UNIVERSIDAD PERUANA DE CIENCIAS APLICADAS

FACULTAD DE INGENIERÍA

CARRERA DE INGENIERÍA DE REDES Y COMUNICACIONES

**PROPUESTA DE UNA INFRAESTRUCTURA DE
CLAVE PÚBLICA PARA EL USO DE CIFRADO Y
FIRMA DIGITAL EN LOS MENSAJES DE CORREO
ELECTRÓNICO DE UN SERVICIO BASADO EN
OFFICE 365.**

**TESIS PARA OPTAR EL TÍTULO PROFESIONAL DE:
INGENIERO DE REDES Y COMUNICACIONES**

PRESENTADO POR:

BACH. RAMOS RAFAEL, ENRIQUE DANIEL (0000-0002-6830-7610)

ASESOR:

ING. SEMINARIO GARCIA, HERNÁN (0000-0001-6971-355X)

Lima, 23 de marzo de 2018

A mi padre que descansa en el señor Dios todopoderoso y espera su despertar en su segunda venida. A mi madre que, junto a Él, supieron dar lo mejor de sí a sus cinco hijos con amor incondicional.

RESUMEN

El presente trabajo tiene como finalidad proponer una de Infraestructura de Clave Pública (PKI), la cual mediante el uso de certificados digitales para el cifrado y firma digital ofrezca

una solución óptima de seguridad de la información contra las amenazas a las que están expuestos actualmente los usuarios de correo electrónico en la organización objetivo.

En el primer capítulo se presentarán los aspectos introductorios del proyecto. En este apartado se identificará la organización objetivo, se describirá la problemática a la cual está expuesta la organización y se describirá el panorama actual de las tecnologías de seguridad de la información que se aplican a un servicio de correo electrónico. Además, se plantearán los objetivos del proyecto, los cuales serán evaluados en el último capítulo del proyecto. En el segundo capítulo se describirá de manera detallada todas las teorías, principios y fundamentos de seguridad de la información a los cuales estará sujeto el tema de investigación. Asimismo, se describirán las tecnologías de las cuales está compuesta la PKI, analizando estándares, normas y políticas de buenas prácticas usadas a nivel internacional. En el capítulo tres se plantean los problemas identificados en la organización objetivo. Asimismo, se identificarán los requerimientos de seguridad en base a la problemática definida. En el capítulo cuatro la propuesta de la PKI basada en la nube para el uso de cifrado y firma digital en los mensajes de correo electrónico será desarrollado. Finalmente, en el quinto capítulo se realizará la evaluación de los objetivos específicos planteados en el capítulo uno.

Palabras clave: PKI, cifrado, firma digital, seguridad de la información, basado en la nube.

ABSTRACT

The purpose of this work is to propose a Public Key Infrastructure (PKI) for the use of digital certificates for encryption and digital signatures to offer an optimal solution for information security, to avoid the threats that are currently exposed to e-mail users in the target organization.

In the first chapter the introductory aspects of the project will be presented. In this section the target organization will be identified, the problem to which the organization is exposed will be described and the current status of information security technologies that may apply to an e-mail service will be described. In addition, the objectives of the project will be proposed, which will be evaluated in the last chapter of the project. In the second chapter will be described in detail all the theories, principles and fundamentals of information security to which the subject of research will be described. Likewise, the technologies of which the PKI is composed will be described, analyzing standards, norms and policies of good practices used in international standards. In chapter three of the project the problems identified in the target organization are raised. Likewise, security requirements will be identified based on the defined problem. In chapter four the approach to the proposal of the cloud based PKI for the use of encryption and digital signature for e-mail messages will be developed. Finally, in the fifth chapter, the evaluation of the specific objectives set out in chapter one will be carried out.

Keywords: PKI, encryption, digital signature, information security, cloud based.

TABLA DE CONTENIDOS

INTRODUCCIÓN.....	1
-------------------	---

CAPÍTULO I: ASPECTOS INTRODUCTORIOS	2
1.1. Organización Objetivo.....	2
1.2. Campo de Acción en la Organización Objetivo	4
1.3. Situación Problemática	4
1.4. Identificación del Problema.....	5
1.5. Objetivos del Proyecto	7
1.5.1. Objetivo General.....	7
1.5.2. Objetivos Específicos	7
1.6. Justificación del Proyecto.....	9
1.7. Estado del Arte	10
1.7.1. Firewall.....	10
1.7.2. VPN	17
1.7.3. Criptografía.....	20
1.7.4. Office 365 Message Encryption	36
1.7.5. Caso de Éxito: Planta de Certificación Digital PKI de RENIEC	42
CAPÍTULO II: MARCO TEÓRICO.....	45
2.1. Concepto de PKI.....	45
2.1.1. Definición de PKI.....	45
2.1.2. Principios fundamentales de una PKI.....	46
2.1.3. Conceptos de seguridad que aplica.....	50
2.1.4. Tecnologías que utilizan una PKI.....	56
2.2. Arquitectura de una PKI.....	59
2.2.1. Componentes de una PKI	59
2.2.2. Procesos en una PKI.....	64
2.2.3. Estructura de una PKI.....	68
2.3. Estándares de una PKI.....	70
2.3.1. Estándar ITU-T X.509.....	70
2.3.2. Estándar PKCS	74
2.3.3. Estándar IETF.....	75
2.4. Certificados Digitales	75
2.4.1. Definición	75
2.4.2. Estructura del Certificado Digital.....	77
2.4.3. Tipos de certificación	78

2.5. Lista de Revocación de Certificados (CRL).....	80
2.5.1. Definición	80
2.5.2. Funcionamiento	80
2.5.3. Estructura de las CRL.....	81
2.6. PKI Gestionada por terceros.....	82
2.6.1. Concepto de PKI Gestionada.....	82
2.6.2. Proveedores de PKI gestionada	83
2.7. Amenazas a las PKI.....	85
2.7.1. Ataques Internos a las CA	85
2.7.2. Ataques Externos a las CA	86
2.7.3. Seguridad para las CA	86
2.8. Normativa nacional de las PKI.....	88
2.8.1. Ley N° 27269 de Firmas y Certificados Digitales.....	88
2.8.2. Ley N° 27291 que Modifica el Código Civil	89
2.8.3. Decreto Supremo N°052-2008-PCM	89
2.8.4. Decreto Supremo N°070-2011-PCM	90
2.9. Servicio de correo electrónico Office 365	90
2.9.1. Exchange Online.....	90
2.9.2. Ventajas	92
2.10. Estándar NIST SP 800-57.....	94
2.11. Metodología del Plan de Pruebas	98
2.11.1. Información Resumen.....	99
2.11.2. Definir el alcance de la prueba	99
2.11.3. Recursos necesarios para la prueba	100
2.11.4. Definir el método de prueba	100
2.11.5. Definir el caso de prueba	100
2.11.6. Ejecución del caso de prueba.....	100
CAPÍTULO III: DEFINICIÓN DEL PROBLEMA	101
3.1. Definición del Problema.....	101
3.1.1. Análisis de la problemática	101
3.1.2. Problemas por Resolver.....	103
3.2. Evaluación del Impacto del Problema en la Organización.....	103
3.2.1. Impacto Tecnológico	103

3.2.2. Impacto Legal	104
3.2.3. Impacto Económico.....	104
3.3. Definición de Requerimientos	105
3.3.1. Registro de Interesados del Proyecto.....	105
3.3.2. Requerimientos Funcionales	107
CAPÍTULO IV: PLANTEAMIENTO DE LA SOLUCIÓN PROPUESTA	110
4.1. Modelo de arquitectura de integración de una PKI y un servicio de correo electrónico Office 365	111
4.2. Especificaciones	113
4.2.1. Definición de los algoritmos de cifrado y firma digital.....	113
4.2.2. Compatibilidad con Certificados Digitales S/MIME	116
4.2.3. Configuración de los certificados digitales S/MIME	118
4.2.4. PKI basada en la nube	126
4.2.5. Servicio de correo electrónico Office 365	132
4.2.6. Administrador de PKI.....	134
4.3. Evaluación y Selección de Recursos	137
4.4. Evaluación de Costos	139
CAPÍTULO V: PRUEBAS, RESULTADOS Y VALIDACIÓN DE LA PROPUESTA.	144
5.1. Desarrollo del Plan de Pruebas por O.E.	144
5.1.1. Ejecución del plan de pruebas O.E. “a”	144
5.1.2. Resultados del plan de pruebas O.E. “a”	152
5.1.3. Validación del plan de pruebas O.E. “a”	155
5.1.4. Ejecución del plan de pruebas O.E. “b”	157
5.1.5. Resultados del plan de pruebas O.E. “b”	165
5.1.6. Validación del plan de pruebas O.E. “b”	166
5.1.7. Ejecución del plan de pruebas O.E. “c”	167
5.1.8. Resultados del plan de prueba O.E. “c”	178
5.1.9. Validación del plan de prueba O.E. “c”	179
CONCLUSIONES.....	181
RECOMENDACIONES PARA TRABAJOS FUTUROS	184
BIBLIOGRAFÍA	185
GLOSARIO	189
SIGLARIO	192

