del Control	Aplicación
40	Correctivo	Tecnología Seguridad Información	Pérdida de contraseñas	No se evidencia cumplimiento de cambio de contraseñas de servidores	3,6,6 Operaciones manuales de administración de claves	Se debe realizar un procedimiento que deje evidencias sobre los cambios de las claves que se encuentren en texto plano, contando con controles dobles y conocimiento dividido de dicha contraseña
41	Correctivo	Tecnología Seguridad Información	Robo de contraseña	No se realiza un seguimiento activo sobre el cambio de contraseñas en el área de Tecnología o para los sistemas administrativos	3,6,7 Políticas documentadas, probadas e implementadas	Realizar la revisión de las políticas de manejo de contraseñas físicas y lógicas
42	Correctivo	Tecnología Seguridad Información	Visualización de todo el tráfico de red	La Cooperativa no tiene implementado ningún certificado de seguridad en sus comunicaciones	4,1 Uso de cifrado en el traspaso de información	Utilizar únicamente SSL/TLS, IPSEC, SSH para los comunicaciones por las que viaja la información de el socio y su PAN
43	Correctivo	Tecnología Seguridad Información	Infección de equipos	No se realizan reportes del uso de los antivirus	5,1 Implementación de Antivirus	Revisar periódicamente por actualizaciones de antivirus mensualmente
44	Correctivo	Tecnología Seguridad Información	Capacidad de respuesta de antivirus	Se deben probar periódicamente los antivirus para certificar su funcionamiento.	5,1,1 Probar la funcionabilidad de los antivirus	Preparar laboratorios de penetración de red que prueben sobre la ejecución en dispositivos finales y servidores
45	Correctivo	Tecnología Seguridad Información	Funcionalidad del antivirus	No se encuentra un sistema de evaluación del funcionamiento de la herramienta por parte del área de Riesgos	5,2 Evaluación de Antivirus	Realizar un informe de actualización, periodicidad de análisis y registros de auditoría que tenga al menos lo especificado en el punto 10,7
46	Correctivo	Tecnología Seguridad Información	Baja de protección temporal	Existen equipos en los que se puede acceder a la modificación de las preferencias de los antivirus	5,3 Proteger contra alteraciones a los antivirus	Mantener controles por medio del AD para prohibir acciones de modificación
47	Correctivo	Tecnología Seguridad Información	Desconocimiento de la capacidad de respuesta ante incidentes de la red	El pentest debe ser llevado a los servicios vigentes de la COOPCCP	6,1 Proceso de identificación de vulnerabilidades	Realizar un Análisis de riesgo contra vulnerabilidades informáticas al menos 1 vez al año
48	Correctivo		Infección de equipos por servicios legítimos de Windows		6,2 Parches de seguridad	

# Control	Tipo de control	Área	Problema	Descripción	Definición del Control	Aplicación
		Tecnología Seguridad Información		No existe una actualización periódica de los parches de seguridad		Verificar constantemente sobre disponibilidad de parches y actualizaciones de seguridad e instalarlos en un máximo de tiempo de 1 mes
49	Correctivo	Tecnología Seguridad Información	Software vulnerable	Diseño de código seguir	6,3Desarrollo de software	Revisar el código por el oficial de seguridad de la información para asegurarse que no existan vulnerabilidades o campos sin encriptar
50	Correctivo	Tecnología Seguridad Información	Escalabilidad de infección	Se debe realizar una DMZ que esté controlada por un IPS como contingencia	6,4,1 Separación de los ambientes de desarrollo y producción	Realizar la separación en la red dentro de una DMZ con un IPS que cense el tráfico saliente
51	Correctivo	Tecnología Seguridad Información	Perdida de sigilo bancario	Filtrado de datos de socios	6,4,3 Datos de producción	Los datos de PAN no se utilizarán para pruebas en desarrollo o pruebas
52	Correctivo	Tecnología Seguridad Información	Base de datos corrompida	Los perfiles de prueba y desarrollo deben ser eliminados para asegurar una instalación limpia	6,4,4 Eliminación de datos y cuentas de prueba	Antes del paso a producción se debe ingresar una base de datos vacía y documentar la conexión a la base de datos de producción.
53	Correctivo	Tecnología Seguridad Información	Desconocimiento de vectores de ataque en BDD	El personal técnico debe capacitarse sobre la respuesta a nuevos tipos de incidentes en las bases de datos	6,5 Conocimiento técnico de vulnerabilidades en el desarrollo de código	Capacitación al personal técnico sobre guías de codificaciones seguras
54	Correctivo	Tecnología Seguridad Información	Acción en eventos de riesgo	Se debe realizar talleres de acción sobre los eventos de seguridad	6,5,1 Talleres de tipos de vulnerabilidades y métodos	Realizar entrevistas para saber cómo el encargado de desarrollo y DBA reaccionaría para evitar errores de inyección de comandos de sistema operativo, LDAP, Xpath, XSS, SQL Injection y desbordamiento de buffer
55	Correctivo	Tecnología Seguridad Información	Pérdida de claves cifradas	El personal técnico debe realizar el almacenamiento correcto de las claves y su encriptación	6,5,3 Almacenamiento cifrado inseguro	Revisar activamente los controles en la política para prevenir errores de cifrado, y revisar las claves y algoritmos criptográficos utilizados
56	Correctivo	Tecnología Seguridad Información	Red vulnerable	No existen controles de acceso apropiado para las bases de datos ni para los sistemas web administrables	6,5,8 Control de accesos inapropiados a BDD y HTTP	Realizar una revisión del uso de los componentes tecnológicos de la cooperativa

# Control	Tipo de control	Área	Problema	Descripción	Definición del Control	Aplicación
57	Correctivo	Tecnología Seguridad Información	Aceptación de concesiones sin verificar	es importante deshabilitar la aceptación automática de certificados de seguridad cuando se pierde la concesión y relación de confianza entre redes	6,5,9 Falsificación de solicitudes entre sitios	Se deben utilizar técnicas de codificación que aseguren que las aplicaciones no confían en las credenciales de autorización ni en los tokens que los exploradores presentan automáticamente
58	Correctivo	Tecnología Seguridad Información	Control de inicio de sesión	Se debe homologar a la política de seguridad los controles de sesión para los usuarios de los sistemas transaccionales	6,5,10 Autenticación y administración de sesión interrumpida	Controlar las sesiones interrumpidas mediante marcas de tokens de sesión como "seguros", no exposición de las ID de la sesión en el URL e incorporación de tiempos de espera inapropiados y rotación de las ID de la sesión después de iniciar sesión satisfactoriamente
59	Correctivo	Tecnología Seguridad Información	Falta de control de primera línea	Es necesario un WAF para poder denegar las solicitudes directas a los sistemas transaccionales sin siquiera pasar por la red interna	6,6 Seguridad en aplicaciones Web -	Implementar un firewall de aplicación web que pueda controlar las aplicaciones públicas mediante herramientas y métodos de evaluación de vulnerabilidades.
60	Correctivo	Tecnología Seguridad Información	Pérdida de sigilo bancario	Exceso de conocimiento del personal	7,2 Sistema de control que restringa el acceso a información del socio dentro de sistemas internos no autorizados	Evaluar los parámetros de conocimiento de los datos del socio PAN para objetos del negocio
61	Correctivo	Tecnología Seguridad Información	falta de pistas de auditoría	Cada sistema transaccional debe tener definidas las pistas de auditoría y estar en capacidad de ajustarse según requerimiento	8,1 Generar controles de auditoría para personal con perfil administrativo sobre los servicios	Implementar pistas de auditoría personalizadas para todos los sistemas de servicios transaccionales
62	Correctivo	Tecnología Seguridad Información	Control de inicio de sesión	Se debe homologar a la política de seguridad los controles de sesión para los usuarios de los sistemas transaccionales	8,1,8 Control de accesos a los sistemas	El oficial de seguridad de la información es el encargado de definir los parámetros para el control de inicio, permanencia y cese de las sesiones en los sistemas de la Cooperativa
63	Correctivo	Tecnología Seguridad Información	Inicio no autorizado	Es necesario implementar claves de doble factor para los sistemas administrativos que generen cambios directos al negocio	8,2 Autenticación de doble factor para servicios sensibles	Implementar autenticación por medio de OTP, token o accesos biométricos para usuarios administradores
64	Correctivo	Tecnología Seguridad Información	Cambio de contraseñas no consentidas	Es necesario implementar claves de doble factor para los sistemas administrativos que generen cambios directos al negocio	8,2,2 Generación de nuevas claves para los cambios y modificaciones del sistema	Manejo de tokens de seguridad vía SMS para realizar cambios de los sistemas sensibles.

# Control	Tipo de control	Área	Problema	Descripción	Definición del Control	Aplicación
65	Correctivo	Tecnología Seguridad Información	Teletrabajo no autorizados	Para el acceso a la red por medio de una IP pública es necesario realizar una doble autenticación	8,3 Autenticación de doble factor para conexiones remotas permitidas	Establecer códigos OTP para conexiones remotas a la intranet de la Cooperativa
66	Correctivo	Tecnología Seguridad Información	Falta de documentación para procesos de seguridad	No se encuentran identificados los informes de funcionamiento y aplicación de la política de seguridad	8,4 Documentación e identificación de procesos	Documentar los cambios señalados en el manual de seguridad de la información
67	Correctivo	Tecnología Seguridad Información	Suplantación de identidad en tablas de enrutamiento	Se debe llevar un registro de usuarios distintos a los patrones ya conocidos para evitar suplantación	8,5 Gestión de contraseñas genéricas	No mantenga un patrón para la asignación de usuarios genéricos, realice una depuración para evitar conflictos de duplicidad de usuarios
68	Correctivo	Tecnología Seguridad Información	Afectaciones a bases de datos no autorizadas	Ningún sistema de administración tendrá acceso a modificar directamente la base de datos	8,7 Los usuarios administradores tendrán acceso restringido a cualquier base de datos que contenga información de tarjetas o instrumentos requeridos para efectuar una transacción.	Los accesos a bases de datos se realizarán únicamente por el DBA y serán documentados según el requerimiento
69	Correctivo	Tecnología Seguridad Información	acceso físico no autorizado	Es importante resguardar el acceso al área de procesamiento de datos	9 Restricción del acceso físico a los datos del socio	Manejar áreas físicas seguras según se especifica en el manual de seguridad de la información
70	Correctivo	Tecnología Seguridad Información	Pérdida de información	No se evidencia un procedimiento de etiquetado de la información	9,6 Clasificación de la información	Utilizar el procedimiento para documentación y etiquetado de la información.
71	Correctivo	Tecnología Seguridad Información	Recuperación de información sensible no autorizada	Se deben aplicar métodos que aseguren la destrucción de información crítica para el negocio	9,8 Destrucción de medios	Una vez terminado el periodo de 10 años por la ley, eliminar mediante el procedimiento de eliminación de información física según se especifica en el manual de seguridades físicas.
72	Correctivo	Tecnología Seguridad Información	Incapacidad de rastreo	Todos los sistemas deben contener sus pistas de auditoría	10,1 Implementación de pistas de auditoría	Habilitar pistas de auditoría para todos los sistema que contemple la vinculación de accesos al sistema, eventos de acceso, transacciones realizadas, intentos de acceso no válidos Uso de cambio de mecanismos de autenticación, creación o eliminación de objetos en el sistema

