Universidad de San Carlos de Guatemala
Facultad de Ingeniería
Escuela de Ingeniería en Ciencias y Sistemas

MODELO PARA LA GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN EN EL SECTOR DE MICROFINANZAS EN GUATEMALA

Wilmer Vinicio Betancourth García
Asesorado por el Ing. Joaquín Adolfo Guerrero Milián

Guatemala, julio de 2020

UNIVERSIDAD DE SAN CAROLOS DE GUATEMALA

FACULTAD DE INGENIERÍA

MODELO PARA LA GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN EN EL SECTOR DE MICROFINANZAS EN GUATEMALA

TRABAJO DE GRADUACIÓN

PRESENTADO A LA JUNTA DIRECTIVA DE LA
FACULTAD DE INGENIERÍA
POR

WILMER VINICIO BETANCOURTH GARCÍA
ASESORADO POR EL ING. JOAQUÍN ADOLFO GUERRERO MILIÁN

AL CONFERÍRSELE EL TÍTULO DE

INGENIERO EN CIENCIAS Y SISTEMAS

GUATEMALA, JULIO DE 2020

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

FACULTAD DE INGENIERÍA

NÓMINA DE JUNTA DIRECTIVA

DECANA	Inga. Aurelia Anabela Cordova Estrada
VOCAL I	Ing. José Francisco Gómez Rivera
VOCAL II	Ing. Mario Renato Escobedo Martínez
VOCAL III	Ing. José Milton de León Bran
VOCAL IV	Br. Christian Moisés de la Cruz Leal
VOCAL V	Br. Kevin Armando Cruz Lorente
SECRETARIO	Ing. Hugo Humberto Rivera Pérez

TRIBUNAL QUE PRACTICÓ EL EXAMEN GENERAL PRIVADO

DECANA	Inga. Aurelia Anabela Cordova Estrada
EXAMINADOR	Ing. César Augusto Fernández Cáceres
EXAMINADOR	Ing. Ricardo Morales Prado
EXAMINADOR	Ing. Herman Igor Véliz Linares
SECRETARIO	Ing. Hugo Humberto Rivera Pérez

HONORABLE TRIBUNAL EXAMINADOR

En cumplimiento con los preceptos que establece la ley de la Universidad de San Carlos de Guatemala, presento a su consideración mi trabajo de graduación titulado:

MODELO PARA LA GESTIÓN DESEGURIDAD DE LA INFORMACIÓN EN EL SECTOR DE MICROFINANZAS EN GUATEMALA

Tema que me fuera asignado por la Dirección de la Escuela de Ingeniería en Ciencias y Sistemas, con fecha julio 2019.

Wilmer Vinicio Betancourth García

Guatemala, 30 de julio de 2019.

Ing. Carlos Azurdia
Coordinador Proyectos de Graduación
Escuela de Ciencias y Sistemas
Facultad de Ingeniería

Por este medio hago de su conocimiento que he revisado el trabajo de graduación del estudiante WILMER VINICIO BETANCOURTH GARCÍA, con carné 199922727 titulado: **"MODELO PARA LA GESTIÓN DESEGURIDAD DE LA INFORMACIÓN EN EL SECTOR DE MICROFINANZAS EN GUATEMALA"**, a mi criterio el mismo cumple con los objetivos propuestos para su desarrollo, según protocolo propuesto, por lo que firmo la presente para que proceda con los trámites correspondientes.

Sin otro particular, me suscribo de usted.

Atentamente:

Joaquín Adolfo Guerrero Milián
Ing. Ciencias y Sistemas
Col. No. 11,570

Joaquín Adolfo Guerrero Milián
Ingeniero en Ciencias y Sistemas
Colegiado No. 11,570
Asesor y revisor de trabajo de graduación

Universidad San Carlos de Guatemala
Facultad de Ingeniería
Escuela de Ingeniería en Ciencias y Sistemas

Guatemala, 14 de agosto de 2019

Ingeniero
Carlos Gustavo Alonzo
Director de la Escuela de Ingeniería
En Ciencias y Sistemas

Respetable Ingeniero Alonzo:

Por este medio hago de su conocimiento que he revisado el trabajo de graduación del estudiante **WILMER VINICIO BETANCOURTH GARCÍA** con carné **199922727 y CUI 1628 41167 0205** titulado **"MODELO PARA LA GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN EN EL SECTOR DE MICROFINANZAS EN GUATEMALA"** y a mi criterio el mismo cumple con los objetivos propuestos para su desarrollo, según el protocolo aprobado.

Al agradecer su atención a la presente, aprovecho la oportunidad para suscribirme,

Atentamente,

Ing. Carlos Alfredo Azurdia
Coordinador de Privados
y Revisión de Trabajos de Graduación

ESCUELA DE INGENIERÍA EN CIENCIAS Y SISTEMAS

UNIVERSIDAD DE SAN CARLOS
DE GUATEMALA

FACULTAD DE INGENIERÌA
ESCUELA DE INGENIERÍA EN
CIENCIAS Y SISTEMAS

El Director de la Escuela de Ingeniería en Ciencias y Sistemas de la Facultad de Ingeniería de la Universidad de San Carlos de Guatemala, luego de conocer el dictamen del asesor con el visto bueno del revisor y del Licenciado en Letras, del trabajo de graduación ***"MODELO PARA LA GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN EN EL SECTOR DE MICROFINANZAS EN GUATEMALA",*** *realizado por el estudiante, WILMER VINICIO BETANCOURTH GARCÍA aprueba el presente trabajo y solicita la autorización del mismo.*

"ID Y ENSEÑAD A TODOS"

Msc. Carlos Gustavo Alonzo
Director
Escuela de Ingeniería en Ciencias y Sistemas

Guatemala, 29 de octubre 2020

Decanato
Facultad de Ingeniería
24189101- 24189102

DTG. 361.2020.

La Decana de la Facultad de Ingeniería de la Universidad de San Carlos de Guatemala, luego de conocer la aprobación por parte del Director de la Escuela de Ingeniería en Ciencias y Sistemas, al Trabajo de Graduación titulado: **MODELO PARA LA GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN EN EL SECTOR DE MICROFINANZAS EN GUATEMALA,** presentado por el estudiante universitario: **Wilmer Vinicio Betancourth García,** y después de haber culminado las revisiones previas bajo la responsabilidad de las instancias correspondientes, autoriza la impresión del mismo.

IMPRÍMASE:

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
DECANA
FACULTAD DE INGENIERÍA

Inga. Anabela Cordova Estrada
Decana

Guatemala, noviembre de 2020

AACE/asga

ACTO QUE DEDICO A:

Dios	Mi guía y refugio en tiempos de incertidumbre y abundancia, inspiración y fuerza en el proceso de tener anhelos deseados.
Mis padres	Gregorio Betancourth y Carmelina García. Por su amor, trabajo, enseñanzas y sacrificio en cada etapa de mi vida.
Mi hijo	Isaac Betancourth, motivación de mi vida, mi razón para superarme cada día.
Mis hermanos	Edwing, Ludwing y Marley Betancourth. Mis confidentes y cultivadores de sueños, agradezco ser ese soporte en cada momento.

AGRADECIMIENTOS A:

Universidad de San Carlos de Guatemala	Casa de estudios que me ha abierto las puertas a grandes oportunidades y a la cual me enorgullezco pertenecer.
Facultad de Ingeniería	Por albergarme todos estos años y nutrirme de conocimientos.
Mis padres	Por el apoyo incondicional que me brindaron a lo largo de estos años, por su afán de asegurarse que nada me faltara.
Mi asesor	Joaquín Guerrero, por el tiempo que ha dedicado al desarrollo de este trabajo, sus directrices y conocimientos han ayudado a hacerlo una realidad.
Mis amigos	María Jiménez, Jennifer Gonzales, Sergio Lemus, Edras Arriza, Manuel Fuentes, Víctor Yoc, Yaremis Godoy, Julissa Castillo, Sonia Gandi.
Mi tía	Izolina García. Sin su cariño y techo hoy nada sería lo que es.

ÍNDICE GENERAL

ÍNDICE DE ILUSTRACIONES IX
LISTA DE SÍMBOLOS XIII
GLOSARIO XV
RESUMEN XIX
OBJETIVOS XXI
INTRODUCCIÓN XXIII

1. INSTITUCIONES DE MICROFINANZAS 1
   1.1. Historia de las microfinanzas 1
   1.2. Instituciones de microfinanzas 2
   1.3. Clasificación de instituciones de microfinanzas 5
   1.4. Microcréditos 5
   1.5. Metodologías crediticias 6
      1.5.1. Grupos solidarios 6
      1.5.2. Bancos comunales 7
      1.5.3. Crédito individual 7
   1.6. Red de microfinanzas a nivel regional 9
   1.7. Red de microfinanzas de Guatemala 10
   1.8. Marco regulatorio de las instituciones de microfinanzas ... 11
      1.8.1. Microfinancieras de ahorro y crédito (MAC) 11
      1.8.2. Microfinancieras de inversión y crédito (MIC) ... 12

2. ESTÁNDARES DE SEGURIDAD DE LA INFORMACIÓN 13
   2.1. Norma UNE-ISO/EIC 27001 13

2.1.1. Origen de la norma 13
2.1.2. Objeto y campo de aplicación 14
2.1.3. Estadísticas de certificación de las empresas .. 17
2.2. COBIT 19
2.2.1. Origen de la norma 19
2.2.2. Objeto y campo de aplicación 20
2.2.2.1. Satisfacer las necesidades de las partes interesadas 22
2.2.2.2. Cubrir la organización de forma integral 23
2.2.2.3. Aplicar un solo marco de referencia 23
2.2.2.4. Habilitar un enfoque holístico 23
2.2.2.5. Separar el gobierno de la administración 24
2.3. PCI - DSS 25
2.3.1. Origen de la norma 25
2.3.2. Objeto y campo de aplicación 26

3. CATEGORIZACIÓN DE LAS AMENAZAS CIBERNÉTICAS 29
3.1. Denegación distribuida de servicios 29
3.1.1. Estadísticas de ataques 31
3.2. Ransomwere 32
3.2.1. Estadísticas de ataques 33
3.3. Spam 34
3.4. Phishing 35
3.5. Inyección SQL 36

4. SITUACIÓN ACTUAL DE LA CIBERSEGUIRDAD EN GUATEMALA 39
4.1. Delitos cibernéticos en Guatemala 39
4.2. Estrategia nacional de seguridad cibernética 40
4.2.1. Marcos legales 41
4.2.2. Educación 41
4.2.3. Cultura y sociedad 42
4.2.4. Tecnología de la información 42
4.2.5. Comité técnico de seguridad cibernética 43
4.3. Ley de lavado de dinero y otros activos 44
4.3.1. Cumplimiento de estándares Internacionales 45
4.3.2. Intendencia de verificación especial 45
4.3.2.1. Transacciones inusuales 46
4.3.2.1.1. Transacciones sospechosas 46

5. MODELO PARA LA GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN 47
5.1. Modelo actual de entidades de microfinanzas 47
5.2. Modelo propuesto para entidades de microfinanzas 48
5.3. Definición de modelo en capas 49
5.4. Capa de datos 51
5.4.1. Riesgos relacionados a los datos 53
5.4.2. Cifrado de datos 54
5.4.3. Hardening a bases de datos 56
5.4.4. Sistema de clasificación y etiquetado de información 57
5.4.5. Sistema de prevención de fuga de información (DLP) 59

5.4.6. Monitoreo de actividad bases de datos..... 61
5.4.7. Identificación y gestión de accesos de usuarios..... 62
5.4.8. Responsables de implementar 63
5.5. Capa de aplicaciones..... 64
5.5.1. Riesgos relacionados a las aplicaciones 67
5.5.2. Gestión de accesos de usuarios..... 69
5.5.3. Control de calidad en aplicaciones 70
5.5.4. Arquitectura de seguridad para aplicaciones ... 70
5.5.5. Validaciones de seguridad aplicaciones 71
5.5.6. Análisis de vulnerabilidades 73
5.5.7. Pruebas de penetración..... 74
5.5.8. Administración unificada de perfiles de usuarios en aplicaciones (SSO)..... 75
5.5.9. Plataforma de gestión de cuentas privilegiadas 77
5.5.10. Software de doble factor de autenticación (2FA) 77
5.5.11. Sistema de prevención de fuga de información (DLP)..... 78
5.5.12. Filtrado de aplicaciones web (WAF) 79
5.5.13. Solución antiphishing/antispam 80
5.5.14. Escaneo/revisión de código fuente 81
5.5.15. Consultoría sobre buenas prácticas de desarrollo de software..... 81
5.5.16. Monitoreo de integridad de archivos (FIM) 82
5.5.17. Gestión de la parametrización de la seguridad transaccional 83
5.5.18. Desarrollo seguro de aplicaciones..... 83

5.5.19. Responsables de implementar 84
5.6. Capa de sistemas operativos 85
5.6.1. Riesgos relacionados con los sistemas operativos 86
5.6.2. Escaneo de vulnerabilidades 88
5.6.3. Aplicación de parches de seguridad 89
5.6.4. Hardening de configuraciones 90
5.6.5. Plataforma de gestión de cuentas privilegiadas 91
5.6.6. Sistema de doble factor de autenticación (2FA) 91
5.6.7. Monitoreo de integridad de archivos (FIM) 92
5.6.8. Sistema de prevención de fuga de información (DLP) 92
5.6.9. Antivirus avanzado 92
5.6.10. Responsables de implementar 94
5.7. Capa de red 95
5.7.1. Riesgos relacionados a la red 96
5.7.2. Control de accesos a la red (NAC) 98
5.7.3. Sistema de prevención de intrusos (IPS) 99
5.7.4. Gestión de accesos remotos 101
5.7.5. Seguridad de las redes inalámbricas 101
5.7.6. Hardening de configuraciones 102
5.7.7. Filtrado de contenido web proxy 102
5.7.8. Diseño y segmentación de redes por capas 103
5.7.9. Sistema de prevención de fuga de información (DLP) 104
5.7.10. *Firewalls* perimetrales robustos capaces de detectar amenazas avanzadas 104

5.7.11. Responsables de implementar 106
5.8. Capa de usuarios finales 107
5.8.1. Riesgos relacionados con los usuarios 108
5.8.2. Educación a usuarios en seguridad de la información 110
5.8.3. Gestión de actualizaciones de seguridad 110
5.8.4. Seguridad del contenido 111
5.8.5. Políticas de seguridad para dispositivos móviles 112
5.8.6. BYOD (Bring Your Own Device) 113
5.8.7. Sistema de prevención de fuga de información (DLP) 113
5.8.8. Sistema de clasificación y etiquetado de información 114
5.8.9. Solución de transferencia segura de información 114
5.8.10. Responsables de implementar 115
5.9. Capa de monitoreo 116
5.9.1. Riesgos relacionados a la falta de monitoreo 117
5.9.2. Monitoreo de integridad de datos 119
5.9.3. Recolector de log para el reenvío de eventos 119
5.9.4. SOC (Centro de Operaciones de Seguridad). 121
5.9.5. Revisión de fuentes externas (noticias, boletines) 121
5.9.6. Servicio de monitoreo de fraudes 122
5.9.7. Evaluación periódica de vulnerabilidades 123
5.9.8. Ampliar el monitoreo de integridad para todas las bases de datos 123

5.9.9. SOC–CERT que cumpla con los requerimientos de monitoreo establecidos 124
5.9.10. Monitoreo reputacional 124
5.9.11. Responsables de implementar 125
5.10. Gobernanza 126
5.10.1. Gobierno de seguridad de la información 128
5.10.2. Adopción de estándares de seguridad 129
5.10.3. Evaluación y rediseño de procesos 130
5.10.4. Seguridad en nuevos productos y servicios 130
5.10.5. Gestión de riesgos y respuesta a incidentes 131
5.10.6. Cultura de seguridad de la información 132

CONCLUSIONES 133
RECOMENDACIONES 137
BIBLIOGRAFÍA 139
APÉNDICES 149
ANEXOS 153

ÍNDICE DE ILUSTRACIONES

FIGURAS

1. Marco legal financiero de microfinanzas 5
2. Clasificación crediticia, participación y alcance 9
3. Clientes y montos de cartera reportados por REDIMIF 10
4. Historia ISO 2701.....14
5. Estructura ISO 27001.....15
6. Fundamentos de la seguridad de la información 16
7. Estadística certificaciones por continente.....17
8. Número de empresas certificadas en Latinoamérica ISO 2701 18
9. Número de empresas certificadas ISO 27001 por año en Guatemala 19
10. Historia de COBIT 20
11. Principios de COBIT 5.....22
12. Categorías para enfoque holístico.....24
13. Historia de la norma PCI DSS.....25
14. Ataque de denegación de servicio 30
15. Top 10 países que generan botnet - 4Q 2018 31
16. Distribución de ataques – 4Q 2018 32
17. Distribución por tipo de ataque – 2017-2018 34
18. Portales suplantados por phishing 2018.....36
19. Principales ejes de la Estrategia Nacional de Seguridad Informática 40
20. Comité técnico de seguridad nacional.....43

21. Historia de cumplimiento de estándar internacional por Guatemala 45
22. Modelo de segmentación actual 47
23. Segmentación del modelo según arquitectura 48
24. Alcance del modelo 50
25. Modelo de capas 51
26. Clasificación de los datos por criticidad 52
27. Sistemas de prevención de fuga de información 60
28. Sistemas de control de accesos 63
29. Segmentación de las aplicaciones por sus servicios 66
30. Aplicaciones de pruebas de seguridad en aplicaciones 73
31. Aplicaciones para el manejo de centralizado de accesos 76
32. Sistemas de filtrado de aplicaciones web 80
33. Sistemas de pruebas de vulnerabilidades 89
34. Soluciones de antimalware 94
35. Sistemas de control de accesos a red 99
36. Herramientas de prevención de intrusos 100
37. *Firewalls* perimetrales 106
38. Sistemas de manejo de Log 120
39. Gestión del gobierno de una institución de microfinanzas 128

TABLAS

I. Diferencias entre instituciones financieras tradicionales y las microfinanzas 4
II. Normas de seguridad de datos de la PCI: descripción general de alto nivel 27
III. Responsables de implementar capa de datos 64
IV. Responsables de implementar capa de aplicaciones 85

V. Responsables de implementar capa de aplicaciones 95
VI. Responsables de implementar la capa de red 107
VII. Responsables de implementar la capa de usuarios 115
VIII. Responsable de implementar la capa de monitoreo 126

LISTA DE SÍMBOLOS

Símbolo	Significado
DoS	Denegación de servicios
$	Dólar
#	Número
%	Porcentaje

GLOSARIO

Agencia virtual	Es un sitio web que ofrece a sus clientes los mismos servicios de los que dispone una agencia convencional. Evita costos de desplazamientos y fronteras.
API	Interfaz de programación de aplicaciones.
COBIT	Objetivos de control para información y tecnologías relacionadas.
Código fuente	Conjunto de líneas de texto que unidas conforman un programa informático. Incluye cada uno de los pasos que debe de seguir la computadora para ejecutar las instrucciones que el usuario le dé.
Criptología	Es la ciencia que estudia la transformación de un determinado mensaje en un código, de forma tal que a partir de dicho código solo algunas personas sean capaces de recuperar el mensaje original.
Cuadrante mágico de Gartner	Representación gráfica sencilla de la situación del mercado de un producto tecnológico en un momento determinado, que muestra el ranking de los fabricantes con las mejores soluciones y productos.

DMZ	Consiste de una red lógicamente segmentada en la que se publican servidores o dispositivos que son accedidos desde redes externas como Internet y contienen información sensible. Se utiliza para evitar intrusiones o posibles ataques a equipos de la red interna.
FINCA	Foundation for International Community Assistance.
Firewall	Software o hardware especializado que es utilizado para permitir o denegar la comunicación entre redes de datos.
INGECOP	Inspección General de Cooperativas.
Inteligencia artificial	Es la combinación de algoritmos lógicos y matemáticos desarrollados con el propósito de crear máquinas que presenten las mismas capacidades que el ser humano.
Internet	Conjunto de redes de comunicación interconectadas para compartir información y recursos empleando el protocolo TCP/IP.
ISO	Organización Internacional de Normalización.
ITIL	Estándar internacional para las buenas prácticas del Gobierno TI.

KRRI	Indicadores de riesgo reputacional.
MAC	Microfinancieras de ahorro y crédito.
Mejores prácticas	Es una compilación de las prácticas innovadoras que empresas reconocidas a nivel mundial han implementado, y que les han dado resultados positivos.
MIC	Microfinancieras de inversión y crédito.
OWASP	Metodología que permite evaluar vulnerabilidades en la seguridad en aplicaciones móviles.
PCI	Industria de pagos con tarjetas
REDCAMIF	Red Centroamericana y del Caribe de Microfinanzas.
REDIMIF	Red de Microfinanzas de Guatemala.
Red oscura	Contenido que es publicado en redes encriptadas donde los usuarios permanecen en el anonimato y comúnmente es para realizar transacciones ilícitas.
SIB	Superintendencia de Bancos.
TLS	En un protocolo criptográfico que se asegura de proporcionar autenticación y cifrado de la información

	entre servidores, máquinas y aplicaciones que operan sobre una red.
VPN	Es una tecnología de red de computadoras que permite una extensión segura de la red de área local sobre una red pública o personal que es interconectada a través del internet.
Vulnerabilidades	Son errores o fallas de seguridad en hardware o software que permiten el acceso de personas no autorizadas obtener información sensible o bien cambiar configuraciones en los sistemas.

RESUMEN

Las instituciones de microfinanzas prestan servicios financieros de ahorro y crédito principalmente a un sector de la población que no dispone de las garantías necesarias (por dedicarse al comercio informal o estar en pobreza) que el sistema bancario tradicional solicita para otorgar un crédito. Está compuesto principalmente de organizaciones no gubernamentales oenegés y cooperativas de ahorro y crédito. Las oenegés no pueden captar ahorros, por lo que únicamente se dedican a otorgar préstamos. Según la cámara de microfinanzas de Guatemala REDIMIF, en el 2018 sus asociados manejaban una cartera de 159 millones de dólares en préstamos, y hacían uso de la tecnología para atender cada día a más clientes. Al no estar reguladas por las Superintendencia de Bancos SIB, no deben cumplir temas regulatorios exigidos a los bancos.

La seguridad de la información se ha convertido en una necesidad de las instituciones y se han creado estándares como ISO 27001, PCI DSS y COBIT que definen controles con la finalidad de mitigar riesgos mediante una gobernanza de seguridad, para facilitar la adaptación en cualquier institución. Según la Organización Internacional de Estandarización ISO, en América Latina 2017 existían 935 instituciones certificadas con la norma ISO 27001; 315 (34 %) de México, 170 (18 %) de Brasil y 148 (16 %) de Colombia. En Guatemala, para esa fecha habrá 6 instituciones certificadas.

Los delincuentes cibernéticos han comenzado realizar robos en América Latina. En 2018, el sistema de pagos interbancario en México fue vulnerado y dejó pérdidas por 10 millones de dólares. Ese mismo año, el Banco de Chile sufrió un ataque en el cual los perpetradores generaron transacciones bancarias a

China por montos de aproximadamente 40 millones de dólares. Las instituciones de microfinanzas manejan información sensible de clientes, colaboradores y proveedores que debe de ser protegida para evitar las fugas o robos. A nivel gubernamental, la legislación de Guatemala no dispone de una ley que ayude a proteger a los usuarios e instituciones de atacantes cibernéticos tanto locales como internacionales. Únicamente se dispone de una iniciativa creada en el 2009, la cual no ha sido aprobada en el Congreso de la República.

El modelo seguridad de la información se centra en la protección de los datos a través de 6 capas de seguridad a nivel tecnológico, las cuales son complementadas con un modelo de gobernanza que debe impulsar una cultura de la seguridad de la información dentro de las instituciones. Las capas del modelo contienen controles pacíficos para mitigar los identificados sobre las personas, procesos y tecnología.

OBJETIVOS

General

Desarrollar un modelo para la gestión de seguridad de la información para el sector de microfinanzas en Guatemala, con el propósito de minimizar los riesgos de pérdida o robo de información a través de mejores prácticas de seguridad de la información.

Específicos

1. Efectuar una recopilación documental de las instituciones de microfinanzas y su importancia en la economía de Guatemala, con base en las referencias de investigadores y organizaciones dedicadas a realizar estadísticas en este sector económico.

2. Identificar los riesgos y vulnerabilidades de seguridad de la información a los cuales están expuestas las instituciones de microfinanzas del país, mediante análisis documental, con el fin de minimizar fraudes, estafas, robos de información y otros delitos comunes que afectan a este sector.

3. Describir a través de recopilación documental, los estándares y mejores prácticas en la gestión de la seguridad de información que han sido probados y son utilizadas continuamente en cualquier tipo de institución a nivel nacional e internacional.

4. Definir un modelo para la gestión de seguridad de la información que sea adaptable y con características específicas para los procesos y funciones operacionales que realizan las instituciones de microfinanzas.

INTRODUCCIÓN

El desarrollo de esta investigación se enfoca en las instituciones de microfinanzas en Guatemala, sector compuesto principalmente por instituciones emergentes. En el transcurso de los años, estas han crecido desmesuradamente bajo administraciones financieras que, ya sea por falta conocimiento o de interés en la protección de la información, no están dispuestas a realizar inversiones económicas para implementar modelos de protección de la información. Al no estar obligadas a cumplir ningún normativo gubernamental de seguridad de la información como lo está el sector bancario tradicional, no se le presta la importancia necesaria, por lo que arriesgan su información financiera, de sus clientes y proveedores entre otros.

Las inversiones económicas que comúnmente se ejecutan en el sector de microfinanzas en temas de seguridad de la información están destinadas a tecnología como, por ejemplo, software de antivirus, dispositivos de red, *firewalls*, entre otros. Estas herramientas no son suficientes a pesar de que brindan cierto nivel de seguridad. Para los requerimientos actuales, donde la información es un activo intangible de cualquier organización, es necesario, además de herramientas tecnológicas, contar con medidas de control y seguimiento para la seguridad de la información.

En cualquier institución, asegurar un nivel de protección total es completamente imposible, incluso en instituciones que puedan disponer de recursos ilimitados. El propósito de un modelo de gestión de la seguridad de la información es, por tanto, garantizar que los riesgos y vulnerabilidades de la seguridad de la información sean evaluados, conocidos, clasificados, asumidos

y gestionados por las instituciones, para que, de una forma documentada y eficiente, permita evaluar el impacto, la reducción o mitigación de los riesgos. Sirva como punto de partida para la implementación en cualquier institución de microfinanzas mediante un análisis de la situación actual.

1. INSTITUCIONES DE MICROFINANZAS

1.1. Historia de las microfinanzas

Las microfinanzas, como son conocidas en la actualidad, se remontan a un país y una persona determinados. En 1974, en Bangladesh, un catedrático con estudios en los EE.UU., con el nombre de Muhammad Yunus, tuvo la iniciativa de dar préstamos de su propio dinero a personas pobres, dinero que ellos devolvían. “En ese tiempo, en Bangladesh existía una gran cantidad de personas con necesidad económica sin la oportunidad de acceder a un crédito en el sistema financiero”.[1]

Contrario a la cultura de los bancos tradicionales, en 1976 nació lo que hoy llamamos microfinanzas. El análisis crediticio de esta metodología tiene criterios completamente diferentes a como se realiza en la banca tradicional. No se basa en garantías prendarias tangibles; es una relación de confianza entre personas, con voluntad de crecer y con la esperanza de salir de la pobreza.

El desarrollo de la metodología para otorgar préstamos consiste en formar grupos de personas con necesidades crediticias, fomentar la competencia y la oportunidad de superación. Además, estos grupos ayudan a mantener el control de los pagos y entre ellos mismos aprueban los montos que serán otorgados en los préstamos de cada uno de los integrantes, generando responsabilidad, compromiso y solidaridad entre cada miembro.

[1] Biblioteca USAC. *Auditoría externa de cuentas por cobrar en una institución de microfinanzas*. http://biblioteca.usac.edu.gt/tesis/03/03_4547.pdf. Consulta: 10 de julio de 2019.

> "El microcrédito, a pesar de todos los pronósticos, logró crecer en los lugares donde se implementó, consolidando el éxito de la metodología. A través de un convenio con el Banco Agrícola de Bangladesh se abrió una sucursal con el nombre de Grameen, que contra todo pronóstico, logró sobresalir con éxito impresionante".[2]

Con el pasar de los años, Grameen ha consolidado su posición como una institución con un crecimiento sostenido y constante. Se ha convertido en institución con una actividad muy específica, diferente del modelo clásico de las intuiciones financieras tradicionales. En 1983, Grameen se independiza del Banco Agrícola y se convierte en una institución de microfinanzas con el nombre de Grameen Bank (Banco de los Pobres).

> "Según datos estadísticos que ha presentado Grameen Bank para 2016, cuentan con 2 568 sucursales y 21 043 empleados los cuales atienden a 7,29 millones de clientes, de los cuales 96,54 de cada 100 son mujeres. La institución dispone una cartera crediticia de 2 388 millones de dólares distribuidos entre todos sus clientes, con una tasa de recuperación de 98,34 por cada 100 dólares que presta".[3]

> "A partir de 2007, Grameen Bank ha tenido presencia en el mercado de microfinanzas de Guatemala por intermedio del Banco de Desarrollo Rural (BANRURAL). En 2018 cuentan con 21 sucursales y 150 empleados que prestan servicios financieros a más de 49 000 prestatarios que se han sido beneficiados con más de 25 millones de dólares en créditos. En Guatemala se tienen cifras de que el 100 % de las mujeres prestatarias han logrado cancelar sus deudas pendientes".[4]

1.2. Instituciones de microfinanzas

Las instituciones de microfinanzas tienen la función especial de facilitar el acceso a los servicios financieros como microcréditos, ahorros, seguros o transferencias a personas de bajos recursos, debido a que tienen presencia en las comunidades en las cuales la mayoría de población puede tener a su disposición servicios financieros.