ANEXOS.....	192
-------------	-----

ÍNDICE DE FIGURAS

Figura 1. Ejemplo de una red con Firewall básico. Adaptado de “Soluciones Fortinet”, por MAPS.COM.MX, 2017.....	16
Figura 2. Ejemplo de una red con un dispositivo UTM. Adaptado de “Soluciones Fortinet”, por MAPS.COM.MX, 2017.....	16
Figura 3. Diagrama de arquitectura de los tipos conexión VPN. Adaptado de “Cisco RV042 Dual WAN VPN Router”, por Cisco.com, 2011.....	19
Figura 4. Medio de comunicación de la información cifrada y la llave. Adaptado de “Cryptography and Data Security”, por DENNING, 1982.	21
Figura 5. Dos pasos del cifrado de transposición. Adaptado de “Cryptography and Data Security”, por DENNING, 1982.....	22
Figura 6. Cifrado Churchyard. Adaptado de “Cryptography and Data Security”, por DENNING, 1982.....	23
Figura 7. Ejemplo de Cifrado por sustitución homofónica. Adaptado de “Cryptography and Data Security”, por DENNING, 1982.	24
Figura 8. Disco de cifrado de Alberti Adaptado de “Cryptography and Data Security”, por DENNING, 1982.	25
Figura 9. Cifrado por permutación y sustitución usada por la LUCIFER de IBM. Adaptado de “Cryptography and Data Security”, por DENNING, 1982.	27
Figura 10. Algoritmo de cifrado DES. Adaptado de “Cryptography and Data Security”, por DENNING, 1982.....	29
Figura 11. Maquina de crackeado DES. Adaptado de “La maquinad de crackeado DES”, por WIKIPEDIA.ORG, 2004.	31
Figura 12. Tiempo en computar un logaritmo discreto a un factor. Adaptado de “Cryptography and Data Security”, por DENNING, 1982.	33
Figura 13. Diagrama de flujo de un mensaje de correo cifrado por OME. Adaptado de “Office 365 Message Encryption Mail Flow”, por OFFICE365SUPPORT.CA, 2015.....	38
Figura 14. Diagrama de flujo del servicio OME en la cual se identifica una brecha de seguridad. Adaptado de “Office 365 Message Encryption (& Decryption) – Steps for Purchase, Configuration, Branding and Use – Everything you need to know”, por MICROSOFT.COM, 2014.	40
Figura 15. Esquema de funcionamiento del cifrado S/MIME donde se identifica que el cifrado proviene desde el cliente de correo electrónico. Adaptado de “S/MIME Certificate for Email Encryption”, por CYBERSECUREASIA.COM, 2015.	41

Figura 16. Infraestructura Tecnológica de la Planta PKI de RENIEC. Adaptado de “Planta de Certificación Digital PKI”, por RENIEC, 2012.	44
Figura 17. Ejemplo de Tarjeta inteligente de autenticación. Adaptado de “Formación PKI – Seminario de Infraestructura de Clave Pública”, por INDRA, 2005.....	52
Figura 18. Comparación entre cifrado simétrico y asimétrico. Adaptado de “Formación PKI – Seminario de Infraestructura de Clave Pública”, por INDRA, 2005.....	53
Figura 19. Representación de una función hash. Adaptado de “Public key infrastructure: building trusted applications and Web services”, por VACCA, 2004.	54
Figura 20. Esquema de firma electrónica. Adaptado de “Formación PKI – Seminario de Infraestructura de Clave Pública”, por INDRA, 2005.....	54
Figura 21. Ejemplo de Integridad de la información con firmas digitales. Adaptado de “Conceptos de Seguridad”, por NORTHSECURE.ES 2013.....	55
Figura 22. Componentes de una PKI. Adaptado de “Formación PKI – Seminario de Infraestructura de Clave Pública”, por INDRA, 2005.....	60
Figura 23. Suscriptor persona natural de un certificado digital. Adaptado de “Firma electrónica y certificados digitales”, por ADLE, 2010.....	62
Figura 24. Diagrama de Parte utilizadora vs Suscriptor (Servidor Web). Adaptado de “Formación PKI – Seminario de Infraestructura de Clave Pública”, por INDRA, 2005....	63
Figura 25. Diagrama de cifrado Asimétrico. Adaptado de “Firma electrónica y certificados digitales”, por ADLE, 2010.....	65
Figura 26. Ejemplo de cifrado de la información. Adaptado de “Conceptos de Seguridad”, por NORTHSECURE.ES 2013	67
Figura 27. Diseño base de una PKI. Adaptado de “Formación PKI – Seminario de Infraestructura de Clave Pública”, por INDRA, 2005.....	68
Figura 28. Diagrama de bloques funcionales de una PKI básica. Adaptado de “Public key infrastructure: building trusted applications and Web services”, por VACCA, 2004.....	69
Figura 29. Autenticación por medio de una Autoridad de Certificación. Adaptado de “Infraestructura para la criptografía de clave pública”, por CNC, 2014.	76
Figura 30. Estructura de Certificado Digital X.509 versión 3. Adaptado de “Formación PKI – Seminario de Infraestructura de Clave Pública”, por INDRA, 2005.....	77
Figura 31. Proceso de validación de la ruta de certificación. Adaptado de “Public key infrastructure: building trusted applications and Web services”, por VACCA, 2004.....	79

Figura 32. Ejemplo de CRL. Adaptado de “Basics of Digital Certificates and Certificate Authority”, por SITES.GOOGLE.COM, 2008.	81
Figura 33. Diagrama funcional de Exchange Online servicio de correo de Office 365. Adaptado de “Diagrama básico de red corporativo de un servicio Exchange Online”, elaboración propia.	94
Figura 34. Diagrama de Flujo del Plan de Pruebas. Adaptado de “Business Continuity Planning y la Gestión de Ensayos”, por ALBERTO G, 2017.	99
Figura 35. Matriz de Poder-Interés del proyecto. Adaptado de “10.1 Identificar los interesados”, por PM-DEVICES, 2012.	106
Figura 36. Modelo de arquitectura de integración de una PKI y un servicio de correo electrónico Office 365, elaboración propia.	112
Figura 37. Algoritmos recomendados por el IETF RFC 5751. Adaptado de “Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.2 - Message Specification”, por IETF RFC 5751, 2010.	117
Figura 38. Jerarquía de las CA que forman parte de la PKI. Adaptado de “Building and Managing a PKI Solution for Small and Medium Size Business”, por SANS.ORG, 2013.	127
Figura 39. Funcionamiento interno de la RA en la PKI basada en la nube. Adaptado de “Modelo de arquitectura de integración entre una PKI y un servicio de correo electrónico basado en Office 365”, elaboración propia.	129
Figura 40. Funcionamiento de la VA en la PKI basada en la nube. Adaptado de “Modelo de arquitectura de integración entre una PKI y un servicio de correo electrónico basado en Office 365”, elaboración propia.	130
Figura 41. Propuesta de Formulario de Solicitud de Certificado Digital. Adaptado de “Un formulario de inscripción estándar”, elaboración propia.	136
Figura 42. Prueba de envío de correo sin cifrado y firma digital. Adaptado de “Prueba de envío de correo electrónico de un cliente de correo electrónico Office 365 desde Outlook 2013”, elaboración propia.	172
Figura 43. Recepción del correo sin cifrado y ni firma digital. Adaptado de “Prueba de envío de correo electrónico de un cliente de correo electrónico Office 365 desde Outlook 2013”, elaboración propia.	173

Figura 44. Detalle de la cabecera del correo enviado, sin cifrado y firma. Adaptado de “Prueba de envío de correo electrónico de un cliente de correo electrónico Office 365 desde Outlook 2013”, elaboración propia.	174
Figura 45. Envío de correo cifrado y firmado desde Outlook 2013. Adaptado de “Prueba de envío de correo electrónico cifrado y firmado desde un cliente de correo electrónico Office 365 con Outlook 2013”, elaboración propia.....	175
Figura 46. Recepción del correo cifrado y con firma digital. Adaptado de “Prueba de envío de correo electrónico cifrado y firmado desde un cliente de correo electrónico Office 365 con Outlook 2013”, elaboración propia.....	176
Figura 47. Ventana de Propiedades de Cifrado en Outlook 2013. Adaptado de “Prueba de envío de correo electrónico cifrado y firmado desde un cliente de correo electrónico Office 365 con Outlook 2013”, elaboración propia.....	176
Figura 48. Ventana de Propiedades de Firma Digital en Outlook 2013. Adaptado de “Prueba de envío de correo electrónico cifrado y firmado desde un cliente de correo electrónico Office 365 con Outlook 2013”, elaboración propia.	177
Figura 49. Ventana de solicitud de PIN. Adaptado de “Symantec PKI Manager Test Drive”, por SYMAUTH.COM, 2015.	193
Figura 50. Ventana de administración principal: PKI Manager. Adaptado de “Symantec PKI Manager Test Drive”, por SYMAUTH.COM, 2015.	194
Figura 51. Opción de Administrar perfiles de certificados. Adaptado de “Symantec PKI Manager Test Drive”, por SYMAUTH.COM, 2015.	195
Figura 52. Ventana de creación de perfil, selección de modo. Adaptado de “Symantec PKI Manager Test Drive”, por SYMAUTH.COM, 2015.	196
Figura 53. Selección de plantilla, opción Correo electrónico seguro. Adaptado de “Symantec PKI Manager Test Drive”, por SYMAUTH.COM, 2015.	196
Figura 54. Creación de perfil, Personalización de certificado. Adaptado de “Symantec PKI Manager Test Drive”, por SYMAUTH.COM, 2015.	197
Figura 55. Creación de perfil, Personalización de certificado. Adaptado de “Symantec PKI Manager Test Drive”, por SYMAUTH.COM, 2015.	197
Figura 56. Opciones de certificado, nivel de seguridad medio. Adaptado de “Symantec PKI Manager Test Drive”, por SYMAUTH.COM, 2015.	198
Figura 57. Opciones de certificado, configuración de campos. Adaptado de “Symantec PKI Manager Test Drive”, por SYMAUTH.COM, 2015.	199