# Control	Tipo de control	Área	Problema	Descripción	Definición del Control	Aplicación
73	Correctivo	Tecnología Seguridad Información	Transacciones sin responsable	Toda pista de auditoría debe estar atada a un usuario	10,3 Registrar pistas por evento	Las pistas levantadas deben ser: Identificación de usuarios Tipo de evento Fecha y hora Indicación de éxito o fallo Origen del evento Identidad de los datos, componentes del sistema o recurso afectado
74	Correctivo	Tecnología Seguridad Información	Vulnerabilidades de sincronización	Es necesario homologar el reloj de todos los sistemas para poder correlacionar eventos	10,4 Actualización de relojes del sistema	Implementar un servidor NTP.
75	Correctivo	Tecnología Seguridad Información	Alteración de pistas de auditoría	Las pistas de auditoría deben estar configuradas como solo lectura dentro de bases de datos y no deben permitirse cambiar desde perfiles administrativos	10,5 Protección de pistas de auditoría	Implementar controles de encriptación de los datos en los campos de controles de auditoría para prevenir su modificación, cambiarlos a solo lectura.
76	Correctivo	Tecnología Seguridad Información	Comportamiento sospechoso	Es importante rastrear toda actividad atípica llevada a cabo en las instituciones	10,6 Anomalías en el sistema	Llevar un control sobre anomalías de los sistemas transaccionales y censar el tráfico generado
77	Correctivo	Tecnología Seguridad Información	Pérdida de información normativa	Se debe llevar un registro de todas las pistas de auditoría y tenerlas disponibles para cuando el ente regulador la requiera	10,7 Conservar el historial de auditoría al menos 1 año y 3 meses para revisión inmediata	Generar espacio en los discos con proyección a 3 años
78	Correctivo	Tecnología Seguridad Información	Adhesión de equipos no autorizados	No se encuentra informes de monitoreo de tráfico o seguimiento de tramas que cuenten los saltos de dispositivos	11,1 Implementación de sistema que detecten puntos de acceso con tecnología 802,11	Realizar el conteo de saltos de las transacciones para identificar equipos de red no autorizados
79	Correctivo	Tecnología Seguridad Información	Adhesión de equipos no autorizados	Es importante llevar actualizado los puntos de accesos	11,1,1 Inventario de puntos de acceso	Documentar el inventario de activos informáticos regularmente y realizar la verificación de su funcionamiento
80	Correctivo	Tecnología Seguridad Información	Adhesión de equipos no autorizados	No se encuentran planes de acción contra este tipo de vulnerabilidades	11,1,2 Plan de acción contra equipos no autorizados	Realizar una renovación de la concesión de autorización de acceso con los firewalls en modo de puerto de escucha cerrado

# Control	Tipo de control	Área	Problema	Descripción	Definición del Control	Aplicación
81	Correctivo	Tecnología Seguridad Información	Debilidades de los sistemas de seguridad implementados	Es importante realizar una revisión interna y externa de los componentes de la red	11,2 Análisis interno y externo de las vulnerabilidades de la red	Se debe realizar análisis de manera trimestral y darlos a conocer en consejos de administración
82	Correctivo	Tecnología Seguridad Información	Seguridad no debidamente administrada	Un proveedor externo debe realizar un pentest cada 3 meses	11,2,2 Pentest Externo	Idealmente, realizar pentest a los sistemas transaccionales cada 3 meses con un proveedor externo
83	Correctivo	Tecnología Seguridad Información	Pentest sin valor real	No se encuentra una directriz clara sobre las solicitudes a los pentest realizados a la institución por proveedores externos	11,3 las metodologías de pruebas de penetración	Debe incluir lo siguiente: Basada en los enfoque aceptados por la industria (NIST) Cobertura a todo el perímetro de los sistemas electrónicos y sistemas críticos de la red pruebas para validar la segmentación ataques a capa de aplicación, capa de red, y sistema operativo reevaluación sobre el anterior pentest
84	Correctivo	Tecnología Seguridad Información	Intentos de intrusión efectivos	No existe una persona dedicada a realizar la expertiz técnica sobre los controles y tráfico de la red	11,4 Monitoreo Activo	Al menos 1 persona de la Cooperativa debe estar encargada únicamente a realizar pentest a todo momento sin comprometer la operatividad de los servicios transaccionales
85	Correctivo	Tecnología Seguridad Información	Infecciones y pérdida de la información	Si no se cumple los lineamientos de la metodología no se puede asegurar la integridad, disponibilidad y confidencialidad de los datos	12,1 Mantenimiento de la política de seguridad	Implementación de los procesos y seguimiento de cumplimiento de la metodología

Tabla 22: Diccionario de Controles PCI DSS.
Elaborado por: Jean P. Rodríguez

7.4 DESCRIPCIÓN ESTADO DE MADUREZ DE LA EMPRESA

En base a lo expuesto en el levantamiento y análisis de la información se pudieron encontrar algunos puntos fuertes en los que la COOPCCP se encuentra, según la estructura de tecnología y los sistemas manejados conjunto con los trabajos del área de Auditoría, se han implementado controles que, si bien es cierto no mitigan todos los puntos de seguridad, logran mantener un buen perfil sobre métodos de ataque tradicionales. Posicionando a la COOPCCP en un estado de madurez nivel 2

Ventajas	Desventajas
1) Llevan a cabo emulaciones en un módulo sandbox 2) No manejan un factor de doble autenticación 3) Tienen antivirus actualizado y corriendo 4) Utilizan métodos DLP 5) El firewall está configurado 6) Constan de ambiente de desarrollo 7) Tienen control sobre el tráfico de red 8) Tienen enlaces redundantes para 9) Tienen un core alterno 10) Tienen un servidor de correo 11) Implementan controles internos para el uso de la información como bloqueo de puertos, lector de cd. 12) Políticas de red establecidas 13) Políticas de contraseñas en AD y sistemas establecidos y vigentes 14) Controles básicos de auditoría en los sistemas	1) No cuentan con equipos de seguridad redundantes 2) No cuentan con redundancia de enlaces 3) No tienen segmentos de red distribuidos 4) No manejan una DMZ 5) El core está en el mismo segmento de red que el servidor de aplicaciones 6) No existe una configuración de VPN´s segura 7) No existen firewalls de aplicaciones web (WAF) 8) No tienen un correlacionador de eventos (SIEM) 9) No realizan balanceo de carga 10) No manejan firewalls de bases de datos 11) No mantienen certificados de seguridad SSL/TLS 12) No tienen IPS / ADS 13) No existe un sistema 14) No utilizan Vlans 15) No constan de cableado estructurado 16) No mantienen una configuración de firewall seguro. 17) No mantienen configuraciones en modo espejo

Tabla 23: Ventajas y desventajas de la COOPCCP.
Elaborado por: Jean P. Rodríguez.

7.5 TIPOS DE ROLES DE USUARIOS

Para el cumplimiento idóneo de todos los procesos de seguridad así también como las recomendaciones dadas en la implementación de nuevas políticas, es necesario contar con al menos el siguiente personal que corresponda a los distintos roles de usuario:

Gestión de Proyectos		
Nombre	**Descripción**	**Cantidad**
Project Manager	Encargado de difundir los cambios en relación con el presupuesto, tiempo y asignaciones, vela por los intereses de la Cooperativa **Puesto recomendado:** Gerente General	**1**
Líder de proyecto	Encargado de realizar todas las comunicaciones y coordinar el desarrollo, operatividad y mantenimiento de los servicios transaccionales, nexo que asegura el correcto funcionamiento del producto entre todos los proveedores que intervengan. **Puesto recomendado:** Coordinador de productos electrónicos	**1**
Arquitecto	Valida el funcionamiento técnico, adhesión y soporte sobre pruebas de la implementación o cambios en la gestión previo al paso a producción **Puesto recomendado:** Coordinador de desarrollo 1;	**1**
Release Manager	Gestión de la infraestructura, adquisición y negociación con los proveedores de acuerdo con los esquemas y directrices dadas. **Puesto recomendado:** jefe de tecnología.	**2**
Ingeniero de Infraestructura	Responsable de la gestión de herramientas y enlaces de red y comunicaciones internas y externas en la cooperativa, monitoreo de red y hardening de servidores	**3**

Gestión de Proyectos		
Nombre	**Descripción**	**Cantidad**
	Puesto recomendado: Administrador de infraestructura; analista de telecomunicaciones; analista de infraestructura.	
Ingeniero de base de datos	Asesora sobre el manejo de información de la base de datos de la Cooperativa y su interacción con demás tablas, deben censar las conexiones y manejar la reportería sin efectuar cambios directos sin autorización de Project Manager. **Puesto recomendado:** DBA; Coordinador de desarrollo 2; Analista programados.	**3**
Seguridad informática	Encargados de la definición y el cumplimiento de las políticas mediante las cuales el producto o servicios funcionará, análisis de tráfico entrante y saliente, regulación de payloads y cargas; análisis activo a las comunicaciones de la red y saltos horizontales posibles por cada conexión. **Puesto recomendado: j**efe de seguridad; Oficial de seguridad de la información; analista de redes e incidentes; Pentester.	**4**
Líder del producto	Se encarga del uso del producto o servicio entregado a clientes, da las directrices para ajustarla de acuerdo al favorecimiento del negocio. **Puesto recomendado:** Subgerente de negocios.	

Tabla 24: Roles de usuarios para COOPCCP.
Elaborado por: Jean P. Rodríguez.

7.6 REQUISITOS RECOMENDADOS PARA EL CUMPLIMIENTO:

Para el cumplimiento de la normativa SEPS 103 se sugieren cambios a nivel de infraestructura, equipos de seguridades, administración y control y sobre las aplicaciones para los proyectos de: Cooperativa en Línea, IVR, Chatbots transaccionales y todo servicio que contemple la afectación de saldos de cuentas ya sea en consultas o movimientos.