---

[2] Ranrural. *Banco de los pobres Grameen Bank*. http://www.grameen.com. Consulta: 5 de julio de 2019.
[3] Ibíd.
[4] Banco Mundial. *Inclusión financiera*. http://www.bancomundial.org/es/topic/financialinclusion/overview. Consulta: 5 de julio de 2019.

La mayoría de las instituciones microfinanzas han centrado sus esfuerzos en el sector del microcrédito. Son préstamos pequeños que permiten a las personas, que generalmente no poseen las garantías tangibles exigidas por el sistema financiero tradicional, iniciar o ampliar su propio emprendimiento y generar ingresos.

Dentro de las instituciones de microfinanzas y las instituciones que pertenecen al sector financiero tradicional existen grandes diferencias. A continuación, se presentan las de mayor relevancia.

- Las instituciones financieras tradicionales basan sus criterios en garantías tangibles, con lo que se reduce el nivel de riesgo al asegurar retorno del monto otorgado al cliente. Las instituciones de microfinanzas se basan en un análisis crediticio en base a solvencia moral, la disposición y solidaridad de pago de los clientes.

- En las instituciones de microfinanzas los asesores de crédito tienen constante comunicación con los clientes; realizan reuniones en cada una de las fechas de pago, los clientes llevan las cuotas cuando se reúnen. Este tipo de cliente necesita mayor atención; de lo contrario, incurre en falta de pagos.

- En las instituciones de microfinanzas los plazos de los préstamos otorgados vencen en un tiempo muy corto, con promedio de 6 meses y un máximo de un año, motivo por el cual la rotación de la cartera es muy elevada.

- Las instituciones financieras tradicionales buscan el mayor beneficio de ganancias posibles. Las instituciones de microfinanzas se enfocan en

aliviar la pobreza, la creación de empleo y mejorar la calidad de vida de sus clientes y colaboradores.

La tabla siguiente ejemplifica de una forma resumida las características que diferencian a las instituciones de microfinanzas de las instituciones financieras tradicionales.

Tabla I. **Diferencias entre instituciones financieras tradicionales y las microfinanzas**

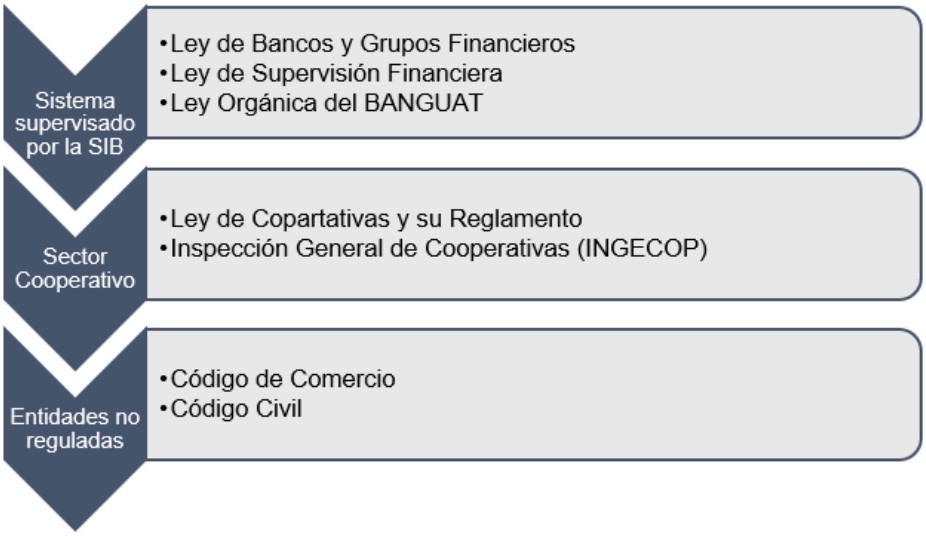
Área	Instituciones financieras tradicionales	Microfinanzas
Metodología crediticia	(1) Basado en colateral (2) Requiere documentación formal (3) En promedio es un poco intensiva en mano de obra (4) Cancelación de préstamos en cuotas mensual, trimestral o anualmente	(1) Basado en reputación (2) Menos documentación (3) Mayor coeficiente de mano de obra (4) Servicio / pago de los préstamos suelen atenderse con pagos semanales y bimensuales
Cartera de préstamos	(1) Menos préstamos (2) Préstamos de mayor tamaño garantizados (3) Plazo más largo de vencimiento (4) Morosidad más estable	(1) Más préstamos (2) Préstamos de menor tamaño no garantizados (3) Plazos más cortos de vencimiento (4) Morosidad más volátil
Estructura institucional y gobierno (de entidades financieras reguladas)	(1) Beneficio maximizado por accionistas institucionales e individuales (2) Creación mediante cesión de institución regulada existente (3) Organización centralizada con sucursales en ciudades	(1) Principalmente accionistas institucionales sin fines de lucro (2) Creación por conversión de ONG o formación de nueva entidad (3) Serie descentralizada de pequeñas unidades en áreas con infraestructura débil

Fuente: SAWERS, Larry, SCHYDLOWSKY, Daniel y NICKERSON, David. *Emerging financial markets in the global economy*. p. 63.

1.3. Clasificación de instituciones de microfinanzas

Dentro del marco legal financiero de Guatemala, según el decreto 25-2016, Ley de instituciones de microfinanzas, están clasificadas y regidas como muestra la figura 1:

Figura 1. **Marco legal financiero de microfinanzas**



Fuente: Decreto 25-2016. *Ley de Entidades de Microfinanzas*. https://www.mineco.gob.gt. Consulta: 5 de marzo de 2019.

1.4. Microcréditos

La pobreza no es natural. Es algo creado por el hombre y por tanto puede ser erradicada por las acciones humanas.

Los microcréditos son programas de concesión de pequeños créditos a los más necesitados para que éstos puedan poner en marcha pequeños negocios

que generen ingresos con los que mejorar su nivel de vida y el de sus familias.

La palabra microcrédito es relativamente nueva y no existía antes de 1970. No es de sorprender que actualmente el término "microcrédito" es utilizado para referirse al crédito agrícola, rural, cooperativo, de consumo, de las asociaciones de ahorro y crédito, las cooperativas de ahorro y crédito o a los prestamistas (prestamistas de diario).

1.5. Metodologías crediticias

En el sector de microfinanzas de Guatemala se utilizan las mismas metodologías conocidas y empleadas en otros países en desarrollo.

1.5.1. Grupos solidarios

Metodología que fue desarrollada por Grameen Bank de Bangladesh y consiste en un tipo de microcrédito que es otorgado a varios miembros de un grupo; la garantía es la solidaridad de grupo. Ante la falta de pago de alguno de los miembros, los demás tienen el compromiso moral de aportar dinero para cubrir la cuota faltante y efectuar el pago a la institución de microfinanzas.

La solidaridad del grupo actúa como colateral y sustituye la falta de garantía tangible. Los grupos son conformados por personas de la misma comunidad que se conocen entre sí y realizan similar clase de actividad económica. Cada grupo cuenta con una organización mínima conformada principalmente por un presidente y un secretario o tesorero, quienes se encargan de dirigir las reuniones del grupo y recolectar el dinero para el pago del préstamo.

> “El grupo o alguno de sus miembros no recibe un nuevo préstamo mientras no esté cancelado el anterior. El monto otorgado para nuevos préstamos va aumentando gradualmente conforme se cumple con la obligación y crece la calidad de vida”.[5]

1.5.2. Bancos comunales

Fue desarrollado durante los años 80, por Ruper Scofild a través de Foundation for International Community Assistance (FINCA). “Los bancos comunales son grupos de entre 30 a 50 personas, con miembros mayoritariamente mujeres, con el propósito de brindar servicios de crédito y ahorro utilizando solidaridad de grupo”.[6]

La garantía funciona de manera similar que los grupos solidarios. Se diferencia de estos en que otorga capacidad de autogestión a los miembros del grupo, quienes son los encargados de administrar la cartera de ahorros y préstamos. Cada grupo cuenta con una junta directiva y un reglamento interno.

En los bancos comunales, como en los grupos solidarios, no existen garantías tangibles. Cada integrante del grupo es aval de los demás; si uno no llegara a pagar, los demás miembros deben pagar. Este método, como el otro, permite atender a un amplio número de personas que no tienen acceso a los créditos en instituciones financieras.

1.5.3. Crédito individual

“Este tipo de metodología en las instituciones de microfinanzas tiene características similares a como se manejan en las instituciones financieras

[5] SIB. *Sector de microfinanzas*. http://www.sib.gob.gt/c/document_library/get_file?folderId=471455&name=DLFE-10346.pdf. Consulta: 11 de marzo de 2019.
[6] Ibíd.

tradicionales. El titular del préstamo es una persona que cuenta con garantías tangibles o avales"[7].

Los montos otorgados para créditos individuales tienden a ser mayores que los otorgados en grupos solidarios o bancos comunales. El plazo y el monto otorgado es mayor, puede ser de hasta 36 meses. Con frecuencia las personas que han pertenecido a un grupo solidario o banca comunal pasan a ser beneficiados con este tipo de préstamo.

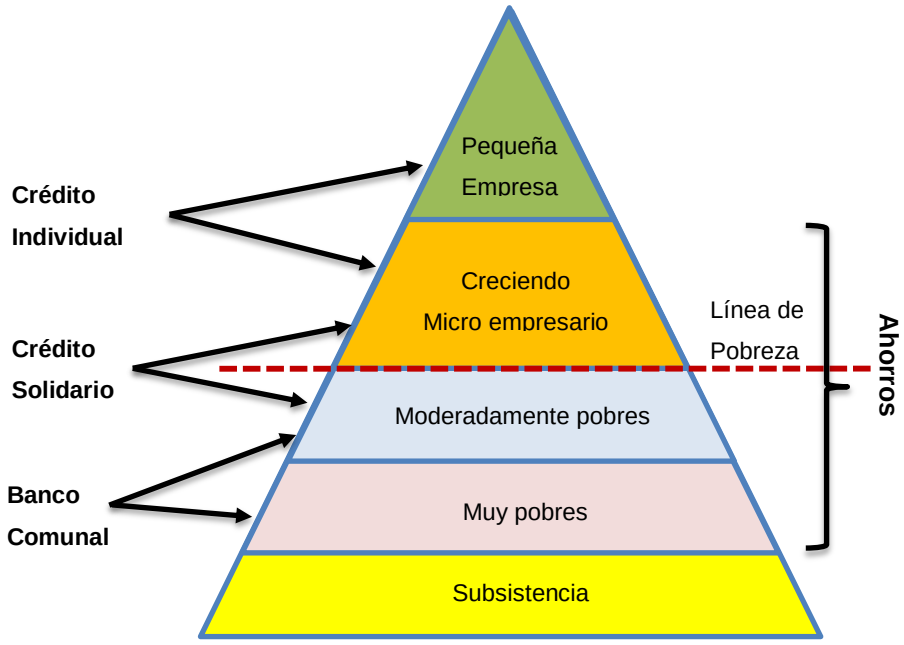
Las instituciones de microfinanzas cumplen un papel fundamental en el crecimiento económico del país, debido a que el sector de la población al que brindan sus servicios no es apto para crédito por las instituciones financieras tradicionales, por carecer de ingresos fijos y garantías tangibles.

> "Según datos de la Superintendencia de Bancos de Guatemala los montos que se otorgan a los grupos de los bancos comunales generalmente son menores de Q 3 mil por integrante. Para grupos solidarios, los rangos otorgados se encuentran entre Q 500 a Q 25 mil y los créditos individuales tienen rangos entre los Q5 mil a Q 50 mil".[8]

La figura 2 ilustra cómo las entidades de microfinanzas logran un alcance de participación de la población con escasos recursos.

[7] SIB. *Sector de microfinanzas*. http://www.sib.gob.gt/c/document_library/get_file?folderId=471455&name=DLFE-10346.pdf. Consulta: 26 de marzo de 2019.
[8] Ibíd.

Figura 2. **Clasificación crediticia, participación y alcance**



Fuente: elaboración propia.

1.6. Red de microfinanzas a nivel regional

> Las instituciones de microfinanzas en Centroamérica y del Caribe se han organizado y creado una red con el nombre de REDCAMIF. Su objetivo principal es promover la industria de microfinanzas e incrementar su impacto en el desarrollo económico y social de Centroamérica y el Caribe, así como incidir e impulsar condiciones políticas, normativas y regulatorias que beneficien y fortalezcan al sector de las microfinanzas en la región centroamericana y en el Caribe.[9]

REDCAMIF está conformada por varias redes de microfinanzas de los países de Centroamérica y el Caribe y realiza estudios de desempeños de las instituciones de microfinanzas asociadas a la red.

[9] REDIMIF. *Red de Instituciones de Microfinanzas de Guatemala*. http://redimif.org. Consulta: 13 de marzo de 2019.

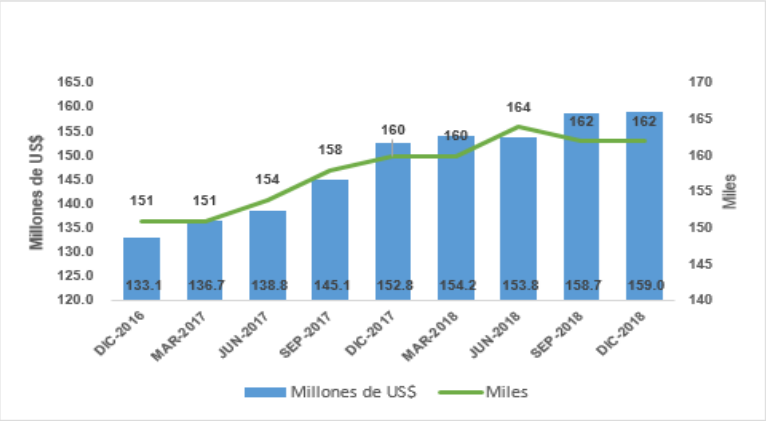
1.7. Red de microfinanzas de Guatemala

> "Es una organización que integra a 16 instituciones que se especializan en la prestación de servicios de microfinanzas REDIMIF. Se constituyó legalmente el 30 de marzo del año 2001, con el propósito de ser la entidad gremial representativa del sector de microfinanzas en Guatemala".[10]

REDIMIF fue creada para el fortalecimiento y mejoramiento continuo de las instituciones asociadas a su red, proporcionarles productos y servicios financieros, técnicos y de capacitación, así como representación gremial.

En la figura 3 se puede observar lo fuerte que son las instituciones de microfinanzas asociadas a REDIMIF, con base en el crecimiento de clientes y los incrementos de cartera han tenido de diciembre 2016 a diciembre 2018.

Figura 3. **Clientes y montos de cartera reportados por REDIMIF**



Fuente: REDIMIF. *Red de instituciones microfinanzas de Guatemala*. http://redimif.org. Consulta: 26 de marzo de 2019.

[10] REDIMIF. *Red de instituciones de Microfinanzas de Guatemala*. http://redimif.org. Consulta: 13 de marzo de 2019.

1.8. Marco regulatorio de las instituciones de microfinanzas

> El 10 de mayo de 2016 se publicó en el diario de Centro América el decreto número 25-2016 *Ley de entidades de microfinanzas y entes de microfinanzas sin fines de lucro*. Esta ley nace con el objeto de regular lo relativo a la constitución, autorización, fusión funcionamiento, operaciones, servicios, suspensión y liquidación de las microfinanzas de ahorro y crédito y microfinanzas sin fines de lucro.[11]

Antes de esta ley no existe ningún marco regulatorio que permita contar con una adecuada supervisión y regulación prudencial que favorezca la efectiva y eficiente acumulación de capital y asignación de recursos, así como la solvencia y solidez de las instituciones en función del bien tutelado (el ahorro de cuenta habientes).

> La ley indica que las instituciones de microfinanzas se podrán constituir como sociedades anónimas de ahorro y crédito o Inversión y crédito. Su capital estará dividido y representado por acciones nominativas. Corresponde a la Superintendencia de Bancos realizar los dictámenes correspondientes para que sean aprobados por la Junta Monetaria.
>
> El 25 de julio de 2018 la Junta Monetaria Reglamento de Aspectos Prudenciales que tiene como objetivo observar a instituciones de microfinanzas en lo relativo a su liquidez, patrimonio requerido y proporciones globales en moneda extranjera.[12]

1.8.1. Microfinancieras de ahorro y crédito (MAC)

> Estas instituciones podrán recibir depósitos de ahorros y otorgar créditos. Para constituirse deben pagar un monto mínimo de cinco millones de dólares de los Estados Unidos de América o su equivalente en moneda nacional (quetzales) en un banco del sistema, monto que será monitoreado de forma anual por la Superintendencia de Bancos.[13]

[11] MINECO, Ministerio de Economía. *Microfinanzas*. https://www.mineco.gob.gt/sites/default/files/MIPYMES/ley_microfinanzas.pdf. Consulta: 13 de marzo de 2019.
[12] Banguat. *Junta Monetaria*. http://www.banguat.gob.gt/inc/ver.asp?id=/Publica/leyaccesoalainfo/indexjm.htm. Consulta: 13 de marzo de 2019.
[13] Op.cit.

1.8.2. Microfinancieras de inversión y crédito (MIC)

Estas instituciones podrán realizar inversiones y otorgar créditos. Para constituirse se deben de pagar un monto mínimo de un millón ochocientos mil dólares de los Estados Unidos de América o su equivalente en moneda nacional (quetzales) en un banco del sistema, monto que será monitoreado de forma anual por la Superintendencia de Bancos.[14]

[14] MINECO. Ministerio de Economía. *Microfinanzas*. https://www.mineco.gob.gt/sites/default/files/MIPYMES/ley_microfinanzas.pdf. Consulta: 13 de marzo de 2019.

2. ESTÁNDARES DE SEGURIDAD DE LA INFORMACIÓN

2.1. Norma UNE-ISO/EIC 27001

A continuación, se muestra la norma UNE-ISO/EIC 27001.

2.1.1. Origen de la norma

ISO e IEC es un sistema especializado para la normalización a nivel mundial de estándares internacionales de mejores prácticas. Los organismos participan en el desarrollo de las normas internacionales a través de comités técnicos establecidos por las organizaciones respectivas para realizar acuerdos en campos específicos de la actividad técnica.[15]

Estos comités técnicos de ISO e IEC colaboran en los campos de interés mutuo para definir mejoras prácticas, que son adoptadas por empresas a nivel mundial.

La norma de seguridad de la información fue preparada inicialmente por el Instituto de Normas Británico como BS 7799. Surge por primera en Inglaterra vez en 1995, con objeto de proporcionar a cualquier empresa un conjunto de buenas prácticas para la gestión de la seguridad de su información.[16]

La primera parte de la norma (BS 7799-1) fue una guía de buenas prácticas, para la que no se establecía un esquema de certificación. Es la segunda parte (BS 7799-2), publicada por primera vez en 1998, estableció los requisitos de un sistema de seguridad de la información (SGSI) para ser certificable por una entidad independiente.[17]

[15] Miembros de Junta Monetaria de Guatemala. *Ley acceso a la información*. http://www.banguat.gob.gt/inc/ve r.asp?id=/Publica/leyaccesoalainfo/indexjm.htm. Consulta: 13 de marzo de 2019.

[16] Norma ISO 27001. *El portal de ISO 27001 en español*. http://www.iso27000.es/otros.html#seccion2. Consulta: 13 de marzo de 2019.

[17] Op.cit.

La Norma Internacional ISO/IEC 27001 fue preparada bajo la supervisión del subcomité de técnicos de seguridad del comité técnico ISO/IEC JTC 1, y en el subcomité SC 27 técnicas de seguridad.

Figura 4. **Historia ISO 2701**

Fuente: elaboración propia.

2.1.2. Objeto y campo de aplicación

> El objetivo principal de la norma ISO 27001 es proteger la confidencialidad, integridad y disponibilidad de la información de cualquier institución. Esto lo hace mediante investigaciones que identifican los potenciales riesgos que podrían afectar la seguridad de la información. Con la información obtenida se define un plan de acción con base en la criticidad de cada riesgo identificado para mitigar las vulnerabilidades en el menor tiempo posible.[18]

La norma ISO 27001 tiene como objetivo principal la gestión de riesgos relacionados a la seguridad de la información: investigar dónde se producen los riesgos, cuáles son y luego cómo deben de ser tratados de forma sistemática, con la finalidad de proteger los recursos de las organizaciones establecen una base de datos confiable para la toma de decisiones, ver figura 5.

[18] SGCI. *Blog especializado en sistemas de gestión de seguridad de la información*. https://www.pmg-ssi.com/. Consulta: 15 de marzo de 2019

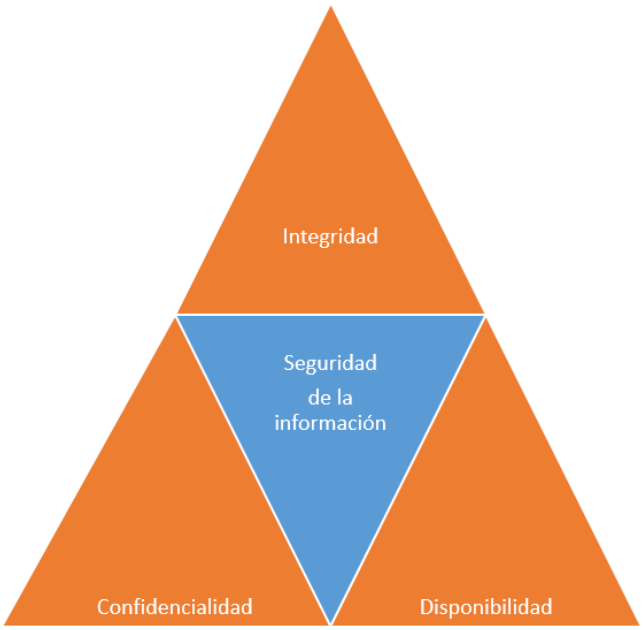
Figura 5. **Estructura ISO 27001**

Fuente: elaboración propia.

Los controles de seguridad necesarios se implementan por lo general, mediante políticas, procedimientos e implementación técnica (software y hardware). En la mayoría de los casos, las instituciones ya disponen del hardware y software necesario, el cual utilizan de forma no segura; por lo tanto, la mayor parte de la implementación de ISO 27001 está relacionada con determinar las reglas organizacionales necesarias para prevenir vulnerabilidades de seguridad.

Eliminar el riesgo de vulnerabilidades en la seguridad de la información es imposible, aun con presupuesto ilimitado. Podemos garantizar mitigar y disminuir los riesgos para lo cual debemos entender los tres principios básicos sobre la información (ver figura 6).

Figura 6. **Fundamentos de la seguridad de la información**



Fuente: Seguridad y firewall. *Triada de seguridad*. https://www.seguridadyfirewall.cl/2016/01/fundamentos-basicos-de-seguridad-de-la.html. Consulta: 15 de marzo de 2019.

- Confidencialidad: principio sobre el cual se asegura que la información únicamente esté disponible para los individuos, entidades o procesos autorizados y no sea revelada a ninguna entidad que no disponga de la autorización necesaria.

- Integridad: la información debe mantener siempre su exactitud y no debe ser alterada por ningún tipo de amenazas o por error humano.

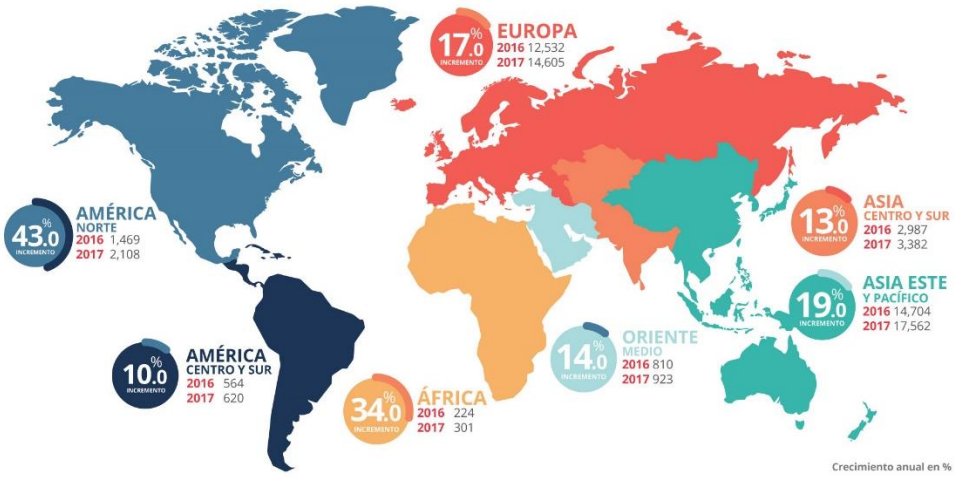
- Disponibilidad: asegura que la información esté disponible a tiempo por los usuarios autorizados en el momento que la requieran.

La norma está divide en 11 capítulos; los capítulos 0 a 3 son introductorios (no son obligatorios para la implementación), mientras que los capítulos 4 a 10 son obligatorios. Una organización debe implementar todos sus requerimientos si quiere cumplir con la norma. Estos capítulos detallan 14 dominios de seguridad, 35 objetivos y 114 controles.[19]

2.1.3. Estadísticas de certificación de las empresas

Una estadística revelada por la organización internacional para la estandarización en agosto 2018, muestra la tendencia de las empresas a nivel mundial a certificarse en la norma ISO 27001.

Figura 7. **Estadística certificaciones por continente**



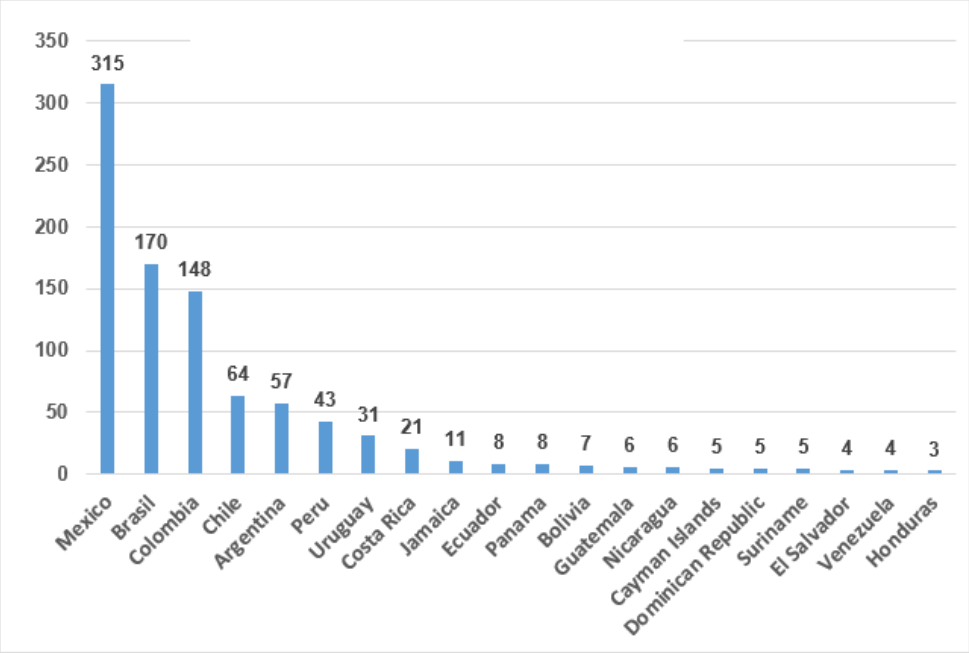
Fuente: GlobalSTD. *Certificación*. https://www.globalstd.com/certificacion/codigo-sqf/iso-survey-2017. Consulta: 26 de marzo de 2019.

En América Latina existen países que han logrado avanzar en la implementación de sistemas de gestión de la seguridad de la información y han

[19] 27001 Academy. *Risk assessment and treatment process*. https://info.advisera.com/hubfs/27001Academy/27001Academy_FreeDownloads/Diagram_of_ISO_27001_risk_assessment_and_treatment_process_EN.pdf. Consulta: 15 de marzo de 2019.

logrado obtener una certificación ISO/EIC 27001. El sector con más certificaciones es el que presta servicios de tecnologías de la información.

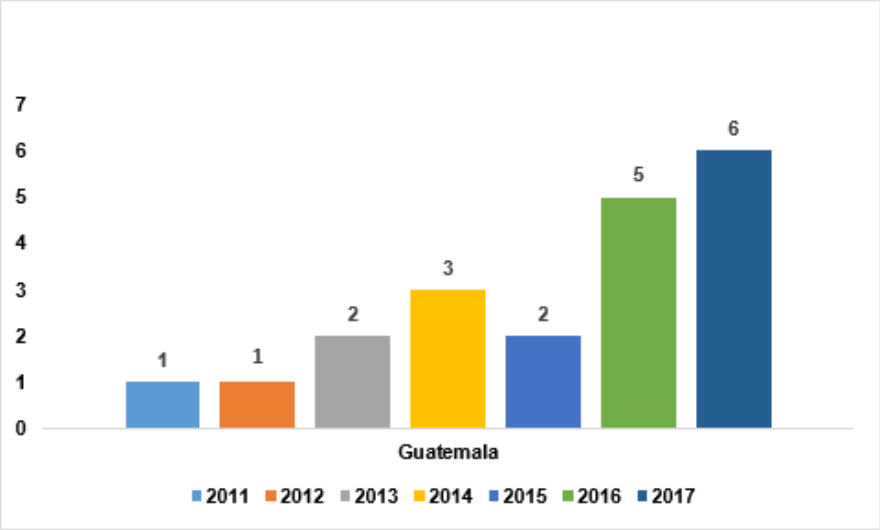
Figura 8. **Número de empresas certificadas en Latinoamérica ISO 2701**



Fuente: International Organization for Standardization (ISO). *Encuesta ISO de certificaciones a los estándares del sistema de gestión.* https://isotc.iso.org/livelink/livelink?func=ll&objId=18808772&objAction=browse&viewType=1. Consulta: 26 de marzo de 2019.