Figura 58. Configuraciones personalizadas del certificado digital. Adaptado de “Symantec PKI Manager Test Drive”, por SYMAUTH.COM, 2015.....	200
Figura 59. Administración de perfiles de certificado (plantillas). Adaptado de “Symantec PKI Manager Test Drive”, por SYMAUTH.COM, 2015.....	200
Figura 60. Barra de opciones de PKI Manager. Adaptado de “Symantec PKI Manager Test Drive”, por SYMAUTH.COM, 2015.	201
Figura 61. Ventana de administración de usuarios. Adaptado de “Symantec PKI Manager Test Drive”, por SYMAUTH.COM, 2015.	201
Figura 62. Agregar usuario con la dirección de correo electrónico. Adaptado de “Symantec PKI Manager Test Drive”, por SYMAUTH.COM, 2015.....	202
Figura 63. Ventana agregar usuarios, configuración de nombres y correo. Adaptado de “Symantec PKI Manager Test Drive”, por SYMAUTH.COM, 2015.	202
Figura 64. Ventana de inscripción para obtener el certificado digital. Adaptado de “Symantec PKI Manager Test Drive”, por SYMAUTH.COM, 2015.	203
Figura 65. Ventana de inscripción de usuario, información adicional. Adaptado de “Symantec PKI Manager Test Drive”, por SYMAUTH.COM, 2015.	204
Figura 66. Ventana de inscripción de usuario, código de inscripción. Adaptado de “Symantec PKI Manager Test Drive”, por SYMAUTH.COM, 2015.	205
Figura 67. Correo de solicitud de inscripción del Enterprise PKI Team. Adaptado de “Symantec PKI Manager Test Drive”, por SYMAUTH.COM, 2015.	206
Figura 68. Web de Inscripción al certificado asignado (Symantec). Adaptado de “Symantec PKI Manager Test Drive”, por SYMAUTH.COM, 2015.....	206
Figura 69. Web de Inscripción al certificado asignado, código de inscripción. Adaptado de “Symantec PKI Manager Test Drive”, por SYMAUTH.COM, 2015.	207
Figura 70. Instalación de complemento Symantec Authentication Client. Adaptado de “Symantec PKI Manager Test Drive”, por SYMAUTH.COM, 2015.	208
Figura 71. Confirmación de identidad a través del navegador web. Adaptado de “Symantec PKI Manager Test Drive”, por SYMAUTH.COM, 2015.....	209
Figura 72. Descarga de Symantec PKI Client en la PC del usuario. Adaptado de “Symantec PKI Manager Test Drive”, por SYMAUTH.COM, 2015.....	209
Figura 73. Instalación del certificado en la PC del cliente. Adaptado de “Symantec PKI Manager Test Drive”, por SYMAUTH.COM, 2015.	210

Figura 74. Solicitud de creación de PIN para la PC cliente (única vez). Adaptado de “Symantec PKI Manager Test Drive”, por SYMAUTH.COM, 2015.	211
Figura 75. Ventana de Instalación del certificado S/MIME. Adaptado de “Symantec PKI Manager Test Drive”, por SYMAUTH.COM, 2015.	211
Figura 76. Ventana de confirmación inscripción de certificado completa. Adaptado de “Symantec PKI Manager Test Drive”, por SYMAUTH.COM, 2015.	212
Figura 77. Ventana de confirmación de correo en Microsoft Outlook 2013. Adaptado de “Configuración para el envío de correo electrónico cifrado y firmado desde un cliente de correo electrónico Office 365 con Outlook 2013”, elaboración propia.	213
Figura 78. Ventana de Importación y Exportación de certificado. Adaptado de “Configuración para el envío de correo electrónico cifrado y firmado desde un cliente de correo electrónico Office 365 con Outlook 2013”, elaboración propia.	214
Figura 79. Selección de Certificado Correo Nivel 1. Adaptado de “Configuración para el envío de correo electrónico cifrado y firmado desde un cliente de correo electrónico Office 365 con Outlook 2013”, elaboración propia.	214
Figura 80. Archivo de certificado digital exportado a usar en el cifrado y firma digital de los mensajes de correo. Adaptado de “Configuración para el envío de correo electrónico cifrado y firmado desde un cliente de correo electrónico Office 365 con Outlook 2013”, elaboración propia.	214
Figura 81. Selección del archivo de certificado a instalar en Outlook 2013. Adaptado de “Configuración para el envío de correo electrónico cifrado y firmado desde un cliente de correo electrónico Office 365 con Outlook 2013”, elaboración propia.	215
Figura 82. Habilitación de Cifrado y Firmado digital de los correos. Adaptado de “Configuración para el envío de correo electrónico cifrado y firmado desde un cliente de correo electrónico Office 365 con Outlook 2013”, elaboración propia.	216
Figura 83. Ventana de configuraciones de seguridad S/MIME en Outlook. Adaptado de “Configuración para el envío de correo electrónico cifrado y firmado desde un cliente de correo electrónico Office 365 con Outlook 2013”, elaboración propia.	216

ÍNDICE DE TABLAS

Tabla 1. Matriz de O.E., Indicadores de Logro, mediciones y métricas	8
Tabla 2. Campos de un Certificado Digital ITU-T X.509 versión 3	71
Tabla 3. Cuadro de ventajas de Exchange Online	92
Tabla 4. Comparativa de la fortaleza de los algoritmos de cifrado	95
Tabla 5. Fortaleza de las claves a lo largo del tiempo	95
Tabla 6. Algoritmos recomendados y sus tamaños de llave.....	96
Tabla 7. Algoritmos Hash recomendadas para una PKI.....	97
Tabla 8. Comparativa de funciones hash SHA.....	98
Tabla 9. Matriz de análisis de la problemática actual.....	101
Tabla 10. Matriz de Registro de Interesados del Proyecto	105
Tabla 11. Matriz de Toma de Requerimientos Funcionales	107
Tabla 12. Cuadro de campos def. en las plantillas de cert. para el campo Subject	120
Tabla 13. Cuadro de niveles de confidencialidad.....	122
Tabla 14. Longitud de clave pública a definir por cada plantilla de certificado	123
Tabla 15. Cuadro del ciclo de vida de las plantillas de certificados.....	124
Tabla 16. Evaluación de especificaciones en productos MPKI basada en la nube	137
Tabla 17. Cuadro de CAPEX del proyecto.....	140
Tabla 18. Cuadro de OPEX del proyecto	141
Tabla 19. Cuadro de Análisis Financiero de la solución Symantec MPKI	142
Tabla 20. Formato de la definición del Caso de Prueba del O.E. A.....	146
Tabla 21. Inventario de Activos.....	148
Tabla 22. Valoración de los Activos de Información	150
Tabla 23. Matriz de análisis y evaluación de riesgos	151
Tabla 24. Matriz de valoración de los activos de información.....	154
Tabla 25. Formato de la definición del Caso de Prueba 1	159
Tabla 26. Lista de comprobación de auditoria a las espec. de la PKI propuesta.....	160
Tabla 27. Resumen de resultados de auditoria a las espec. de la PKI propuesta.....	165
Tabla 28. Formato de la definición del Caso de Prueba 1	169
Tabla 29. Formato de la definición del Caso de Prueba 2	170
Tabla 30. Evaluación de riesgos de vulnerabilidades.....	179

INTRODUCCIÓN

En la última década, la seguridad de la información ha tomado mayor importancia en el mundo empresarial, principalmente debido a la constante y creciente cantidad de amenazas informáticas provenientes de internet. Por ello, numerosos esfuerzos se vienen realizando para proteger el activo intangible más importante que posee toda organización: La información.

Bajo esa premisa, el trabajo se desarrolla en un contexto en donde la información transmitida por un servicio de correo electrónico, a través de internet, constituye un valor fundamental a proteger por las organizaciones en la actualidad.

En ese sentido, se busca evaluar una solución de Infraestructura de Clave Pública o PKI provista por un tercero, la cual brinde un sistema de criptografía asimétrica de claves públicas/privadas, certificados digitales y entidades certificadoras, las cuales, aplicadas al flujo de mensajes de correo electrónico mediante el uso de firmas digitales y cifrado de datos, provean un alto nivel de seguridad en las comunicaciones realizadas a través de internet. Asimismo, esta solución se presenta como una propuesta para resolver la problemática en seguridad de la información del servicio de correo electrónico, basado en Office 365, en la organización objetivo.

CAPÍTULO I: ASPECTOS INTRODUCTORIOS

1.1. Organización Objetivo

La organización objetivo que se tendrá en cuenta para el cumplimiento de los objetivos del proyecto será: Toyota del Perú (Toyota). Esto se debe a que Toyota hace uso del servicio de Office 365, el cual ofrece Exchange Online para el servicio de correo electrónico. Este servicio lo usa a nivel nacional con sus socios de negocios, con su base de operaciones en Japón y otras sedes a nivel internacional. Toyota cuenta con poco más de 150 empleados en la actualidad que hacen uso de este servicio.