1) Requerimientos de Infraestructura:

CHECK LIST REQUERIMIENTOS - INFRAESTRUCTURA					
Requerimientos Administrativos y de control Cooperativa COOPCCP Fecha: 22/05/2018 Sección 4 - 5		Proyecto Banca en línea - 1ra fase Requerimientos funcionales y normativos Resolución No. SEPS-IGT-IR-ISF-ITIC-IGJ-2017-103			
Guía	**Requerimientos mínimos**	**Responsables**	**Cumple**	**Parcialmente**	**No cumple**
TI	Cambio de Firewall : Por renovación y crecimiento sobre los servicios tecnológicos.	Tecnología		x	
TI	Switch Capa 3: Dispositivos administrables para separar los segmentos de la red – Seguridad	Tecnología			
S4-ART9-13	Storage: Es necesario la implementación de un sistema de respaldos así también como el aumento de storage debido al tipo de información a almacenar.	Tecnología		x	
S4-ART9-16	Centro de Contacto: Generar respaldos mínimos de las llamadas realizadas hasta 6 meses atrás.	Seguridad de la información - TI		x	
TI	Clustering: Redundancia en dispositivos administrables (Switch de agencias, balanceo de carga, etc)	Seguridad de la información - TI			x
S4-ART9-11	Servidor NTP: Alineamiento de los relojes de sistema para transacciones	Seguridad de la información - TI		x	
S4-ART8-1	Data center alterno: Continuidad de operaciones, uso de equipos de respaldo y planes de contingencia.	Tecnología	x		
S4-ART9-14	Centros de atención telefónica y líneas de emergencias (consultas de saldo y bloqueo de tarjetas y cuentas) 24/7	Comercial		x	
Tipo	**Plan sobre controles**	**Responsables**	**Cumple**	**Parcialmente**	**No cumple**
Manual	Políticas sobre parámetros de almacenaje de información en M-Files	Seguridad de la información			X
manual	Definición de logs guardados según importancia las tablas de bases de datos de todos los sistemas	Seguridad de la información		X	
Procedimiento	Configuración de medidas de segmentación de red (Vlans - switching o routing) que permita aislar los puntos de red adecuadamente para evitar el daño masivo en caso de intrusiones.	Seguridad de la información - TI			X
Procedimiento	Configuración de reglas de Firewall así también como equipos de seguridad.	Seguridad de la información - TI			X

Tabla 25:Requerimientos de Infraestructura para COOPCCP.
Elaborado por: Jean P. Rodríguez.

2) Requerimientos de Seguridades:

CHECK LIST REQUERIMIENTOS - SEGURIDADES					
Requerimientos Administrativos y de control Cooperativa COOPCCP Fecha: 22/05/2018 Sección 4 – 5		Proyecto Banca en línea Requerimientos funcionales y normativos Resolución No. SEPS-IGT-IR-ISF-ITIC-IGJ-2017-103			
Guía	**Requerimientos mínimos**	**Responsables**	**Cumple**	**Parcialmente**	**No cumple**
Dispositivo	Web Application Firewall (WAF)	Seguridad de la información			x
S4-ART10-3B	Certificados de seguridad SSL	Seguridad de la información			x
Dispositivo	Security Information Event Management (SIEM)	Seguridad de la información			x
S4-ART9-4	Ethical Hacking	Seguridad de la información		x	
S4-ART9-5	Políticas de desarrollo seguro	Seguridad de la información		x	
S4-ART10-3C	Validación de usuarios por medios distintos a internet.	Seguridad de la información			x
S4-ART10-3A	Escaneo activo sobre duplicidad de páginas web y servicios transaccionales	Seguridad de la información			x
Dispositivo	IPS - Fortigate configuración	Seguridad de la información		x	
Tipo	**Plan sobre controles**	**Responsables**	**Cumple**	**Parcialmente**	**No cumple**
Manual	Actualización del manual de seguridad de la información. Transacciones electrónicas.	Seguridad de la información		x	
Manual	Campaña sobre capacitaciones de seguridad - Activa	Seguridad de la información		x	
Procedimiento	Gestión de la UBA.	Seguridad de la información			x
Procedimiento	Manejo de OTP	Seguridad de la información			x
Procedimiento	Métodos anti Phishing	Seguridad de la información			x
Procedimiento	Monitoreo activo para Black SEO	Seguridad de la información			x

Tabla 26: Requerimientos de Seguridades para COOPCCP.
Elaborado por: Jean P. Rodríguez.

3) Requerimientos de Administración y Control

CHECK LIST REQUERIMIENTOS - ADMINISTRATIVO Y CONTROL					
Requerimientos Administrativos y de control Cooperativa COOPCCP Fecha: 22/05/2018 Sección 4 - 5		Proyecto Banca en línea - 1ra fase Requerimientos funcionales y normativos Resolución No. SEPS-IGT-IR-ISF-ITIC-IGJ-2017-103			
Guía	**Requerimientos mínimos**	**Responsables**	**Cumple**	**Parcialmente**	**No cumple**
S4-ART9-4	Establecer y ejecutar procesos de auditoría por lo menos 1 vez al año para transferencias electrónicas (Ethical Hacking)	Seguridad de la Información - UTIC		x	
S4-ART9-5	Disponer de políticas de desarrollo seguro de software y procedimientos de control de cambios en los sistemas de transferencia electrónica.	Seguridad de la Información - UTIC		x	
S4-ART9-5	Procedimientos de control de cambios en los sistemas de transferencia electrónica.	Seguridad de la Información - Procesos			x
S4-ART9-10	Asegurar que exista una adecuada segregación de funciones para quienes administran, operan, mantienen y en general acceden a los terminales y sistemas de trasferencias electrónicas	Seguridad de la Información - Procesos	x		
S5-ART11-1	El CAD aprobará las políticas, procesos y procedimientos referentes a la seguridad en transferencias electrónicas, definiendo las responsabilidades internas y del proveedor	Riesgos			x
S5-ART11-2	El CAIR, conocerá las políticas, procesos y procedimientos referentes a la seguridad en las transferencias electrónicas y recomendará al CAD su aprobación.	Seguridad de la información			x
S5-ART11-3	El representante legal implementará las políticas, procesos y procedimientos referentes a la seguridad en transferencias electrónicas.	Área Legal - UTIC			x
S5-ART11-4	El área de Tecnología elaborará y propondrá a CAIR las políticas, procesos y procedimientos referentes a la seguridad en transferencias electrónicas y actualizaciones tomando en cuenta estándares y buenas prácticas.	UAIR			x
S5-ART11-5	El auditor interno verificará la efectividad de las medidas de seguridad en las transferencias electrónicas y recomendará medidas correctivas. Además deberá custodiar los informes de las pruebas de vulnerabilidad y ponerlos a disposición de la SEPS cuando lo requiera.	UAI - Riesgos - Tecnología			x
Tipo	**Plan sobre controles**	**Responsables**	**Cumple**	**Parcialmente**	**No cumple**
Manual	Actualización del manual de seguridad de la información - Canales transaccionales.	Seguridad de la información	x		
Manual	Definición de controles para protección contra ataques dirigidos a los servicios web.	Seguridad de la información		x	
Plan de contingencia	Definición de responsables y procedimiento a seguir en caso de existir intrusiones.	Seguridad de la información	x		
Informe	Reporte de avance con cronograma para la Unidad de Auditoría Interna sobre aplicación de controles	Seguridad de la información			x
Informe	Reporte de resultados de Pentest caja blanca realizado de manera interna según manual a los servicios transaccionales	Seguridad de la información		x	

Tabla 27: Requerimientos de Administración y Control COOPCCP.
Elaborado por: Jean P. Rodríguez.

4) Requerimientos de la aplicación

CHECK LIST REQUERIMIENTOS - APLICACIÓN					
Requerimientos Administrativos y de control Cooperativa COOPCCP Fecha: 22/05/2018 Sección 3 - 5 - Disposiciones Generales		Proyecto Banca en línea - 1ra fase Requerimientos funcionales y normativos Resolución No. SEPS-IGT-IR-ISF-ITIC-IGJ-2017-103			
Guía	**Requerimientos mínimos**	**Responsables**	**Cumple**	**Parcialmente**	**No cumple**
103	Plataforma tecnológica que permita encriptación sólida	Proveedor	x		
103	Autorización, autenticación y controles de acceso lógico. Controles biométricos	Proveedor	x		
103	Precautelar la integridad y privacidad de los registros e información de los clientes	Proveedor	x		
103	Reconocer la validez de las transferencias realizadas.	Proveedor	x		
103	Establecer límites para cada transferencia autorizada.	Proveedor	x		
103	Imposibilitar que el valor de la transferencia supere el saldo disponible o el límite establecido para un periodo de tiempo.	Proveedor	x		
103	Permitir que el saldo de la cuenta se consulte, valide, acredite o debite en tiempo real.	Proveedor	x		
103	Facilitar reportes para conciliación de movimientos informando la temporalidad máxima a la que pueda acceder a la consulta.	Proveedor		x	
103	Generar comprobantes necesarios para conciliación.	Proveedor	x		
103	Los sistemas deberán generar archivos que permitan respaldar el detalle de los antecedentes de cada operación usados para certificación o auditoría.	Proveedor	x		
103	Los sistemas deberán contar con perfiles de seguridad que garanticen que la transacción sea efectuada por la persona autorizada.	Proveedor	x		
103	Al detectarse eventos inusuales, situaciones fraudulentas o intentos fallidos de acceso, los sistemas deberán permitir el bloqueo en tiempo real.	Proveedor	x		
103	Se deberá establecer procedimientos seguros para levantar el bloqueo, incluyendo notificación al cliente o usuario.	Proveedor	x		
103	La continuidad de las operaciones debe cubrir elementos fortuitos considerando equipo de respaldo o contingencia. No se debe interrumpir el funcionamiento.	COOPCCP			x
103	Informar al cliente a través de mensajes en línea, el acceso y la ejecución de transacciones realizadas mediante terminales electrónicas.	Proveedor	x		
103	Mantener informados a los clientes/usuarios sobre medida de seguridad al realizar transferencias electrónicas.	COOPCCP			x
103	Informar y capacitar a los clientes /usuarios sobre los procedimientos de: Uso, ubicación, bloqueo, inactivación, reactivación y cancelación de transferencias electrónicas.	COOPCCP			x
103	Establecer y ejecutar auditoría al menos 1 vez al año para identificar vulnerabilidades y mitigar riesgos	COOPCCP			x
103	Disponer de políticas de desarrollo seguro de software y procedimiento de control de cambios con el fin de precautelar la seguridad de información a lo largo del ciclo de vida del desarrollo de software.	Proveedor	x		
103	Incorporar la renovación de claves para acceso al sistema de transferencias electrónicas al menos 1 vez al año.	COOPCCP			x
103	Permitir que el registro y modificación de la información para notificación se realice con medidas de verificación y seguridad.	Proveedor	x		