En Guatemala la cantidad de empresas certificadas en ISO/EIC 27001 es todavía pequeña. Esto demuestra la falta de interés o despreocupación de la industria guatemalteca en proteger su información y la de sus clientes.

Figura 9. **Número de empresas certificadas ISO 27001 por año en Guatemala**



Fuente: International Organization for Standardization (ISO). *Encuesta ISO de certificaciones a los estándares del sistema de gestión.* https://isotc.iso.org/livelink/livelink?func=ll&objId=18808772&objAction=browse&viewType=1. Consulta: 26 de marzo de 2019.

2.2. COBIT

A continuación, se muestra la norma COBIT.

2.2.1. Origen de la norma

COBIT es un marco de gobernanza que fue creado para ayudar en el área de tecnología mediante herramientas que permitan conectar los requerimientos de control con los aspectos técnicos y los riesgos del negocio, mejorando el desarrollo de políticas y buenas prácticas para el control de las tecnologías en las

instituciones. Se puede aplicar a instituciones sin importar los tamaños, tanto en el sector privado, público o entidades sin fines de lucro.[20]

"Las siglas COBIT significan Objetivos de control para tecnología de información y tecnologías relacionadas (Control Objectives for Information Systems and related Technology). El modelo es resultado del esfuerzo de especialistas de muchos países, desarrollado por ISACA (Information Systems Audit and Control Association)".[21]

Figura 10. **Historia de COBIT**

Fuente: elaboración propia.

2.2.2. Objeto y campo de aplicación

COBIT fue diseñado con el objetivo de ayudar a las instituciones a obtener el valor óptimo de la tecnología, maximizando la realización de beneficios, desempeño de recursos y mitigación de riesgo identificados. COBIT brinda la posibilidad que las áreas de tecnología sean gobernadas y gestionadas desde múltiples puntos de vista dentro de las instituciones, tomando en consideración el área de negocios y de operaciones, así como los clientes internos y externos.[22]

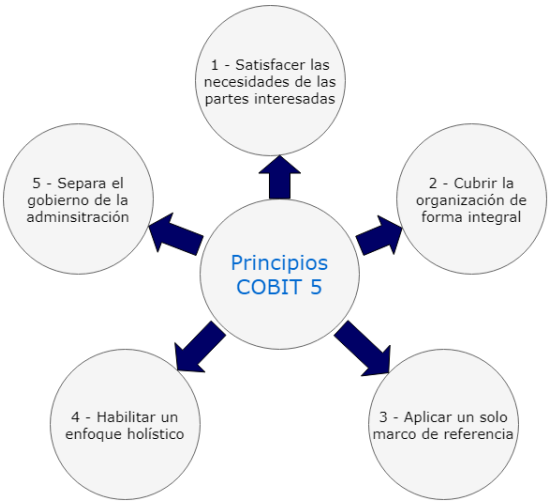
[20] Organización Internacional para la Estandarización. *La ciudad sostenible*. https://www.iso.org. Consulta: 15 de marzo de 2019.
[21] ISACA. *Documentación COBIT español*. https://www.isaca.org/cobit. Consulta: 15 de marzo de 2019.
[22] Wikipedia. *Objetivos de control para la información y tecnologías relacionadas.* https://www.isaca.org/cobit. Consulta: 15 de marzo de 2019.

A partir de la versión COBIT 5 (actual) se busca la creación de valor a través una gobernanza y gestión efectiva de la información y de los activos tecnológicos de las instituciones. Se centra en el compromiso de los servicios prestados al negocio, lo que permite incrementar la satisfacción de usuarios y personas que participan en la cadena de valor mediante la gestión de la tecnología. Enfatiza los cumplimientos regulatorios, incrementa su valor a través de las tecnologías, y permite el alineamiento de objetivos de negocio.

Es un modelo genérico utilizado por quienes tienen la responsabilidad principal de los procesos de negocios y la tecnología. Dependen de la tecnología para obtener información relevante y confiable, y adiciona calidad, confiabilidad y control de la información y la tecnología relacionada. Está basado en un marco de trabajo idealizado para que las instituciones puedan alcanzar sus objetivos estratégicos para el gobierno de tecnología.

Se basa en 5 principios claves (ver figura 11). Cada uno de estos principios se subdivide en las actividades y prácticas de la organización relacionadas con a la tecnología en las dos principales áreas (Gobierno y Administración); a su vez, se dividen en dominios que se deben implementar en la gobernanza y en la administración.

Figura 11. **Principios de COBIT 5**



Fuente: ISACA. *Documentación COBIT español*. https://www.isaca.org/cobit. Consulta: 3 de mayo de 2019.

2.2.2.1. Satisfacer las necesidades de las partes interesadas

Cualquier institución que existe, tiene como finalidad crear valor, sea privada, gubernamental o sin fines de lucro, lo que significa conseguir metas con un costo óptimo mientras se mitigan los riesgos. El sistema de gobierno como lo nombra COBIT 5 debe tomar en cuenta todas las partes interesadas en cualquier proceso al tomar decisiones sobre beneficios y evaluación de riesgos y recursos.

El ámbito en el que la institución opera está determinado por factores internos y externos diferentes, por lo cual requiere de un modelo de gobierno y gestión personalizado para a su entorno. Debido a que los motivos y las necesidades de las partes interesadas influyen en todas las áreas de una

institución, estas deben alinearse entre las necesidades institucionales y las soluciones y servicios de tecnología.

2.2.2.2. Cubrir la organización de forma integral

El modelo propuesto por COBIT brinda una visión general del gobierno y la gestión de una institución. Incluye a todo aquel que sea relevante para la gestión de información, interno y externo. Cubre todas las funciones y procesos necesarias para gestionar la información sin dejar ningún criterio que no sea tomado en cuenta.

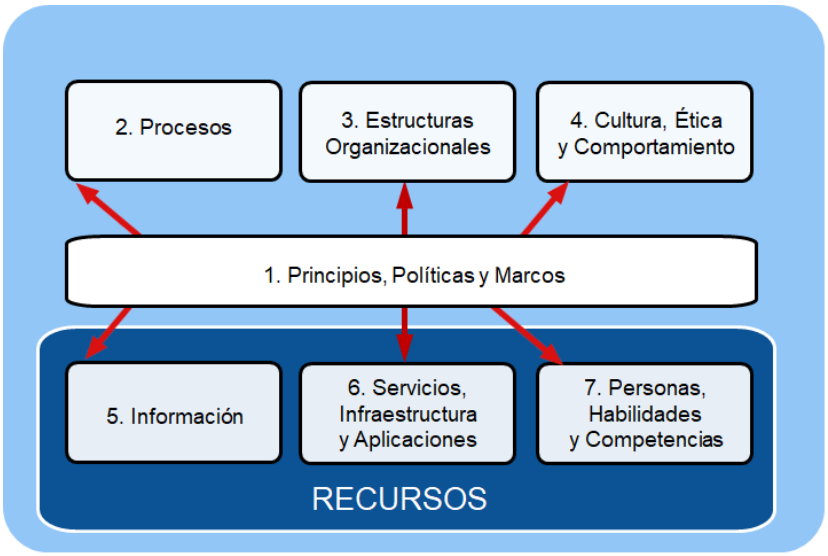
2.2.2.3. Aplicar un solo marco de referencia

Estar alineado con los estándares, normas y políticas relevantes usados por las organizaciones distingue a COBIT como un marco integrador efectivo, el cual proporciona una arquitectura fácil de implementar a través de materiales guía que ayudan a unificar todas las buenas prácticas TI como ISO/IEC 38500, ITIL, la serie ISO/IEC 27000, ISO/IEC 9000, ISO/IEC 31000, PMBOK, CMMI.

2.2.2.4. Habilitar un enfoque holístico

Considerar la gestión empresarial como un todo da la oportunidad de entender la sinergia que existe en las organizaciones, en sus operaciones y bases elementales que la constituyen. Ayuda a tomar de mejor manera las decisiones, tratándolas de forma sistemática, involucra a todos los grupos de interés debido a que todos están interrelacionados.

Figura 12. **Categorías para enfoque holístico**



Fuente: ISACA. *Documentación COBIT español*. https://www.isaca.org/cobit. Consulta: 3 de mayo de 2019.

2.2.2.5. Separar el gobierno de la administración

> La separación entre estas áreas es relativamente fácil debido a las funciones y responsables. El gobierno tiene como funciones evaluar, orientar y supervisar. Regularmente está a cargo de la junta directiva bajo la dirección del presidente. La administración tiene como función planificar, construir, ejecutar, supervisar.[23]

Dependiendo de su situación particular, una institución puede disponer de procesos como le sea conveniente, manteniendo las metas de gobierno y administración cubiertas.

[23] ISACA. *Documentación COBIT español*. https://www.isaca.org/cobit. Consulta: 3 de marzo de 2019.

2.3. PCI - DSS

A continuación, se muestran la norma PCI – DSS.

2.3.1. Origen de la norma

El estándar de seguridad de datos para la información relacionada con las tarjetas de crédito y débito se desarrolló por las compañías que procesan tarjetas (Visa, Mastercard, American Express y Discover). Está formado por un comité denominado PCI SSC (Payment Card Industry Security Standards Council) para fomentar y mejorar la seguridad.

Es una guía que especializada para instituciones que procesan, almacenan y transmiten información sensible de usuarios de tarjetas de pago débito y crédito, Asegura que los datos se mantengan protegidos, evita fraudes que causan pérdidas millonarias. Según un informe, en el 2015 se fueron US$21.000 millones y se espera que para el 2020 alcance los US$31.000 millones.[24]

Figura 13. **Historia de la norma PCI DSS**

Fuente: PCI. *Asegurar juntos el futuro de los pagos*. https://es.pcisecuritystandards.org. Consulta: 4 de abril de 2019.

[24] Wikipedia. *Objetivos de control para la información y tecnologías relacionadas*. https://www.isaca.org/cobit. Consulta: 11 de marzo de 2019.

2.3.2. Objeto y campo de aplicación

> La norma consiste en estándares de seguridad que se aplican a todas las instituciones que participan en el procesamiento de las tarjetas de crédito y débito. Define el conjunto de requerimientos para definir políticas, procedimientos de seguridad, arquitectura de red, diseño de software y medidas de protección que intervienen en el tratamiento de la información de tarjetas, entre las que se incluyen comerciantes, procesadores, adquirentes, entidades emisoras y proveedores de servicios.[25]

Su objetivo es la reducción del fraude relacionado al incrementar la seguridad de los datos. Se compone de 12 requisitos agrupados en 6 grandes objetivos (tabla II), alrededor de 200 controles y 250 procedimientos, que al aplicarlos reducen las filtraciones de los datos.

Lo que hace especial a esta norma es su enfoque en la protección de datos sensibles de los clientes. Los controles que recomiendan con el único objetivo de asegurar que los datos de los clientes no sean vulnerados.

[25] BBC. *Fraudes con tarjetas de crédito*. https://www.bbc.com/mundo/vert-cap-40638275. Consulta: 26 de marzo de 2019.

Tabla II. **Normas de seguridad de datos de la PCI: descripción general de alto nivel**

Principios	Requerimientos
Desarrolle y mantenga redes y sistemas seguros	1. Instale y mantenga una configuración de *firewall* para proteger los datos del titular de la tarjeta
	2. No usar los valores predeterminados suministrados por el proveedor para las contraseñas del sistema y otros parámetros de seguridad.
Proteger los datos de las tarjetas	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. Proteger todos los sistemas contra malware y actualizar los programas o software antivirus regularmente
	6. Desarrollar y mantener sistemas y aplicaciones seguros
Implementar medidas sólidas de control de acceso	7. Restringir el acceso a los datos del titular de la tarjeta según la necesidad de saber que tenga la empresa.
	8. Identificar y autenticar 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 del titular de la tarjeta
	11. Probar periódicamente los sistemas y procesos de seguridad
Mantener una política de seguridad de información	12. Mantener una política que aborde la seguridad de la información para todo el personal

Fuente: PCI. *Asegurar juntos el futuro de los pagos*. https://es.pcisecuritystandards.org. Consulta: 4 de abril de 2019.

3. CATEGORIZACIÓN DE LAS AMENAZAS CIBERNÉTICAS

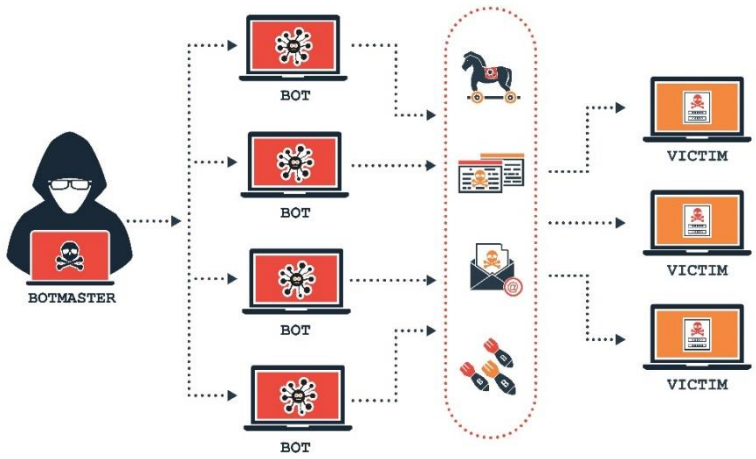
En la actualidad, la información es uno de los activos de mayor importancia en cualquier institución, sea esta de microfinanzas o de otra índole. Este valor la hace muy codiciada y siempre existe alguien que la quiera obtener a través de métodos no éticos.

Se describen los métodos que en la actualidad son utilizados por los ladrones de información y los cuales son efectivos en las instituciones que no le prestan la suficiente atención a la seguridad de la información.

3.1. Denegación distribuida de servicios

Este tipo de ataque DoS (por sus siglas en inglés, Denial of Service) aprovecha las capacidades específicas que disponen los equipos en una red, debido a la cantidad de peticiones realizadas a la infraestructura. La intención es provocar pérdida de servicio al sobrecargar la capacidad de un sitio web, un equipo de cómputo, un equipo de red, para administrar solicitudes y evitar que este funcione correctamente y genere pérdida de servicio.

Figura 14. **Ataque de denegación de servicio**



Fuente: Oficina de Seguridad del Internauta. *¿Qué son los ataques DoS y DDoS?.* https://www.osi.es/es/actualidad/blog/2018/08/21/que-son-los-ataques-dos-y-ddos. Consulta: 4 de abril de 2019.

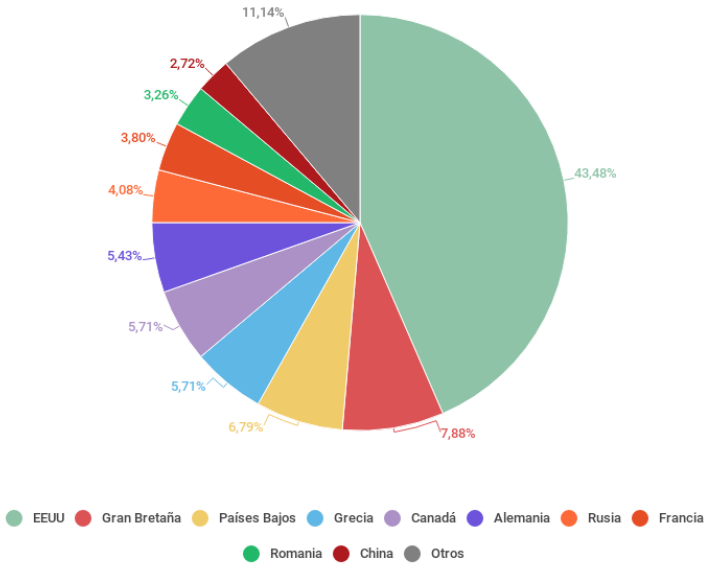
Estos ataques pueden originarse en una institución de microfinanzas por el uso de un troyano, una aplicación maliciosa, correo o una USB infectada. Comúnmente los objetivos son tiendas en línea, instituciones gubernamentales e instituciones financieras que prestan servicios en línea o tienen información financiera de muchas personas.

En el año 2000, este tipo de ataque era común y los equipos de tecnología tenían que lidiar de forma continua debido a la efectividad. Actualmente, este tipo de ataque se han reducido; el tipo de algoritmos que se utilizan en *firewall* y antivirus son la primera línea para repeler ataques de este tipo.

3.1.1. Estadísticas de ataques

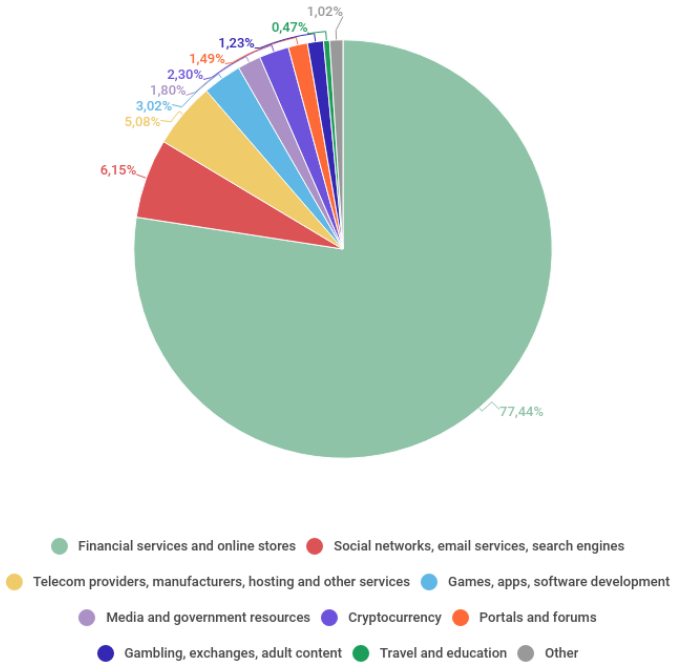
Según estadísticas de Karpesky, en el 4 trimestre del 2018, EEUU es el país con 43,48 % en hospedar servidores de comandos botnets. El sistema operativo Linux es de donde se lanzan más botnets 97,11 % sobre un 2,98 % que corresponde al sistema operativo Windows. La figura 10 muestra el top 10 de países que lanzan botnet.

Figura 15. **Top 10 países que generan botnet - 4Q 2018**



Fuente: Kaspersky Lab. *Ataques DDoS en el cuarto trimestre de 2018.* https://securelist.lat/ddos-attacks-in-q4-2018/88346. Consulta: 4 de abril de 2019.

Figura 16. **Distribución de ataques – 4Q 2018**



Fuente: Kaspersky Lab. *Ataques DDoS en el cuarto trimestre de 2018.* https://securelist.lat/ddos-attacks-in-q4-2018/88346. Consulta: 4 de abril de 2019.

3.2. Ransomwere

"Este tipo de ataque está diseñado para restringir el acceso a la información de un equipo de cómputo a su propietario y exige un pago por la liberación. Si se realiza el pago por recuperar la información no hay garantías que las claves de desencriptación funcionen".[26]

[26] Avast. *¿Cómo se previene el ransomware?* https://www.avast.com/es-es/c-ransomware. Consulta: 26 de marzo de 2019.

“Tiene la capacidad de cifrar todos los archivos del sistema a través de una clave que es proporcionada luego de realizar un pago que es de unos $350 por equipo y el plazo de pago es aproximadamente de 96 horas”.[27]

“Los ataques más sobresalientes son: WannaCry, Petya, Cerber, Cryptolocker y Locky”.[28]

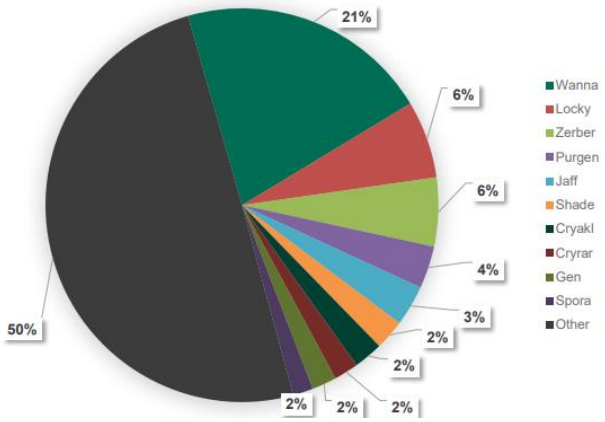
“El número total de usuarios que se encontraron con ramsomware se redujo en casi un 30 %: de 2.581.026 en 2016-2017 a 1.811.937 en 2017-2018”.[29]

3.2.1. Estadísticas de ataques

En la figura 17 podemos observar los diferentes tipos de ataques ramsowere que se tienen identificados por la empresa de Kaspersky, donde WannaCry es el más común.

[27] Karspesky. *¿Qué es el ransomware?* https://latam.kaspersky.com/resource-center/definitions/what-is-ransomware. Consulta: 22 de marzo de 2019.
[28] Oficina de Seguridad Internauta. *¿Qué son los ataques DoS y DDoS?* https://www.osi.es/es/actualidad/blog/2018/08/21/que-son-los-ataques-dos-y-ddos. Consulta: 23 de marzo de 2019.
[29] BBC. *Noticias Ransomwer*. https://www.bbc.com/mundo/noticias-36905385. Consulta: 26 de marzo de 2019.

Figura 17. **Distribución por tipo de ataque – 2017-2018**



Fuente: Kaspersky Lab. *Informe KSN: Ransomware y criptomineros maliciosos 2016-2018*. https://media.kasperskycontenthub.com/wp-content/uploads/sites/58/2018/06/27125925/KSN-report_Ransomware-and-malicious-cryptominers_2016-2018_ENG.pdf. Consulta: 4 de abril de 2019.

3.3. Spam

El spam tradicionalmente es un correo masivo no deseado que, haciéndose pasar por grandes empresas, ofrece publicidad sobre productos o servicios. En informática es conocido como correo basura; en la actualidad ya no es una amenaza dirigida únicamente a correo electrónico; se puede encontrar en blogs, mensajería instantánea, sitios de redes sociales, entre otros.[30]

En el 2018, el tráfico de correo que se generó por spam fue del 52,48 % con una disminución de 4,15 % en relación al año 2017. El país que generó una mayor cantidad de spam fue China con un 11,68 %. Se estima que del total de usuarios afectados por spam es el 18,32 %.[31]

[30] Kaspersky. *Informe KSN: Ransomware y criptomineros maliciosos 2016-2018*. https://securelist.lat/ransomware-and-malicious-crypto-miners-in-2016-2018/87155. Consulta: 26 de marzo de 2019.

[31] Avast. *Qué es el spam: la guía esencial para detectar y prevenir el spam*. https://www.avast.com/c-spam. Consulta: 26 de marzo de 2019.

Para eludir las soluciones de antispam y convencer a los usuarios de que los archivos adjuntos no representan ningún riesgo, están en formatos ISO, IQY, PIF y PUB. Simulan correos de instituciones de crédito y beneficencia y ofrecen ofertas lucrativas, sorteos, ayuda para niños. Su objetivo son datos personales o transferencia de dinero.

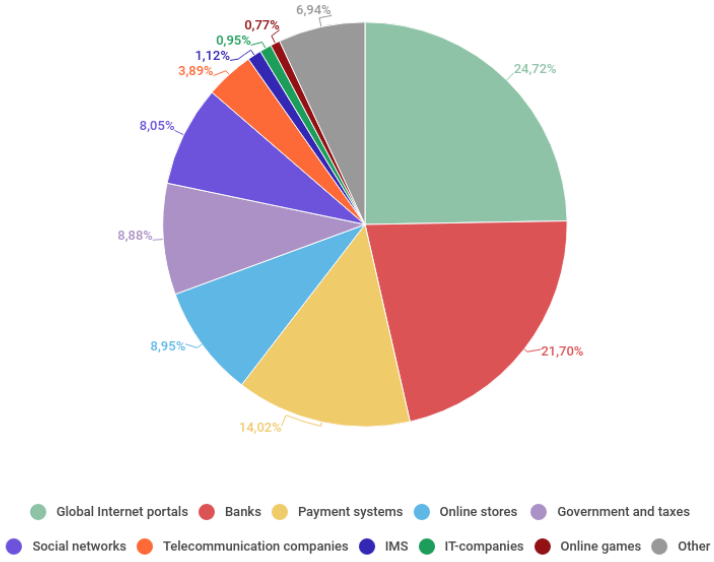
3.4. Phishing

> Es una estrategia que los delincuentes cibernéticos utilizan para engañan y conseguir que los usuarios revelen información sensible, como contraseñas, datos de tarjetas de crédito, números de cuentas bancarias. Es un ataque a través de spam, que da razón de urgencia o sorpresa y dirige a la víctima a un sitio web falso con características idénticas a las del sitio web oficial de un banco, agencia gubernamental, universidades u organización legitima.[32]

En los últimos años, los sitios de phishing con dominios certificados SSL han aumentado. Para los cibercriminales no es difícil obtener estos certificados. Esto provocó que Chrome, a partir de la versión de septiembre 2018, identificara a las páginas web como seguras y no seguras. En las páginas identificadas como seguras aparece un candado y son marcadas con verde, lo que proporciona mayor información del dueño del portal.

[32] Avast. *Guía esencial del phishing: cómo funciona y cómo defenderse*. https://www.avast.com/es-es/c-phishing. Consulta: 26 de marzo de 2019.

Figura 18. **Portales suplantados por phishing 2018**



Fuente: Kaspersky Lab. *Informe KSN: Ransomware y criptomineros maliciosos 2016-2018.* https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2019/03/11150819/en-attacked-organizations.png. Consulta: 4 de abril de 2019.

3.5. Inyección SQL

Este ataque aprovecha vulnerabilidades de programación que contiene un sitio web, con el objetivo de manipular la base de datos y obtener información sensible potencialmente valiosa. Se considera un ataque común y altamente efectivo debido a que se puede aplicar a cualquier sitio web que utilice una conexión a base de datos SQL.

Consiste en inyectar código adicional en cualquier consulta SQL que se realiza en un sitio web, comenzando con el inicio de sesión a través de un formulario, lo que permitirá el acceso a un sistema. El inconveniente se debe a

que muchos formularios no disponen reglas para ingreso de información adicional, que permite enviar solicitudes a la base de datos para obtener información confidencial.

4. SITUACIÓN ACTUAL DE LA CIBERSEGUIRDAD EN GUATEMALA

4.1. Delitos cibernéticos en Guatemala

> "Guatemala en el marco regulatorio no dispone de una ley que tipifique los delitos cibernéticos. Debido a esta ausencia jurídica no existe una institución gubernamental especializada, con equipo enfocado en coordinar a nivel nacional el seguimiento a incidentes de seguridad informática".[33]

> Se tiene una iniciativa de ley en el congreso de la república, 'Iniciativa de Ley de cibercrimen 4055'. Esta ley fue de conocimiento en pleno de diputados el 18 de agosto del 2009 y tiene como objetivo proteger y sancionar todos los delitos que tengan naturaleza informática y sean cometidos en el territorio de Guatemala. Sin embargo, no ha sido aprobada por el pleno.[34]

La iniciativa de ley 4055 busca establecer un marco jurídico que permita aplicar sanciones a los responsables de ilícitos como fraude informático, pornografía infantil, espionaje, falsificación informática, sistemas falsos o fraudulentos, daño informático, entre otros, con el fin de prevenir sancionar cualquier acción que limite el comercio electrónico y la confidencialidad de la información a las instituciones del país.

---

[33] The OWASP Foundation. *Inyección de código.* https://www.owasp.org/index.php/Inyecci%C3%B3n_SQL. Consulta: 26 de marzo de 2019.

[34] Mingob. *Estrategia de seguridad cibernética.* http://uip.mingob.gob.gt/wp-content/uploads/2019/03/E strategia-Nacional-de-Seguridad-Cibern%C3%A9tica.pdf. Consulta: 26 de marzo de 2019.

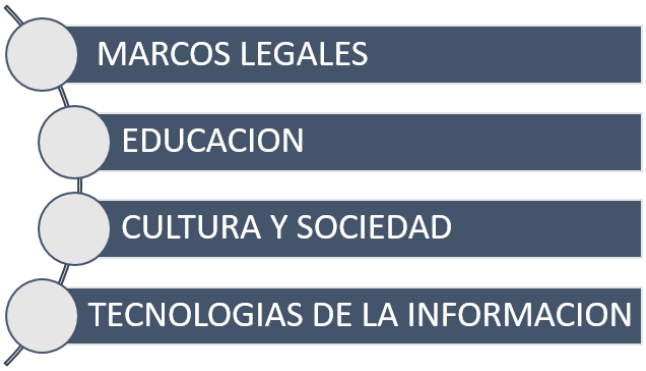
4.2. Estrategia nacional de seguridad cibernética

En junio del 2018, el gabinete ejecutivo del gobierno de Guatemala presenta un plan para la Estrategia Nacional de Seguridad Informática, con el objetivo de crear las capacidades necesarias en el país para salvaguardar la seguridad e integridad de las personas, entidades privadas y gubernamentales, en ejercicio de sus derechos en el ámbito de seguridad informática.

Con esta iniciativa, Guatemala se une a Colombia, Chile, Costa Rica, Jamaica, México, Panamá, Trinidad y Tobago y Paraguay, países que buscan implementar medidas de ciberseguridad.

La estrategia de gobierno consiste de 4 ejes estratégicos que se muestran en la figura 19, con 10 objetivos y 37 acciones, las cuales deben ser asumidas e implementadas por los actores y sectores involucrados directa o indirectamente:

Figura 19. **Principales ejes de la Estrategia Nacional de Seguridad Informática**



Fuente: Mingob. *Estrategia Nacional de Seguridad Informática*. http://uip.mingob.gob.gt/wp-content/uploads/2019/03/Estrategia-Nacional-de-Seguridad-Cibern%C3%A9tica.pdf. Consulta: 4 de abril de 2019.