La principal razón por la cual se beneficiaría la compañía a través del proyecto sería la oportunidad de optimizar la seguridad de la información de los mensajes de correo electrónico que se transmiten a través de internet. Principalmente, los mensajes que son enviados y recibidos a su base de operaciones en Japón, los cuales son enviados por los altos ejecutivos de la compañía, siendo esta información sumamente sensible para los intereses de la organización.

Para entender mejor el objetivo de la organización, citaremos su visión, misión, valores y objetivos estratégicos que sigue la compañía:

Visión: “Ser el líder indiscutible en la industria automotriz y una de las empresas más admiradas en el Perú.”

Misión: “Ofrecer una inmejorable experiencia de compra y servicio superando las expectativas de los clientes a través de los mejores recursos humanos de la industria.”

Valores:

- Genchi Genbutsu: "ir al origen para encontrar los hechos que nos ayuden a tomar decisiones correctas, crear consensos y alcanzar metas".
- Kaizen: “mejora constante”.
- Retos: En Toyota tenemos una visión a largo plazo y afrontamos los retos con el valor y creatividad.
- Trabajo en equipo: Toyota estimula el crecimiento personal y profesional, ofrece oportunidades para el desarrollo y optimiza el rendimiento individual y del equipo.
- Respeto: En Toyota respetamos a los demás y aceptamos nuestras responsabilidades. Este respeto se extiende a nuestros competidores ya que entendemos que no "todo vale" para desarrollar las expectativas de un proyecto empresarial.

Objetivos Estratégicos:

- Corregir los problemas, poniendo la seguridad de los clientes y la comodidad como primer lugar.
- Crear un plan de acción medio ambiental, con la finalidad de tomar medidas proactivas tendientes a reducir el impacto ambiental.
- Mejorar la productividad, la calidad y tiempos de entrega.
- Introducir al mercado más productos innovadores con la finalidad de satisfacer las futuras necesidades de los clientes.
- Ser la empresa número uno en la mayor fabricación de automóviles y ser conocida por la calidad de sus productos.
- Ser una empresa rentable y líder del mercado automotriz.

- Fabricar vehículos y desarrollar tecnologías que anticipen las necesidades de la sociedad y de los clientes.
- Conseguir los sistemas de producción más rápidos y más baratos del mundo.¹

1.2. Campo de Acción en la Organización Objetivo

El campo de acción donde se aplicaría la solución PKI, comprendería a las cuentas de los usuarios que poseen el cargo de directores, gerentes y jefes de área que utilizan el servicio de correo electrónico. Esto se debe a que dichos usuarios son los que envían y reciben información mucho más crítica y confidencial que los demás usuarios de la compañía. Asimismo, son los usuarios que mantienen comunicación constante con la base de operaciones en Japón, el cual es un factor clave para tomar la decisión de seleccionarlos como objeto de estudio en la solución de PKI para el cifrado y firma digital de sus mensajes de correo electrónico.

1.3. Situación Problemática

Desde los inicios de su actividad empresarial, Toyota del Perú ingresó al mercado peruano para ser líder indiscutible en la industria automotriz del país. Para cumplir con la misión y los objetivos de la organización, se plantearon estrategias de posicionamiento del mercado. Cada vez más, la empresa ha tenido carga competitiva de otras empresas que entraron al mercado automotriz peruano. Por ello, Toyota ha tenido la filosofía de la mejora continua, lo cual ha significado un enfoque en la reducción constante de los problemas en sus procesos en todas las áreas de trabajo de la compañía. Con el objetivo de ser los mejores, sus

¹ Cfr. TOYOTA.COM.PE

estándares en cada área siempre apuntan a lo óptimo, es por ello, por lo que las tecnologías de la información no son una excepción en esa regla.

La situación problemática donde se desarrolla el trabajo es sobre un servicio de correo electrónico alojado en la nube, el cual no posee mecanismos de encriptación para la protección de la información que se transmite a través de internet. Esto se deriva en amenazas que podrían vulnerar la confidencialidad, integridad, autenticación y no repudio de la información de los correos electrónicos en la organización.

Los problemas que se presentan y se podrían presentar en Toyota, de no tomarse las medidas necesarias, son los siguientes:

1. Los usuarios no poseen un mecanismo de identificación digital en sus mensajes de correo electrónico, el cual valide la identidad de la persona, pues los métodos convencionales de identificación con firma al final del mensaje pueden ser fácilmente vulnerados.
2. En ciertas ocasiones, los usuarios difunden su contraseña. Sea de manera intencionada o no, esto causa que se corra el riesgo de ataques *spoofing* enviándose mensajes sin autorización del usuario dueño de la cuenta de correo electrónico.
3. Los mensajes de correo electrónico que viajan a través de internet corren el riesgo de ser interceptados por un *sniffer* de red o analizador de tráfico que este situado en una ubicación precisa de la red, lo cual podría vulnerar la confidencialidad e integridad de la información.
4. Creciente número de delitos informáticos y la facilidad con la que son encontradas las herramientas para perpetrarlos. Esto hace que el riesgo de amenazas de ataque a las cuentas de correo electrónico aumente, sobre todo a los altos ejecutivos de una compañía como Toyota que es blanco de mucha competencia.

1.4. Identificación del Problema

El ámbito donde enfocaremos la identificación de los problemas que ponen en riesgo la seguridad de la información es el servicio de correo electrónico basado en Office 365 que

posee Toyota del Perú. Teniendo en cuenta que el funcionamiento del servicio de correo electrónico cumple con su función normal, se identifican los siguientes problemas de seguridad de la información en el servicio:

1. Los usuarios de correo electrónico por lo general no son personas instruidas en hábitos de seguridad de la información. Dichos usuarios, por lo general significan un foco potencial en donde pueden ocurrir problemas de seguridad que perjudiquen al servicio de correo electrónico. Estos principalmente constan de malos hábitos en la confidencialidad de la información que se les es otorgada para el control de acceso a los recursos de la compañía. Algunos ejemplos son, la facilidad con la cual muchas veces difunden su usuario y contraseña de acceso al correo y otros sistemas, lo cual genera un riesgo de posible suplantación de identidad y acceso no autorizado a su información personal o de la compañía.
2. El servicio de correo electrónico, del cual dependen las comunicaciones tanto internas con los usuarios de la compañía como externas con los socios de negocio que posee Toyota, posee características de seguridad de la información básicas. Ello se debe a que, a diferencia de un servicio de correo electrónico interno, en el cual la mayor cantidad de tráfico de la información pasa a través de la red privada, un servicio de correo electrónico basado en la nube como Office 365 envía todo el tráfico de su servicio a través de internet. Debido a la naturaleza de esta tecnología, de la cual no se duda que traiga muchos más beneficios de los problemas que pueda dar, existe un riesgo intrínseco toda vez que la comunicación y el flujo de datos de los mensajes de correo electrónico se realizan a través de internet.
3. El ambiente del negocio y la importancia que tiene la marca en el mercado nacional e internacional, hacen que el servicio de correo electrónico corporativo corra el riesgo de recibir ataques direccionados a las cuentas de correo de la compañía. En la actualidad, existen muchos ataques que no solo consisten en desvelar la contraseña con programas informáticos, también existen ataques de ingeniería social los cuales pueden afectar a los usuarios de Toyota. Es por ello, que el ambiente en donde está posicionado Toyota en el mercado lo hace susceptible a ataques más sofisticados e incluso direccionados a los altos ejecutivos de la compañía, de los cuales se tiene información pública.
4. Otro factor para tomar en consideración es, que el servicio de correo electrónico de Toyota del Perú no cuenta con un mecanismo de identificación digital que prevenga la falsificación de los mensajes. Es decir, no hay manera de autenticar la identidad del emisor de un correo electrónico, ya que, con los medios actuales, los correos pueden ser enviados desde un origen distinto al usuario dueño de la cuenta con la misma dirección de correo. El problema radica entonces en la poca de certeza que se tiene cuando un mensaje es recibido, ya que surge la pregunta de que si el emisor del correo electrónico es realmente quien dice ser, no teniendo otra certeza más que en la simple firma escrita al pie del correo.

1.5. Objetivos del Proyecto

1.5.1. Objetivo General

Proponer una Infraestructura de Clave Pública (PKI) basada en la nube, la cual provea mecanismos de criptografía asimétrica para el uso de cifrado y firmas digitales, que permitan optimizar la seguridad de la información en los mensajes de correo electrónico de un servicio basado en Office 365.

1.5.2. Objetivos Específicos

- a.** Determinar los principales riesgos que podrían afectar a la seguridad de la información y los costos que implican los incidentes de seguridad que podrían presentarse en un servicio de correo electrónico basado en Office 365.
- b.** Elaborar las especificaciones técnicas requeridas para una Infraestructura de Clave Pública (PKI) basada en la nube, siguiendo los estándares internacionales para el cumplimiento de las buenas prácticas de la industria, que permitan el uso del cifrado y firmas digitales en los mensajes de correo electrónico de un servicio basado en Office 365.
- c.** Elaborar un modelo de arquitectura, que integre una Infraestructura de Clave Pública (PKI) basada en la nube sobre un servicio de correo electrónico basado en Office 365, el cual aplique cifrado y firma digital en los mensajes de correo electrónico con el fin de reducir las vulnerabilidades que puedan poner en riesgo la seguridad de los activos de información en la organización objetivo.