CHECK LIST REQUERIMIENTOS - APLICACIÓN					
Requerimientos Administrativos y de control Cooperativa COOPCCP Fecha: 22/05/2018 Sección 3 - 5 - Disposiciones Generales		Proyecto Banca en línea - 1ra fase Requerimientos funcionales y normativos Resolución No. SEPS-IGT-IR-ISF-ITIC-IGJ-2017-103			
Guía	**Requerimientos mínimos**	**Responsables**	**Cumple**	**Parcialmente**	**No cumple**
103	Registrar las direcciones IP y números celulares desde los cuales se realizan las transacciones. Para efectuar transacciones con IP y número celulares de exterior se debe poseer autorización expresa del cliente.	Proveedor	x		
103	Establecer un tiempo de inactividad para cancelar la sesión y exigir una nueva autenticación.	Proveedor	x		
103	Asegurar una adecuada segregación de funciones del personal que accede a los terminales y sistemas usados para transferencias electrónicas.	COOPCCP	x		
103	conservar para disponibilidad del cliente como mínimo 12 meses el registro electrónico de las transacciones electrónicas.	COOPCCP	x		
103	Mantener los archivos contables físicos 10 años y en digital 15 años.	COOPCCP	x		
103	para transferencias con tarjetas de débito y crédito se debe establecer un acceso directo o centro de atención telefónica y una línea de emergencias 224/7	COOPCCP			x
103	Los centros de atención telefónica deberán validar y confirmar la identidad del socio.	COOPCCP			x
103	Mantener durante 6 meses la grabación de las llamadas. (consultas, reclamos, emergencias)	COOPCCP			x
103	mecanismos para detectar copia de los diferentes componentes del sitio web.	COOPCCP			x
103	Verificar constantemente que no sean modificados los enlaces, suplantados sus certificados digitales o modificada la resolución de sistema de nombres de dominio.	COOPCCP			x
103	Mecanismos de autenticación, nombre de usuario distinto al de la cédula. Nombre de usuario y clave con caracteres alfanuméricos y longitud mínima de 6.	COOPCCP			x
103	Validar o verificar la autenticación del cliente mediante un canal diferente al de internet.	COOPCCP			x
103	las operaciones y servicios financieros deben ser autorizados por la SEPS.	COOPCCP			x
103	Contabilización diaria de transferencia electrónica.	COOPCCP			x
103	Asociación entre entidades previa autorización de la SEPS. Se podrá implementar procesos y procedimientos de seguridad del administrador del convenio.	Proveedor	x		
103	Compañías de servicio auxiliares podrán prestar servicios de transferencia electrónica previa autorización de la SEPS.	COOPCCP			x
Tipo	Plan sobre controles	**Responsables**	**Cumple**	**Parcialmente**	**No cumple**
	Cambiar el diseño de la página web - dinámica			x	
	OTP debe ser entregada manualmente o mediante servicio telefónico				x

Tabla 28: Requerimientos de aplicaciones para COOPCCP
Elaborado por: Jean P. Rodríguez.

Una vez cumplidos los requisitos y documentados los procesos la COOPCCP podrá realizar la solicitud a la SEPS para la revisión del cumplimiento y autorización de salida a producción de los nuevos servicios financieros.

Tarjetas de débito y crédito

En COOPCCP existe un servicio transaccional que se encuentra tercerizado y actualmente se encuentra en un periodo de actualización, la tarjeta de débito COOPCCP con tecnología Contact Less es un proyecto que para su aplicación se requiere lo mencionado en las matrices y adicionalmente, el cumplimiento con varias instrucciones dadas según las instituciones que intervienen en el trabajo.

COONECTA Y CAPTEC son empresas autorizadas por la SEPS como auxiliar de servicios financieros y para respaldo del manejo seguro de la información de los tarjetahabientes, cuentan con la certificación PCI DSS. Cumpliendo así con la exigencia de la normativa de riesgo operativo SEPS-IGT-IR-IGJ-2018-0279.

El proyecto de cambio a ContactLess tiene varios pasos de implementación que COOPCCP no tuvo que desarrollar en temas de actualización del enlace de comunicaciones que permitan la adhesión de nuevos campos programados en la antena transmisora/receptora ya que el macroproyecto lo lleva CPN.

7.7 SUGERENCIAS DE CAMBIOS EN COOPCCP

Normativa interna (Manual y política): A continuación, se muestra una sugerencia para la actualización del manual de seguridad de la información así también como de creación de procedimientos que puedan ser aplicados a todos los sistemas transaccionales.

4.13 Políticas de Uso del ATM (Automated Teller Machine)

Las siguientes políticas descritas a continuación son realizadas en base a lo establecido en la JB-1851 y JB-2148 además de algunas buenas prácticas y/o controles establecidos en la ISO27002 en su versión 2013. Los involucrados directos en esta sección son el área de Operaciones, Riesgos-Seguridad de la Información, Servicios Generales-Seguridad Física y demás áreas quienes interactúen indirectamente con los procesos que intervienen;

Objetivos de la seguridad y uso del ATM

a) Prevenir el acceso no autorizado de terceros en los sistemas de ATM
b) Resguardar el activo para no comprometerlo en integridad, disponibilidad y confiabilidad para su uso para el usuario final
c) Gestionar el uso de los controles aplicados dentro de la COOPCCP que cumpla con lo establecido en la presente política de seguridad de la información.
d) Reducir el impacto generado por agentes externos que atenten contra la integridad, disponibilidad y confiabilidad del cajero automático.
e) Establecer responsabilidades y procedimientos para la gestión de la operación, incluyendo instrucciones operativas, procedimientos para respuestas a incidentes y definición de funciones.
f) Cada responsable junto con el responsable de seguridad y el responsable de Operaciones, determinará los requerimientos para resguardar los recursos por los cuales son responsables.

Principales funciones relativas. -

Operaciones: Es responsabilidad del Jefe de Operaciones elaborar en conjunto con las áreas de Procesos y Riesgos - Seguridad de la información el esquema de operación que se llevará a cabo en el ATM en cada aspecto de funcionalidad que brinde a la COOPCCP incluyendo, Procesos y procedimientos de mantenimiento, actualización o reparación del ATM, constatación de no alteración a los ATM´s, Proceso de verificación diario de sistema de los cajeros y cualquier otro proceso pertinente relativo a la actividad del servicio.

Riesgos – Seguridad de la información: Es responsabilidad del oficial de seguridad de la información en dirección con el jefe de riesgos diseñar, gestionar, aplicar y actualizar los planes de contingencia que giran alrededor de los eventos que se puedan suscitar en relación al ATM para asegurar la continuidad del negocio. Así también, es responsabilidad del oficial de seguridad de la información realizar los cambios pertinentes a la presente política para que se alineé a las modificaciones (en caso de existir) que se hagan por ubicación geográfica de los dispositivos y constatar la aplicación de los controles aplicados sean estos físicos, electrónicos o digitales.

Servicios Generales – Seguridades físicas: Es responsabilidad del oficial de seguridades físicas en dirección con el encargado de servicios generales la aplicación, monitoreo y gestión de los controles físicos establecidos en la presente política así también como de su interacción en los procesos de mantenimiento e interacciones en general entre el ATM y los usuarios.

Procesos: Es responsabilidad del jefe de procesos la creación, modificación y actualización de todas las actividades existentes que interactúen directa o indirectamente con el objeto de esta sección (ATM) definiendo los procesos, procedimientos y actividades pertinentes para asegurar el correcto funcionamiento del mismo.

Todo el personal: Es responsabilidad de todo el personal de cumplir con lo que se norma en la presente política de seguridad para así minimizar el riesgo por posibles eventos que puedan existir dados por agentes internos o externos de manera causal o casual. El desacato de la normativa puede sujetarse a los manuales internos con sanciones institucionales y de ser requerido el debido reporte con las autoridades competentes.

4.13.1 Medidas de seguridad Física: Es responsabilidad del oficial de seguridades físicas la aplicación, monitoreo y gestión de los controles físicos con los que contarán las áreas designadas a los dispositivos ATM, establecidos a continuación:

1) **Protección al teclado:** En todo momento, el ATM debe contar con dispositivos “protectores de teclado” siendo éstos verificados de manera mensual en permanencia, funcionalidad y estado. Así también como su uso efectivo
2) **Protección contra clonación de tarjetas:** Se debe contar con dispositivos electrónicos y/o elementos físicos que impidan y detecten la colocación de falsas lectoras de tarjetas.
3) **Protección del ambiente físico del ATM:** Verificar en todo momento que las medidas de seguridad física relacionadas al mantenimiento (en caso de que aplique) estén en buen estado y cumplan con su función específica de manera correcta.

4) **Alarmas de dispositivos electrónicos:** Se debe contar con las debidas alarmas provenientes de los dispositivos electrónicos ubicados en el ATM así también como de los accesos al mismo. Dichas alarmas deben ser gestionadas, monitoreadas y atendidas por el personal pertinente. En relación a los sistemas de respuesta que se establezcan de la presente política.
5) **Iluminación:** Se debe contar con la iluminación adecuada y necesaria para poder visualizar toda la actividad existente en el ATM sea éste que esté ubicado en interiores o exteriores de las oficinas de la COOPCCP.
6) **Mecanismos de anclaje:** Se debe contar con mecanismos de anclaje adecuados para la tenencia del ATM que dificulte su remoción a excepción de aquellos que se encuentren anclados a la pared.
7) **Accesos físicos al interior de los cajeros automáticos:** Se deben contar con controles de acceso a los puntos de ingreso al interior del cajero automático, estos controles sean físicos o electrónicos deben ser gestionados en relación a lo que menciona la presente política en su punto 4.6 POLITICAS DE CONTRASEÑAS.
8) **Cámaras de seguridad:** Se deberá mantener un archivo de cintas, de discos de video digital (DVD) o cualquier otro sistema de grabación que cubra por lo menos tres (3) meses de grabación de acuerdo a las normativas vigentes (al menos dos cámaras por cajero automático). Así mismo deben inspeccionarse las cámaras de video – vigilancia para comprobar que éstas no hayan sido manipuladas.