4.2.1. Marcos legales

En ausencia a un marco jurídico establecido en el país, se busca desarrollar las bases que permitan determinar un alcance sobre el cual se construya un marco legal acerca de la seguridad cibernética, que ayude a fortalecer los procesos investigativos y la admisibilidad de evidencia electrónica en casos de crímenes cibernéticos.

Los objetivos principales que busca la iniciativa son los siguientes:

- Adecuar el marco legal guatemalteco con un enfoque de prevención y manejo de riesgos cibernéticos para fortalecer la seguridad cibernética.

- Promover la investigación criminal para mantener niveles aceptables de seguridad cibernética.

- Determinar una estrategia de divulgación que promueva la transparencia de la información.

4.2.2. Educación

Fortalecer las capacidades en educación para formar profesionales en materia de seguridad informática que dispongan de una formación y contenidos curriculares, acorde a las tendencias regionales y poder cubrir la demanda técnica de expertos en el país. Para cumplir se han fijado los siguientes objetivos.

- Crear la oferta educativa y formativa en seguridad de la información que permita desarrollar especialistas para cubrir la demanda técnica y profesional en el país.

- Promover e implementar programas de educación y habilidades sobre investigación/desarrollo de la seguridad de la información

4.2.3. Cultura y sociedad

Implementar una cultura de seguridad de la información a nivel nacional no es posible sin la inclusión de todos los sectores de la sociedad, por lo cual es necesario fortalecer las mejores prácticas de seguridad de la información en la empresa privada y gubernamental con enfoque en gestión del riesgo.

Diseñar programas de concientización en los distintos sectores de la sociedad para establecer convenios público-privados que permitan generar campañas que promuevan el uso de producto y servicios en línea bajo un entorno seguro que promuevan el comercio electrónico.

4.2.4. Tecnología de la información

Plantea la sistematización de la continuidad de servicios digitales en los distintos sectores del país y planes para la protección de infraestructuras críticas. Disponer de un centro de respuesta ante incidentes de seguridad a infraestructuras críticas (CSIRT-GT-IC), con el fin de coordinar la relación empresa y gobierno en caso de cualquier tipo de ataque.

Los objetivos principales de esta estrategia son los siguientes:

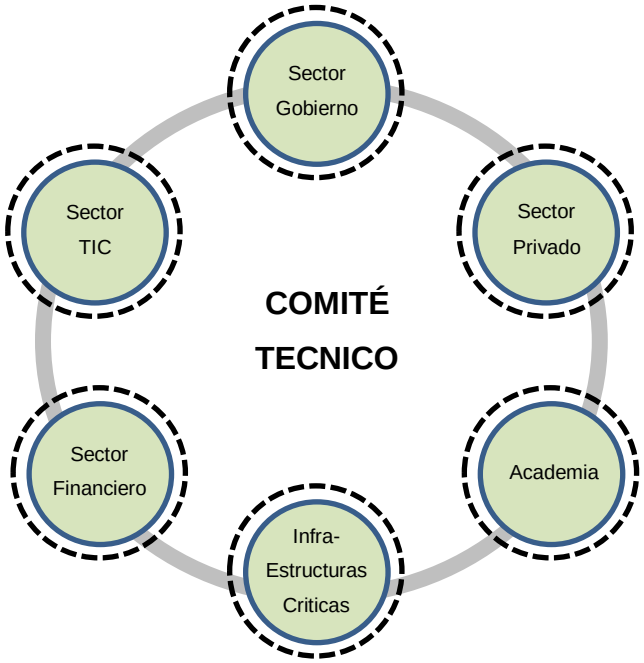
- La protección de los sistemas de información en los sectores público y privado, que permita disponer de la continuidad de los servicios.

- Establecer metodologías para coordinación en la seguridad cibernética nacional.
- Tener un plan de protección nacional de infraestructuras críticas para fortalecer las reacciones de recuperación en caso de ataques.

4.2.5. Comité técnico de seguridad cibernética

Un comité con la participación de entidades gubernamentales, sector privado, sociedad civil y academia, que funcione como asesor y se encargue de la coordinación y adaptación de las políticas interinstitucionales e intersectoriales, reforzando los vínculos de los distintos planes estratégicos con visión compartida.

Figura 20. **Comité técnico de seguridad nacional**



Fuente: Mingob. *Comité Técnico de Seguridad Nacional*. http://uip.mingob.gob.gt/wp-content/uploads/2019/03/Estrategia-Nacional-de-Seguridad-Cibern%C3%A9tica.pdf. Consulta: 3 de mayo de 2019.

4.3. Ley de lavado de dinero y otros activos

Derivado a los cambios en las tecnologías, las nuevas estrategias para delinquir y financiar ilícitamente, actividades y movimientos que generan diversidad de violencia e inseguridad, los grupos organizados financian cibercriminales expertos para robar grandes sumas de dinero, como fue en el Banco de Bagladesh, en donde robaron 81 millones de dólares.

"Cualquier acto o intento de acto dirigido a ocultar o disfrazar la identidad de recaudaciones obtenidas ilegalmente de manera que parezcan haber sido originadas de fuentes legítimas".[35]

> Guatemala ha logrado avances en la línea de establecer un marco jurídico que le permita cumplir con requerimientos a nivel internacional establecidos por el Grupo de Acción Financiera Internacional (GAFI), entidad mundial encargada de establecer estándares y promover la implementación efectiva de medidas legales, regulatorias y operativas para prevenir y combatir el lavado de activos[36].

La ley contra el lavado de dinero y otros activos en Guatemala es gestionada por la Super intendencia de Bancos (SIB). Para eso tiene el decreto de ley 67-2011 "Ley contra el lavado de dinero y otros activos" aprobado por el congreso de la república.[37]

> El decreto 67-2011 tiene por objeto prevenir, controlar, vigilar y sancionar el lavado de dinero u otros activos procedentes de la comisión de cualquier delito, y establece las normas que para este efecto deberán observar las personas obligadas. Esta ley

[35] El Periódico. *Robo al banco de Bangladesh*. https://www.elperiodico.com/es/sociedad/20161230/el-mayor-ciberatraco-del-mundo-tuvo-topos-en-el-banco-5696007. Consulta: 4 de abril de 2019.
[36] Dolitte. *La importancia de los reportes de Transacciones sospechosas*. http://www.ebg.edu.gt/oldSite/wp-content/files_mf/1468950515Patriciachacon.pdf. Consulta: 4 de abril de 2019.
[37] Oro y finanzas. *Grupo de acción financiera internacional*. https://www.oroyfinanzas.com/2015/05/que-es-grupo-accion-financiera-internacional-gafi-financial-action-task-force-fatf/. Consulta: 12 de abril de 2019.

obliga a cualquier institución financiera reportar cualquier transacción superior a los 10 mil dólares a la Intendencia de verificación especial (IVE).[38]

4.3.1. Cumplimiento de estándares Internacionales

Guatemala, como otros 180 países, ha avalado las 40 recomendaciones realizadas por el grupo GAFI, que se han convertido en un estándar internacional contra el lavado de dinero y otros activos. Los países que no cumplen con estas recomendaciones son calificados como paraísos fiscales.

Figura 21. **Historia de cumplimiento de estándar internacional por Guatemala**

Fuente: elaboración propia.

4.3.2. Intendencia de verificación especial

Es un órgano gubernamental de naturaleza administrativa, que se encargada de velar por el cumplimiento de las leyes contra el lavado de dinero y

[38] Banguat. *Ley contra el lavado de dinero y otros activos*. http://www.banguat.gob.gt/leyes/2002/lavado.pdf. Consulta: 12 de abril de 2019.

prevenir y reprimir el financiamiento del terrorismo en Guatemala. Realiza funciones de una unidad de inteligencia financiera en cumplimiento con los estándares y tratados internacionales.

Entre sus funciones tiene la tarea de analizar todas las transacciones bancarias sospechosas, transacciones inusuales con patrones de lavado de dinero. En caso de indicios de delito de lavado de dinero presenta las denuncias a las autoridades correspondientes y provee los medios probatorios.

Todas las instituciones financieras del país están obligadas a reportar cualquier transacción inusual o sospechosa de sus clientes a la IVE para que esta institución analice el origen del dinero, con lo cual se evita la procedencia de dinero de actividades ilícitas.

4.3.2.1. Transacciones inusuales

"Son aquellas transacciones cuya cuantía, frecuencia, monto o características no guardan relación con el cliente de una institución financiera".[39]

4.3.2.1.1. Transacciones sospechosas

"Son aquellas transacciones inusuales debidamente examinadas y documentadas por la persona obligada que, de no tener un fundamento económico o legal evidente, podría constituir un ilícito penal".[40]

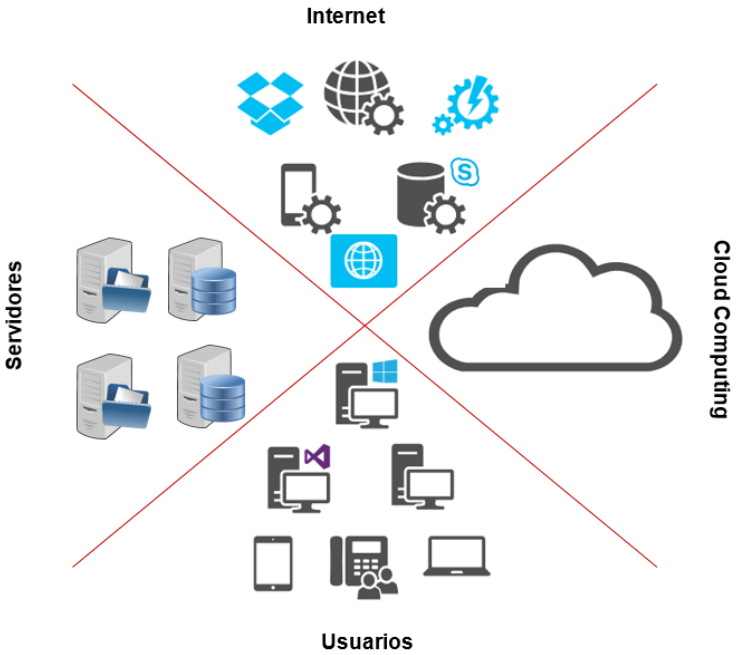
[39] Google Chrome. *¿Cómo administrar las advertencias sobre sitios no seguros?* https://support.google.com/chrome/answer/99020?co=GENIE.Platform%3DDesktop&hl=es-419. Consulta: 26 de marzo de 2019.
[40] Ibíd.

5. MODELO PARA LA GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

5.1. Modelo actual de entidades de microfinanzas

En la actualidad, las instituciones de microfinanzas utiliza un modelo que contempla cuatro áreas de impacto, usuarios, servidores, internet; algunas comienzan a agregar a su infraestructura el cloud computing. Esta infraestructura se ve limitada a medida que las instituciones crecen e incrementan el riesgo de la exposición de la información.

Figura 22. **Modelo de segmentación actual**

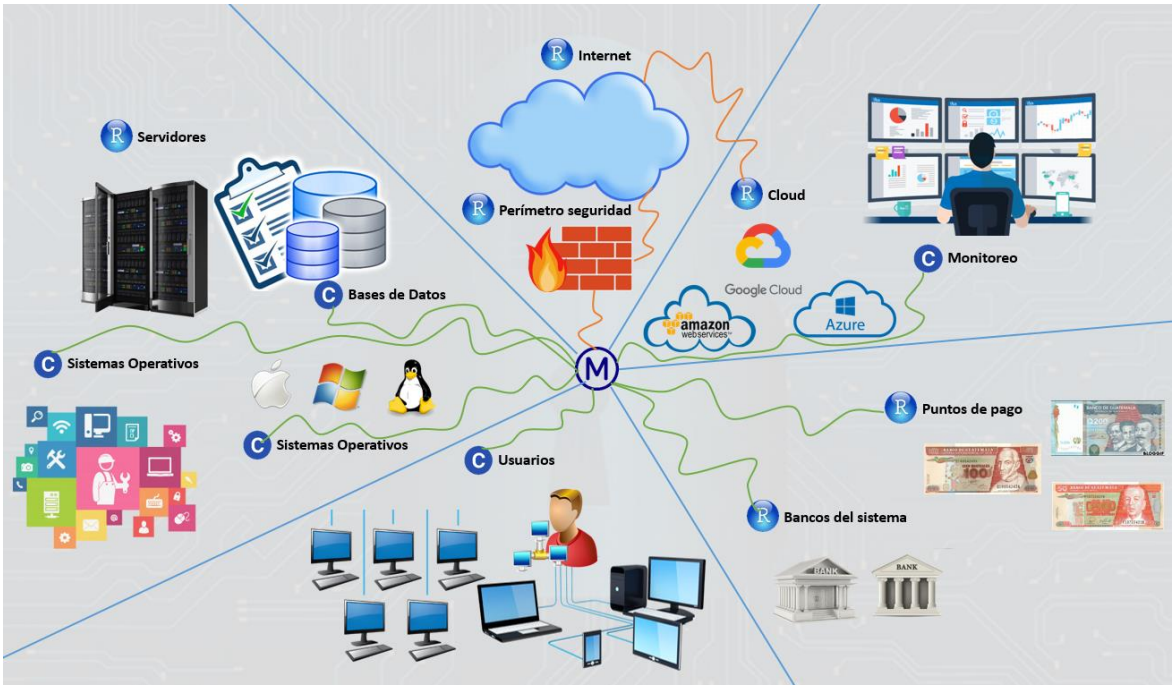


Fuente: elaboración propia.

5.2. Modelo propuesto para entidades de microfinanzas

El modelo que se propone está diseñado en base a capas, enfocadas en cubrir las áreas críticas que manejan la información sensible de una institución de microfinanzas. Adicionalmente, soportar el crecimiento del negocio y la infraestructura física que se necesite. En la figura 23 se pude ver de forma gráfica el alcance general.

Figura 23. **Segmentación del modelo según arquitectura**



Fuente: elaboración propia.

El modelo se diseña para integrar cada una las áreas de una institución en una sola infraestructura con diferentes segmentos, con base en los servicios que se prestan a personas, procesos y aplicaciones con el fin de proteger la

información en sus tres fundamentos esenciales, según ISO 27000 (integridad, confiabilidad, disponibilidad).

> Dentro de las instituciones de microfinanzas se brinda diversos servicios financieros a sus clientes, que son soportados a través de la tecnología. Las inversiones en tecnología cada día crecen en la compra de nuevos equipos de cómputo, servidores, firewall, dispositivos red, entre otros. Sin embargo, las inversiones en seguridad de la información se mantienen.[41]

Las inversiones en seguridad de la información comúnmente son percibidas como un gasto que afecta la rentabilidad institucional, razón por la cual, no se le presta la importancia que esta actividad requiere. La prioridad en el gasto es baja.

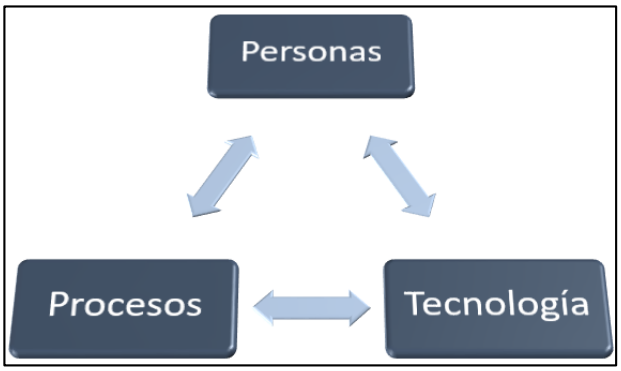
5.3. Definición de modelo en capas

El objetivo principal del modelo es asegurar la protección de la información mediante un encapsulamiento llamado capas. A través de la implementación de varios controles que tienen un alcance de personas, procesos y aplicaciones (ver figura 24), brindando protección a los datos contra robo, alteración y fuga de información.

El modelo de seguridad que se propone está basado principalmente en herramientas tecnológicas que se complementa con fundamentos de gobernanza.

[41] Super Intendencia de Bancos, SIB. *Intendencia de Verificación Especial, IVE*. https://www.sib.gob.gt/web/sib/lavado_activos/funciones-IVE. Consulta: 4 de abril de 2019.

Figura 24. **Alcance del modelo**



Fuente: elaboración propia.

El modelo se compone de 6 capas que protegen la información a través de controles específicos que se encargan de mitigar posibles vulnerabilidades en la seguridad de la información (ver figura 25). En el apéndice A se muestra una tabla con el total de las capas y los controles.

Las capas están diseñadas con base en el conocimiento de estándares ISO 27001, COBIT y PCI DSS y son soportadas sobre una base/soporte compuesta de controles específicos de gobernanza COBIT y ISO 27001.

Figura 25. **Modelo de capas**

Fuente: elaboración propia.

A continuación, se define cada una de las capas propuestas en el modelo, con el respectivo detalle de controles que las conforman.

5.4. Capa de datos

"Los datos son un activo muy valioso, que no debe ser expuesto a accesos no autorizados. Se recomienda clasificar en críticos y no críticos".[42]

De esta segmentación dependerán las medidas de seguridad que se deben implementar para asegurar su protección ante cualquier amenaza interna o externa que pueda provocar pérdida, alteración o divulgación no autorizada.

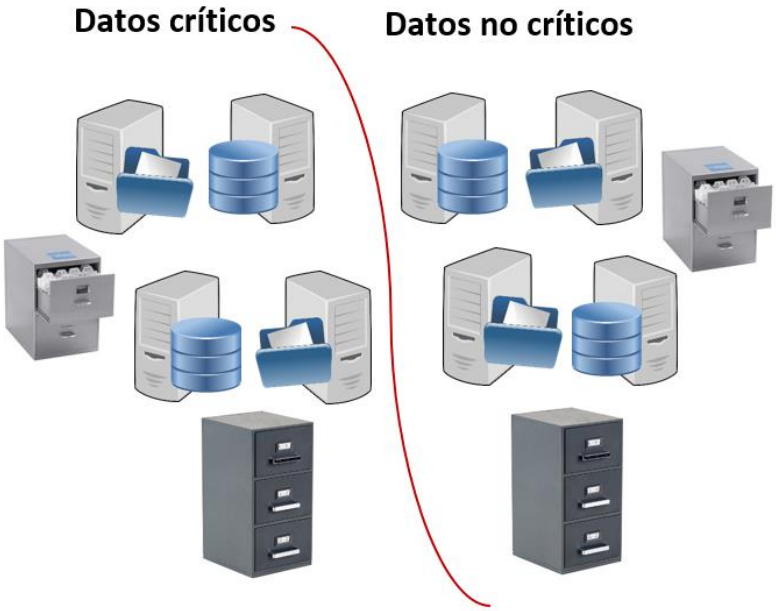
- Datos críticos: cualquier dato que ponga en riesgo la continuidad de las operaciones de forma diaria o permanente, que afecte la reputación de la

[42] El Periódico. *Inversión en tecnología*. https://elperiodico.com.gt/inversion/2017/10/19/region-debe-invertir-en-tecnologia-e-innovacion. Consulta: 4 de abril de 2019.

institución o ponga en riesgo la integridad de clientes, proveedores y colaboradores debe de considerarse crítico.

- Datos no críticos: son datos a disposición del público en general. Pueden encontrarse disponibles en distintos medios como redes sociales, páginas web, periódicos, revistas, televisión, radio, entre otros. Su publicación no afecta negativamente a la institución o a sus clientes.

Figura 26. **Clasificación de los datos por criticidad**



Fuente: elaboración propia.

Las instituciones de microfinanzas manejan bases de datos que contienen información financiera de clientes activos, cancelados y rechazados, a los que les han prestado un servicio financiero en el transcurso del tiempo. También almacenan información de sus colaboradores activos, de baja y solicitudes de empleo.

La información que las entidades de microfinanzas generan y almacenan se hace en base a los servicios que prestan a los clientes (ver apéndice B). Estos servicios son la razón porque los datos deben estar disponibles en todo momento; caso contrario, la institución tendrá problemas para realizas sus operaciones.

Es importante que la información esté disponible siempre que sea requerida por una persona, proceso o aplicación. Sin embargo, debe disponer de medidas de seguridad para permitir el acceso únicamente a aquellos que tienen autorización; de lo contrario, debe de negar los accesos.

5.4.1. Riesgos relacionados a los datos

El objetivo de implementar los controles que se describen en la capa de datos es asegurar un perímetro de protección a los datos críticos de la institución de microfinanzas, con la finalidad de mitigar los riesgos siguientes:

- Fuga de información: es la extracción de información no autorizada de una persona, proceso o aplicación ajena o de parte de la institución que no debería tener acceso a esa información.

- Robo de información: extracción de información sensible con el fin de comercializar o realizar un fraude que afecta a la institución, a sus clientes, proveedores o colaboradores.

- Alteración de los datos: con la finalidad de afectar positiva o negativamente a clientes, proveedores o colaboradores se puede alterar la información, causando pérdidas económicas a la institución.

- Caída de servicios críticos: la falta de disponibilidad de los datos puede provocar que la institución deje de brindar servicios a sus clientes, provocando inconformidad y mala reputación.

- Pérdida de información: los dispositivos que almacenan información crítica o sensible como laptops, máquinas de escritorio, memorias USB, discos duros, servidores, tienen que estar encriptados para asegurar que la información que alojan no sea accedida en caso de extravío o robo.

- Fraudes: los fraudes pueden ser provocados por lavado de dinero, por servicios financieros a clientes que no existen, cobros indebidos a clientes, lo que afecta a la institución en pérdidas económicas.

Para mitigar los riesgos identificados en la capa de aplicaciones se proponen implementar los siguientes controles:

5.4.2. Cifrado de datos

> Este control aborda el tema de la sensibilidad de la información que es almacenada en distintos medios, con la finalidad de lograr que los datos críticos de la institución sean ilegibles e imposibles de acceder. Se utiliza mecanismos de ofuscación que permitan el acceso solo a personal autorizado mediante el uso de claves o contraseña.[43]

El cifrado completo de los dispositivos de almacenamiento ayuda a proteger los datos en caso de pérdida o robos. Se sugiere que estén encriptados: laptops, máquinas de escritorio, servidores, USB, discos duros externos y teléfonos inteligentes.

[43] ISO Tools. *¿Cómo clasificar la información según ISO 207001*? https://elperiodico.com.gt/inversion/2017/10/19/region-debe-invertir-en-tecnologia-e-innovacion. Consulta: 4 de abril de 2019.

La información institucional de clientes, proveedores y colaboradores que se almacena de manera temporal en el disco duro o en memoria portátil de cualquier dispositivo debe estar encriptada con base en los algoritmos aleatorios. Debe existir una política para el manejo, control y gestión de claves criptográficas.

Estos dispositivos podrán ser accedidos a través del uso de contraseñas al inicio de la sesión del sistema. La logística dependerá de las características de la solución de encriptación que se utilice. Es importante que el método elegido no permita utilizar lo siguiente:

- Autentificación con base en las cuentas de usuario del sistema operativo.

- Las contraseñas no deben estar asociadas a una base de datos de cuentas de usuario locales.

- Las credenciales que permiten el inicio de sesión no deben estar dentro de la red.

> "Entre las tendencias tecnológicas actuales para el cifrado de datos se puede mencionar varios productos líderes en el mercado, por ejemplo Microsoft BitLocker, Sophos SafeGuard, Symantec Endpoind Encription y Trend Micro Endpoind Encription".[44]

[44] Binance Academy. *Encriptación Simétrica vs. Asimétrica*. https://www.binance.vision/es/security/symmetric-vs-asymmetric-encryption. Consulta: 4 de abril de 2020

5.4.3. Hardening a bases de datos

Las bases de datos representan uno de los puntos centrales de acumulación de datos y uno de los focos para los ladrones de información, por lo tanto, deben estar encriptadas a nivel de archivo e internamente a nivel de columnas.

Las bases de datos comúnmente ofrecen dos técnicas para encriptar los datos: encriptación a nivel de las columnas para los datos que requieren mayor seguridad y cifrado en tiempo real (archivos y copias de respaldo) mediante certificado y claves maestras.

La encriptación de columnas específicas dentro de las tablas de la base de datos permite proteger de accesos a personal no autorizado a la información sensible, particularmente al que tiene acceso a tareas de administración de bases de datos.

La encriptación en tiempo real permite que el contenido completo de la base de datos permanezca encriptado en cualquier medio de almacenamiento y en las copias de seguridad. Mantiene la información de forma nativa y transparente para cualquier persona, proceso o aplicación.

“Se recomienda revisar cada una de las configuraciones, de las bases de datos de acuerdo a la guía PCI-DSS, con lo que se mitigaran vulnerabilidades relacionadas a configuración”.[45]

[45] Gartner. *Protección para dispositivos móviles*. https://www.tecnozero.com/wp-content/uploads/2018/01/gartner-guia-2017.pdf. Consulta: 4 de abril de 2019.

5.4.4. Sistema de clasificación y etiquetado de información

La norma 27001 no define un estándar específico para los niveles de clasificación de la información. Se recomienda que una institución de microfinanzas establezca los niveles de clasificación siguientes:

- Información altamente confidencial: información muy importante para una institución de microfinanzas. Solo puede ser accedida por posiciones clave: Junta directiva, Gerencias, jefes de área, debido a que el mal uso puede afectar negativamente a la institución.

- Información confidencial: información que debe de ser socializada y utilizada por un reducido número de personas, para quienes es vital para realizar sus actividades laborales. Su divulgación o uso no autorizados podría provocar pérdidas significativas para la institución de microfinanzas.

- Información restringida: información que debe de ser visible para un número limitado y específico de personas, los que hacen uso del conocimiento de esta información para el cumplimiento de sus tareas diarias.

- Información interna: información puede ser socializada y utilizada por todos los colaboradores de la institución de microfinanzas y algunas instituciones externas, con la debida autorización. El uso no autorizado de este tipo de información causaría riesgos o pérdidas moderadas.

- Información pública: Información que puede ser accedida y utilizada sin autorización por cualquier persona (se encuentra disponible en cualquier

medio de comunicación), sea colaborador de la institución de microfinanzas o no.

El etiquetado de la información debe de realizarse de acuerdo al tipo y clasificación de información. Se recomienda utilizar la siguiente segmentación:

- Documentos en papel: en los documentos en papel que contienen información que no es de acceso público, se debe indicar el nivel de clasificación en la portada y cada una de las páginas que lo componen.

- Documentos electrónicos: los documentos digitales que contienen información que no es de acceso público, deben indicar el nivel de clasificación en cada una de las páginas.

- Correo electrónico: se debe indicar en la primera línea del cuerpo del correo electrónico, el nivel de clasificación de la información que contiene.

- Almacenamiento electrónico: el nivel de clasificación se debe de especificar en la superficie de cada unidad de almacenamiento.

- Información transmitida oralmente: cuando se transmite información confidencial mediante teléfono, notas de voz o algún otro medio de comunicación que utilice voz, se especifica el nivel de clasificación que se transmite.

"Existe una variedad de herramientas tecnológicas que pueden ayudar a automatizar la clasificación de la información, entre las que se encuentran Titus, Veritas Technologies y Data Dynamics".[46]

5.4.5. Sistema de prevención de fuga de información (DLP)

En las instituciones de microfinanzas es común observar casos de deslealtad de los empleados, que intentan extraer información sensible para compartir con otras instituciones por remuneración económica o posiciones laborales. La fuga de datos, por lo regular, se da a través de envío de correos, extracción electrónica de datos o documentos impresos con datos sensibles.

Con la finalidad de mitigar el riesgo que se produzca extracción no autorizada de la información se proponen las siguientes acciones:

- Clasificación de información: se necesita disponer de una política que permita clasificar la información acorde a las necesidades y realidad actual de cada institución de microfinanzas.

- Roles y responsabilidades: a través de roles y responsabilidades se debe determinar el principio de accesos mínimos que el personal debe tener para la visualizar y manipular la información dentro de la institución de acuerdo a sus funciones.

- Concientizar al personal: realizar campañas y evaluaciones que permitan la concientización de todo el personal de la entidad de microfinanzas de forma periódica.

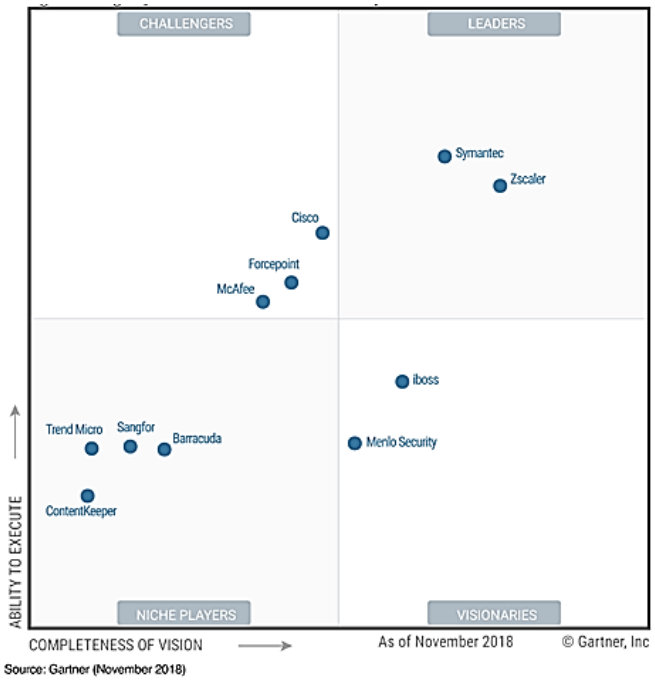
[46] PCIDSS. *Hardening Guia V3.2*. https://www.pcihispano.com/?descargas=40465. Consulta: 4 de abril de 2019.

- **I**mplementar controles: implementar software DLP para el monitoreo de datos en movimiento, en uso y en reposo dentro de la infraestructura de red.