Tabla 1*Matriz de O.E., Indicadores de Logro, mediciones y métricas*

O. E.	Indicador de Logro	Medición	Métrica	Objetivo
a	Se determinan los principales riesgos midiendo el porcentaje a la exposición de riesgos y el costo que ocasionan los incidentes de seguridad mediante una matriz de análisis de riesgos de seguridad de la información de un servicio de correo electrónico basado en Office 365.	Exposición al Riesgo Costo de incidente de seguridad	% de riesgos altos y medios más allá del límite aceptable costo de las pérdidas por incidentes de seguridad	< % definido para la Organización. < 4 % del presupuesto de TI
b	Se determina el grado de cumplimiento de las especificaciones del producto seleccionado como PKI basada en la nube para la propuesta, mediante una lista de comprobación con los controles del marco de auditoría <i>WebTrust for CAs</i> , el cual está basado en el estándar ISO 21188:2006.	Grado de cumplimiento del marco de auditoría	% de cumplimiento	> 85%
c	Reducción del porcentaje de activos de información vulnerables a las amenazas provenientes del servicio de correo electrónico mediante los resultados de la integración de una PKI basada en la nube sobre un servicio de correo electrónico basado en Office 365 para el cifrado y firma digital de los mensajes.	Evaluación de vulnerabilidades	% de Reducción de vulnerabilidades (Verde=100%, Naranja>=75%, Rojo<75%)	Naranja

Nota. Adaptado del formato del formato de Libro de Tesis, de la UPC, p. 4, Copyright 2018 de UPC.

1.6. Justificación del Proyecto

La solución propuesta de Infraestructura de Clave Pública o PKI constituye un conjunto de tecnologías orientadas a la seguridad de la información transmitida en redes inseguras como el internet. Las aplicaciones empresariales que usan esta tecnología obtienen grandes ventajas criptográficas, como lo son: el cifrado, criptografía asimétrica, funciones hash y firmado digital de la información, los cuales son mecanismos que aseguran la confidencialidad, integridad, autenticación y no-repudio de la información de los participantes de la comunicación. Como resultado, se brinda un alto nivel de seguridad de la información sensible y crítica que maneja la organización.

Desde el punto de vista organizacional, se justifica el proyecto debido a que, en la actualidad, Toyota posee un riesgo latente en la seguridad de la información de los mensajes de correo que son enviados a su base de operaciones en Japón u otras sedes a nivel mundial a través de su servicio basado en Office 365. Bajo esta premisa, se presenta una oportunidad para reducir los riesgos a través de una propuesta de seguridad de una PKI mediante la firma digital y el cifrado de los mensajes de correo electrónico enviados al exterior.

Asimismo, se justifica la necesidad de un modelo de arquitectura de una PKI integrada a un servicio de correo electrónico basado en la nube que cumpla el objetivo de brindar cifrado y firma digital a los mensajes de correo electrónico. El modelo presentado busca ser una guía referencial para organizaciones como Toyota que estén interesadas en implementar una PKI para optimizar la seguridad de su servicio de correo electrónico basado en la nube.

1.7. Estado del Arte

En la actualidad existen diversos mecanismos de seguridad para proteger la información que ingresa a la red privada de la organización desde internet y viceversa. Muchos de estos mecanismos de seguridad han ido evolucionando con los años para abarcar muchos más niveles teniendo como referencia el modelo OSI (*Open System Interconnection*). Esto se debe a que las TIC en las organizaciones, tienden cada vez más a almacenar y administrar la información en la nube como una alternativa más rentable para el negocio.

Para proteger la seguridad de la información de un servicio de correo electrónico basado en la nube, existen mecanismos efectivos para garantizar un nivel de seguridad estándar en las comunicaciones. Sin embargo, para obtener un nivel óptimo de seguridad de la información, se necesitan soluciones que alcancen niveles más altos del modelo OSI. A continuación, se analizarán las tecnologías actuales que ayudan a solucionar el problema, así como casos de éxito que nos ayudaran a tener un panorama de las soluciones actuales que existen para dar solución al problema que se plantea en el proyecto.

1.7.1. Firewall

El termino *Firewall* es de origen inglés y fue usado por primera vez por *Lightoler* en 1764 para referirse a una pared que separaba una fuente de fuego del resto de cosas, se podría decir que separaba una cocina del resto de la estructura de la casa o edificación. Estas paredes estaban especialmente diseñadas para prevenir que el fuego que se producía en ese lugar no pueda dañar el resto del edificio.

Los que precedieron a los *firewalls* en la seguridad de la red, fueron los equipos *router*, que en 1980 eran usados para separar las redes una de la otra. Estas medidas de seguridad fueron establecidas para evitar que los problemas que acontecían en una red no se trasladasen a otra red adyacente. De esa manera, se tenían aislados problemas de tráfico excesivo de *broadcast* que por lo general sufrían las redes en ese entonces, así como problemas de configuración de protocolos de red, las cuales eran considerados como “amenazas” para la disponibilidad de la red.

En los años posteriores las redes se proliferaron de manera acelerada, el afán de vivir en una comunidad en donde la información pueda ser compartida libremente y desde cualquier parte del mundo entusiasmaba a las diversas compañías que desarrollaban estas tecnologías sin pensar en un segundo en el concepto de seguridad. El año 1988 marcó un hito importante en la historia de la seguridad en internet (en ese entonces conocida como ARPANET). Fue creado el primer malware llamado el Gusano Morris, este software malicioso fue creado accidentalmente por un joven estudiante llamado Robert Morris, el cual a posterior fue sentenciado por sus actos cuando aún no existía legislación para ese tipo de crímenes. Posteriores a Morris, comenzaron a producirse más amenazas y ataques en la inmensa red de computadoras llamada internet. Finalmente, la comunidad, que una vez busco tener una red abierta a la colaboración y el compartir del conocimiento e información, cambió de parecer. Internet se había convertido en un lugar inseguro y con usuarios que buscaban hacer el mal con o sin motivo alguno.

Luego de estos acontecimientos, la sociedad se vio necesitada de un mecanismo de seguridad de red que fijara los límites entre lo seguro y lo inseguro, fue así como nació lo que hoy conocemos como *Firewall*. El primer modelo fue creado por un equipo de Ingenieros de la

DEC (*Digital Equipment Corporation*), el cual fue un sistema básico de filtrado de paquetes que eran transmitidos por internet, este mecanismo de seguridad analizaba la información de los paquetes de red y tomaba la decisión de aceptarlos o rechazarlos de acuerdo con políticas básicas establecidas.

A pesar de que el *Firewall* comenzó filtrando solo paquetes de la capa de red y siendo básicamente un hardware especializado, en la actualidad este dispositivo o conjunto de dispositivos de seguridad perimetral, puede estar basado en hardware y/o software. Un firewall básico tiene como principal función el filtrado de paquetes de la tres (red) y cuatro (transporte) del modelo OSI y sirve para proteger a las organizaciones, de accesos no autorizados que provienen desde las redes externas e inseguras como internet. Es comúnmente usado para discriminar el nivel de seguridad entre la red privada segura de otras redes inseguras, para lo cual se emplean políticas de filtrado de paquetes de la capa de red y de transporte.

En cuanto al enfoque de un sistema de gestión de la seguridad de la información, y los principios básicos que busca, el firewall solo provee Disponibilidad. Esto se debe a que, por lo general, es implementado con sistemas de redundancia y bajo estrictas condiciones físicas de disponibilidad en el centro de datos donde se encuentra alojado. Este dispositivo es un elemento complementario, el cual brinda seguridad perimetral de red en una infraestructura de TI dentro de las organizaciones.

Por otro lado, existe una versión mejorada basada en el funcionamiento básico de un firewall: El UTM (*Unified Threat Management*), o “Gestión Unificada de Amenazas”. Este dispositivo es una evolución del *firewall* tradicional. El concepto de UTM fue usado por

primera vez en el año 2004 en un artículo de investigación publicado por el IDC (*International Data Corporation*), en el cual se hablaba de la necesidad de la creación de un dispositivo de seguridad que, a partir de un *Firewall*, agregara más funcionalidades como un IPS (*Intrusion Prevention System*) y un Antivirus de red. En base a su largo desarrollo efectuado por compañías privadas de seguridad, estos dispositivos por lo general han sido “*Appliance*” que mantienen un sistema operativo propietario del fabricante que los diseña. En años posteriores, estos dispositivos se han ido desarrollando y han unificado cada vez más funcionalidades como los *Antispam*, *Antiphishing*, Filtro de contenidos, Proxy, etc. Estas funcionalidades hacen que la seguridad de la información sea más completa al momento de filtrar las amenazas que provienen desde internet.

El Firewall posee varias fortalezas es cuanto a seguridad de la información. Una de ellas es que permite la segmentación de las redes, protegiendo así la información que se encuentra administrada por los servidores internos de la organización. Gracias a ello, la infraestructura de red de una organización se encuentra aislada de internet, fuente de donde provienen las amenazas informáticas por lo general. Además, centraliza los accesos que provienen desde internet hacia la red interna en un solo punto de administración y control. Esto significa que los potenciales usuarios no autorizados que traten de acceder a la información de la organización estarán comprometidos a pasar a través de los mecanismos de control que aplica el firewall; asimismo, se facilita la administración por parte del personal encargado de la seguridad de la información, ya que es un solo equipo que cumple varias funcionalidades de seguridad.