4.13.2 Procedimientos y segregación de funciones: Es responsabilidad del Jefe de Procesos y el Jefe de Operaciones realizar en conjunto la correcta segregación de funciones de todo el personal que intervenga dentro de todos los procesos en relación al ATM, ya que estos son procedimientos Operativos será el responsable directo de la correcta segregación de funciones, así también como de la verificación del cumplimiento de dichos procedimientos alineados a los controles que se establezcan por medio de la presente política de seguridad. Lo que incluye pero no se limita a:

1) Revisar periódicamente los anclajes, iluminación, cámaras y entorno del cajero automático
2) Atender una señal de alarma o de siniestro
3) Respuesta inmediata ante la interrupción del servicio eléctrico.
4) Contar con personal capacitado para la operación y mantenimiento diario del cajero.
5) Abastecer de dinero permanentemente a los cajeros automáticos.
6) Etc.

Así también es responsabilidad del jefe de Operaciones el reporte de las actividades del ATM con la frecuencia que se establezca de acuerdo al uso del cajero y las transacciones que éste realice.

4.13.3 Medidas de Seguridad Informática: Es responsabilidad del Oficial de seguridad de la información gestionar, monitorear y constatar la existencia de los controles establecidos en la presente política así también como de constatar la eficacia de los proveedores de los diferentes servicios incluyendo la instalación, Red de datos, métodos de verificación del sistema. Dichas actividades deben ser coordinadas con el Jefe de Operaciones y los proveedores del servicio para llegar a aplicar los controles correctos y/o reportes de la gestión del servicio. La gestión de la seguridad informática incluye pero no se limita a:

1) **Acceso al menú de supervisor:** Se debe verificar en todo momento los niveles de accesos de usuarios establecidos de acuerdo a lo que dice la política de seguridad de la información en el punto 5.7 POLITICAS DE CUENTAS DE USUARIO, inciso 2 y así, junto con el área de Operaciones designar los procesos correspondientes a las personas que cuenten con dicho nivel de acceso dentro del menú de supervisor de los ATM. Así mismo las contraseñas deben ser gestionadas en relación a lo que norma la presente política en el punto 4.6 POLITICAS DE CONTRASEÑAS con el apoyo de seguridades físicas (de ser requerido).
2) **Software:** Se debe contar con un programa anti-malware que permita proteger el software instalado en el cajero automático y que detecte oportunamente cualquier alteración en su código, configuración y/o funcionalidad. Así mismo, se deberá instalar mecanismos que sean capaces de identificar conexiones no autorizadas a través de los puertos USB, comunicaciones remotas, cambio de los discos duros y otros componentes que guarden o procesen información. En una situación de riesgo deben emitir alarmas a un centro de monitoreo o dejar inactivo al cajero automático hasta que se realice la inspección por parte del personal especializado de la institución
3) **Conexiones seguras:** Se debe verificar el estado de las conexiones existentes que intervengan dentro del *uso normal*[1] del ATM, así también como verificar el correcto funcionamiento de los controles existentes para asegurar la integridad, disponibilidad y confidencialidad de los datos.
4) **Contraseñas:** Debe existir la verificación del cumplimiento de los controles de acuerdo a lo establecido en el punto 4.6 POLITICAS DE CONTRASEÑAS.

5) **Procedimientos de auditoría de seguridad en ATM:** Se debe tener acceso a los datos manejados en el ATM en todo momento ya que la información manejada dentro del mismo es de carácter público en capa 7 (Aplicación) y todo lo manejado en capa 2 a capa 6 (Desde enlace de datos hasta Presentación) al ser de carácter confidencial se deben contar con los controles de auditoría que permitan el mapeo de las transacciones y la concatenación con el movimiento siempre y cuando éste sea requerido y supervisado por el Jefe de Operaciones.
6) **Perfiles de usuario:** Los perfiles de usuario que se manejen para los distintos niveles dentro del ATM deben ser manejados de acuerdo a lo que dice la política de seguridad de la información en el punto 5.7 POLITICAS DE CUENTAS DE USUARIO, inciso 2. Así también debe guardar relación con lo establecido en el punto 4.6 POLITICAS DE CONTRASEÑAS.

4.13.4 Capacitación y campañas de seguridad: Es responsabilidad del Oficial de Seguridad de la información crear, monitorear y mejorar los planes de capacitación sobre el uso correcto de los cajeros, eficiencia de atención y solución a inconvenientes frecuentes (FAQ) que se den por parte de los usuarios. Así también es responsabilidad del área de Riesgos generar boletines de seguridad informática periódica para los usuarios finales del ATM así también como para los funcionarios que interactúen con él directa o indirectamente.

4.13.5 Ejecución de planes de contingencia: Es responsabilidad de todo el departamento de Riesgos el crear, monitorear y mejorar los planes de contingencia existentes para los eventos de seguridad[1] que se susciten, en dichos procesos se requiere la intervención específica del Jefe de Riesgos, Analista de riesgos y Oficial de seguridad de la información, así también el área de Riesgos debe apoyarse en las áreas de Procesos y Operaciones para asegurarse que los planes de contingencia estén alineados a salvaguardar los activos prioritarios dependiendo el grado de siniestro ocurrido, así también como tener una clara segregación de actividades de los funcionarios de la COOPCCP para ejecutar los planes.

4.14 Políticas de gestión de equipos de tarjetas de débito

Estas políticas tratan sobre el uso de los sistemas relacionados con el producto de tarjeta de débito así también como la gestión de eventos de riesgo.

Objetivos de la seguridad en tarjetas de débito

a) Prevenir el acceso no autorizado dentro de la consola de visualización que existe denominada echelong perteneciente al sistema Extreme web FX.
b) Determinar los responsables de aplicar los controles sobre eventos de riesgos relacionados a la tarjeta de débito
c) Manejar los incidentes de seguridad tipificados por la normativa vigente como “emergencias” para obtener una respuesta rápida.

Principales funciones relativas. –

Negocios. – Como dueños del proceso, el área de negocios debe designar a un colaborador que se encargue de coordinar cada una de las acciones que se requieran para solucionar los problemas de comunicación de enlaces, reclamos y problemas con la respuesta del core financiero ya que, el mayor interesado y dueño de proceso debe encargarse de que no existan interrupciones en la oferta del servicio para los socios a nivel nacional. Este colaborador debe compartir la responsabilidad de realizar la revisión activa sobre los eventos que suscitan en vivo en la consola de visualización e interpretar los tipos de errores de los canales por los que viaja la transacción, coordinar y generar los reportes de negocios.

Operaciones. – Son los encargados de generar los plásticos y realizar la impresión de los tarjetahabientes para posteriormente entregar el producto a las agencias y conjunto con ellos, manejar la operatividad de empaquetamiento y entrega a los socios ya sean nuevos o por actualización.

Tecnología. – Son los encargados directos de revisar las conexiones con el core financiero, respuestas y consulta de afectaciones que tengan que ver con el movimiento en bases de datos de los socios. El contingente tecnológico es el primer grado de solución de problemas.

4.14.1 Intermitencias del servicio. – Es responsabilidad del proveedor, así como del área de negocios el comunicar a todo el personal responsable de las conexiones y problemas que ocasionen la inoperatividad del sistema.

4.14.2 Segregación de funciones. – Es responsabilidad del área de Negocios y talento humano realizar la definición de segregación de funciones adecuada para la entrega y operatividad del producto.

4.14.3 Transferencia de información. – Toda información relacionada al proceso de tarjetas debe ser debidamente documentado y gestionar con los demás colaboradores la transferencia del conocimiento relacionado con la gestión de los procesos automatizados así también como la reportería llevada a cabo

4.14.4 Creación y mantenimiento de claves. – Es responsabilidad del personal operativo en todas las agencias responsables de la entrega del producto al cliente, la creación y mantenimiento de las claves y contraseñas, así también como responsabilidad compartida con el administrador del sistema el correcto funcionamiento en los dispositivos ATM propiedad de la COOPCCP.

4.14.5 Ejecución de planes de contingencia del servicio. – Es responsabilidad del área de tecnología de levantar los sistemas fuera de línea al momento de experimentar intermitencias que duren más de 1 hora si se encuentran realizando procesos de mantenimiento normales o más de 20 minutos si es un evento inesperado

4.15 Políticas de gestión para servicios transaccionales

Estas políticas son un compendio de controles utilizados en base a la normativa legal vigente y buenas prácticas de seguridad de la normativa ISO 27002 y PCI DSS aplicable a todos los servicios transaccionales que será aplicable de acuerdo a su naturaleza en el desarrollo, mantenimiento y control sobre los servicios.

Principales funciones relativas. –

Seguridad de la Información. – Se encarga directamente del control monitoreo y acción a cualquier inconveniente de seguridad sea que se origine en las redes o en uno de los terminales dentro de los canales electrónicos provistos por la Cooperativa.

Tecnología. – Son el primer punto de contacto por sobre el cual se debe resolver los problemas relacionados con la respuesta del core.

Operaciones. – Son los responsables de hacer la compensación mediante mallas comunicadas mediante FTP con las organizaciones que brindan servicios financieros auxiliares.

4.15.1 Controles criptográficos. - El responsable de seguridad deberá realizar un protocolo de compartición de información sensible y/o de alto riesgo que contemple el uso de controles criptográficos para el intercambio de información digital que cumpla con los estándares nacionales y pueda ser verificado mediante los procesos legales pertinentes.

4.15.2 Seguridad del Negocio. - Los principales objetivos son los siguientes:

- Garantizar el funcionamiento correcto y seguro de las instalaciones de procesamiento operativo.
- Establecer responsabilidades y procedimientos para la gestión de la operación, incluyendo instrucciones operativas, procedimientos para la respuesta a incidentes y definición de funciones.
- Cada Responsable Operativo, junto con el Responsable de Seguridad y el Responsable del Área Tecnológica, determinará los requerimientos para resguardar los recursos por los cuales es responsable.

4.15.3 Continuidad de Operaciones. –

- Minimizar los efectos de las posibles interrupciones de las actividades normales de La Compañía (sean éstas resultado de desastres naturales, accidentes, fallas en el equipamiento, acciones deliberadas u otros hechos) y proteger los procesos críticos mediante una combinación de controles preventivos y acciones de recuperación.
- Analizar las consecuencias de la interrupción del servicio y tomar las medidas correspondientes para la prevención de hechos similares en el futuro.
- Maximizar la efectividad de las operaciones de contingencia de La Compañía con el establecimiento de planes que incluyan al menos las siguientes etapas:

  a) Activación: Consistente en la detección y determinación del daño y la activación del plan de emergencia.
  b) Reanudación: Consistente en la restauración temporal de las operaciones y recuperación del daño producido.
  c) Recuperación: Consistente en la restauración de las capacidades de proceso del sistema a las condiciones de operación normales.