- Evaluar controles: es vital evaluar los controles al menos una vez al año por un grupo de auditores o consultores externos al departamento de tecnología de la institución de microfinanzas.

Las tecnologías Symantec y Zcaler, según informe de Gartner a noviembre 2018, se pueden utilizar para automatizar la protección contra la fuga de información.

Figura 27. **Sistemas de prevención de fuga de información**



Fuente: Zcaler. *Productos > prevención de pérdida de datos*. https://www.zscaler.com/products/data-loss-prevention. Consulta: 11 de junio de 2019.

5.4.6. Monitoreo de actividad bases de datos

Conocer lo que sucede dentro de la base de datos a través de recolectar y analizar todos los sucesos, permite mantener el control y desempeño, prevenir fallas en el rendimiento, pérdida de información y problemas de continuidad que pueden causar pérdidas económicas a cualquier institución.

El monitoreo es una actividad que se realiza a la base de datos para responder de forma proactiva a incidentes que pueden ocurrir, como incremento en tamaño, daños en archivos de la base de datos, detección de accesos no autorizados y uso indebido de la información por administradores.

Los administradores de las bases de datos representan un riego latente a la seguridad de la información. Ellos tienen acceso total a las funcionalidades para extracción y modificación. De no disponer de monitoreo a los cambios que realizan se corre el riesgo de fuga de información.

El monitoreo de los log es una actividad que permite evaluar el volumen de transacciones, que están ocurriendo dentro de la base de datos e identificar quien está realizando transacciones, así como la información que se consulta, los cambios que se producen y los horarios de las actividades. Esta información es valiosa para tomar decisiones de desempeño, privilegios sobre la información, accesos entre otros.

Las bases de datos cuentan con generación de log de forma automática de las transacciones que se generan de forma interna, llamadas pistas de auditoría. Por lo general, esta funcionalidad está desactivada por defecto; es importante asegurar que estén activas y se disponga del espacio necesario para almacenar un periodo de tiempo considerable los log que se desea generar.

Las herramientas tecnológicas Imperva data base firewall y Mcafee database activity son especializadas para el monitoreo de log de bases de datos que pueden ayudar a los departamentos de tecnología o seguridad de la información a automatizar este procedimiento.

5.4.7. Identificación y gestión de accesos de usuarios

Asegurar el principio de menor privilegio [50] al acceso de la información es la meta primordial de toda institución. Debido a esta premisa se debe definir roles específicos para grupos de usuarios, con la finalidad de permitir el acceso de acuerdo a las funciones y posición que desempeñe en la institución de microfinanzas.

Se debe disponer de una política de accesos (matriz de accesos) que esté diseñada para identificar los roles y accesos de los diferentes sistemas con base en la identificación, autentificación y autorización. Esto ayudará a mantener protegida la información financiera de los clientes y proveedores.

Las tecnologías CyberArk, Beyondtrust, Centrify y CA Technologies (veracode) según informe de Gartner a noviembre 2018, son las que se pueden utilizar para automatizar el control de usuarios.

Figura 28. **Sistemas de control de accesos**

Fuente: Real Security. *BeyondTrust como líder en el cuadrante mágico de administración de acceso privilegiado de Gartner.* https://www.real-sec.com/2018/12/beyondtrust-as-leader-in-gartners-privileged-access-management-magic-quadrant. Consulta: 11 de junio de 2019.

5.4.8. Responsables de implementar

Con el apoyo de la gerencia, los responsables de implementar los controles establecidos en la capa de datos son infraestructura, administrador de base de datos, riesgos y oficial de seguridad (ver tabla III). Para su cumplimiento es importante que cada control sea asignado a un responsable del equipo propuesto, para implementación, control y monitoreo.

Tabla III. **Responsables de implementar capa de datos**

Roles / Responsabilidades: **R**= Responsable, **A**= Aprobador, **C**= Consultado, **I**= Informado.

Actividad	Roles / Responsabilidades						
Nombre	Administrador BD	Infraestructura	Riesgos	Oficial de seguridad	Director de tecnología	Departamento legal	Gerencia General
Cifrado de datos	R	R		I			
Hardening a bases de datos	R	R		I			
Sistema de clasificación y etiquetado de información	R		C	R		C	I
Sistema de prevención de fuga de información (DLP)	R	R	I	I	I		
Monitoreo de actividad bases de datos	R	I		I			I
Identificación y gestión de accesos de usuarios	R				R		
Cumplimiento de controles	C		R	I	I		I

Fuente: elaboración propia.

Luego de implementar los controles en capa de datos, es necesario realizar evaluaciones periódicas por el departamento de riesgos y seguridad a través de auditorías, para asegurar el nivel de cumplimiento a cada control establecido y proponer mejoras a los procesos establecidos.

5.5. Capa de aplicaciones

En una institución de microfinanzas, las aplicaciones son el medio que hace posible la ejecución de la mayoría de las actividades tanto críticas como no críticas, para personas y procesos. Las aplicaciones permiten el acceso a la información que se encuentra almacenada en las distintas bases de datos.

Las aplicaciones son el medio que hace posible visualizar, crear y modificar la mayoría de información, motivo por el cual casi todos los colaboradores de las

instituciones tienen acceso a ellas, lo que las convierte en un riesgo para la seguridad de la información.

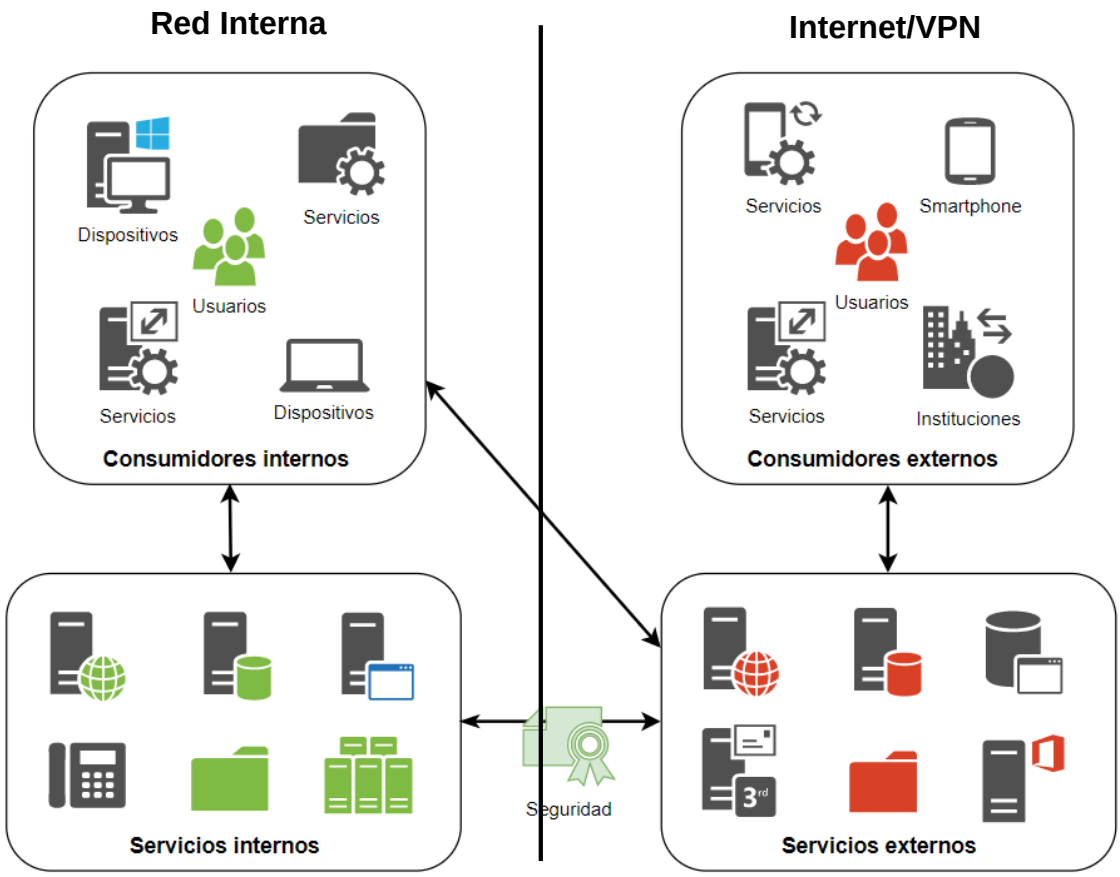
Son herramientas que interactúan directamente con las bases de datos de la institución, independiente del modelo de arquitectura que se utilice. Entre sus principales funciones está la de ingresar, consultar y modificar la información de clientes, proveedores y colaboradores.

Con la finalidad de asegurar la seguridad de la información en base a los servicios que prestan las aplicaciones, se sugiere segmentarlas en aplicaciones que prestan servicios internos y servicios externos. A continuación, se describen estos servicios:

- Aplicaciones con servicios internos: prestan servicios únicamente a personas y procesos internos a la institución y no pueden ser accedidas fuera de las instalaciones. Entre estas aplicaciones se puede mencionar al sistema bancario, planillas, recursos humanos, contabilidad, activos fijos, entre otros.

- Aplicaciones con servicios externos: son aplicaciones que prestan servicios a personas, procesos y otras aplicaciones externas o internas. Estas aplicaciones están expuestas al internet o a otras instituciones. Entre estas aplicaciones se puede mencionar a las API, banca virtual, páginas web, correo electrónico, intranet entre otros.

Figura 29. **Segmentación de las aplicaciones por sus servicios**



Fuente: elaboración propia.

La figura 27 permite visualizar de forma gráfica cómo las aplicaciones deben exponer la información a las personas, procesos y servicios. Define los servicios que únicamente pueden ser accedidos dentro de la red interna de la institución (servicios internos) y servicios que pueden ser accedidos desde cualquier lugar (servicios externos).

Las aplicaciones para su funcionamiento necesitan mantenimiento periódico, en especial a los usuarios autorizados. Las instituciones de

microfinanzas tienen una rotación alta de personal, motivo por el cual continuamente están contratando y dando de baja a los colaboradores y es importante disponer de controles que asegure que usuarios de baja no tienen accesos.

En instituciones de microfinanzas que desarrollan su propio software el esfuerzo está focalizado en la creación e innovación de nuevas herramientas que faciliten las labores diarias del personal, reduzcan los costos operativos y den ventaja competitiva. Sin embargo, la importancia que se le da a la seguridad de la información en estas herramientas en casi nula.

Las aplicaciones deben disponer de factores de autentificación que limiten el acceso a la información únicamente a personal autorizado. Una persona, proceso o aplicación debe de acceder únicamente a la información que le es necesaria para desempeñar las funciones que le han sido asignadas.

Se debe disponer de controles automatizados que permitan monitorear las actividades de las aplicaciones internas, de tal manera que si una aplicación intenta generar algún tipo de acción sospechosa sea restringida y bloqueada de forma automática. Esto previene los ataques de phishing, cuando los usuarios son vulnerados.

5.5.1. Riesgos relacionados a las aplicaciones

El objetivo de implementar los siguientes controles relacionados a la capa de aplicaciones es la protección de los datos críticos que se administran en las aplicaciones de la institución de microfinanzas, con la finalidad de mitigar los riesgos siguientes:

- Acceso no autorizado: dentro de las aplicaciones el acceso no autorizado se puede dar cuando alguien vulnera una cuenta de usuario, un usuario; comparte sus credenciales con otros usuarios o a nivel de configuración a un usuario se le dan accesos a información que no está autorizado a visualizar.

- Escalonamiento de privilegios: si un atacante logra vulnerar una cuenta de usuario y esta no tiene los permisos necesarios para poder acceder a información sensible, códigos fuentes o administración de aplicaciones, el atacante comienza a realizar análisis de vulnerabilidades que le permiten detectar puntos de falla y logra incrementar sus privilegios dentro de la infraestructura para poder administrar aplicaciones.

- Fuga de información: es la extracción de información no autorizada a través una persona, proceso o aplicación ajena o parte de la institución que no debería de tener acceso a esa información.

- Robo de información: es la extracción de información sensible con el fin de comercializar o realizar un fraude que afecta a la institución, a sus clientes, proveedores o colaboradores.

- Explotación de vulnerabilidades en código fuente: las aplicaciones están expuestas a ataques en donde la intención aprovechar fachas en el código fuente para obtener la información de usuarios o bien accesos a las bases de datos de clientes, proveedores o colaboradores.

Para mitigar los riesgos identificados en la capa de aplicaciones se propone implementar los siguientes controles.

5.5.2. Gestión de accesos de usuarios

Para la administración de la seguridad de aplicaciones es necesario disponer de un procedimiento o política que defina el ciclo de vida de los usuarios que cubra las altas, modificaciones y bajas. Debe tener un estricto cumplimiento y una revisión periódica.

- Alta de usuario: toda persona que tenga acceso a una o más aplicaciones debe disponer de un usuario de sistema único que lo identifique del resto de colaboradores. Se debe disponer un procedimiento que especifique involucrados y responsabilidades dentro del proceso; este procedimiento debe ser revisado periódicamente para asegurar que solo existan altas autorizadas con los roles establecidos según funciones.

- Modificación de permisos: en el ciclo de vida de los usuarios existen diferentes modificaciones a los permisos de los usuarios como los bloqueos temporales, cambio de accesos, cambios de contraseñas, accesos especiales, entre otros, para los cuales se debe disponer de un procedimiento definido y revisado periódicamente.

- Bajas de usuario: cuando un usuario queda fuera de la institución, sus accesos deben de ser eliminados y la cuenta de usuario no debe ser reutilizada por ningún usuario ni por el titular original, en caso de que se incorpore nuevamente a la institución. Este procedimiento debe ser revisado periódicamente para asegurar que no existan usuarios dados de baja con accesos en el sistema.

5.5.3. Control de calidad en aplicaciones

El compromiso con la calidad debe ser una responsabilidad de todo departamento de desarrollo, por lo que se debe tener procedimientos que aseguren que en los desarrollos no se produzca errores o bien otra condición que provoque vulnerabilidades en el software.

Es importante que los responsables de realizar este procedimiento jueguen un rol que medie entre la parte de negocios y la parte técnica y no limitarse únicamente a encontrar y reportar fallos. Su papel debe ser integrador y con amplios conocimientos sobre el giro de negocios y la criticidad de los datos.

"Es recomendable aplicar las sugerencias que proponen PCI PSS en el requisito 6.5 Abordar las vulnerabilidades de codificación comunes en los procesos de desarrollo de software".[47]

Los equipos de desarrollo deben ser capacitados periódicamente en técnicas de desarrollo de código con normas de seguridad.

5.5.4. Arquitectura de seguridad para aplicaciones

Las aplicaciones son utilizadas en las instituciones para diferentes propósitos y son accedidas por diferentes usuarios, entidades o procesos. Es importante clasificar e individualizar la exposición de cada aplicación de acuerdo a los servicios que prestan y la criticidad de la información que manejan.

La arquitectura de las aplicaciones debe estar diseñada en base a los principios de ISO 27001 que son disponibilidad, integridad y confidencialidad.

[47] ESET. *Principio del menor privilegio*. https://www.welivesecurity.com/la-es/2018/06/08/principio-menor-privilegio-limitar-acceso-imprescindible. Consulta: 4 de abril de 2019.

Debe identificar los tipos de datos que deben ser ofuscados en todo momento y que protocolos de seguridad utilizar para la transmisión de datos.

Una arquitectura debe contemplar métodos de factor de doble autentificación (2FA), identificación de cambios en archivos de configuración, pruebas de seguridad utilizando metodologías OWASP y un control de accesos unificado a todas las aplicaciones.

5.5.5. Validaciones de seguridad aplicaciones

En el análisis y diseño de una aplicación de software los departamentos de desarrollo enfocan sus esfuerzos en temas de funcionalidad y desempeño, dejando al margen la seguridad de la información y las implicaciones que tiene la pérdida, modificaciones no autorizadas o el mal uso de información que estas herramientas manejan.

Entre las vulnerabilidades de validación comunes en las aplicaciones podemos encontrar las siguientes:

- Autenticación de usuarios: es la habilidad de un sistema de demostrar que una persona o una aplicación es realmente quien asegura ser, independiente de la metodología que se utilice. Es importante disponer de una política de seguridad de contraseñas donde se especifique cuáles son las características para formarla, tiempos de vencimiento, cómo restaurarla y porqué se puede bloquear.

- Gestión de sesiones: es el control que identifica a los usuarios o aplicaciones que están conectados a un sistema a través de un código único asignado en el instante de la autentificación. El código debe ser

aleatorio y debe de asegurar las sesiones sean limitadas y que caduquen por inactividad.

- Control de acceso: asegura que cada usuario o aplicación disponga de un rol definido asociado a los recursos mínimos que necesita para realizar sus funciones de forma eficiente. Se debe mantener registros de la navegación y las acciones fallidas que se suscitan dentro del sistema.

- Manejo inadecuado de errores: las aplicaciones interactúan con los usuarios a través de mensajes, que tratan de indicar una alerta o un error en el manejo de la información. Estos mensajes pueden contener sentencias SQL que descubran los nombres de bases de datos, tablas o segmentos de código que pueden ser aprovechados por un atacante.

Para un control adecuado de las revisiones de vulnerabilidades en las aplicaciones se hace necesario seguir la metodología OWASP y PCI DSS requisito 6.5.

Las tecnologías CA Technologies (veracode), Micro Focus, Checkmsarx, IBM, Synopsys según informe de Gartner a febrero 2018, son las que se pueden utilizar para automatizar las pruebas de seguridad en aplicaciones.

Figura 30. **Aplicaciones de pruebas de seguridad en aplicaciones**

Fuente: Security Intelligene. *IBM mantiene una posición de liderazgo en el Cuadrante Mágico de Gartner 2018 para pruebas de seguridad de aplicaciones*. https://securityintelligence.com/ibm-sustains-a-leadership-position-in-2018-gartner-magic-quadrant-for-application-security-testing. Consulta: 11 de junio de 2019.

5.5.6. Análisis de vulnerabilidades

Se pude considerar vulnerabilidad informática a toda aquella debilidad independiente del tipo que pone en riesgo el funcionamiento o seguridad de un equipo informático. La norma ISO 27001 hace referencia al constante seguimiento de parches de seguridad mediante el uso de herramientas de análisis de vulnerabilidades.

Para el análisis de vulnerabilidades se debe considerar los sistemas operativos y aplicaciones de software, evitando quedarse atrás en la actualización de nuevas versiones o actualizaciones liberadas. Es importante evitar el uso de software de esta fuera del soporte del fabricante.

Se debe utilizar herramientas que permiten hacer escaneo automático de vulnerabilidades a todos los sistemas operativos, software, estaciones de trabajo y equipos de red de la institución, debido a que permite tener visibilidad de toda la infraestructura.

> "Es importante que se disponga de una tabla de referencia que estandarice cómo deben realizarse las métricas de la criticidad de las vulnerabilidades encontradas (Anexo A). Se recomienda aplicar estándares de puntuación de criticidad de vulnerabilidades como CVSS".[48]

5.5.7. Pruebas de penetración

Las pruebas de penetración están diseñadas para poner a prueba la seguridad de la infraestructura técnica, con el fin de encontrar vulnerabilidades que una persona mal intencionada podría utilizar como medio para obtener un acceso no autorizado, poniendo en riesgo la seguridad de la información.

El objetivo de estas pruebas es encontrar vulnerabilidades de seguridad que pongan al descubierto la falta de cumplimiento de las políticas establecidas, falencia no conocidas y, por ende, comprometer la información; conocer la sensibilización de los empleados en temas de seguridad y las capacidades de identificar y responder a estos incidentes.

[48] KirkpatrickPrice. *Vulnerabilidades comunes de codificación*. https://kirkpatrickprice.com/video/pci-requirement-6-5-address-common-coding-vulnerabilities-software-development-processes/. Consulta: 4 de abril de 2019.

Estas pruebas detectan problemas de seguridad sobre todo en aplicaciones que prestan servicios externos (expuestos al internet). Los puntos clave con el control de parches, la encriptación de la información que se transporta y la encriptación de la información que se almacena por las aplicaciones.

La evaluación de estas pruebas puede estar enfocada a las personas y consiste en evaluar la concientización de los colaboradores en la seguridad de la información. A través de phishing se busca que los colaboradores proporcionen contraseñas de correo, información financiera, datos sensibles que comprometan la información.

5.5.8. Administración unificada de perfiles de usuarios en aplicaciones (SSO)

Las instituciones actualmente cuentan con diversas herramientas de software que ayudan en las distintas tareas de las diferentes áreas. Cada una de estas herramientas utiliza su propio método de autentificación sus usuarios, su política de claves, sus perfiles, entre otros.

Tener perfiles y usuarios por herramienta provoca el riesgo de no dar a un colaborador los accesos necesarios para que desempeñe las funciones del puesto al que está asignado. También, al momento de una baja se incrementan las posibilidades de dejar un usuario activo dentro de las diversas herramientas.

Se necesita un sistema de inicio de sesión unificado (SSO – Single Sign On) que disponga de políticas de seguridad, el control y la gestión de usuarios y perfiles, al que todas las aplicaciones que requieran de un control de accesos se conectan para confirmar la autenticidad y certeza del usuario o aplicación que indica ser.

Las tecnologías Okta, Microsoft, Oracle, Ping Identity, IBM, Synopsys, según informe de Gartner a junio 2018, son las que se pueden utilizar para automatizar la centralización de accesos.

Figura 31. **Aplicaciones para el manejo de centralizado de accesos**

Fuente: OneLogin. *OneLogin nombrado visionario en el cuadrante mágico de gestión de acceso 2018 de Gartner* https://www.onelogin.com/resource-center/analyst-reports/gartner-mq. Consulta: 11 de junio de 2019.

5.5.9. Plataforma de gestión de cuentas privilegiadas

No todos los usuarios son iguales; existen usuarios que tienen cuentas con privilegios que trascienden las medidas de seguridad habitual y se llega al límite entre lo que se considera riesgo operacional y operatividad que realizan estos usuarios según funciones.

Para el control de cuentas privilegiadas se debe disponer de una plataforma que organice y gestione las cuentas con privilegios de una forma segura cumpliendo con los siguientes controles:

- Procedimiento estandarizado: debe tener identificada a la lista de las cuentas con privilegios dentro de la institución y contar con los niveles de aprobación para estas, un flujo documentado que se utilizará para la aprobación y cambio de privilegios.

- Política de contraseñas: las contraseñas de usuarios con privilegios deben de cambiarse de manera periódica y asegurar que cumpla con un estándar de contraseñas seguras.

5.5.10. Software de doble factor de autenticación (2FA)

Consiste básicamente en un segundo método de autentificación que puede ser mediante un pin o un código cualquiera de seguridad cuando nos autentificamos en un sistema crítico. Se debe considerar obligatorio para usuarios con privilegios en aplicaciones de alta criticidad o servicios que realicen operaciones de dinero.

Existen varios métodos que pueden ayudar a disponer de una doble autentificación, entre los que se pueden mencionar:

- Hardware: este método requiere de un dispositivo de hardware que genera una llave aleatoria cada cierto tiempo. Este tipo de método tiene el problema de que los dispositivos tienen un costo; por su tamaño son fáciles de extraviar y tienden a deteriorarse con el paso del tiempo.

- Envio de mensajes: este método de autentificación es el más común y se basa en enviar un pin o código a través de correo o mensaje de texto, el cual el usuario debe de ingresar a la aplicación. Las desventajas que tiene este método es la facilidad con que el pin puede ser visto por una persona que se encuentra cerca.

- Software: este método utiliza una aplicación móvil en la cual se escanea un código que proporciona el servicio principal. Con el aplicativo permite enviar notificaciones de pin o código a los usuarios.

Entre las herramientas de doble factor de autentificación se pueden mencionar Google Authenticator, Authy y Microsoft Multi-Factor Authentication, que están entre las más utilizadas a un menor costo.

5.5.11. Sistema de prevención de fuga de información (DLP)

Este control se encuentra descrito en la capa de datos (sección 5.4.5) y es aplicable a la capa de aplicaciones.

5.5.12. Filtrado de aplicaciones web (WAF)

Es un método de protección implementado a través del uso de firewall de aplicaciones web a través de un conjunto de reglas conocidas como políticas, que protegen a las aplicaciones expuestas al internet de ataques como inyección de código SQL, inyección de código javascript (cross-site-scripting), falsificación de petición en sitios cruzados (cross-site).

Entre sus capacidades está limitar el acceso a los servidores únicamente a los servicios que se prestan; resguarda el perímetro de seguridad y vulnerabilidades adicionales que se tengan a nivel desarrollo o actualizaciones de software.

Las tecnologías imperva y Akamai, según informe de Gartner a agosto 2018, son las que se pueden utilizar para automatizar el filtrado de aplicaciones web.

Figura 32. **Sistemas de filtrado de aplicaciones web**

Fuente: Forcepoint. *Gartner cuadrante mágico 2019 para firewalls de red.* https://www.forcepoint.com/blog/insights/forcepoint-named-sole-visionary-2018-gartner-magic-quadrant-enterprise-network. Consulta: 2 de junio de 2019.

5.5.13. Solución antiphishing/antispam

Estas soluciones ayudan a protegen los buzones de correo electrónico de los usuarios al filtrar los correos que se reciben. Esta acción evita que los usuarios se expongan a correo no deseado, a través de la utilización de algoritmos inteligentes que identifican los mensajes que contienen información no deseada y se aísla de la vista principal de los usuarios.

Se puede contar con la mejor solución tecnológica y el personal de seguridad mejor capacitado para repeler ataques de phishing y spam; sin embargo, el mayor riesgo de las instituciones son sus colaboradores. Se debe contar con un plan de capacitación sobre seguridad para el personal nuevo y capacitaciones periódicas para el personal en general.

5.5.14. Escaneo/revisión de código fuente

Los desarrolladores enfocan sus esfuerzos en el desarrollo de las funcionalidades que les son requeridas, Gran parte del tiempo están enfocados en cumplir tiempos de entrega, son pocos los departamentos de desarrollo que estiman tiempos para asegurar la eficiencia del código fuente.

> "Emplear una metodología (como OWASP) ayuda a mejorar la seguridad de las aplicaciones comenzando por la parte estructural, que es el código fuente. Permite tener un marco de referencia estándar de mejores prácticas, las cuales identifican de manera secuencial las revisiones que se deben realizar".[49]

5.5.15. Consultoría sobre buenas prácticas de desarrollo de software

En el desarrollo de software es importante implementar buenas prácticas en cada una de las fases del ciclo de vida del desarrollo, que va desde la toma de requerimientos hasta la implementación y monitoreo. Se garantiza de esta forma la seguridad de la información en cada proceso de negocios y disminuye el riesgo de vulnerabilidades.

Una empresa externa con personal calificado es capaz de identificar debilidades en cualquier fase del ciclo de vida del desarrollo de software. Hacer

[49] Pcihispano. *Gartner puntación de herramientas de clasificación de información*. https://www.pcihispano.com/?descargas=40465. Consulta: 4 de abril de 2019.

visibles las debilidades en las áreas de desarrollo permite tomar conciencia sobre la responsabilidad de la seguridad de la información e implementar acciones que mitiguen debilidades tanto presentes como futuras.

5.5.16. Monitoreo de integridad de archivos (FIM)

Las personas, procesos y aplicaciones continuamente están modificando la información contenida en diferentes archivos que se encuentran en diferentes ubicaciones. Es importante tener identificados los archivos de configuración o que contienen información sensible para la institución.

Los archivos con información de configuración y los que contienen información sensible representan un riesgo a la seguridad de la información, por lo cual se debe realizar un monitoreo periódico que ayude identificar personas, procesos y aplicaciones que los alteren. El resultado del análisis debe ser reportado a la gerencia general y hacer énfasis de los indicios de accesos no autorizados.

Este tipo de monitoreo es esencial para identificar los cambios no autorizados que pueden ser realizados por usuarios con privilegios de administrador, ya son quienes tienen los permisos para realizar modificaciones a cualquier archivo.

“Las tecnologías Okta, Microsoft, Oracle, Ping Identity, IBM, Synopsys según informe de Gartner a noviembre 2018, son las que se pueden utilizar para automatizar el monitoreo de integridad”.[50]

[50] OWASP. *Seguridad de aplicaciones*. https://www.owasp.org/index.php/Main_Page. Consulta: 4 de abril de 2019.

5.5.17. Gestión de la parametrización de la seguridad transaccional

Las aplicaciones generan transacciones de diferente índole que permiten que las instituciones realicen la actividad comercial para la que están constituidas. Sin embargo, si estas transacciones no cuentan con medidas de seguridad, la información puede ser vulnerada.

Es importante que las transacciones que se realizan por las aplicaciones dispongan de los medios de seguridad necesarios para impedir que los datos sean interceptados y modificados por personas, procesos y aplicaciones sin autorización.

Para cumplir con este requerimiento es importante que las aplicaciones utilicen certificados TLS o encriptación de campos críticos, conexiones por medio de VPN.

Dentro de las aplicaciones existen datos de configuración que son críticos y es necesario asegurar la gestión de los cambios se les realizan. Si se provoca alguna alteración a estos datos de configuración se debe identificar y mostrar alertas de las modificaciones realizadas.

5.5.18. Desarrollo seguro de aplicaciones

En los departamentos de desarrollo de aplicaciones se debe disponer de una metodología (como OWASP) enfocada en la importancia que solo las personas, entidades y procesos autorizados pueden acceder a consultar y modificar datos que su nivel de autorización les permita.

Realizar pruebas de vulnerabilidades a las aplicaciones por personal externo a los departamentos de desarrollo mitiga el riesgo de liberar aplicaciones a producción con riesgos de seguridad que expongan información sensible de clientes, proveedores o colaboradores.

5.5.19. Responsables de implementar

Con el apoyo de la gerencia, los responsables de implementar los controles establecidos en la capa de aplicaciones son: infraestructura, administrador de base de datos, riesgos y oficial de seguridad, director de tecnología (ver tabla IV). Para su cumplimiento es importante que cada control sea asignado a un responsable del equipo propuesto, para implementación, control y monitoreo.