Por otro lado, un Firewall traduce direcciones IP (NAT) de una red privada hacia una red pública como internet y viceversa, protegiendo la identidad de los servidores internos al no

difundir las direcciones IP privadas de los servicios internos de la organización. En otro aspecto, controla el acceso a los servicios protegiendo la conexión a los puertos TCP o UDP. Esto asegura que la información privada de la organización no pueda ser accedida desde internet, solo los servicios publicados como la web http, el ftp, el correo electrónico, etc. podrían ser accedidos por los usuarios externos que ingresan a través de internet de manera controlada.

Al ser una tecnología complementaria dentro de una arquitectura de seguridad, el *firewall* básico no aplica seguridad a nivel de las capas superiores de la de transporte del modelo OSI. Al ser un dispositivo de seguridad perimetral, solo puede proteger de los accesos no autorizados que provienen desde internet. Por lo tanto, si un atacante logra tener acceso a la red protegida, por algún otro medio, podrá seguir realizando ataques desde la red interna sin que el firewall de cuenta de ello. De esa manera, no se puede evitar que la información manipulada por el atacante pueda ser filtrada por los usuarios o el mismo atacante desde la red interna. Los ataques que sean direccionados a las aplicaciones y no al servicio en sí mismo, son perpetrados con facilidad en la actualidad. Para solucionar las deficiencias de un Firewall convencional se creó el concepto de UTM, el cual trabaja hasta la capa de siete del modelo OSI, lo cual le permite brindar seguridad a nivel de las aplicaciones y de los datos que son transmitidos a ese nivel.

Estos dispositivos unifican y centralizan la administración de la seguridad en la arquitectura de TI en un solo dispositivo, evitando así la diversidad de interfaces de administración por cada funcionalidad o servicio de seguridad que se haya implementado en la red interna. Al integrar varias funcionalidades de seguridad en un solo dispositivo, ahorran el costo de adquisición de hardware de varios equipos de seguridad, ya que resultaría un costo elevado

la adquisición de un dispositivo por cada funcionalidad por separado. De la misma manera, se ahorra espacio físico en el centro de datos, teniendo un solo dispositivo en lugar de tener varios que ocupan más espacio en un rack de comunicaciones.

El lado negativo de la tecnología UTM es que se crea otro problema al centralizar la seguridad en un solo punto, se crea un cuello de botella. Es decir, si el dispositivo por algún motivo se queda fuera de servicio, la organización entera quedaría sin protección alguna contra las amenazas. Asimismo, si es que la organización tuviese como núcleo de negocio la publicación de un servicio web u otros, las pérdidas al quedar fuera de servicio hacia internet serían cuantiosas. Es por ello, que un UTM no es totalmente recomendable en una organización con una arquitectura de red grande (corporativa o multinacional). Esto se debe a que la cantidad de tráfico a enviarse a través de él haría muy difícil su procesamiento por un solo dispositivo encargado de la seguridad de miles de usuarios concurrentes. Además, esta tecnología no protege el contenido de la información que se transmite desde la red interna hacia internet, una vez que la información es enviada, pasa por diversas redes antes de llegar a su destino, y se crea un riesgo de probable interceptación y manipulación de la información confidencial de la organización por usuarios no autorizados. En ese sentido, esta evolución del *Firewall* no pasa de ser parte de la solución y no la solución definitiva a los problemas de seguridad de la información. Lo máximo que podría garantizarnos es la disponibilidad, y confidencialidad de la información, sin embargo, falla en los aspectos de autenticación e integridad de la información que es transmitida por la red.

Figura 1. Ejemplo de una red con Firewall básico. Adaptado de “Soluciones Fortinet”, por MAPS.COM.MX, 2017

Figura 2. Ejemplo de una red con un dispositivo UTM. Adaptado de “Soluciones Fortinet”, por MAPS.COM.MX, 2017

1.7.2. VPN

Una VPN (*Virtual Private Network*), es una tecnología capaz de extender una red LAN privada a través de una WAN (*Wide Area Network*) como internet, mediante la creación de un túnel seguro entre ambos segmentos de red física y/o geográficamente separados. El concepto de VPN fue creado a finales de la década de los noventa, cuando las redes de computadoras se conectaban a internet a través de líneas telefónicas *Dial-Up* que iban de velocidades desde 56 kbps a un T1. Estas conexiones eran demasiado costosas en su época y por lo general cada red LAN poseía una línea por cada sucursal remota a la cual se conectaba, lo cual encarecía aún más la interconexión de redes LAN a través de internet. Para dar solución a esta problemática, fue que se idearon las VPN, las cuales hacían que mediante una única conexión *Dial-Up* desde una computadora o red LAN, se pudiese conectar con varias redes remotas, reduciendo así los costos de las conexiones hacia internet y optimizando su uso.

Más tarde, a principios del siglo XXI, la tecnología se desarrollaba cada vez más y como es común en el desarrollo de tecnologías de la información, vienen acompañadas con el desarrollo de las amenazas a la seguridad de la información. Por ello, se desarrollaron diversos métodos para hacer que la información que era transmitida a través de internet, ahora por medio de las redes *Ethernet*, sea lo suficientemente segura para los intereses de las organizaciones. En consecuencia, se crearon protocolos seguros para el manejo de las comunicaciones a través de VPN, los protocolos más usados en la actualidad son:

1. IPSec
2. PPTP
3. L2TP
4. SSH

Existen cuatro arquitecturas definidas para implementar una VPN. La primera de ellas es el Acceso Remoto, el cual permite a un usuario remoto conectarse desde cualquier parte en el mundo en donde tenga acceso a internet, de esta manera el usuario estará virtualmente conectado a la red privada como si estuviese físicamente allí. La segunda arquitectura es llamada *site-to-site* o punto a punto, esta permite que dos redes LAN geográfica o físicamente separadas puedan conectarse como si estuviesen en la misma ubicación. Este método, se hace a través de dispositivos Gateway VPN que hacen posible la conexión de las redes en su totalidad. La tercera arquitectura es la de *Tunneling*, esta técnica es comúnmente usada entre dispositivos ruteadores que manejan tráfico TCP/IP y encapsulan el tráfico a nivel de PDU. Es usado en escenarios *point-to-point* para garantizar la seguridad en un canal de comunicación entre hosts. La última arquitectura, es la VPN *over* LAN, es similar a la primera, la diferencia es que se realiza dentro del ámbito de una LAN. Es de utilidad principalmente en entornos en los cuales existen redes internas grandes, en las cuales existen muchas subredes y se requiere la seguridad de ciertos servicios dentro de la red interna.

En cuanto a los principios de seguridad de la información, una VPN ofrece confidencialidad e integridad de la información transmitida. Los datos de un correo electrónico, por ejemplo, son cifrados por los protocolos que usan algoritmos para convertir la data legible en un texto cifrado que no podrá ser interpretada hasta llegar a su destino. Asimismo, usan funciones hash para validar la integridad de la información al llegar a su destino. De esta manera, la información no puede ser modificada, ni leída en todo su recorrido a través de internet, causando que usuarios terceros que malintencionadamente intenten interceptar la información, no puedan descifrar y utilizar la información obtenida.

En contraste a las bondades que ofrece la comunicación a través de una VPN, esta es criticada por su rendimiento en comunicaciones con un gran flujo de datos. Es decir, la transmisión de estos suele ser mucho más lenta de lo normal. Por lo cual, no es recomendable usar esta tecnología si se desea transmitir tráfico de datos de una aplicación que requiera de niveles bajos de latencia, *delay* y *jitter*, o un ancho de banda efectivo.

Figura 3. Diagrama de arquitectura de los tipos conexión VPN. Adaptado de “Cisco RV042 Dual WAN VPN Router”, por Cisco.com, 2011

1.7.3. Criptografía

1.7.3.1. Definición

En términos académicos, la criptografía es la ciencia y el estudio de la escritura oculta. En términos prácticos, es la ciencia que se encarga del estudio de los métodos de cifrado que se encargan de transformar un texto plano (entendible por la escritura humana) a un texto cifrado. El proceso de transformación de estos textos es llamado cifrado o “encriptación”. Sin embargo, no es correcto usar el término de encriptación, encriptado o “encriptar”, pues según la RAE, este término es un anglicismo que proviene de la palabra en inglés “*Encrypt*”, el cual es aceptado, pero no recomendado de usarse en el lenguaje español formal. El proceso usado para transformar el texto cifrado a un texto legible es llamado descifrado. Ambos procesos requieren de una clave o llave secreta para poder efectuar su objetivo. Existen dos tipos básicos de cifrado, la transposición y la sustitución. La transposición reordena los bits de la información a ser cifrada siguiendo un patrón basado en una referencia, de esta manera, los bits de la información no son cambiados, pero si son reordenados haciendo que esta sea inentendible. El cifrado por sustitución reemplaza los bits de la información por una o varias cadenas de bits de diferente tamaño, basándose en un libro de códigos. El libro de códigos sirve como una guía para convertir un bloque de bits en otro dependiendo de la definición del código. Existen muchos métodos de cifrado en la actualidad que usan uno u otro método, o incluso ambos en combinación, para hacer más efectiva la tecnología de cifrado.

En lo que respecta a la seguridad de la información transmitida a través de los canales de comunicación, la criptografía ofrece la confidencialidad, la cual previene el acceso no autorizado de la información; y la integridad, la cual previene la modificación de la información no autorizada de la información:

Figura 4. Medio de comunicación de la información cifrada y la llave. Adaptado de “Cryptography and Data Security”, por DENNING, 1982.