- Asegurar la coordinación con el personal de La Compañía y los contactos externos que participarán en las estrategias de planificación de contingencias. Asignar funciones para cada actividad definida.

- El Responsable de Seguridad participará activamente en la definición, documentación, prueba y actualización de los planes de contingencia. Todo el personal restante de La Compañía cumplirá las siguientes funciones:

  a) Identificar las amenazas que puedan ocasionar interrupciones de los procesos y/o las actividades de La Compañía.
  b) Evaluar los riesgos para determinar el impacto de dichas interrupciones.
  c) Identificar los controles preventivos.
  d) Desarrollar un plan estratégico para determinar el enfoque global con el que se abordará la continuidad de las actividades de La Compañía.
  e) Elaborar los planes de contingencia necesarios para garantizar la continuidad de las actividades de La Compañía.

Topología de red propuesta

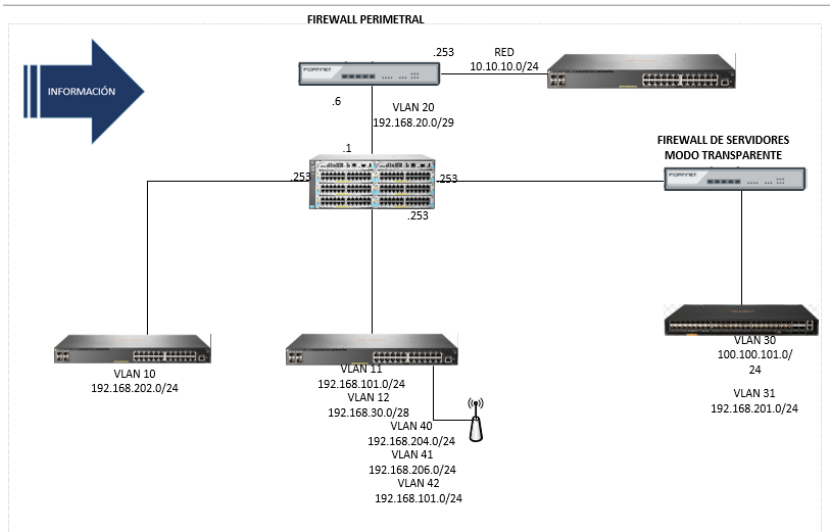


Figura 28: Topología de red propuesta para COOPCCP.
Elaborado por: Jean P. Rodríguez.

Descripción de la topología:

La topología presentada se realizó en base a lo evidenciado en la matriz de riesgos informáticos cotejada con la normativa PCI DSS y van directamente orientados a realizar una configuración de equipos segura, en búsqueda de mantener una infraestructura redundante y segura ante diferentes tipos de intrusiones fruto de nuevos vectores de ataque y puertos abiertos por la inclusión de nuevos servicios que por medio de instrucciones programadas afecten los saldos de los socios de la COOPCCP. A continuación, se explica la topología de red expuesta:

Descripción de la topología de red

Se consideró el uso de un Firewall perimetral que cense todo el tráfico junto a un IPS a modo de Software que está configurado como un host bastión, del firewall salen dos conexiones, la primera a un switch ethernet capa 2 que a su vez se conecta a un servidor de prueba, cuarentena y Honeypots en un segmento de red aislado. La otra conexión es a un cluster de switch de distribución capa 3 para realizar balanceo de carga el mismo que está conectado a 3 segmentos, el primero a una VLAN destinada a un servidor de correos, el segundo a un firewall en modo transparente que se conecta a un switch que interconecta los servidores de aplicaciones, físicos y virtuales. El último segmento se encuentra conectado a un switch capa 2 que direcciona a la red institucional. Se muestra un esquema general sobre la estratificación mencionada:

- Internet
- Router
- Firewall Perimetral / Software IPS
- Switch de Core
- Switch Ethernet
- Servidores de prueba / cuarentena / Honey Pots

- Cluster a Switchs de distribución Capa 3
    - Switch Capa 2
        - Red interna
        - AP – Wireless
    - Switch Capa 2
        - Servidor de correo
    - Firewall de servidores – Transparente
        - Switch Capa 2
            - Granja de servidores

7.8 CUMPLIMIENTO Y SEGUIMIENTO MONITOREO.

Para el cumplimiento de la metodología y monitoreo de las actividades se deben realizar las siguientes acciones:

- Probar las conexiones de seguridad con intentos de penetración con scripts dedicados a pasar a través de la configuración realizada.
- Realizar pruebas de seguridad y funcionamiento de los controles de firewall antes de lanzarlos a producción.
- En caso de realizar cambios en la topología o equipos de infraestructura, se debe definir previamente el impacto en el alcance de los requisitos de la PCI DSS
- El departamento de seguridad de la información debe enviar comunicados al área de tecnología para recordar revisar las configuraciones de seguridad
- Realizar pruebas mensuales sobre rastreo de transacciones a modo de simulación ante eventos de seguridad y reportarlos debidamente.
- El equipo de seguridad informática es el encargado de poner en marcha las buenas prácticas de seguridad de la información en los sistemas que componen la topología de

red, por tal motivo se realizará un documento de reporte a manera de bitácora que conste de lo siguiente:

1. Nombre de dispositivo
2. Reporte de conexiones entrantes y salientes
3. Reporte de actividades anómalas
4. Cotejo de información normalizado
5. Monitoreo de controles de seguridad vigentes
6. Observaciones

7.9 DESCRIPCIÓN DE PRUEBAS DE SEGURIDAD PENTEST

Tras el análisis previo al desarrollo de la metodología se evidenció el resultado de un ethical hacking realizado por una empresa experta en consultorías de seguridad, el resultado fue relevante para los sistemas implementados hasta la fecha, sin embargo, no se tomaron en cuenta ciertos puntos de la infraestructura, el modelo realizado fue de caja gris, sin embargo, no fue dirigido a los servicios transaccionales que se encuentran vigentes actualmente. Por tal motivo se sugiere realizar pentest más profundos acerca de movimientos horizontales como por ejemplo la explotación de vulnerabilidades en servidores conectados entre sí, para buscar un hueco de intercomunicación.

7.10 PLAN DE CAPACITACIÓN DE SEGURIDAD

Se debe incrementar en el manual el procedimiento para realizar el plan de capacitación de seguridad de la información de acuerdo a la metodología:

Fase de Preparación

Problemática:

La información es parte vital de la institución y cada día existen nuevas brechas de seguridad que buscan vulnerar no solo los servicios tecnológicos sino también el capital humano, es por eso que se presenta este proyecto que busca reforzar dicho eslabón así también como

Esta campaña se realiza con el fin de crear concientización y entrenamiento sobre cómo actuar ante eventos de seguridad reforzando los conocimientos de todos los empleados, siendo agentes de cambio en la sociedad

Objetivo:

Concientizar a todo el personal sobre la importancia de la seguridad de la información mediante una campaña persistente en un promedio de tiempo.

Elaboración del plan de acción - Fases de desarrollo:

1. Diseño
    a. Estructura del programa
    b. Evaluación de necesidades
    c. Desarrollo de estrategias y planes
    d. Definición de prioridades
    e. Aprobación
    f. Financiamiento
2. Desarrollo del material
    a. Concientización
        i. Selección de temas
        ii. Fuentes para el material
    b. Entrenamiento
        i. Modelo del programa de entrenamiento
        ii. Fuentes para el Material
        iii. Cursos de entrenamiento
3. Implementación del Programa
    a. Difusión
    b. Técnicas para entrega del material
        i. Posters
        ii. Videos
        iii. Conferencias
        iv. Boletines
        v. Concursos
        vi. Etc.
    c. Desarrollo del material
4. Mantenimiento
    a. Monitoreo del programa
    b. Métodos de evaluación y retroalimentación
    c. Gestión del cambio
    d. Mejora continua
    e. Indicadores

Aplicación del plan

1. Definición de grupos a capacitar:
    a. Consejo de Administración y Vigilancia
    b. Áreas de control
    c. Gerencia General
    d. Jefes de áreas
    e. Líderes de procesos
    f. Personal Operativo Administración – Oficinas – Mantenimiento
2. Definición de módulos para los 6 grupos objetivos a capacitar
    a. (Ver sección “temas de capacitación”)
3. Definición e impartición de talleres prácticos
    a. Talleres de seguridad en casa
    b. Talleres de seguridad en su puesto de trabajo
    c. Talleres de seguridad en la institución

7.11 IMPARTIENDO LA METODOLOGÍA

La aplicación de esta metodología debe ser realizada en base a los proyectos de la planificación estratégica institucional designadas para ser cumplidas en el año 2019 sumado a los servicios ya aplicados. Por lo tanto, se definen una línea de pasos a seguir:

Próximos pasos para la implementación de la metodología.

El éxito o fracaso de esta metodología depende de las adaptaciones que el responsable de seguridad pueda ejercer tomando en cuenta factores como presupuesto, tiempo y separación del personal de la institución ya que esto puede afectar en la toma de decisiones, tiempos de implementación e incremento de costos. Por tal motivo se debe iniciar con una verificación de la veracidad de la información entregada. Esta verificación debe ser realizada por un colaborador distinto a la persona que realizó el levantamiento. A continuación, se especifican los pasos a seguir:

1. **Verificación de matriz de riesgos. –** Es importante que el colaborador responsable de la aplicación de la presente metodología en la COOPCCP realice la verificación del material entregado en el punto 6.3 ya que, servirá de insumo para poder realizar futuros cambios que puedan suscitarse de acuerdo con factores económicos o burocráticos dentro de la institución y así poder encontrar nuevas alternativas de solución.
2. **Análisis de factibilidad tecnológica, operativa y financiera. –** Este trabajo será realizado conjunto con los jefes de área de tecnología, talento humano y financiero, directamente el responsable se encargará de buscar la aprobación del punto 6.2 en la medida posible de acuerdo a la realidad de cada institución teniendo en cuenta los

tiempos de contratación de nuevo personal o los tiempos en reestructura de presupuestos anuales.