Se debe implementar controles que den seguimiento al cumplimiento de cada uno de los controles establecidos, reportes periódicos a la gerencia con vulnerabilidades detectadas y evaluaciones periódicas que ayuden a redefinir controles.

Tabla IV. **Responsables de implementar capa de aplicaciones**

Roles / Responsabilidades: **R**= Responsable, **A**= Aprobador, **C**= Consultado, **I**= Informado.

Actividad	Roles / Responsabilidades					
Nombre	Administrador BD	Infraestructura	Riesgos	Oficial de seguridad	Director de tecnología	Gerencia General
Gestión de accesos de usuarios	C	C	I		R	I
Control de calidad en aplicaciones			R		R	
Arquitectura de seguridad para aplicaciones	C	C		R	R	
Validaciones de seguridad aplicaciones	R	R		R	I	
Análisis de vulnerabilidades			I	R		I
Pruebas de penetración	C	C	I	R	C	I
Administración unificada de perfiles de usuarios en aplicaciones (SSO)		R				
Plataforma de gestión de cuentas privilegiadas		R				
Software de doble factor de autenticación (2FA)		R				
Sistema de prevención de fuga de información (DLP)	R	R		R	I	
Filtrado de aplicaciones web (WAF)		R			I	
Solución antiphishing/antispam		R		R	I	
Escaneo/revisión de código fuente				R	I	
Consultoría sobre buenas prácticas de desarrollo de Software					R	I
Monitoreo de integridad de archivos (FIM)		R		R	I	
Gestión de la parametrización de la seguridad transaccional		R		R	I	
Desarrollo seguro de aplicaciones					R	
Cumplimiento de controles	C	C	R	C,I	C,I	I

Fuente: elaboración propia.

5.6. Capa de sistemas operativos

Los sistemas operativos son la espina vertebral que soporta el funcionamiento de todas las aplicaciones que se utilizan para realizar las operaciones dentro de una institución. Cada dispositivo que se usa en la infraestructura de la institución emplea un sistema operativo para realizar sus funciones.

Estas herramientas, como todo software, están expuestas a diversas vulnerabilidades que son identificadas y actualizadas por los fabricantes. Son

estas vulnerabilidades las que los atacantes intentan utilizar para tener acceso a los equipos y extraer información o para controlarlos de acuerdo a sus intenciones.

Se debe realizar esfuerzos para la detección y manejo de vulnerabilidades, ya que representan un riesgo a la seguridad de la información. Este riesgo mediante la gestión de parches de seguridad de forma periódica (según el fabricante los ponga a disposición) a cada dispositivo independiente del sistema operativo.

Es importante disponer de controles adecuados para la gestión de vulnerabilidades que se suscitan en los sistemas operativos y, de esta forma, mitigar las posibilidades de exponer información a personas, procesos y aplicaciones sin autorización que pueden afectar negativamente a la institución.

5.6.1. Riesgos relacionados con los sistemas operativos

Implementar los distintos controles que se proponen en la capa de sistemas operativos protege datos críticos gestionados por los sistemas operativos de la institución, con la finalidad de mitigar los riesgos siguientes:

- Acceso no autorizado: dentro de los sistemas operativos el acceso no autorizado se puede dar en el momento en que una persona, proceso o aplicación vulnera una cuenta de usuario; cuando un usuario comparte sus credenciales con otros usuarios o a nivel de configuración un usuario recibe acceso a información que no necesita para sus funciones.

- Escalonamiento de privilegios: un atacante logra vulnerar una cuenta de usuario y esta dispone de los permisos necesarios para acceder a

información sensible, a códigos fuentes o a la administración de aplicaciones. El atacante, con la cuenta vulnerada, comienza a realizar análisis que le permiten detectar puntos de falla y logra incrementar sus privilegios dentro de la infraestructura para poder administrar aplicaciones y obtener información sensible.

- Alteración de configuraciones: un usuario no autorizado que dispone de permisos para alterar las configuraciones en los sistemas operativos, tiene la capacidad para deshabilitar funciones de protección e instalar herramientas de monitoreo que no serían identificadas por otros sistemas de protección.

- Disponibilidad de los servicios instalados: denegación de servicios a aplicaciones por cambios en las configuraciones o el bloqueo de puertos podrían hacer que la institución detenga sus operaciones por un periodo de tiempo indeterminado.

- Bloqueo de acceso a la información: bloquear las máquinas a través de software malicioso, puede causar daños críticos que impedirían acceder a la información, que es secuestrada hasta pagar un rescate. El gasto del rescate dependerá de cuántos equipos sean infectados, dejando un problema reputacional e inseguridad sobre la institución.

- Alteración en información: las vulnerabilidades en sistemas operativos pueden dar permisos necesarios a personas, procesos y aplicaciones a que tengan la capacidad de modificar la configuración de cualquier archivo a su conveniencia, con el fin de tener acceso a información sensible.

Con la finalidad de mitigar los riesgos expuestos anteriormente se propone la implementación de una serie de controles que están diseñados con base en mejores prácticas y estándares internacionales.

5.6.2. Escaneo de vulnerabilidades

Son pruebas de vulnerabilidades que se realizan a los sistemas operativos con el objetivo de detectar puntos de falla. Están enfocadas en revisar las configuraciones, librerías y paquetes que exponen vulnerabilidades conocidas en los sistemas operativos.

> "Los escaneos de vulnerabilidades son exclusivamente técnicos y se enfocan en la identificación y detección de posibles inconvenientes dentro de los sistemas operativos de una institución. Se basa principalmente en la comparación con bases de datos conocidas y reportadas de vulnerabilidades".[51]

Los escaneos deben ser realizados de forma automática y periódica a todos los sistemas operativos registrados en la infraestructura. Estas pruebas comúnmente tienen una base alta de falsos negativos, por lo que los reportes generados deben de analizarse de forma detalla.

Al gestionar las vulnerabilidades se logra identificarlas y clasificarlas, lo cual permite priorizarlas dependiendo del nivel de riesgo (ver Apéndice C) que represente vulnerabilidad.

Las herramientas de software Synopsys, Veracode, Micro Focus, Ceckmarx, según informe de Gartner a febreo 2019, que se pueden utilizar para automatizar el escaneo de vulnerabilidad.

[51] Calidificación Gartner. *Gestión de accesos BeyondTrust*. https://www.beyondtrust.com/blog/entry/beyondtrust-named-a-leader-in-first-ever-gartner-magic-quadrant-for-privileged-access-management. Consulta: 4 de abril de 2019.

Figura 33. **Sistemas de pruebas de vulnerabilidades**

Fuente: Microfocus. *Gartner 2020 Magic Quadrant para pruebas de seguridad de aplicaciones.* https://www.microfocus.com/en-us/assets/security/magic-quadrant-for-application-security-testing. Consulta: 11 de junio de 2019.

5.6.3. Aplicación de parches de seguridad

Los proveedores de aplicaciones están generando parches de seguridad de manera continua, los cuales deben ser actualizados por el equipo técnico de forma manual o bien utilizando una herramienta que permite hacerlo de forma automática.

Los parches son un conjunto de cambios que se implementan a un sistema operativo y están diseñados para corregir vulnerabilidades de seguridad, especialmente las funcionalidades que están expuestas al internet. Comúnmente, no modifican las funcionalidades.

Es importante disponer de una política de actualización que permita especificar la periodicidad con que deben de aplicarse los parches de seguridad. Se recomienda no instalar las actualizaciones más recientes de ambientes utilizados en producción, debido a que puede ocasionar fallas en la operativa.

"Las herramientas de software como IBM BigFix, Ivanti Patch, SolarWinds, pueden ser una buena opción para implementar para automatizar el manejo de parches".[52]

5.6.4. Hardening de configuraciones

Asegurar el endurecimiento en las configuraciones de los sistemas operativos limita las posibilidades a un usuario no autorizado de lograr ingresar a un sistema operativo. PCI DSS enumera un conjunto de actividades que se deben realizar a los sistemas operativos para endurecer las configuraciones.

Se puede tomar como referencia la comunidad CIS Benchmarks que es un grupo dedicado a seguridad y se especializa en brindar recomendaciones para la configuración de los diferentes tipos de sistemas operativos. Entre las sugerencias recomendadas se pueden mencionar:

[52] Security Planet. *Soluciones tecnologías para manejo de parches*. https://www.esecurityplanet.com/products/ top-patch-management-solutions.html. Consulta: 4 de abril de 2019.

- Política de contraseñas
- Políticas de auditorías
- Permisos de usuarios
- Opciones de seguridad
- Log de eventos

Hay varias configuraciones críticas que se deben de tener en cuenta en los sistemas operativos. Deshabilitar usuarios cada sesenta días, limitar accesos rápidos, bloqueo de contraseñas, cifrado de accesos administrativos, cifrado de discos duros, entre otros.

5.6.5. Plataforma de gestión de cuentas privilegiadas

Este control se encuentra descrito en la capa de datos (sección 5.4.9) y es aplicable a la capa de sistemas operativos.

Se debe mantener un control de las cuentas con rol de administrador de los sistemas operativos. Asegurar el resguardo de las claves, mediante una plataforma que las gestione.

5.6.6. Sistema de doble factor de autenticación (2FA)

Este control se encuentra descrito en la capa de aplicaciones (sección 5.4.9) y es aplicable a la capa de sistemas operativos.

A nivel sistemas operativos, así como las define en la capa de aplicaciones, se debe disponer de una validación de doble factor para las cuentas que tienen rol de administrador.

5.6.7. Monitoreo de integridad de archivos (FIM)

Este control se encuentra descrito en la capa de aplicaciones (sección 5.4.14) y es aplicable a la capa de sistemas operativos.

En la capa de sistemas operativos se debe identificar las rutas críticas que alojan archivos que contienen configuraciones de usuarios, contraseñas, carpetas que contienen códigos fuentes, instaladores web o de escritorio. Estos repositorios deben ser monitoreados.

5.6.8. Sistema de prevención de fuga de información (DLP)

Este control se encuentra descrito en la capa de datos (sección 5.4.5) y es aplicable a la capa de aplicaciones.

Es necesario establecer políticas de protección que identifique los tipos de datos para que estos sean protegidos y se evite la fuga información sensible como de archivos de configuración, archivos de contraseñas, listados de clientes, nóminas de salarios, entre otros.

5.6.9. Antivirus avanzado

Disponer de un software que permita detectar, prevenir y eliminar amenazas de aplicaciones maliciosas ayuda a la gestión de seguridad en caso que fallen los procedimientos estandarizados y socializados con el personal de la institución.

La función principal del antimalware es detectar y eliminar amenazas de malware. Para realizar esta tarea es importante que se actualice de forma

periódica y disponga de bases de datos reciente. Un antimalware desactualizado no será capaz de detectar amenazas de malware reciente.

Se deben hacer dos apartados, antivirus que se basan en firmas

- Antivirus tradicionales: estas soluciones de antimalware basan su análisis a través de firmas y bases de conocimientos que se deben actualizar constantemente, ya que se vuelven obsoletos. En esta gama de soluciones se encuentran Symantec, Trend Micro, Kaspesky, McAfee.

- Antivirus avanzados: son soluciones de antimalware que basan su análisis a través de algoritmos matemáticos machine learning, patrones de comportamiento, lo que les da mayor efectividad. En esta gama de soluciones se encuentran Cylance, carbon black, crowd strike.

Las herramientas de software Trend Micro, Sophos, Symantec según informe de Gartner a enero 2018 son las que se pueden utilizar para automatizar la detección automática de malware.

Figura 34. **Soluciones de antimalware**

Fuente: Next Vision. *Ciber seguridad inteligente*. https://www.nextvision.com/tag/antimalware. Consulta: 11 de junio de 2019.

5.6.10. Responsables de implementar

Los responsables de implementar los controles establecidos en la capa de sistemas operativos son: infraestructura, administrador de red, área de monitoreo, riesgos y oficial de seguridad (ver tabla V). Para su cumplimiento es importante que cada control sea asignado a un responsable del equipo propuesto, para implementación, control y monitoreo.

Tabla V. **Responsables de implementar capa de aplicaciones**

Roles / Responsabilidades: **R**= Responsable, **A**= Aprobador, **C**= Consultado, **I**= Informado.

Actividad	Roles / Responsabilidades						
Nombre	Administrador BD	Infraestructura	Riesgos	Oficial de seguridad	Director de tecnología	Gerencia General	
Escaneo de vulnerabilidades	C	C		R	I	I	
Aplicación de parches de seguridad	R	R					
Hardening de configuraciones	R	R		C	I		
Plataforma de gestión de cuentas privilegiadas	R	R		C		I	
Sistema de doble factor de autenticación (2FA)		R		C	I		
Monitoreo de integridad de archivos (FIM)	R	R	I	R			
Sistema de prevención de fuga de información (DLP)	R	R		R	I		
Antimalware avanzado		R					
Cumplimiento de controles	C	C	R	C,I	C,I	I	

Fuente: elaboración propia.

5.7. Capa de red

En capa de red define todo lo relacionado a la conectividad de cada dispositivo y la información que fluye entre las personas, procesos, aplicaciones y dispositivos. Adicional, se enmarca la información que es transmitida entre instituciones externas con las cuales se tiene una conexión de red.

La infraestructura de red en la mayoría de instituciones de microfinanzas tiene un crecimiento desordenando. Con el paso del tiempo, con el fin de cumplir con los requerimientos del negocio se van agregando más componentes que no son planificados.

La falta de planificación y el desarrollo de diseños apropiados en la infraestructura son la mezcla perfecta para provocar fallas en las interconexiones

de la red, que afecta negativamente el desempeño de las comunicaciones y generan vulnerabilidades a la seguridad de la información.

La importancia de las redes en el manejo de la información es esencial debido a que en ellas se transporta la información de cada transacción que la institución genera, permite a personas, procesos y aplicaciones comunicarse entre ellas u otras instituciones.

Es recomendable que la información se encuentre separada de acuerdo a niveles de sensibilidad, con lo que se evita que se den accesos no autorizados, manteniendo en todo momento la integridad de los datos.

5.7.1. Riesgos relacionados a la red

El objetivo de implementar los controles descritos en la capa de red es determinar un perímetro de protección a los datos críticos que son transmitidos en la infraestructura de red de la institución de microfinanzas, con la finalidad de mitigar los riesgos siguientes:

- Denegación de servicios: Comúnmente esto ocurre cuando los atacantes inundan la red y genera un volumen de tráfico a través de peticiones que los equipos no pueden soportar, lo que impide que se tenga accesos a los servicios que se brindan a los usuarios.

- Intercepción de información (Man-in-the-Middle): el atacante introduce una herramienta de monitoreo entre las personas, procesos o aplicaciones y la fuente de información. Este tipo de ataque es muy efectivo y difícil de detectar.

- Fuga de información: es la extracción de información no autorizada de una persona, proceso o aplicación ajena o parte a la institución que no debería tener acceso a esa información.

- Robo de información: extracción de información sensible con el fin de comercializar o realizar un fraude que afecta a la institución, a sus clientes, proveedores o colaboradores.

- Caída de servicios críticos: la disponibilidad de los datos puede provocar que la institución deje de brindar servicios a sus clientes, provocar inconformidad y mala reputación.

- Acceso no autorizado: dentro de la red el acceso no autorizado se puede dar cuando alguien vulnera un dispositivo de red a nivel de configuración y puede monitorear todo el tráfico que la red transmite. Este riesgo compromete la información confidencial de forma fácil.

- Escalonamiento de privilegios: si un atacante logra vulnerar un dispositivo de red y este se conecta con toda la red, tiene el control para acceder a la información, a códigos fuentes o administración de aplicaciones. El atacante comienza a realizar análisis de vulnerabilidades, lo que le permite detectar puntos de falla e incrementar sus privilegios.

En la capa de red se debe buscar medidas de control que permitan mitigar los riesgos en la seguridad de la información que es transmitida, para lo cual se proponen los siguientes controles.

5.7.2. Control de accesos a la red (NAC)

Refuerza la seguridad perimetral de los equipos que forman parte de la infraestructura de red. Su finalidad es permitir el acceso a la red únicamente a los dispositivos que cumplen con la política de seguridad establecida dentro de la institución y evitar el acceso no autorizado a los servicios de red.

El control de accesos a la red permite establecer requisitos de conexión a través de perfiles de usuarios y dispositivos mediante políticas de seguridad, para visualizar los dispositivos conectados a la red, monitorear su comportamiento y detectar dispositivos infectados, estableciendo un entorno seguro.

Las herramientas de software Synopsys, Cisco, Aruba, Extreme Networks, según informe de Gartner a junio 2018, son las que se pueden utilizar para automatizar el control de accesos a la red.

Figura 35. **Sistemas de control de accesos a red**

Fuente: Fortinet. *Gartner magic quadrant reports*. https://www.fortinet.com/solutions/gartner-magic-quadrants.html. Consulta: 11 de junio de 2019.

5.7.3. Sistema de prevención de intrusos (IPS)

Es una solución adicional a la que ofrece un *firewall* perimetral, que a través de hardware o software se encarga de identificar y bloquear amenazas sofisticadas con comportamientos y eventos sospechosos de forma proactiva en la red o en un dispositivo.

Basan su funcionamiento en el monitoreo del tráfico y la identificación de patrones de comportamiento de eventos ocurridos en tiempo real dentro de una red o en un dispositivo, eventos que comparan en su base de conocimiento, reglas definidas y datos aprendidos, para identificar una actividad sospechosa o inusual.

Las herramientas de software Cisco, Trend Micro, McAfee según informe de Gartner a diciembre 2017, se pueden utilizar para la detección automática de intrusos (malware).

Figura 36. **Herramientas de prevención de intrusos**

Fuente: Cyber Securiry Meno. *Cuadrante mágico de Gartner para sistemas de detección y prevención de intrusiones*. https://www.51sec.org/2018/11/gartner-magic-quadrant-for-intrusion-detection-and-prevention-systems-2017-2015-2013-2012-2010. Consulta: 3 de mayo de 2019.

5.7.4. Gestión de accesos remotos

Un acceso remoto es cualquier conexión a una red privada o sistemas informáticos que no está expuesta al público en general y la persona o usuario se encuentra fuera del perímetro permitido. Este tipo de acceso necesita tener autorización.

Es importante disponer de una política o procedimiento que defina quiénes son los responsables de autorizar los accesos remotos, el monitoreo periódico que se debe realizar y la identificación de perfiles a quienes se les debe de permitir este tipo de accesos.

5.7.5. Seguridad de las redes inalámbricas

Las redes inalámbricas representan un riesgo latente dentro de las instituciones. Debido a su exposición son visibles por cualquier dispositivo y extiende el perímetro de red fuera de las instalaciones físicas, razón por la cual incrementa la vulnerabilidad a accesos o autorizados.

Se debe disponer de procedimientos que aíslen el acceso a la red inalámbrica a través políticas de cifrado recomendadas, limitando el uso de algoritmos de criptográficos obsoletos como WEP y WPA.

Se debe asegurar que la red inalámbrica está en un segmento diferente a cualquier segmento de la infraestructura de red. Cada conexión que se registre debe tener doble factor de autentificación.

El ingreso a la red debe ser por autentificación en un portal web que solicite usuario y contraseña, para colaboradores que tienen autorizado el acceso las

credenciales únicas. Para usuarios invitados se debe crear un usuario temporal con un periodo de caducidad.

Las herramientas de software líderes en el mercado que se pueden utilizar para la protección del perímetro de seguridad de las redes inalámbricas se pueden visualizar en la siguiente ilustración:

Las herramientas de software Cisco, VMware, Silver Peak, según informe de Gartner a octubre 2018, se pueden utilizar para la protección del perímetro de seguridad

5.7.6. Hardening de configuraciones

Este control se encuentra descrito en la capa de aplicaciones (sección 5.6.4) y es aplicable a la capa de redes.

Adicionalmente, para garantizar el *hardening* se deben eliminar todas las configuraciones que los dispositivos traen de fábrica. Se recomienda consultar la guía NIST y CIS para seguridad de contraseñas y configuraciones de dispositivos.

5.7.7. Filtrado de contenido web proxy

Se debe controlar la navegación web que los usuarios realizan, con la finalidad de evitar que se acceda a sitios web sospechosos o con mala reputación. Esto ayuda a que se descargue cualquier tipo de malware que pueda infectar la red.

Los permisos de navegación dependerán se controlan en base a perfiles, usuario, grupos, horarios. Permite tener listas blancas y negras y sitios web. Es importante tener identificados a los usuarios que por sus funciones tienen permisos a sitios web de redes sociales, multimedia, investigaciones, entre otros.

5.7.8. Diseño y segmentación de redes por capas

En una institución hay diversos servicios de red que permiten soportar las operaciones, como los servidores para uso interno, servidores con servicios expuestos al internet, servidores en la nube, las máquinas de los usuarios, las cámaras de seguridad, la red inalámbrica, entre otros.

Es importante tener identificados y segmentados en capas los recursos de acuerdo a sus servicios y criticidad. Esto permitirá que los recursos tengan accesos únicamente a lo que está autorizado para desempeñar sus funciones y no haya accesos no autorizados.

Cada uno de los incisos que se describen a continuación, deben estar en un segmento de red diferente. La conectividad entre ellos debe ser únicamente a los servicios requeridos:

- Bases de datos con información crediticia.
- *Firewall*, antivirus, IPS.
- Servidores expuestos al internet.
- Conectividad con otras instituciones.

- Departamentos segmentados (contabilidad, RRHH, tecnología, entre otros).

- Ambientes de desarrollo y pruebas.

- Cámaras de seguridad y biométricos.

- Servidores en la nube.

Los servidores que se encuentren alojados en la nube también deben estar segmentados de acuerdo a los servicios que brindan. La comunicación entre ellos debe de ser limitada y monitoreada.

5.7.9. Sistema de prevención de fuga de información (DLP)

Este control se encuentra descrito en la capa de datos (sección 5.4.5) y es aplicable a la capa de aplicaciones.

5.7.10. *Firewalls* perimetrales robustos capaces de detectar amenazas avanzadas

Representan uno de los dispositivos con mayor relevancia dentro de la arquitectura de red, debido a que es capaz de gestionar todas las capas del protocolo OSI.

Analiza todo el tráfico a través de UTM y a través de las reglas definidas determina qué puede entrar o salir de una red privada a una red pública.

Es algo que permite o deniega accesos y segmenta redes que interconecta.

Los *firewalls* han evolucionado de manera paralela a los tipos de ataques que se presentan. Actualmente son capaces de repeler ataques sobre la capa de aplicaciones y malware avanzado.

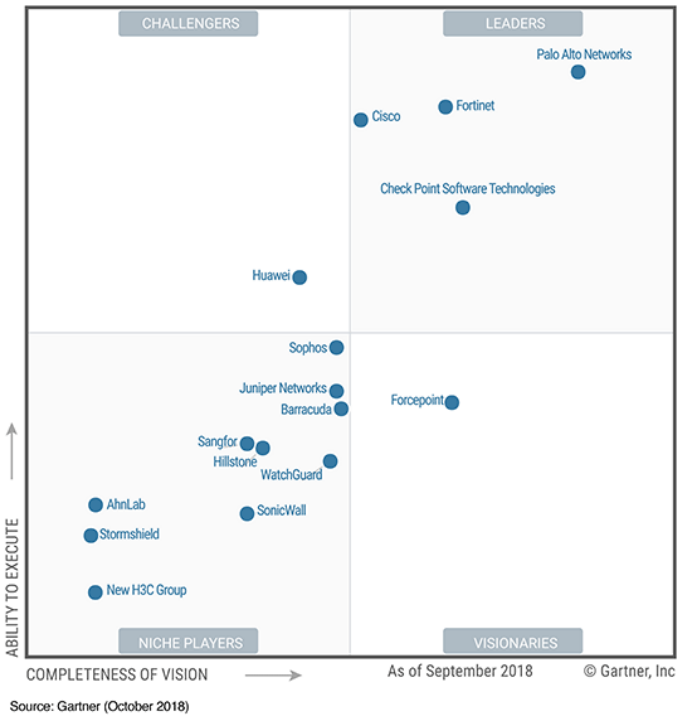
De acuerdo a las funcionalidades, los *firewall* pueden ser divididos en dos tipos, los cuales se detallan a continuación:

- *Firewall* tradicional: conocidos como *firewall* de UTM son parte de la seguridad perimetral de la red que controla el tráfico entrante y saliente, decide qué tipo de tráfico es permitido o es bloqueado, por medio de la configuración de un conjunto definido de reglas de seguridad.

- *Firewall* de tercera generación: conocidos como NGFW, aparte de las funciones de un *firewall* tradicional, mediante el uso de software está diseñado para detectar *malware*, IPS, crear VPN, entre otras. Dispone de funciones de análisis minucioso del tráfico en la red, que son capaces de detectar y minimizar riesgos, problemas en la seguridad, operaciones sospechosas, fugas de datos, entre otros.

Las marcas de *firewall* Palo alto, Fortinet, Cisco y Ceck Point, según informe de Gartner a septiembre 2018, se pueden utilizar en la implementación de un perímetro de seguridad.

Figura 37. ***Firewalls* perimetrales**



Fuente: Fortinet. *Gartner reconoció a Fortinet como Líder en el Cuadrante Mágico 2019 para Firewalls de Red.* https://www.fortinet.com/solutions/gartner-enterprise-firewalls-mq.html#report. Consulta: 11 de junio de 2019.

5.7.11. Responsables de implementar

Los responsables de implementar los controles establecidos en la capa de la red son: infraestructura, administrador de red, riesgos, administrador de *firewall* y oficial de seguridad (ver tabla VI). Para su cumplimiento es importante que cada control sea asignado a un responsable del equipo propuesto, para implementación, control y monitoreo.

Luego de implementar los controles en capa de red, es necesario realizar evaluaciones periódicas por el departamento de riesgos a través de auditorías, para asegurar el nivel de cumplimiento a cada control y proponer mejoras a los procesos establecidos.

Tabla VI. **Responsables de implementar la capa de red**

Roles / Responsabilidades: **R**= Responsable, **A**= Aprobador, **C**= Consultado, **I**= Informado.

Actividad	Roles / Responsabilidades						
Nombre	Administrador de red	Administrador de firewall	Infraestructura	Riesgos	Oficial de seguridad	Director de tecnología	Gerencia General
Control de accesos a la red (NAC)	R	R			C		
Sistema de prevención de intrusos (IPS)	R	R	C		C		
Gestión de accesos remotos		R				I	I
Seguridad de las redes inalámbricas	R				R		
Hardening de configuraciones	R	R			C		
Filtrado de contenido web Proxy	R	R					
Diseño y segmentación de redes por capas	R	R					
Sistema de prevención de fuga de información (DLP)	R	R	R	I	R		
Firewalls perimetrales robustos capaz de detectar amenazas avanzadas		R				C	
Cumplimiento de controles	C		C	R	C,I	C,I	I

Fuente: elaboración propia.

5.8. Capa de usuarios finales

Pareciera que, por tratarse de personas, es la capa con más facilidad de controlar y la menos vulnerable. Sin embargo, esta es la capa que está más expuesta a los ataques debido a que los usuarios tienen interacción con otras personas, se trasladan a muchos lugares y son fáciles de engañar.

Los usuarios continuamente están en creando, modificando y transportando información. Dependiendo de las funciones que desempeñen en la institución

tienen acceso a información sensible de clientes, colaboradores y proveedores, que es la que buscan los atacantes.

Se debe prestar especial atención a los dispositivos móviles del personal de negocios; estos contienen información de los clientes. En un país como Guatemala son muy comunes los robos de estos dispositivos, lo que puede poner en peligro confidencialidad de los clientes y exponerlos a fraudes o extorciones.

Los colabores de una institución de microfinanzas utilizan diversos dispositivos de almacenamiento como laptops, memorias USB, teléfonos, entre otros, para almacenar bases de datos de clientes, fotografías de clientes, DPI, estados financieros, estados de cuentas que, de ser accedidos por una persona con malas intenciones, puede afectar a los clientes.

A diferencia de los usuarios normales, los usuarios con privilegios especiales, como los administradores o los altos directivos, son quienes están en la mira de los atacantes, ya que tienen acumulación de información y de accesos.

5.8.1. Riesgos relacionados con los usuarios

El objetivo de implementar los controles descritos en la capa de usuarios mejora la protección de los datos críticos que gestionan los usuarios de la institución de microfinanzas, con la finalidad de mitigar los riesgos siguientes:

- Fuga de información: es la extracción de información no autorizada de una persona, proceso o aplicación ajena o parte a la institución que no debería de tener acceso a esa información.

- Robo de información: extracción de información sensible que se encuentre en dispositivos móviles, con el fin de comercializar o realizar un fraude que afecta a la institución, a sus clientes, proveedores o colaboradores.

- Acceso no autorizado: dentro de la red el acceso no autorizado se puede dar cuando alguien vulnera un dispositivo a nivel de configuración, y puede monitorear todo el tráfico que la red transmite. Este riesgo compromete la información confidencial de forma fácil.

- Infección de dispositivos: si los empleados utilizan dispositivos propios que no disponen de las medidas de seguridad necesarias y está infectado pueden provocar que los dispositivos de la institución se infecten.

- Suplantación de identidad: es uno de los delitos que crece a pasos agigantados debido a la información que se encuentra en dispositivos móviles al ser robados o lo que se publica en redes sociales. Consiste en robar información sensible de una persona y luego utilizarla para suplantar la identidad financiera, hacer compras u obtener créditos.

- Ataques de *phishing:* son ataques dirigidos a través del correo electrónico donde a través de suplantación de sitios web solicitan a los usuarios información sensible ya sea personal, laboral o de clientes.