El criptoanálisis es la ciencia y el estudio de los métodos de “rompimiento” de la información cifrada. Un método de cifrado es rompible si es posible de determinar fácilmente cual es la llave o clave para descifrar el texto plano. Este estudio se encarga de realizar ensayos para lograr obtener la llave con la cual puedan descifrar y así romper el método de cifrado. Existen tres métodos básicos de ataque a estos métodos de cifrado:

- Ataque al texto cifrado: El criptoanalista usa los métodos necesarios para obtener la llave secreta mediante métodos como la fuerza bruta, diccionario de datos, etc.
- Ataque de texto plano conocido: El criptoanalista conoce parte del texto plano el cual quiere descifrar, en base a eso realiza ataques de descifrado de los datos.
- Ataque a un texto cifrado elegido: El criptoanalista intercepta y elige parte del texto cifrado del cual tiene el texto plano descifrado. Este escenario es el más favorable para un atacante, pues de esta manera puede obtener, mediante el análisis de ambos datos, la llave para descifrar el resto del mensaje completo.

Podemos concluir entonces que la criptografía, y por ende el cifrado, no puede proteger por si sola que la información de las claves sea obtenida o que un mensaje sea borrado.

Para ello se requerirán de otras tecnologías que complementen los beneficios de la criptografía.

1.7.3.2. Algoritmos de Cifrado

Cifrado de Transposición

Como mencionamos con anterioridad, uno de los métodos de cifrado básico es el de transposición. Este método usa comúnmente una figura geométrica para realizar el reordenamiento. La figura geométrica consta por lo general de 2 dimensiones (matriz), la cual es usada para transposicionar la información en texto plano de acuerdo con la forma de la figura, creando así la figura geométrica y por consecuencia el texto cifrado:

Figura 5. Dos pasos del cifrado de transposición. Adaptado de “Cryptography and Data Security”, por DENNING, 1982.

La primera parte del cifrado consta en escribir el texto plano dentro de la figura geométrica para obtener un texto cifrado. La segunda parte consiste en retirar el texto plano de la figura geométrica que lo contiene para obtener nuevamente el mensaje descifrado.

Cifrado por sustitución simple

Existen cuatro tipos de cifrado por sustitución, de los cuales el de sustitución simple es el más sencillo. Este cifrado consiste en reemplazar cada carácter del texto plano con un carácter correspondiente al texto cifrado. Ambos textos, el plano y el cifrado, contienen caracteres del alfabeto, sin embargo, el texto cifrado corresponde a un tipo distinto llamado el “criptoalfabeto”, el cual consiste en un alfabeto reordenado el cual convertirá cada letra del alfabeto normal a una letra del criptoalfabeto sustituyéndola en el texto cifrado.

Este método de sustitución simple puede ser empleado no solo con el alfabeto, sino también con caracteres de otro tipo de escritura. La única condición es que este debe ser mapeado de uno a uno, es decir, un carácter solo puede reemplazar a otro carácter en el cifrado.

<div> <div>⌈⋮⌋</div> <div>⌈⋮⌋</div> <div>⌈⋮⌋</div> <div>⌈⋮⌋</div> <div>⌈⋮⌋</div> <div>⌈⋮⌋</div> <div>⌈⋮⌋</div> <div>⌈⋮⌋</div> <div>⌈⋮⌋</div> <div>⌈⋮⌋</div> <div>⌈⋮⌋</div> <div>⌈⋮⌋</div> </div>											
ciphertext											
A •	B •	C •	K ⋮	L ⋮	M ⋮	T	U	V			
D •	E •	F •	N ⋮	O ⋮	P ⋮	W	X	Y			
G •	H •	I-J •	Q ⋮	R ⋮	S ⋮	Z					

Figura 6. Cifrado Churchyard. Adaptado de “Cryptography and Data Security”, por DENNING, 1982.

El cifrado Churchyard es un ejemplo de cifrado por sustitución, esta primera escritura fue descubierta en una lápida en Trinity Churchyard en Nueva York el año 1794. Luego se encontraron ejemplares de esta misma escritura en otras lápidas. La solución al cifrado no fue descubierta hasta el año 1896, más de 100 años después de su descubrimiento, la cual proponía la clave indicada en la *figura 6* mostrada.

Cifrado por sustitución homofónica

A diferencia del cifrado por sustitución simple, el cifrado por sustitución homofónica reemplaza cada carácter del texto plano, basado en un alfabeto normal, a un grupo de textos cifrados llamados homófonos.

Letter	Homophones
A	17 19 34 41 56 60 67 83
I	08 22 53 65 88 90
L	03 44 76
N	02 09 15 27 32 40 59
O	01 11 23 28 42 54 70 80
P	33 91
T	05 10 20 29 45 58 64 78 99

One possible encipherment of the message is:

M =	P	L	A	I	N	P	I	L	O	T
C =	91	44	56	65	59	33	08	76	28	78

Figura 7. Ejemplo de Cifrado por sustitución homofónica. Adaptado de “Cryptography and Data Security”, por DENNING, 1982.

Este tipo de cifrado se caracteriza por ser más complicado de descifrar, sobre todo porque la matriz de homófonos por lo general posee tantos valores por letra proporcionalmente a la frecuencia de uso de las letras en el texto plano. Esta matriz de cifrado establecida por números aleatorios que son definidos por el mecanismo de cifrado es la llave para descifrar el texto cifrado. Sin embargo, tenemos que construir esta matriz antes de realizar el cifrado también. De acuerdo con el tamaño y la cantidad de homófonos usados en la matriz, será más difícil de descifrar el mensaje para una persona no autorizada que no posea la llave del texto cifrado. Este método de cifrado básico es comúnmente usado como complemento de otros métodos de cifrado más avanzados en la actualidad, ya que este provee mayor complejidad a otras tecnologías y métodos más robustos.

Cifrado por sustitución polialfabética

Este cifrado aplica un grado superior de complejidad al cifrado simple, mientras que el cifrado simple proveía de una sustitución simple entre dos tipos de alfabetos, este cifrado hace este proceso con múltiples alfabetos en diferentes tiempos. Este cifrado fue primera vez desarrollado por León Battista Alberti, llamado el padre de la criptografía del oeste. Alberti publicó en 1568 el siguiente disco de cifrado:

Figura 8. Disco de cifrado de Alberti Adaptado de “Cryptography and Data Security”, por DENNING, 1982.

Este disco tenía la particularidad de usar el alfabeto en latín con veinte letras y cuatro números de código. La idea de Alberti era simple, cada vez que realizaba la sustitución de una letra del alfabeto, este giraba el disco con cierta frecuencia para obtener otra combinación distinta del alfabeto. De esta manera, la cantidad de alfabetos que podía

tener en distintos tiempos del proceso de cifrado era muy grande, haciendo que este método de cifrado sea muy aceptado. A partir de este primer modelo de cifrado por sustitución polialfabética, se crearon otros métodos de cifrado como el de Vigenere y Beaufort, el índice de coincidencia, el método de Kasiski, el método de cifrado por *running-key*, las máquinas de Rotor y Hagelin, el cifrado de Vernam, entre otros que usaron este método de cifrado por sustitución mucho más complejo de descifrar por personas no autorizadas.

Cifrado por Sustitución de poligramas

Este tipo de cifrado hace que el criptoanálisis sea mucho más dificultoso de realizar, ya que no posee ninguna de las características de frecuencia o alfabéticas como los métodos de sustitución anteriores, estos poseen métodos particulares de sustitución. Algunos ejemplos son los siguientes:

Cifrado *Playfair*: Este cifrado fue usado por los británicos durante la primera guerra mundial. Usa un par de letras cifradas de acuerdo con unas reglas que se establecen a través de una matriz de 5 x 5 letras.

Cifrado *Hill*: Este cifrado efectúa una transformación lineal de un texto plano para obtener una cantidad de caracteres definida.

Cifrado por Producto

Un producto de cifrado es un dispositivo que realiza el trabajo de cifrado mediante varios métodos de cifrado. Este se compone de varias funciones, las cuales pueden ser de sustitución o de transposición.

Cifrado por sustitución-permutación:

Estos dispositivos fueron creados con la finalidad de mezclar distintas funciones de cifrado, las cuales podían aplicar cifrado por sustitución en un paso, luego, podrían aplicar cifrado por transposición y operaciones lineales. La cantidad de pasos era limitada por la tecnología. Un ejemplo de estas máquinas de cifrado es la LUCIFER diseñada en IBM por Feistel, la cual usaba transformaciones que alternaban entre los métodos de sustitución y transposición para el cifrado de la información.

Figura 9. Cifrado por permutación y sustitución usada por la LUCIFER de IBM. Adaptado de “Cryptography and Data Security”, por DENNING, 1982.

Este diagrama nos muestra como era aplicado el cifrado en una máquina que contiene 12 bloques de funciones de sustitución y permutación las cuales eran aplicadas alternativamente. En la practica la maquina LUCIFER poseía más de 12 bloques, sin embargo, podemos darnos la idea de que mientras más bloques poseía el mensaje, era sumamente más complicado de descifrar el mensaje cifrado por este tipo de máquinas.

Cifrado DES (Data Encryption Standard)

El cifrado DES fue anunciado en 1977 como un estándar de cifrado para documentos no clasificados por el gobierno de los Estados Unidos. Este algoritmo de cifrado fue desarrollado por IBM como una mejora al que usaba LUCIFER. Este algoritmo de cifrado usa 64 bits en su bloque de datos con una llave de 56 bits.