3. **Presentación del proyecto a áreas de control necesarias. –** En algunas instituciones, de acuerdo a los niveles de aprobación o estructura para tratar temas de alta importancia que realicen cambios a los procesos internos y del negocio, el presente proyecto deberá ser presentado y aprobado según los cambios y modificaciones realizadas en el punto anterior, tomando en cuenta consideraciones de PMBOOK para la gestión de proyectos tecnológicos asignando tiempos reales de aplicación así también como la carga laboral para otras áreas que intervienen de manera directa o indirecta en el desarrollo de la aplicación de la metodología.
4. **Designación de equipos y recursos. –** Según se requiera, es necesario formar un grupo de 4 o 5 colaboradores máximo que se encarguen del cumplimiento de todas las actividades que contempla el proyecto y son descritas en el presente documento. Como método, se sugiere desarrollar una reunión con los involucrados y hacerles partícipes del proyecto así también como de su participación en el mismo y compromiso con el cumplimiento del mismo además de sus actividades normales.
5. **Adhesión a proyectos de planificación iniciados. –** El proyecto de implementación del sistema de seguridad debe ir a la par con los proyectos vigentes en desarrollo, en el caso de la COOPCCP se presentó un cronograma de desarrollo general de actividades en los proyectos a realizarse en año 2019, a los cuales se deben adaptar para estar preparados en el periodo de levantamiento del sistema en ambiente de desarrollo o preproducción ya que es cuando se debe solicitar el permiso de la SEPS para el funcionamiento y lanzamiento a producción.
6. **Readecuación tecnológica según matriz de riesgos. –** En base a los hallazgos dados en la matriz de riesgos cotejada con la normativa PCI DSS, se establecieron los cambios

en los componentes tecnológicos para el cumplimiento normativo de y un correcto manejo de los riesgos informáticos. En este punto el responsable debe apoyarse con el área de Tecnología y Servicios generales para la adquisición de equipos o readecuación del esquema tecnológico vigente.

7. **Gestión de cambios en servicios transaccionales ya vigentes según borrador de manual SGSI. –** Previo a la aprobación de los manuales de seguridad de información primero deben realizarse los cambios en los servicios transaccionales vigentes ya que, una vez actualizado el manual, el cumplimiento del mismo debe ser inmediato.
8. **Creación de procesos de seguridad. –** Previo a realizar los cambios en los manuales, es necesario crear los procesos necesarios para el control en los sistemas transaccionales así también como la gestión de los eventos de riesgo con guías prácticas de solución del problema.
9. **Cambios en manuales y políticas. –** La actualización debe hacerse, entre otros puntos, con respecto a las recomendaciones dadas en la presente metodología en el punto 6.8. los cambios a los manuales deben ser realizados por el comité de riesgos al consejo de administración y socializados y aplicados por el responsable de la seguridad de la información en la Cooperativa.
10. **Capacitación a personal técnico de seguridad de la información. –** Es importante traspasar los conocimientos de seguridad de la información sobre las exposiciones y prácticas realizadas para el mantenimiento de los sistemas transaccionales al menos 1 vez al año y de igual manera saber encontrar fuentes de información confiable como un CSIRT sobre el cual se pueda tener una participación, en COOPCCP se tiene apertura como miembro de desarrollo del ECUCert.
11. **Levantamiento de informes, reportes y matrices según manuales y políticas. –** Una vez implementados los controles de seguridad y realizados los cambios en la política, es

necesario llevar un reporte de cada uno de los cambios así también como la gestión operativa mensual acerca de sus transacciones.

12. **Capacitación general de la institución. –** De manera ideal, la capacitación debe ser llevada como un proyecto que contemple al menos los procedimientos mencionados en el punto 6.11 de la metodología.
13. **Cumplimiento y seguimiento de la metodología. –** Como último punto es necesario dar seguimiento de acuerdo con los lineamientos dados por PCI DSS, 6 puntos específicos:
    a. Monitorear los controles de seguridad, tales como firewalls, IDS/IPS (sistemas de intrusión-detección o de intrusión-prevención), FIM (monitorización de la integridad de archivos), antivirus, controles de acceso, entre otros.
    b. Garantizar la detección de todas las fallas en los controles de seguridad y solucionarlas oportunamente.
    c. Revisar los cambios implementados en el entorno (por ejemplo, incorporación de nuevos sistemas, cambios en las configuraciones del sistema o la red) antes de finalizar el cambio
    d. Si se implementan cambios en la estructura organizativa (por ejemplo, la adquisición o fusión de una empresa), se debe realizar una revisión formal del impacto en el alcance y en los requisitos de las PCI DSS.
    e. Se deben realizar revisiones y comunicados periódicos para confirmar que los requisitos de las PCI DSS se siguen implementando y que el personal cumple con los procesos de seguridad.
    f. Estas revisiones también se pueden usar para verificar que se mantiene la evidencia correspondiente, por ejemplo, registros de auditorías, informes de análisis de vulnerabilidades, revisiones de firewall, etc.

CAPITULO 5

CONCLUSIONES Y RECOMEDACIONES

Conclusiones:

Para el diseño de la metodología, tanto en el análisis de los procesos e infraestructura, como en la definición del estado de madurez, es importante entender el rol y SLA definidos de cada proveedor de servicios dentro de la institución financiera ya que, de aquella información depende el proceso para dar respuesta inmediata ante cualquier incidente de seguridad para cada uno de los servicios transaccionales. Además, esta información permite gestionar adecuadamente los requerimientos de seguridad normativos y presentar al organismo de control la evidencia que sustenta el cumplimiento de estos.

La normativa PCI DSS fue diseñada para el tratamiento de la información en el uso de tarjetas de pago, sin embargo, contiene controles que hoy en día son relevantes en la aplicación de las tecnologías financieras *FINTECH*, los cuales dentro del proceso de desarrollo de la metodología fueron analizados y adaptados de acuerdo con las necesidades de las aplicaciones que permiten ofrecer servicios transaccionales de acuerdo a la manera en la que interactúan con los datos del usuario final de dichos sistemas.

Para medir la efectividad de la metodología, se realizó el diccionario de controles que mitigan los 82 riesgos críticos identificados según la matriz de riesgos (ERM) que, tras concatenarlo con el mismo documento, se evidencia una reducción significante de la

probabilidad de ocurrencia de eventos que atenten contra la información presente en el proceso de uso de los servicios transaccionales vigentes y aquellos que se encuentran por implementar según el POA de la Cooperativa.

Es necesario que toda institución financiera tenga procesos internos para la identificación de riesgos informáticos, diseñados de acuerdo a su realidad y que sean realizados periódicamente una vez al año así también, como procesos para efectuar revisiones de puntos críticos de los sistemas al menos cada 3 meses debido a que, existen potenciales atacantes que se dedican a buscar vulnerabilidades en equipos de seguridad y desarrollar código malicioso para poder explotarlas antes de que exista un parche que solucione el error. Es importante recordar que, sin importar que tanto se logre mitigar el riesgo, siempre existe maneras en las que la información se encontrará vulnerable, ya sea por errores técnicos, fallas en el proceso o descuido del capital humano.

Es importante saber reconocer los puntos críticos sobre los cuales se puede implementar una normativa. Como se evidenció durante el desarrollo del diccionario de controles basado en la PCI DSS, existen vacíos que deben ser sustentados por el responsable de seguridad de la información complementando las reglas y controles de los sistemas de seguridad propuestos en la metodología con el SGSI, de este modo, con la adhesión de 3 o más normativas, se puede obtener un sistema de gestión integrado que responda ante cualquier incidente de riesgo que afecte directa o indirectamente a la seguridad de la información

Tras lo expuesto en el presente proyecto, se puede probar que la correcta gestión de un sistema de seguridad es un ámbito que inmiscuye todas las aristas relacionadas con la información encontrada en equipos tecnológicos y el trabajo a realizar únicamente está limitado

por el personal disponible y los montos aprobados para la adquisición de los equipos de seguridad, es por tal motivo que el responsable de la aplicación de la metodología o *Project Manager* debe realizar las gestiones de cambio a medida que se implementen los equipos, sistemas o controles del proyecto.

Aunque la normativa legal ecuatoriana no es muy específica con respecto al manejo de la información en bases de datos fuera del país, es importante ser consciente del riesgo inherente que dicha actividad supone. Esta metodología busca brindar completo entendimiento al personal técnico de los controles a implementar para dar respuesta inmediata ante cualquier evento de seguridad sea cual sea el modelo escogido. Y de ninguna forma desestima los beneficios de las economías a escala y la implementación de soluciones en un modelo *SaS*.

La presente metodología se realizó en base a la realidad de la Cooperativa de Ahorro y Crédito COOPCCP, fue presentada y aprobada por el comité de tecnología, conformado por el área de Riesgos – Seguridad de la información, el área de tecnología, área de procesos y Gerencia.

Actualmente, la metodología se encuentra en estado de implementación de acuerdo con el documento *SOW* presentado al comité de tecnología. Previo a la presentación al consejo de administración y regularización tipificada del documento de la metodología, se encuentran en desarrollo las modificaciones en la normativa interna por parte de procesos, adquisición de equipos y distribución de recursos. Alineado a la Plan Operativo Anual de la COOPCCP.

Recomendaciones:

Es importante tener en cuenta que, los organismos de control para las Cooperativas de Ahorro y Crédito se encuentran desarrollando reformas a las resoluciones para el tratamiento del riesgo informático, sin embargo, al no existir modificaciones que hablen sobre configuración específica y relevante para la protección de los datos en servicios transaccionales, se recomienda a los responsables de la seguridad de la información participar activamente en los proyectos de análisis sobre el tratamiento de eventos de los riesgo informáticos, uno de ellos es el ECUCERT, un centro de respuesta de emergencias informáticas desarrollado por el ARCOTEL, en el cual se pueden aportar con datos y documentos técnicos para desarrollar una red de información y respuesta a incidentes accesible a toda institución que desee participar. De esta manera, apoyándose dicha institución, se puede proponer la inclusión de nuevos controles en la normativa nacional.

Es indispensable que se realice una evaluación para incorporar al equipo de seguridad de la información un analista de seguridad y un *pentester*, los cuales se encarguen de realizar los controles activos y el monitoreo integral de los eventos de riesgo. Esto, debido a que en julio del presente año, se pondrá en producción los sistemas transaccionales aprobados según el plan operativo anual (POA). Lo que quiere decir que se abrirá un nuevo vector de ataque que debe ser censado y resguardado debidamente.

Previo a la implementación de la presente metodología es importante tener en cuenta las bases de los sistemas de gestión de seguridad de la información, así también como los controles y sus ámbitos de aplicación ya que, es fundamental que exista una conciencia de seguridad de

la información previo a la integración de nuevos servicios transaccionales, sobre todo de aquellos que no interactúan directamente con la base de datos o tercerizan sus servicios

Para la aplicación de la presente metodología, el profesional dedicado a la seguridad de la información debe tener una formación integral de riesgos operativos y conocimiento sobre las distintas normativas que aplican para el sector financiero, de esta manera se puede realizar una adecuada interpretación y gestión de cambios con respecto al presupuesto, tiempo y direccionamiento estratégico de la institución en la que se aplique.