En esta capa se busca implementar medidas que ayuden a proteger a los usuarios y mitigar los riesgos en la seguridad de la información que es utilizada de forma recurrente, para lo cual se proponen los siguientes controles:

5.8.2. Educación a usuarios en seguridad de la información

Las instituciones de microfinanzas deben disponer de una plataforma web para realizar cursos en línea. Los cursos deben de estar diseñados con material didáctico preferible a través de videos, que permitan capacitar y certificar a todos los colaboradores.

Es necesario que se puedan capacitar a todo colaborador de nuevo ingreso a la institución y de forma periódica a todo el personal antiguo, comenzando con la alta dirección y usuarios con privilegios de administrador, quienes son los que mayor información poseen.

El material didáctico debe transmitir principalmente conocimiento de *phishing*, seguridad de contraseñas, ingeniería social, cómo proteger la información confidencial, los tipos de ataques comunes, el riesgo de publicar información sensible en redes sociales, entre otros. Se debe hacer conciencia que la información que manejan es valiosa.

Se debe monitorear constantemente el cumplimiento a estas capacitaciones y bloquear los accesos a los recursos informáticos a todo el colaborador que no logre obtener la certificación.

5.8.3. Gestión de actualizaciones de seguridad

Es importante disponer de una política de obsolescencia que defina los estándares de actualización de los diferentes dispositivos que utilizan los usuarios. Los fabricantes de software o hardware liberan actualizaciones de seguridad para sus equipos y es difícil que los usuarios finales estén aplicando estas actualizaciones.

A través de una o varias herramientas especializadas en manejo de actualizaciones es posible realizar liberaciones de nuevas versiones o parches de seguridad controladas de los distintos tipos softwares que se utilizan y lograr tener versiones estándar en toda la institución.

5.8.4. Seguridad del contenido

Es una capa de seguridad que tiene como objetivo detectar y mitigar ataques de inyección de código y *phishing.* Se utilizan herramientas como los antivirus, antimalware, antispam, IDS/IPS y firewall para detener este tipo de amenaza.

Las herramientas de software líderes en el mercado que se pueden utilizar para el manejo controlado del contenido se pueden visualizar en la siguiente ilustración:

Las herramientas de software Symantec, Trend Micro, Sophos, según informe de Gartner a enero del 2018, se pueden utilizar para el manejo de la seguridad de contenido

Si la institución de microfinanzas dispone de este tipo de dispositivos es importante mantenerlos configurados de forma correcta. Si la última versión de firmware o software instalada en los equipos no es la última disponible por el fabricante no debe de ser más antigua a dos versiones; esto ayuda mantener un perímetro de seguridad estable.

5.8.5. Políticas de seguridad para dispositivos móviles

En la actualidad, los dispositivos móviles deben ser administrados y controlados de la misma forma que se hace con computadora portátil, debido a que en estos dispositivos se almacenan una gran cantidad de información de clientes, colaboradores y proveedores, que es importante proteger.

Es necesario definir una política con las normas de seguridad que establezca los lineamientos para el control y manejo de dispositivos móviles dentro de la institución. Además, especificar acciones que se deben realizar caso de robo, obsolescencia y cambio de dispositivos.

Las instituciones de microfinanzas deben tener clara su estrategia sobre los dispositivos móviles, si se utilizarán únicamente dispositivos corporativos o se permitirá al uso de dispositivos propios de los empleados para realizar sus tareas asignadas dentro de la institución.

La estrategia definida permitirá establecer lineamientos de seguridad que ayuden a mitigar las vulnerabilidades en la información de los dispositivos móviles.

Los controles que definan deben contemplar manejo de altas y bajas, control de bloqueos para inicio de sesión, control de instalación de nuevas aplicaciones, debe permitir realizar eliminación de datos remoto en caso de robo o eliminación de datos en demasiados intentos de desbloqueo. Es importante tener un inventario de los dispositivos móviles que se utilicen.

Las herramientas MDM Microsoft Intune, Trend Micro Mobile, AirWatch pueden ayudar a automatizar el control de los aplicativos móviles.

5.8.6. BYOD (Bring Your Own Device)

Es una nueva tendencia que consiste en permitir a los colaboradores utilizar sus dispositivos móviles propios, para acceder a cualquiera de los recursos que la institución ofrece a empleados, con la finalidad de que desempeñe las funciones por las que fue contratado.

Que los colaboradores manejen información sensible en sus dispositivos personales incrementa el riesgo a vulnerar la información. Se necesita disponer de herramientas de software que ayuden a mantener la información de la institución protegida sin interferir con la información personal del usuario.

Las herramientas MAM como Microsoft y Intune, AirWatch implementan un repositorio dentro del dispositivo que es propio de la intuición y permiten controles específicos que ayudan a mantener resguardada la información, minimizando las posibilidades de que la información sea vulnerada.

5.8.7. Sistema de prevención de fuga de información (DLP)

Este control se encuentra descrito en la capa de datos sección (5.4.5) y es aplicable a la capa de usuarios.

Adicionalmente, se debe garantizar que del lado de dispositivos y de laptops el agente de DLP controle los bloqueos de dispositivos de almacenamiento, la información que envía y recibe por correo, las capturas de pantallas y los documentos que se están imprimiendo.

5.8.8. Sistema de clasificación y etiquetado de información

Este control se encuentra descrito en la capa de datos sección (5.4.4) y es aplicable a la capa de usuarios.

Los usuarios son los responsables de la adecuada clasificación de la información. Cada reporte y documento debe estar clasificado; por otro lado, se recomienda disponer de tecnología alineada a las políticas de clasificación de la información que asegure que lo que los usuarios realizan esté acorde a las políticas.

5.8.9. Solución de transferencia segura de información

La institución de microfinanzas debe disponer de herramientas digitales con licencia institucional para la transferencia de información y no utilizar herramientas públicas (Skype, WhatsApp, entre otros) para este propósito, debido a que en las herramientas publicas los usuarios no son controlados.

La información que se transporte por otros medios debe utilizar protocolos de encriptación como HTTPS o SFTP. Se debe de evitar transferir información por HTTP o FTP.

Se debe permitir a los usuarios el uso de carpetas compartidas o entre usuarios. Las transferencias de información siempre deben ser a través herramientas que manejan protocolos cifrados, garantizando que la transferencia de datos sea segura.

5.8.10. Responsables de implementar

Los responsables de implementar los controles establecidos en la capa de los usuarios son: gerencia general, riesgos, recursos humanos, oficial de seguridad (ver tabla VII). Para su cumplimiento es importante que cada control sea asignado a un responsable del equipo propuesto, para implementación, control y monitoreo.

Luego de implementar los controles en capa de usuarios, es necesario realizar evaluaciones periódicas por el departamento de riesgos, a través de auditorías, para asegurar el nivel de cumplimiento a cada control establecido y proponer mejoras a los procesos establecidos.

Tabla VII. **Responsables de implementar la capa de usuarios**

Roles / Responsabilidades: **R**= Responsable, **A**= Aprobador, **C**= Consultado, **I**= Informado.

Actividad	Roles / Responsabilidades					
Nombre	Recurso humano	Infraestructura	Riesgos	Oficial de seguridad	Director de tecnología	Gerencia General
Plataforma de entrenamiento de seguridad para usuarios finales, desarrolladores y administradores	C	R		C	I	
Gestión de actualizaciones de seguridad		R		C		
Seguridad del contenido		R			I	
Políticas de seguridad para dispositivos móviles		C	C	R	C	I
BYOD (Bring Your Own Device)		R	C	R		
Sistema de prevención de fuga de información (DLP)	R	R		R		
Sistema de clasificación y etiquetado de información			R	R		I
Antimalware avanzado		R		R		
Solución de transferencia segura de información		R		R		
Cumplimiento de controles	C	C	R	C,I	C,I	I

Fuente: elaboración propia.

5.9. Capa de monitoreo

El monitoreo de personas, procesos y aplicaciones permite tener visibilidad de los datos que se están generando y transmitiendo dentro de cada una de las capas planteadas. Esto permite asegurar el cumplimiento de los controles y posibles ajustes a los diseños establecidos.

Debido a la madurez de las instituciones de microfinanzas es la capa a la que se le pone menos atención para ser implementada, debido a que se requiere de trabajo continuo por el personal de tecnología y/o riesgos para cubrir los controles críticos por observar.

La importancia de implementar esta capa es que permite observar los controles definidos en las capas anteriores, lo que da la posibilidad de evaluar el desempeño de los controles. Si en la evaluación se encuentran debilidades es posible realizar mejoras.

Para implementar un área dedicada al monitoreo, es importante tener conocimientos de las opciones y tendencias que se ofrecen. Dependerá del presupuesto asignado si se implementa un centro de monitoreo interno o a través de una firma especializada.

Una de las tendencias actuales es la tercerización de los servicios de monitoreo a empresas con personal altamente calificado en el área de seguridad de la información y con servicio 7/24. Contrario a si se hace interno, se debe de disponer de personal capacitado y herramientas especializadas.

5.9.1. Riesgos relacionados a la falta de monitoreo

El objetivo de implementar los controles que se describen en la capa de monitoreo es ser proactivos en la protección de los datos críticos que son gestionados por las personas, procesos y aplicaciones de la institución de microfinanzas, con la finalidad de mitigar los riesgos siguientes:

- Robo de información: extracción de información sensible con el fin de comercializar o realizar un fraude que afecta a la institución, a sus clientes, proveedores o colaboradores.

- Infiltración de amenazas avanzadas: consiste en infiltrarse a través de software malicioso especializado, por un corto periodo en la red, en el cual se obtienen los accesos a la información que el atacante busca, incluso la que se considera inaccesible.

- Denegación de servicios: comúnmente esto ocurre cuando los atacantes inundan la red y generan una cantidad de transacciones que los equipos no pueden el acceso a los servicios que brindan a los usuarios.

- Comercialización de información de clientes: la competencia con malas prácticas se da en el sector de microfinanzas. Existen instituciones que motivan económicamente a los colaboradores de la competencia para que brinden las carteras de clientes, lo que genera pérdidas económicas.

- Incumplimiento en controles de seguridad: implementar nuevos controles es una tarea rutinaria dentro de cualquier institución; sin embargo, por falta de monitoreo, estos controles quedan sin cumplimiento y no mitigan la alteración de configuraciones: un usuario no autorizado que dispone de

permisos para alterar las configuraciones en los sistemas operativos, tiene la capacidad para deshabilitar funciones de protección e instalar herramientas de monitoreo que no serían identificadas por otros sistemas de protección.

- Disponibilidad de los servicios instalados: denegación de servicios a aplicaciones por cambios en las configuraciones o el bloqueo de puertos podrían hacer que la institución detenga sus operaciones por un tiempo indeterminado.

- Bloqueo de acceso a la información: bloquear las máquinas a través de software malicioso puede causar daños críticos que impedirían acceder a la información que es secuestrada, hasta pagar un rescate. El gasto del rescate dependerá de cuántos equipos sean infectados, dejando un problema reputacional e inseguridad sobre la institución.

- Alteración en información: las vulnerabilidades en sistemas operativos pueden dar permisos necesarios a personas, procesos y aplicaciones a que tengan la capacidad de modificar la configuración de cualquier archivo a su conveniencia, con el fin de tener acceso a información sensible.

Con la finalidad de mitigar los riesgos expuestos se propone la implementación de una serie de controles diseñados con base en las mejores prácticas y estándares internacionales.

5.9.2. Monitoreo de integridad de datos

Es importante garantizar que los datos (de clientes, proveedores, colaboradores y archivos de configuración) no sufran cambios de forma accidental o mal intencionado por personas, aplicaciones o procesos no autorizados, cuando se encuentren almacenados en cualquier medio.

El estándar PCI DSS, dentro de sus requerimientos hace referencia a utilizar una herramienta de software (por ejemplo, Snare) que ayude a monitorear la integridad de los datos, generando alertas que ayuden a identificar cualquier tipo de modificación no autorizada a los sistemas de la institución que se definan como críticos.

Se debe integrar con el monitoreo de actividad de bases de datos (sección 5.4.6) especificado en la capa de datos.

Se recomienda que las validaciones relacionadas a la integridad de los datos se realicen por lo menos una vez a la semana y cubran archivos de parámetros de configuración y registros de auditoría.

5.9.3. Recolector de log para el reenvío de eventos

Es una herramienta que permite unificar los log de los sucesos que ocurren en los datos, las aplicaciones, la red y sistemas operativos. Permite dar visibilidad a eventos que ocurren y por lo regular pasan desapercibidos para los equipos de seguridad de la información.

Es importante contar con un equipo humano capacitado para la administración y manejo de las herramientas de software implementadas; esto

ayudará a explotar de manera efectiva la información que se recolecta de las diferentes capas que se proponen en el modelo.

Las tecnologías Splunk, IBM, LogRhythm, Dell (RSA), Exabeam y McAfee, según informe de Gartner a octubre 2018; se pueden utilizar para el monitoreo de log.

Figura 38. **Sistemas de manejo de Log**

Fuente: Bankinfo Security. *Gartner Magic Quadrant 2018 para SIEM.* https://www.bankinfosecurity.com/whitepapers/2018-gartner-magic-quadrant-for-siem-w-5170. Consulta: 11 de junio de 2019.

5.9.4. SOC (Centro de Operaciones de Seguridad)

Con el objetivo de garantizar la confidencialidad, integridad y disponibilidad de la información que se transmite en la red y se almacena en los servidores, se debe monitorear para anticipar, detectar y responder a amenazas que se identifican como sospechosas.

Trasladar la responsabilidad del monitoreo de la seguridad a una empresa especializada se ha convertido en una tendencia, debido a los servicios atractivos que prometen los proveedores. Se traduce en una baja inversión de las instituciones por delegar la responsabilidad a un tercero.

Las empresas proveedoras dedicadas a la seguridad informática son especialistas en esta área, por lo que dedican recursos a la actualización y seguimiento de nuevas tecnologías relacionadas con riesgos y seguridad.

La institución de microfinanzas no tiene que invertir en personal interno altamente capacitado al cual debe capacitar periódicamente, situación que disminuye los costos sin perder la calidad de servicio debido a los acuerdos entre ambas instituciones (SLA).

Los SOC son centros de servicio 7/24 por 365 que notifican a las áreas de seguridad de la información y tecnología cualquier incidente que se detecte y puede atentar contra la seguridad de la información.

5.9.5. Revisión de fuentes externas (noticias, boletines)

Se debe tener acceso a diferentes fuentes de tecnología que informen de forma periódica de fallas a la seguridad en temas de tecnología como nuevos

parches de seguridad, vulnerabilidades detectadas a las aplicaciones, capacitaciones, nuevas tecnologías, entre otros.

Las personas asignadas a la seguridad de la información y de tecnología deben estar suscritas a las fuentes de información que les provean actualizaciones de forma periódica.

5.9.6. Servicio de monitoreo de fraudes

Las instituciones de microfinanzas se encuentran expuestas a la posibilidad de fraude en los diferentes servicios que prestan a los clientes, poniendo en peligro la integridad de los datos de los clientes y a la misma institución en temas de reputación y salud financiera.

El fraude comúnmente es provocado por la fuerza laboral de la institución, en los casos donde se realizan desembolsos a clientes que no existen, cobro de comisiones no oficiales por otorgar préstamos, recibir dinero de clientes donde se emite un recibo que no es reportado, el cajero puede revertir pagos y quedarse con el efectivo, entre otros.

Monitorear y generar alertas por medio de una base de conocimiento de fraudes conocidos a través del tiempo, logra a mitigar la ocurrencia. Además, de implementar controles que generen alertas en tiempo real por medio de aplicaciones de software.

Existen herramientas tecnológicas como Monitor Plus y Businessware que pueden ayudar a automatizar el control de transacciones en tiempo real y generar alertas al momento de encontrar inconsistencias en las transacciones que pueden evitar fraudes.

5.9.7. Evaluación periódica de vulnerabilidades

De forma periódica se debe generar análisis automáticos sobre las vulnerabilidades y pruebas de penetración a la infraestructura y a los colaboradores mediante pruebas de *phishing.*

Estas evaluaciones son capaces de ayudar a las instituciones de microfinanzas a comprobar la efectividad y madurez de los procesos establecidos, a desarrollar planes de acción para mejorar en las áreas débiles y representen un riesgo para la seguridad de la información.

Es recomendable realizar los escaneos de vulnerabilidades de forma trimestral y las pruebas de penetración cada 6 meses o bien cada año, como mínimo.

5.9.8. Ampliar el monitoreo de integridad para todas las bases de datos

Dentro de las instituciones de microfinanzas hay varias bases de datos (Core Banking, recursos humanos, planillas, entre otros) que ayudan a las operaciones diarias y contienen información confidencial, por lo que deben ser integradas a un sistema de monitoreo. Este control se complementa con el control y monitoreo de actividad de las bases de datos (sección 5.4.6) especificado en la capa de datos.

Los motores de bases de datos (DBMS) en general, cuentan con variedad de opciones para activar la configuración de pistas de auditoría (encargadas de dar visibilidad a los eventos de la base de datos). Estas ayudan a generar los log que se producen dentro de los sistemas de bases de datos.

Las pistas de auditorías deben ser almacenadas en un sistema externo con la capacidad de monitorear y generar alertas cuando se detecten actividades inusuales o sospechosas dentro de las bases de datos y permitan identificar a las personas, aplicaciones o procesos que intenten alterar la información sin las autorizaciones correspondientes.

5.9.9. SOC–CERT que cumpla con los requerimientos de monitoreo establecidos

Un SOC no es suficiente para resolver incidentes de seguridad; se necesita un soporte especializado que ayude al equipo de tecnología a resolver vulnerabilidades relacionadas con la seguridad de la información y realizar análisis forenses a sistemas comprometidos.

Las instituciones de microfinanzas pueden contratar los servicios especializados de SOC-CERT mediante contratos de forma anual, por un bolsón de horas o por una cantidad de eventos al año o por mes, o en caso de ocurrir un incidente de seguridad.

Un SOC-CERT como parte de la prevención mantiene vigilancia sobre amenazas de seguridad a la información que están ocurriendo a nivel país o bien a nivel internacional, lo que les da ventaja para resolver incidentes al ser solicitados.

5.9.10. Monitoreo reputacional

El riesgo reputacional puede impactar de manera negativa a una institución en el entorno social, limita la capacidad para generar negocios y causa problemas a la imagen institucional. Es provocada por brindar un mal servicio al cliente, caer

en delitos regulatorios, evasión de impuestos, cobros excesivos, cuando estos se dan en radio, televisión o redes sociales.

Como práctica recomendada se debe monitorear de forma periódica los comentarios que se realizan a la entidad de microfinanzas en las principales fuentes de información (dominios, logos, cuentas de correos, la marca de la empresa) por medio de un software especializado, que identifique la información que puede ser perjudicial y de la cual no se tenga conocimiento.

Se debe tener en cuenta que la mayor fuente de información está en la Red Oscura, que es donde está la información buscadores web no muestran y es donde circula la infracción de cuentas que se pudieron haber robado, datos de clientes, intentos de ataques.

Con base en los datos recolectados a través del monitoreo y el análisis se puede reaccionar de forma rápida y generar planes de acción que ayuden a identificar los riesgos claves relacionados al reputacional (KRRI) con el fin de mitigarlos.

5.9.11. Responsables de implementar

Los responsables de implementar los controles establecidos en la capa de monitoreo son: gerencia general, riesgos, infraestructura, oficial de seguridad (ver tabla VIII). Para su cumplimiento es importante que cada control sea asignado a un responsable del equipo propuesto, para implementación, control y monitoreo.

Luego de implementar los controles en capa de monitoreo, es necesario realizar evaluaciones periódicas por el departamento de riesgos a través de

auditorías, para asegurar el nivel de cumplimiento a cada control establecido y proponer mejoras a los procesos establecidos.

Tabla VIII. **Responsable de implementar la capa de monitoreo**

Roles / Responsabilidades: **R**= Responsable, **A**= Aprobador, **C**= Consultado, **I**= Informado.

Actividad	Roles / Responsabilidades				
Nombre	Infraestructura	Riesgos	Oficial de seguridad	Director de tecnología	Gerencia General
Monitoreo de integridad de datos	R		R	I	
SOC (Centro de Operaciones de Seguridad para red, servidores)		R			I
Revisión de fuentes externas (noticias, boletines)	R	R			I
Servicio de monitoreo de fraudes		R			I
Evaluación de vulnerabilidades periódicamente		R	R		I
Ampliar el monitoreo de integridad para todas las bases			R	I	
SOC-CERT que cumpla con los requerimientos de monitoreo establecidos		R			I
Monitoreo reputacional		R			I
Recolector de logs para el reenvío de eventos a SOC		R	R		I
Tercerización de monitoreo de seguridad		R			I
Cumplimiento de controles	C	R	C,I	C,I	I

Fuente: elaboración propia.

5.10. Gobernanza

En la gobernanza está la clave para implementar con éxito un modelo de seguridad de la información. Una dirección comprometida con la estrategia de seguridad centra sus esfuerzos para que cada colaborador dentro de la institución tome conciencia de la importancia de la información.

A diferencia de las capas anteriores que son enfocadas a temas técnicos, esta capa busca mejoras a la gestión institucional que involucra a personas, procesos y tecnología.

Es necesario definir políticas de seguridad de la información acordes a la realidad y estrategia institucional para cumplir con los estándares que se establezcan. Estos estándares deben ser monitoreados y puestos a prueba periódicamente para identificar los niveles de cumplimiento.

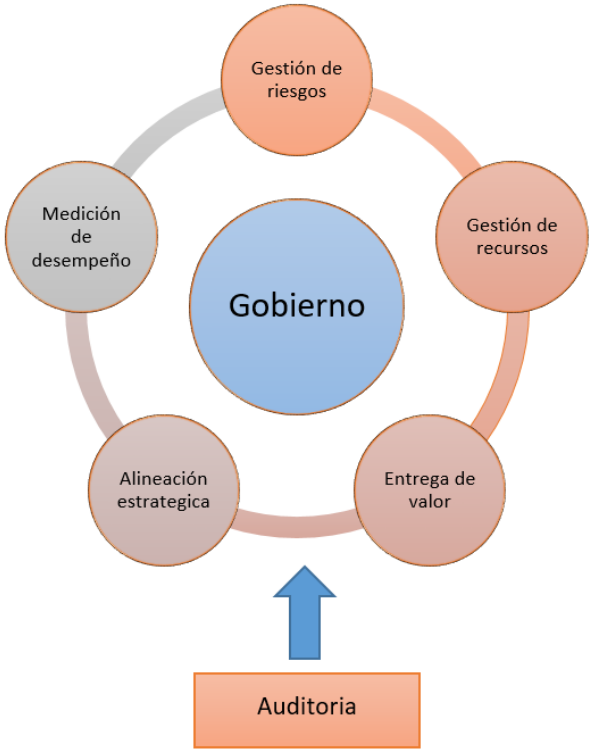
La cultura organizacional sobre seguridad de la información tiene más probabilidad de ser exitosa dentro de una institución de microfinanzas si es liderada desde la gerencia general.

Es recomendable que todos los empleados sean capacitados periódicamente a través de cursos en línea, preparados especialmente para la realidad de la institución de microfinanzas. Los cursos deben estar dirigidos a todo el personal, sin excepciones.

Para una mejora continua en la seguridad de la información se recomienda realizar evaluaciones periódicas a las personas, procesos y tecnología, debido a que estos van quedando desactualizados con el pasar del tiempo y es necesario actualizar y reforzar de acuerdo a las necesidades del momento.

A los nuevos proyectos o productos que la institución implemente, es importante se les pueda realizar un análisis de riesgos desde un inicio, por parte del departamento de riesgo y seguridad de la información, con la finalidad de identificar riesgos mitigados en las etapas de desarrollo o implementación.

Figura 39. **Gestión del gobierno de una institución de microfinanzas**



Fuente: Instituto tecnológico de Yucatán. *Gestión del gobierno*. http://izrammstein.blogspot.com/p/17-proceso-de-implantacion-del-gobierno.html. Consulta: 3 de mayo de 2019.

5.10.1. Gobierno de seguridad de la información

El gobierno de seguridad de la información es un derivado del gobierno institucional que tiene como objetivo proporcionar una dirección estratégica para la seguridad de la información, alineado con los objetivos del negocio y asegurando la efectiva gestión del riesgo.

La norma ISO 27014 recomienda seis principios sobre los cuales debe de alinearse el gobierno de seguridad de la información (Anexo B). Estos principios

establecen y definen el apetito de riesgo que la institución está o debería estar dispuesta a sacrificar en temas de costos y riesgos.

Entre las funciones del gobierno de seguridad de la información se encuentra la concientización de los colaboradores en temas de seguridad, asignar los recursos necesarios para la gestión de riesgo, definir las inversiones sobre la seguridad de la información, crear políticas, realizar auditorías independientes, evaluar los niveles de riesgo.

El gobierno de seguridad de la información debe ser el responsable directo de la cultura organizacional de seguridad de la información dentro de la institución y de que todos los colaboradores sean parte de ella.

5.10.2. Adopción de estándares de seguridad

Los estándares de seguridad contienen normas y procedimientos que han tomado auge y cada día son adoptadas por más instituciones, lo que los hace confiables y efectivos, con una alta probabilidad de éxito de funcionar en las instituciones que desea implementarlas.

Es conveniente que las instituciones tengan establecido un estándar de seguridad como la norma ISO 27001, si no en la totalidad de sus controles, en los que se adapten al giro de negocio, lo que permitiría mitigar los riesgos en las diferentes áreas.

Si se carece de un estándar de seguridad de la información, es importante que se establezca dentro del plan estratégico institucional (se necesita compromiso por la gerencia general) y se le asigne presupuesto para que se

implemente dentro de un periodo no mayor a 3 años, tiempo suficiente para lograr una organización con cultura de seguridad de la información.

5.10.3. Evaluación y rediseño de procesos

Las instituciones de microfinanzas tienen establecidos diferentes procesos para las actividades de negocio y los procesos críticos, los cuales ayudan a establecer la forma de realizar las tareas cotidianas. Entre los procesos que se tienen existen procesos nuevos y otros que tienen años de haber sido implementados.

Por lo general, los procesos luego de ser implementados no son evaluados de forma periódica, con el objetivo de asegurar su eficiencia, que no haya procesos que con el paso del tiempo se hallan vuelto obsoleto.

Las instituciones de microfinanzas están evolucionando constantemente en su forma de hacer negocios y su relación con sus clientes, con procesos obsoletos se pone en riesgo la seguridad de la información.

Se sugiere que el área encargada de establecer los procesos, riesgos, seguridad de la información evalúe de forma periódica los procesos establecidos que involucran personas y tecnología. La evaluación identificará los procesos que necesitan rediseño o los que son obsoletos.

5.10.4. Seguridad en nuevos productos y servicios

En la creación de nuevos productos y servicios se definen las necesidades del área de negocios y de operaciones, se estiman los tiempos y el presupuesto

necesarios para crear o implementar el nuevo producto y servicio. No se involucran las áreas que miden el riesgo.

Es importante que las áreas de riesgos, seguridad de la información, legal y tecnología estén involucrados en las nuevas iniciativas, por lo menos en la fase inicial. Esto ayuda a identificar los riesgos en la seguridad de la información y el impacto que tendrá en los tiempos y el presupuesto para crear o desarrollar.

Se sugiere identificar que la institución disponga de una matriz (aprobada por el gobierno de seguridad) de riesgos que ayude a asignar el nivel de riesgo de acuerdo a la criticidad y probabilidad de ocurrencia.

5.10.5. Gestión de riesgos y respuesta a incidentes

Toda institución debe tener en claro que el riesgo es inherente a las personas, procesos y tecnología y es imposible evitar en un 100 %. Por esta razón se debe implementar una cultura de seguridad de la información que en todo momento esté en alerta a identificar riesgos operacionales y tecnológicos con la finalidad de mitigarlos.

Cada área dentro dela institución debe identificar los riesgos que correspondan a personas, procesos y tecnología asociados a las funciones de las cuales son responsables, con el objetivo de definir una ruta crítica que ayude a mitigarlos en un corto plazo.

Según el apetito de riesgo que la institución esté dispuesta a tolerar, hay riesgos que se deben aceptar; sin embargo, siempre deben de ser monitoreados y evaluados.

5.10.6. Cultura de seguridad de la información

Una cultura de seguridad de la información es la vivencia que tienen las personas que interactúan con la información (en procesos y tecnología), en la cual cada uno esta consiente de la responsabilidad e importancia de la seguridad de la información.

La cultura de seguridad genera una inteligencia emocional en las personas que las prepara para actuar y razonar para mitigar cualquier vulnerabilidad que ponga en riesgo la información.

Para implementar una cultura de seguridad de la información se sugiere aplicar mecanismos que hagan conciencia a las personas de la importancia de la información en campañas que contengan boletines, notificaciones, carteles evaluaciones, cursos todos relacionados a seguridad de la información.

CONCLUSIONES

1. La inclusión financiera que han logrado las instituciones de microfinanzas en sectores de la población que tiene acceso a un crédito bancario, en el 2017 a 2018 ha crecido un 10 % (volumen de cartera) y un 3,5 % (en clientes), según información de la Red de Microfinanzas de Guatemala -REDIMIF-. Este crecimiento ha necesitado la implementación de nuevas tecnologías para administrar el aumento de la cartera de clientes. La tecnología móvil se ha convertido en una herramienta poderosa para el personal que trabaja en campo. Este crecimiento ha dado lugar a que en el congreso de la república de Guatemala en enero 2018 se apruebe la Ley de Entidades de microfinanzas y Entes de microfinanzas sin fines de lucro -ley 25-2016- que ayuda a la Superintendencia de Bancos -SIB- a regular esta actividad económica. Al día de hoy ninguna institución de microfinanzas se ha adherido a esta ley, probablemente debido a los requisitos monetarios y regulaciones impuestas por la Superintendencia de Bancos -SIB-.