Se recomienda además realizar anualmente un análisis de riesgos, debido a que es un procedimiento que necesita ser actualizado periódicamente. En cada actualización concatenarlo con la anterior para así poder evidenciar los cambios dados e identificar el factor que lo permitió, ya sea tecnológico, de controles o actualización de manuales.

En las cooperativas de ahorro y crédito, la gestión del riesgo informático en varias ocasiones, se ve limitado por el presupuesto que conlleva aplicar controles de seguridad por lo que, es importante que el colaborador responsable de aplicar la presente metodología pueda realizar un análisis de factibilidad en relación al costo, el tiempo y la calidad para cada uno de los controles a aplicarse, dando respuesta a las necesidades de la institución preparados para responder ante cualquier evento que pueda suscitarse.

BIBLIOGRAFÍA

A&L Goodbody. (2018). Fintech law 2018. *The international Comparative Legal Guide to Fintech*, 1-9.

Albors. (17 de 04 de 2015). *ESET*. Obtenido de We Live Security: https://www.welivesecurity.com/la-es/2015/04/17/que-es-un-backdoor/

Allende, D., & Gui, S. (2011). Sistema de gestión de la seguridad de la información. *Universidad Oberta de Catalunya*, 4-5.

Amaya, C. G. (2012). *welivesecurity*. Obtenido de Welivesecurity by ESET: https://www.welivesecurity.com/la-es/2012/08/16/en-que-consiste-analisis-riesgos/

Andrade, I. (2015). *Seguridad de la información UNAM*. Obtenido de Revista Seguridad - Cultura de prevención para TI: https://revista.seguridad.unam.mx/numero25/dlp-tecnolog-para-la-prevenci-n-de-la-fuga-de-informaci-n

ARBOR NETWORKS. (2018). *LATAM DDos Attack Trends.* Ecuador: ARBOR NETWORKS.

Bancaria, J. (2014). (JB-2014-3066, 2014). En *Seguridad informática.*

Bancaria, J. (s.f.). Gestión del Riesgo Operativo. En JB, *JB-2012-2148 ,2012.*

BANRED. (2018). *AppAdvice*. Obtenido de Bimo By Banred: https://appadvice.com/app/bimo-by-banred/1374358687

Baquero, J. (2015). *Arsys*. Obtenido de ¿Qué son los web services y qué tecnología usar en su desarrollo? : https://www.arsys.es/blog/programacion/diseno-web/web-services-desarrollo/

Calderón , C., & Castro, L. (2013). Gestión de incidentes y gestión para la continuidad del negocio. *Universidad Piloto de Colombia,* , 1-14.

Calderon , C., & Castro, L. (2017). Gestión de incidentes y gestión para la continuidad del negocio. Procesos iguales, paralelos o complementarios. *Universidad Piloto de Colombia*.

Carles, J. (08 de 2017). *GEEKLAND*. Obtenido de geekland tecnología: https://geekland.eu/que-es-y-para-que-sirve-un-sandbox/

COOPCCP. (2017). Manual de clasificación de activos de la información. En COOPCCP, *Manual de clasificación de activos de la información.* Quito - Ecuador: COOPCCP.

DELOITTE. (2017). *Seguridad de la información en Ecuador.* Quito: Deloite Ecuador.

Diario de México. (15 de mayo de 2018). Tras hackeo, Banxico anuncia reformas para blindar operaciones. *Diario de México*, págs. 1-2.

Dirección Nacional de Información, D. N. (2016). *Superintendencia de economía popular y solidaria*. Obtenido de SEPS: http://www.seps.gob.ec/estadisticas?sector-cooperativo

Doina, F. F. (enero de 2013). *Metolodología para la gestión y seguridad informática.* Obtenido de https://instituciones.sld.cu/dnspminsap/: http://instituciones.sld.cu/dnspminsap/files/2013/08/Metodologia-PSI-NUEVAProyecto.pdf

Duk, S., Bjelobrk, D., & Čarapina, M. ((2013, May)). SEO in e-commerce: Balancing between white and black hat methods. *In 2013 36th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)*, 390-395.

EQUIFAX. (2007). *Equifax*. Obtenido de EquifaxEC: https://www.equifax.com.ec/WebSite/PrincipiosBasicos.html

ESET. (2018). Ecuador, en el puesto 7 de los cyberataques. *Diario Expreso Ecuador*, 1-2. Obtenido de https://www.pressreader.com/ecuador/diario-expreso/20181108/281668255992923

Grijalva, D. (2018). Diseño de un Plan Estratégico de Seguridad de la Información, Mediante la Aplicación de Análisis de Riesgos con la Norma ISO/IEC 27005 Caso de Estudio INAMHI. *INNOVA Research Journal*, 30-31.

Heredia, R. J. (2017). *La revolución digital y el futuro de los servicios financieros. .* Chile.

IMPERVA. (2017). *WEB APPLICATION SECURITY CENTER*. Obtenido de Incapsula: https://www.incapsula.com/web-application-security/siem.html

INTERDIN. (2015). *Optar*. Obtenido de Interdin emisora y administradora de tarjetas de crédito: https://www.optar.com.ec/Optar.Static/establecimientos/internet.html

ISO/IEC 27001, 2. (2018). *Information security management systems.* ISO.

ISOTOOLS. (2017). *Aspectos Clave de la seguridad de la información según ISO 27001*. Obtenido de ISO TOOLS: https://www.isotools.cl/aspectos-clave-de-la-seguridad-de-la-informacion-segun-iso-27001/

ISOTools Excellence. (2014). *PMG-SSI*. Obtenido de SGSI - Blog Especializado en Sistemas de Gestión de Seguridad de la Información: https://www.pmg-ssi.com/2014/06/iso-27001-como-confeccionar-un-plan-de-concienciacion-sobre-la-seguridad-de-la-informacion/

Karina, M. (2013). *Guía metodológica para implementar un sistema de seguridad en instituciones.* Piura, Perú: Universidad de Pirua. Facultad de Ingeniería.

Karspersky. (10 de 04 de 2013). *Latam Karspersky*. Obtenido de Karspersky lab dialy: https://latam.kaspersky.com/blog/que-es-un-ataque-man-in-the-middle/469/

Karspersky Lab. (25 de 04 de 2013). *AO Karspersky Labs*. Obtenido de Karspersky lab dialy: https://www.kaspersky.es/blog/que-es-un-botnet/755/

Mell, P., & Scarfone, K. (2007). Guide to Intrusion Detection . *Recommendations of the National Institute*, 3-7.

Moreira, M., & Alcívar, P. (2018). Seguridad en la Capa de Enlace de Datos del Modelo OSI en Redes LAN Cableadas CISCO. *ournal of Science and Research: Revista Ciencia E Investigación,* , 106-112.

OEA, O. d. (2018). *Estado de la Ciberseguridad en el sector bancario en américa latina y el caribe.* OEA - Canada.

Ortiz, S. (2019). Manual de seguridad de la información. En COOPCCP, *Manual de seguridad de la información* (pág. 30). Quito - Ecuador: COOPCCP.

OWASP. (2016). *Web Aplication Firewall*. Obtenido de OWASP organization: https://www.owasp.org/index.php/Web_Application_Firewall

PCI Council, P. S. (2016). Payment Card Industry (PCI) Data Security Standard. En P. S. Council, *Payment Card Industry (PCI) Data Security Standard* (págs. 1 - 139). PCI Security Standards Council, LLC.

Perez, D. (27 de 10 de 2017). *ESET*. Obtenido de We live Security: https://www.welivesecurity.com/la-es/2017/10/27/reglas-de-yara-nessus/

Pollari, I., & Ruddenklau, A. (2018). The pulse of Fintech 2018. *KPMG*, 1-58.

Prieto, V. M., & Pan, R. A. (2006). *Virus Informáticos.* Coruña: Universidad de Coruña.

Rodríguez, C. E. (2011). *Clasificación de Operaciones Bancarias*. Obtenido de Derecho Comercial Uruguay: http://www.derechocomercial.edu.uy/claseintfincontratos.htm

Rodríguez, J. (2016). Diseño de un sistema de gestión de seguridad de la información para instituciones de alto riesgo. *UISEK*.

Rodríguez, J. (2018). Matriz de Usuarios COOPCCP. En COOPCCP, *Matriz de Usuarios COOPCCP.* Quito - Ecuador: COOPCCP.

Rouse, M. (2015). *TechTarget*. Obtenido de Gestión de relaciones con clientes: https://searchdatacenter.techtarget.com/es/definicion/CRM-Gestion-de-relaciones-con-los-clientes

Ruiz, M. S. (2016). *www.eldiario.es*. Obtenido de hojadelrouter.com: https://www.eldiario.es/hojaderouter/seguridad/malware-inteligencia_artificial-seguridad_informatica-ciberseguridad_0_577792339.html

Schul, J. (2018). Chatbots en Facebook y Whatsapp Enterprice para el sector financiero. *EL COMERCIO*.

SEPS. (2017). Resolución No. SEPS-IGT-IR-ISF-ITIC-IGJ-2017-103. En *Gestión de la seguridad de la información.*

SEPS. (23 de 11 de 2017). Resolución No. SEPS-IGT-IR-ISF-ITIC-IGJ-2017-103. Quito, Pichincha, Ecuador.

Sinembargo Periodismo Digital. (15 de mayo de 2018). Quincena caótica en bancos, hoy | Es hackeo, y millones de pesos sí se movieron hacia… algún lado. *sinembargo.mx*, pág. 1.

SINERMEDIA. (2016). *Siner/media*. Obtenido de Qué son y qué opciones aportan los SMS transaccionales: https://www.sinermedia.com/opciones-aportan-los-sms-transaccionales/

Subsecretaría de telecomunicaciones. (2018). *Subsecretaría general de presidencia.* Obtenido de Ministerio de Hacienda Colombia: https://www.csirt.gob.cl.

Tapia, E., & Maldonado, P. (2018). *Revista líderes Ecuador.* Obtenido de Líderes: https://www.revistalideres.ec/lideres/ecuador-fintech-tecnologia-desarrollo-banca.html

Tarazona, C. (2018). AMENAZAS INFORMÁTICAS Y. *Etek International* , 137-145.

Tariffi, L., Cutillas, S., & Soley, J. (2011). Banca transaccional: ¿tabla de salvación de empresas y entidades financieras? . *IESE Insight* .

Veritas, J. (2005). *Information Security Management System - ISO 27001*. ISO / IEC.

Zauzich, I. (2016). *COBIS: Financial Agilitty Partners*. Obtenido de Cloud Banking: http://blog.cobiscorp.com/banca-en-la-nube-cloud-banking