2. Los casos de fraudes cibernéticos se hacen visibles con más frecuencia en la región de América Latina. De los casos sobresalientes en el 2018 se puede mencionar al sistema interbancario de México, con un robo de 10 millones, y el Banco de Chile, que sufrió pérdidas por más de 40 millones de dólares cuando un grupo de atacantes realizo transacciones a bancos de China. Los principales riesgos identificados están relacionados al robo de información, fuga de información, fraudes y estafas para lo que comúnmente los atacantes utilizan ataques como: denegación de servicios, *ransomwer, spam, phishing* donde según información de

Kaspersky el 73,93 %. Los ataques están dirigidos a instituciones de servicios financieros y sus clientes.

3. Los principales estándares de seguridad han tomado auge en las instituciones financieras, en especial en el sistema bancario. Estándares como COBIT dirigido a la supervisión y gestión de la información y de tecnología e ISO 27001 permite la disponibilidad, integridad y confidencialidad de la información, PCI DSS orientado a la protección de datos de tarjetas de pago. En el 2017, según la Organización Internacional de Estandarización -ISO-, en América Latina al 2017 habrían 935 instituciones certificadas con la norma ISO 27001, de las cuales 315 son de México, 170 de de Brasil y 148 de Colombia. En Guatemala a la misma fecha habría 6 instituciones, de las cuales ninguna pertenece a las instituciones de microfinanzas. Aunque hay adelantos en la región, falta para alcanzar a países como Japón, que en el 2017 tenía 9,161 instituciones certificadas con la norma ISO 27001.

4. Se propone un modelo de seguridad de la información tecnológico, que consta de 6 capas, las cuales son: capa de datos (clasificación de los datos y seguridad en almacenamiento de datos), capa de aplicaciones (administración, configuración, autentificación y desarrollo de aplicaciones), capa de sistemas operativos (administración, configuración, prevención de fuga de información y monitoreo en el cambio de archivos sensibles), capa de red (seguridad en el transporte de los datos), capa de usuarios finales (gestión y control de los datos utilizados por los usuarios), capa de monitoreo (controles para el monitoreo de los controles de las capas establecidas). En cada una de las capas se identifican riesgos y se detallan los controles necesarios para mitigar dichos riesgos. El modelo debe estar soportado por una gobernanza con el compromiso de adoptar

estándares de seguridad, evaluación de los controles establecidos y establecer una cultura organizacional de seguridad de la información. El modelo propuesto es una guía que las instituciones de microfinanzas pueden adoptar para proteger la información de los clientes, proveedores y colaboradores; está basado en una recopilación de buenas prácticas de seguridad y puede implementarse de forma escalable.

RECOMENDACIONES

1. Considerar las estadísticas de crecimiento y la creación de la nueva la ley de microfinanzas, se recomienda a las instituciones de microfinanzas iniciar un proceso de diagnóstico y evaluación para preparar los requisitos financieros y tecnológicos que les permitan la adición a la nueva ley como una microfinanciera de ahorro y crédito (MAC) o una microfinanciera de inversiones y crédito (MIC).

2. Que las instituciones de microfinanzas efectúen un análisis anual de riesgos, orientados a la seguridad información que incluya personas procesos y tecnología. Deben estar actualizadas en lo referente a las nuevas amenazas de índole tecnológico que puedan representar algún riesgo la seguridad de la información en la institución.

3. Que las entidades de microfinanzas adopten las buenas prácticas de seguridad establecidas en los estándares Cobit, ISO 207001 y PCI DSS con la finalidad de obtener una certificación ISO 27001 que permita mitigar los riesgos en la seguridad de la información. Desarrollar una gobernanza que implemente en las instituciones una cultura de seguridad de la información y mida la efectividad de los controles implementados mediante programas de auditorías periódicas bajo los estándares COBIT, ISO 27001 y PCI DSS.

4. Que las instituciones de microfinanzas adopten los controles propuestos en el modelo, los cuales pueden ser implementados de acuerdo con las necesidades y presupuestos de las instituciones mencionadas. Para la implementación debe haber un compromiso de la alta dirección y asegurar controles que se implementen sean medibles y auditables para garantizar la efectividad.

BIBLIOGRAFÍA

1. Advanced Persistent Threat. *Qué es una APT*. [en línea]. <http://www.christiandve.com/2018/05/que-es-apt-advanced-persistent-threat-protegerse/>. [Consulta: 02 de mayo de 2019].

2. AENOR ediciones. *Guía de aplicación de la Norma UNE-ISO/IEC 27001 sobre seguridad en sistemas de información para pymes*. [en línea]. <http://www.varios.cen7dias.es/documentos/documentos/90/iso.pdf>. [Consulta: 15 de marzo de 2019].

3. Avast. *Definición de Phising*. [en línea]. <https://www.avast.com/es-es/c-phishing>. [Consulta: 29 de marzo de 2019].

4. _____. *Definición de Spam*. [en línea]. <https://www.avast.com/c-spam>. [Consulta: 29 de marzo de 2019].

5. _____. *Ransonwere* [en línea]. <https://www.avast.com/es-es/c-ransomware>. [Consulta: 23 de marzo de 2019].

6. Banco mundial. *Entendiendo la pobreza*. [en línea]. <http://www.bancomundial.org/es/topic/financialinclusion/overview>. [Consulta: 10 de marzo de 2019].

7. Banguat. *Junta Monetaria de Guatemala*. [en línea]. <http://www.banguat.gob.gt/inc/ver.asp?id=/Publica/leyaccesoalainfo/indexjm.htm>. [Consulta: 13 de marzo de 2019].

8. _____. *Ley contra el lavado de dinero y otros activos* [en línea]. <http://www.banguat.gob.gt/leyes/2002/lavado.pdf>. [Consulta: 12 de abril de 2019].

9. _____. *Miembros de Junta Monetaria de Guatemala*. [en línea]. <http://www.banguat.gob.gt/inc/ver.asp?id=/Publica/leyaccesoalainfo/indexjm.htm>. [Consulta: 13 de marzo de 2019].

10. BANRURAL, Grameen Bank en Guatemala. *Banco de los pobres*. [en línea]. <https://www.facebook.com/pg/Banrural-Grameen-Guatemala-137250376289611/about/?ref=page_internal/>. [Consulta: 10 de marzo de 2019].

11. BBC. *Fraudes con tarjetas de crédito*. [en línea]. <https://www.bbc.com/mundo/vert-cap-40638275>. [Consulta: 20 de marzo de 2019].

12. _____. *Noticias Ransomwer*. [en línea]. <https://www.bbc.com/mundo/noticias-36905385>. [Consulta: 23 de marzo de 2019].

13. Biblioteca Usac. *Auditoría externa de cuentas por cobrear en una institución de microfinanzas*. [en línea]. <http://biblioteca.usac.edu.gt/tesis/03/03_4547.pdf>. [Consulta: 8 de marzo de 2019].

14. Binance Academy. *Encriptación Simétrica vs. Asimétrica.* [en línea]. <https://www.binance.vision/es/security/symmetric-vs-asymmetric-encryption>. [Consulta: 23 de abril de 20].

15. Calidificacion Gartner. *Gestión de accesos BeyondTrust*. [en línea]. <https://www.beyondtrust.com/blog/entry/beyondtrust-named-a-leader-in-first-ever-gartner-magic-quadrant-for-privileged-access-management>. [Consulta: 28 de abril de 2019].

16. CIS*. Centro de seguridad de internet*. [en línea]. <https://www.cisecurity.org/>. [Consulta: 29 de abril de 2019].

17. COBIT. *Documentación COBIT español*. [en línea]. <https://www.isaca.org/cobit>. [Consulta: 15 de marzo de 2019].

18. CVSS. *Sistema de puntuación de vulnerabilidad*. [en línea]. <https://www.first.org/cvss>. [Consulta: 26 de abril de 2019].

19. Dolitte. *La importancia de los reportes de Transacciones sospechosas*. [en línea]. <http://www.ebg.edu.gt/oldSite/wp-content/files_mf/1468950515Patriciachacon.pdf>. [Consulta: 12 de abril de 2019].

20. El Periódico. *Guatemala Inversión en tecnología.* [en línea]. <https://elperiodico.com.gt/inversion/2017/10/19/region-debe-invertir-en-tecnologia-e-innovacion>. [Consulta: 12 de abril de 2019].

21. _____. *Robo al banco de Bangladesh*. [en línea]. <https:// www.elperiodico.com/es/sociedad/20161230/el-mayor-ciberatraco-del-mundo-tuvo-topos-en-el-banco-5696007>. [Consulta: 12 de abril de 2019].

22. Enciclopedia Kaspersky. *Denegación de servicios*. [en línea]. <https://encyclopedia.kaspersky.com/glossary/dos-denial-of-service-attack/>. [Consulta: 22 de marzo de 2019].

23. eSecurity Planet. *Soluciones tecnologías para manejo de parches*. [en línea]. <https://www.esecurityplanet.com/products/top-patch-managemen t-solutions.html>. [Consulta: 29 de abril de 2019].

24. ESET. *Guía de doble autentificación*. [en línea]. <https://www.welivesecurity.com/wp-content/uploads/2014/01/guia-autenticacion-eset.pdf>. [Consulta: 28 de abril de 2019].

25. _____. *Principio del menor privilegio.* [en línea]. <https://www.welivesecurity.com/la-es/2018/06/08/principio-menor-privilegio-limitar-acceso-imprescindible>. [Consulta: 24 de abril de 2019].

26. Gartner. *Protección para dispositivos móviles*. [en línea]. <https://www.tecnozero.com/wp-content/uploads/2018/01/gartner-guia-2017.pdf>. [Consulta: 23 de abril de 2019].

27. _____. *Puntación de herramientas de clasificación de información*. [en línea]. <https://www.pcihispano.com/ ?descargas=40465>. [Consulta: 24 de abril de 2019].

28. Google. *Sitios WEB no seguros*. [en línea]. <https://support.google.com/chrome/answer/99020?co=GENIE.Platform%3DDesktop&hl=es-419>. [Consulta: 29 de marzo de 2019].

29. Grameen Bank. *Banco de los pobres*. [en línea]. <http://www.grameen.com>. [Consulta: 8 de marzo de 2019].

30. GUERRERO MILÍAN, Joaquín Adolfo. *Plan estratégico para la implementación de un sistema de telemedicina nacional*. Trabajo de graduación de Ing. en Ciencias y Sistemas. Facultad de Ingeniería, Universidad de San Carlos de Guatemala, 2011. 54 p.

31. ISACA. *Riesgo reputacional*. [en línea]. <http://m.isaca.org/chapters12/costa-rica/events/Documents/Presentaciones% 20congreso%20Isaca%202016/11.%20El%20riesgo%20reputacional%20en%20el%20entorno%20estrat%C3%A9gico.pdf>. [Consulta: 05 de mayo de 2019].

32. Isec Auditor*. Consultores de seguridad*. [en línea]. <https://www.isecauditors.com/implantacion-pci-dss>. [Consulta: 21 de marzo de 2019].

33. ISO. *Recursos y respuestas ISO.* [en línea]. <https://www.iso.org>. [Consulta: 15 de marzo de 2019].

34. ISO 27000. *El portal de ISO 27001 en español*. [en línea]. <http://www.iso27000.es/otros.html#seccion2>. [Consulta: 13 de marzo de 2019].

35. ISO 27001 Academy. *Risk Assessment and Treatment process.* [en línea]. <https://info.advisera.com/hubfs/27001Academy/27001Academy_FreeDownloads/Diagram_of_ISO_ 27001_risk_

assessment_and_treatment_process_EN.pdf>. [Consulta: 15 de marzo de 2019].

36. ISO Tools. *Como clasificar la información según ISO 207001*. [en línea]. <https://elperiodico.com.gt/inversion/2017/10/19/region-debe-invertir-en-tecnologia-e-innovacion>. [Consulta: 20 de abril de 2019].

37. IVE. *Intendencia de verificación especial*. [en línea]. <https://www.sib.gob.gt/web/sib/lavado_activos/funciones-IVE>. [Consulta: 12 de abril de 2019].

38. Kaspersky. *Definición de Phising.* [en línea]. <https://latam.kaspersky.com/resource-center/preemptive-safety/what-is-phishing-and-how-does-it-affect-email-users>. [Consulta: 29 de marzo de 2019].

39. _____. *Estadísticas sobre Spam.* [en línea]. <https://securelist.lat/spam-and-phishing-in-2018/88487/>. [Consulta: 29 de marzo de 2019].

40. _____. *SecureList ramsomwere.* [en línea]. <https://securelist.lat/ransomware-and-malicious-crypto-miners-in-2016-2018/87155>. [Consulta: 23 de marzo de 2019].

41. _____. *Ransonwere.* [en línea]. <https://latam.kaspersky.com/resource-center/definitions/what-is-ransomware>. [Consulta: 22 de marzo de 2019].

42. KirkpatrickpPrice. *Vulnerabilidades comunes de codificación*. [en línea]. <https://kirkpatrickprice.com/video/pci-requirement-6-5-address-common-coding-vulnerabilities-software-development-processes/>. [Consulta: 26 de abril de 2019].

43. Libros Google. *Emerging financial markets in the global economy*. [en línea]. <https://books.google.com.gt/books?id=oSUsTnevzWoC&pg=PA63&lpg=PA63&dq=Behrenbach+y+Churchill&source=bl&ots=4VffEMs3A6&sig=IgecPPoYsDWbgrepyvH->. [Consulta: 13 de marzo de 2019].

44. MINECO. *Microfinanzas*. [en línea]. <https://www.mineco.gob.gt/sites/default/files/MIPYMES/ley_microfinanzas.pdf>. [Consulta: 13 de marzo de 2019].

45. Mingob. *Estrategia de seguridad cibernética*. [en línea]. <http://uip.mingob.gob.gt/wp-content/uploads/2019/03/Estrategia-Nacional-de-Seguridad-Cibern%C3%A9tica.pdf>. [Consulta: 29 de marzo de 2019].

46. Noticias Kaspersky. *Denegación de servicios.* [en línea]. <https://www.avast.com/es-es/c-ransomware>. [Consulta: 23 de marzo de 2019].

47. Oficina de Seguridad Internauta. *¿Qué son los ataque DOS y DDOS?* [en línea]. <https://www.osi.es/es/actualidad/blog/2018/08/21/que-son-los-ataques-dos-y-ddos>. [Consulta: 23 de marzo de 2019].

48. Oro y finanzas. *Grupo de acción financiera internacional.* [en línea]. <https://www.oroyfinanzas.com/2015/05/que-es-grupo-accion-financiera-internacional-gafi-financial-action-task-force-fatf/>. [Consulta: 12 de abril de 2019].

49. Ostec blog. *Firewall de última generación*. [en línea]. <https://ostec.blog/es/seguridad-perimetral/firewall-utm-ngfw-diferencia>. [Consulta: 29 de abril de 2019].

50. OWASP. *Seguridad de aplicaciones*. [en línea]. <https://www.owasp.org/index.php/Main_Page>. [Consulta: 28 de abril de 2019].

51. PCI. *Guías PCI DSS*. [en línea]. <https://www.pcisecurity standards.org/document_library>. [Consulta: 20 de marzo de 2019].

52. _____. *Monitor de integridad de archivos.* [en línea]. <http://www.christiandve.com/2018/05/que-es-apt-advanced-persistent-threat-protegerse/>. [Consulta: 02 de mayo de 2019].

53. _____. *Resumen PCI DSS*. [en línea]. <https:// www.pcisecuritystandards.org/documents/PCI_DSS_Summary_of _Changes_3-2-1.pdf?agreement=true&time=1561740770765>. [Consulta: 21 de marzo de 2019].

54. PCIDSS. *Hardening guia V3.2* [en línea]. <https://www.pcihispano.com/?descargas=40465>. [Consulta: 23 de abril de 2019].

55. PERÉZ JIRÓN, Ana Virginia. *Prácticas internacionales para la auditoria de gestión de tecnología de la información*. Trabajo de graduación de Ing. en Ciencias y Sistemas. Facultad de Ingeniería, Universidad de San Carlos de Guatemala, 2013. 20 p.

56. Redes zone. *Escaneo de vulnerabilidades de aplicaciones*. [en línea]. <https://www.redeszone.net/2018/12/01/escaneres-vulnerabilidades-auditar-software>. [Consulta: 28 de abril de 2019].

57. Redimif*. Red Centro Americana y del Caribe de Microfinanzas*. [en línea]. <http://redimif.org>. [Consulta: 13 de marzo de 2019].

58. _____. *Red de instituciones de Microfinanzas de Guatemala*. [en línea]. <http://redimif.org>. [Consulta: 13 de marzo de 2019].

59. SGSI. *Blog especializado en Sistemas de Gestión de Seguridad de la Información*. [en línea]. <https://www.pmg-ssi.com/>. [Consulta: 15 de marzo de 2019].

60. _____. *Cultura de seguridad de la información*. [en línea]. <https://www.pmg-ssi.com/2014/04/iso-27014-gobernanza-de-seguridad-de-la-informacion/>. [Consulta: 08 de mayo de 2019].

61. _____. *Gobernanza de seguridad de la información*. [en línea]. <https://www.pmg-ssi.com/2014/04/iso-27014-gobernanza-de-seguridad-de-la-informacion/>. [Consulta: 08 de mayo de 2019].

62. SIB. *Sector de microfinanzas*. [en línea]. <http://www.sib.gob.gt/c/document_library/get_file?folderId=471455&name=DLFE-10346.pdf>. [Consulta: 11 de marzo de 2019].

63. SOMOZA MORALES, Byron Alberto. *Auditoría externa de cuentas por cobrar en una institución de microfinanzas.* Trabajo de graduación de Contador Público y Auditor. Facultad de Ciencias Económicas, Universidad de San Carlos de Guatemala, 2014. 3 p.

64. The OWASP Foundation. *Inyección de código*. [en línea]. <https://www.owasp.org/index.php/Inyecci%C3%B3n_SQL>. [Consulta: 29 de marzo de 2019].

65. Wikipedia. *Objetivos de control para la información y tecnologías relacionadas*. [en línea]. <https://www.isaca.org/cobit>. [Consulta: 15 de marzo de 2019].

66. _____. *PCI DSS Estándar de Seguridad de Datos para la Industria de Tarjeta de Pago*. [en línea]. <https://es.wikipedia.org/wiki/PCI_DSS>. [Consulta: 20 de marzo de 2019].

67. _____. *Single Sign-On*. [en línea]. <https://es.wikipedia.org/wiki/Single_Sign-On>. [Consulta: 26 de abril de 2019].

APÉNDICES

Apéndice 1. **Capas y controles de modelo propuesto**

Fuente: elaboración propia.

Apéndice 2. **Servicios críticos que prestan las instituciones de microfinanzas**

No.	Nombre del servicio
1	Cobro de cuotas de prestamos
2	Cobro de cuotas de seguros médicos
3	Cobro de energía eléctrica
4	Venta de tiempo de aire de empresas telefónicas
5	Venta de seguros médicos
6	Pago de remesas
7	Solicitudes de préstamos
8	Desembolsos de préstamos
9	Consultas de saldo de préstamos
10	Generación de estados de cuenta de préstamos
11	Cancelación anticipada de préstamos
12	Aplicación de abonos de capital a préstamos
13	Entrega de finiquitos
14	Apertura de cuentas de ahorros
15	Retiros de dinero cuentas de ahorros
16	Depósitos de dinero a cuentas de ahorros
17	Cambios de cheque
18	Generación de estados de cuenta de ahorros
19	Cancelación de cuentas de ahorros
20	Pagos en línea a través de puntos de pagos

Fuente: elaboración propia.

Apéndice 3. **Riesgos que se deben de evaluar de forma mensual a tecnología**

No.	Indicador Clave de Riesgo (KRI)	Apetito de riesgo		
		Ideal	Alerta	Limite
1	Número de ocurrencias de incidentes de alta gravedad (CBS)			
2	Porcentaje de sistemas críticos probados (DR)			
3	Número de sistemas críticos con software obsoleto			
4	Porcentaje de procesos críticos de tecnología que han sido evaluados en los últimos 6 meses			
5	Porcentaje de backups que han tenido error al restaurar (CBS)			
6	Porcentaje de equipos que están actualizados con parches de seguridad			
7	Porcentaje de cambios en el CBS sin aprobación			
8	Número de permisos especiales a revisar información de usuarios			
9	Porcentaje de usuarios nuevos capacitados			
10	Número de problemas críticos de IT que no han sido atendidos			
11	Número de equipos vulnerados por equipos vulnerados			
12	Número de dispositivos robados			
13	Número de pruebas de vulnerabilidades a los sistemas críticos en los últimos 6 meses			

Fuente: elaboración propia.

Apéndice 4. **Riesgos que se deben de evaluar de forma mensual a recursos humanos**

No.	Indicador Clave de Riesgo (KRI)	Apetito de riesgo		
		Ideal	Alerta	Limite
1	Porcentaje de rotación en el mes			
2	Empleados que han sufrido accidentes en el mes			
3	Porcentaje de usuarios nuevos capacitados			
4	Número de empleados nuevos que no han firmado contrato de confidencialidad			
5	Número de empleados de baja en el mes			
6	Número de empleados asaltados en el mes			
7	Número de empleados acusados de robo de información			
8	Número de empleados demandados por fraude			
13	Número de campañas de seguridad a todos los empleados en el mes			

Fuente: elaboración propia.

ANEXOS

Anexo 1. **Métricas de evaluación de vulnerabilidades**

Se recomienda utilizar el *framework* CVCC (Common Vulnerability Scoring System), que es una herramienta utilizada universalmente para establecer métricas que ayudan a comunicar las características, impacto y severidad de las vulnerabilidades que se detectan y ponen en riesgo la seguridad de la información en cualquier institución. Se clasifican en:

- Clasificación de métricas CVSS

Continuación del anexo 1.

Es un sistema de medición diseñado mediante un método estándar para establecer la gravedad de una vulnerabilidad. Se compone principalmente de tres grupos de métricas: base, temporal y de entorno, (figura 28). A su vez, cada estos se componen de un conjunto de métricas.

- Métricas de impacto

Toda la vulnerabilidad: sin embargo, las que corresponden a las de confidencialidad (C), integridad (I) y disponibilidad (A) representan un riesgo crítico para las instituciones. En las Tablas IX, X, XI se especifica el valor métrico para cada una de estas métricas de impacto.

- Confidencialidad

Valor Métrico	Descripción
Alto (H)	Existe una pérdida total de confidencialidad, lo que hace que todos los recursos dentro del componente afectado se divulguen al atacante. Alternativamente, se obtiene acceso a solo cierta información restringida, pero la información divulgada presenta un impacto directo y serio. Por ejemplo, un atacante roba la contraseña del administrador o las claves de cifrado privadas de un servidor web.
Bajo (l)	Hay una cierta pérdida de confidencialidad. Se obtiene acceso a cierta información restringida, pero el atacante no tiene control sobre qué información se obtiene, o la cantidad o el tipo de pérdida son limitados. La divulgación de información no causa una pérdida directa y grave al componente afectado.
Ninguno (N)	No hay pérdida de confidencialidad dentro del componente impactado.

Continuación del anexo 1.

- Integridad

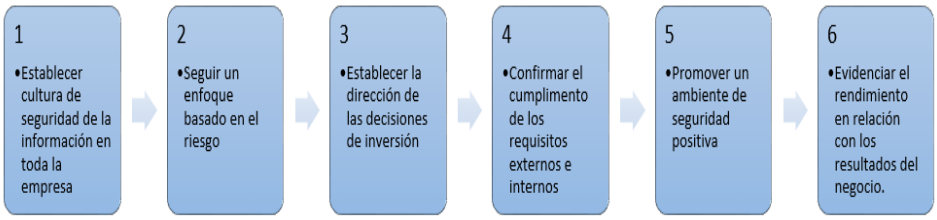
Valor Métrico	Descripción
Alto (H)	Existe una pérdida total de integridad o una pérdida total de protección. Por ejemplo, el atacante puede modificar cualquiera o todos los archivos protegidos por el componente afectado. Alternativamente, solo algunos archivos pueden modificarse, pero la modificación maliciosa presentaría una consecuencia directa y grave para el componente afectado.
Bajo (l)	La modificación de los datos es posible, pero el atacante no tiene control sobre la consecuencia de una modificación, o la cantidad de modificación es limitada. La modificación de los datos no tiene un impacto directo y serio en el componente afectado.
Ninguno (N)	No hay pérdida de integridad dentro del componente impactado.

- Disponibilidad

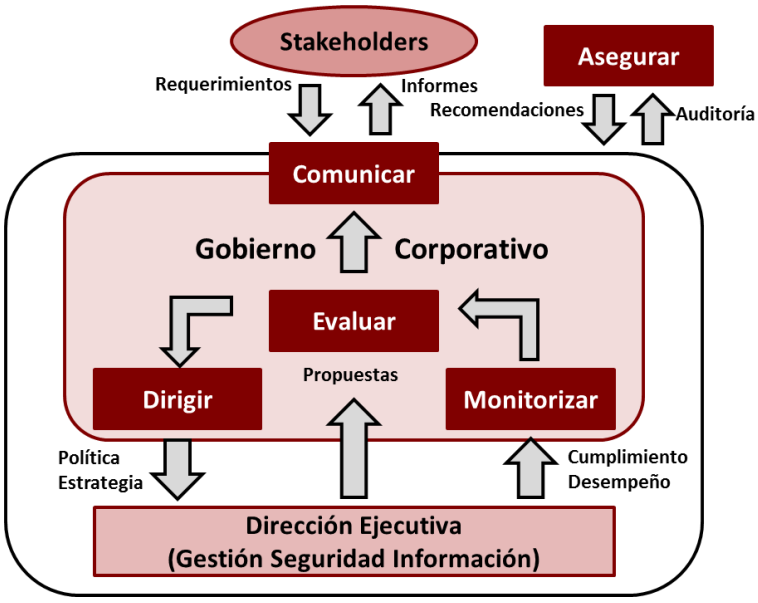
Valor Métrico	Descripción
Alto (H)	Existe una pérdida total de disponibilidad, lo que hace que el atacante pueda negar completamente el acceso a los recursos en el componente afectado; esta pérdida es sostenida o persistente. Alternativamente, el atacante tiene la capacidad de negar cierta disponibilidad, pero la pérdida de disponibilidad presenta una consecuencia directa y seria para el componente afectado, en cada instancia de un ataque exitoso, pierde una pequeña cantidad de memoria, pero después de una explotación repetida hace que un servicio no esté completamente disponible).
Bajo (l)	El rendimiento se reduce o hay interrupciones en la disponibilidad de recursos. Incluso si es posible la explotación repetida de la vulnerabilidad, el atacante no tiene la capacidad de negar completamente el servicio a usuarios legítimos. Los recursos en el componente impactado están parcialmente disponibles todo el tiempo, o están completamente disponibles solo parte del tiempo, pero en general no existe una consecuencia directa y seria para el componente impactado.
Ninguno (N)	No hay impacto en la disponibilidad dentro del componente afectado.

Fuente: First Improving Security Together. *Sistema de puntuación de vulnerabilidad común versión 3.1: Documento de especificación.* https://www.first.org/cvss/specification-document. Consulta: 11 de junio de 2019.

Anexo 2. **Principios de ISO 27014**

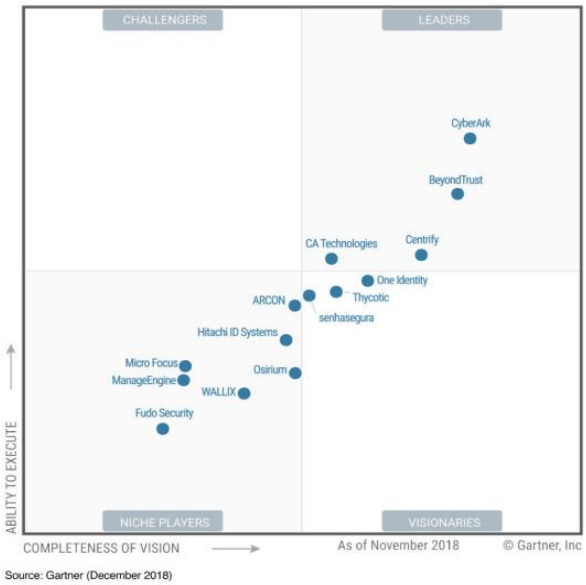


- Modelo para la implementación del gobierno de la seguridad de la información



Fuente: ABAST. *Calidad de las TIC*. http://calidadtic.blogspot.com/2014/03/gobierno-de-la-seguridad-de-la.html. Consulta: 11 de junio de 2019.

Anexo 3. **Sistemas de control de accesos**



- Herramientas de seguridad inalámbricas

Fuente: Fortinet. *La red: Guía del líder para SD-WAN seguro*. https://www.fortinet.com/demand/gated/gartner-magic-quadrant-wan-edge.html. Consulta: 5 de junio de 2019.

Anexo 4. **Fuentes tecnológicas**

Las fuentes tecnoló gicas que se sugiere conocer para estar actualizado sobre información de seguridad de la información son:

- US-CERT: Centro Nacional de Integración de Ciberseguridad y Comunicaciones: https://www.us-cert.gov

- NIST: mejores prácticas de ciberseguridad y la privacidad a través de la divulgación y la aplicación efectiva de los estándares: https://www.nist.gov/topics/cybersecurity

- Oracle Magazine: revista informativa de Oracle sobre avances en diferentes áreas de tecnología: https://blogs.oracle.com/oraclemagazine

- Microsoft magazine: revista digital que provee información relacionada con productos Microsoft: https://blogs.oracle.com/oraclemagazine

- Kaspersky: boletín de seguridad en el que puedes encontrar noticias relevantes y las amenazas actuales: https://securelist.lat

- IT NOW: revista regional con temas de tendencia tecnología y amenazas de seguridad de la información en Centroamérica y el Caribe: https://revistaitnow.com

Fuente: Revista It Now. *Noticias*. https://revistaitnow.com. Consulta: 2 de junio de 2019.