Este algoritmo de cifrado y descifrado de datos posee varios pasos en su proceso de cifrado y de igual manera utiliza varios métodos de cifrado en su recorrido. Este inicia con una permutación inicial, luego es pasada a través de un bloque de 16 iteraciones de una función y finalmente es transpuesta a la inversa de la permutación inicial. Para ejemplificar el funcionamiento de este algoritmo podemos analizar la figura a continuación:

Figura 10. Algoritmo de cifrado DES. Adaptado de “Cryptography and Data Security”, por DENNING, 1982.

Entre las transposiciones iniciales y finales el algoritmo efectúa 16 iteraciones de una función “ f ”, la cual se compone de la combinación de funciones de transposición y sustitución.

El algoritmo DES es uno de los algoritmos más usados en la actualidad desde la época en que se creó. Ha sido implementado en plataformas de hardware y software, siendo los dispositivos de hardware los que poseen mayor ratio de bps (bits por segundo).

En 1976 fue demandado por parte de Diffie y Hellman la posible debilidad de este algoritmo de cifrado, luego otros como Morris, Sloane y Wyner reportaron que DES poseía dos fuertes debilidades: La primera tenía que ver con el tamaño de la llave o clave, esta era muy pequeña (56 bits), lo cual no daba la seguridad que se requería para un algoritmo de cifrado robusto el cual sería usado como estándar para el gobierno de los EE. UU. La segunda debilidad que sugerían era que los bloques “S”, los cuales hacían referencia a cualquiera de los 16 bloques de iteración, podrían tener deficiencias ocultas o también llamadas “*trapdoors*”.

Diffie y Hellman argumentaron que el algoritmo de DES podía ser roto mediante un método de fuerza bruta debido a su llave de 56 bits. Ellos formularon una máquina que consistía en millones de LSI chips, los cuales eran muy costosos en su época, la cual podría romper la llave en 10^6 días. Sin embargo, ellos argumentaban que, con el tiempo, la tecnología iba abaratarse más y el costo de estos chips iba disminuir considerablemente e incluso iban a mejorar su capacidad. Concluyendo que para los años 90, esta máquina podría romper fácilmente este algoritmo. Basándose en los hechos propuestos por Diffie y Hellman muchos años atrás, en 1998 la *Electronic Frontier Foundation* (EFF) invirtió un coste aproximado de 250,000 dólares en la construcción de una máquina de crackeado DES. Esta máquina estaba compuesta de 1536 chips los cuales podían romper un clave DES en aproximadamente 2 días. Este fue el precedente con el cual muchos se aventuraron a realizar la hazaña en menos tiempo, puesto que muchos en el gobierno de los EEUU alegaban que DES era irrompible.

Figura 11. Máquina de crackeado DES. Adaptado de “La maquinad de crackeado DES”, por WIKIPEDIA.ORG, 2004.

Cifrado de Exponenciales

Estos algoritmos de cifrado constan de un esquema basado en exponenciales computacionales sobre un campo finito. Este esquema fue publicado por primera vez en 1978 por Pohling y Hellman. Casi al mismo tiempo, fue publicado un esquema similar por Rivest, Shamir y Adleman, pero con un pequeño cambio en su estructura. Este pequeño cambio hizo que los científicos del MIT de EE. UU. Crearan un cifrado de clave pública que es llamado hasta nuestros días como Diffie y Hellman. Los esquemas Pohling-Hellman y RSA cifran la información por bloques usando exponenciales computados con métodos matemáticos complejos. A continuación, describiremos con más detalle algunos de estos métodos de cifrado por exponenciales.

Esquema de Pohling-Hellman

El esquema de cifrado Pohling- Hellman usa un módulo escogido por un número primo con varios dígitos. La seguridad en este esquema es proporcionada por la complejidad de

los logaritmos discretos que son calculados en este algoritmo. Todo este esquema depende del tamaño de la llave, que en este caso es la longitud del exponencial p . Es decir, mientras más largo es el exponencial, más tiempo se tardará en descifrar este algoritmo en un ataque de fuerza bruta.

Por ejemplo:

$$T = 2.7 \times 10^{11} \rightarrow \text{Tarda unos pocos días}$$

$$T = 1.2 \times 10^{23} \rightarrow \text{Tarda millones de años}$$

Donde:

$$T = \text{Tiempo de descifrado por fuerza bruta}$$

Entonces se puede concluir que el esquema de cifrado es muy robusto ante ataques de fuerza bruta. Sin embargo, en la actualidad existen ataques que utilizan los criptoanalistas que pueden romper la llave de este esquema en poco tiempo, sin importar la cantidad de bits que posea la llave, lo cual deja este esquema relegado en su uso como un método de cifrado moderno.

Esquema RSA (Rivest-Shamir-Adleman)

En este esquema, a diferencia del anterior, usa como modulo el producto de dos números primos de gran longitud. Este esquema de RSA puede ser usado para el cifrado de clave pública bajo una PKI, ya que este esquema usa dos factores para determinar un producto que será la llave del sistema. Este decir, uno de los factores podría ser determinado como público, ya que para que se halle la clave de ambos, es necesario ambos factores para determinar el producto. Es de esta manera, que la seguridad del sistema está basada en la

complejidad del número que resulta de la factorización que se realiza para obtener el producto “ n ”, donde p y q son los factores primos que conforman el producto del módulo.

$$X(n) = (p - 1) (q - 1).$$

Figura 12. Tiempo en computar un logaritmo discreto a un factor. Adaptado de “Cryptography and Data Security”, por DENNING, 1982.

La complejidad en este sistema depende básicamente de la selección de los números primos que son escogidos. Se recomienda que sean escogidos aleatoriamente y que ambos factores tengan aproximadamente 100 dígitos para que así el producto primo tenga 200 dígitos. Romper el esquema RSA puede dejar de ser más difícil que factorizar, ya que un algoritmo de rápida factorización automáticamente puede brindar un criptoanálisis más eficiente.

Este esquema de cifrado es usado en la actualidad por los sistemas de cifrado de intercambio de llaves asimétricas como PKI, debido a su gran usabilidad y calidad de cifrado. Asimismo, este esquema genera mensajes largos, los cuales pueden ser solucionados con el uso de funciones de resumen (hash) para así aprovechar el espacio de almacenamiento.

Cifrado Knapsack

Existen tres esquemas de cifrado Knapsack. Dos de estos tres métodos de cifrado son usados para obtener confidencialidad de la información como todos los métodos de cifrado. Sin embargo, uno de ellos, solo puede ser usado para autenticación y no para confidencialidad. En el estudio de este tipo de esquemas de cifrado realizado por Shamir, en la cual pretendía hacer un esquema Knapsack que realizara ambas funciones de confidencialidad y autenticación, no pudo hacer que estos sean usados para ambos al mismo tiempo. Esto se debía a la misma naturaleza matemática que comprendían a este tipo de esquemas, ya que eran fácilmente polinomialmente solubles.

Merkle-Hellman Knapsack

Merkle y Hellman idearon este esquema de seguridad basado en la dificultad en solucionar un problema. El problema fue adaptado de un problema propuesto por Karp Knapsack, del cual proviene el nombre del esquema. Este se basaba en determinar una solución para la siguiente ecuación si M existe.

$$C = \sum_{i=1}^n a_i m_i .$$

Por ejemplo:

Si: $n = 5$, $C = 14$, y $a = (1, 10, 5, 22, 3)$.

Entonces: $m = (1, 1, 0, 0, 1)$ es una solución.

Para solucionar esta ecuación se idearon diversos algoritmos los cuales tardaban mucho tiempo en solucionar. Este esquema se convirtió en algo difícil de resolver sin información adicional. Por otro lado, debido a esta propiedad, se convirtió en uno de los primeros algoritmos de cifrado de clave pública, el cual solo podía ser utilizado para cifrado, más no para la autenticación mediante firmas digitales. La particularidad de sus pares de llaves es que, la llave privada en si es fácil de descifrar y de almacenar, sin embargo, la llave publica es difícil de descifrar.

Graham-Shamir Knapsacks

Graham y Shamir descubrieron por separado descubrieron una manera de aminorar la creciente propiedad de *trapdoor Knapsacks*. Ellos idearon una mejora en el sistema de Merkle-Hellman, haciendo que el cifrado a implementar sea más rápido, seguro y simple de implementar a diferencia del esquema de Merkle-Hellman. Realizando algunas variantes a su propio esquema, pudieron solventar algunos de los problemas que tenía el sistema anterior. Este esquema, al ser similar al anterior, es usado solo para asegurar la confidencialidad de la información cifrada.

Shamir Knapsacks para firma digital

Este esquema de cifrado creado por Shamir trato de comprobar que los trapdoors knapsack no solo pueden ser usados para ofrecer confidencialidad mediante el cifrado de

la información. Sino que estos fueron contruidos para proveer firmas digitales. Este sistema fue creado en base al mismo problema de knapsack, pero es una extensión de esta.

$$M = \sum_{j=1}^{2k} c_j a_j \bmod n ,$$

Al igual que los sistemas anteriores, estos se basan en el mismo problema, pero propuesto de otra manera. A eso se debe que este esquema de cifrado solo pueda ser resuelto para realizar tareas de autenticación más no de cifrado. Este sistema tiene la ventaja de ser rápido, pero como los otros esquemas knapsack, no es tan conocido por la dificultad que representa en solucionar el problema completo NP (knapsack) del cual está basado.

Se puede concluir, que la criptografía y sus métodos de cifrado han existido desde la antigüedad. En la actualidad persisten varios métodos de cifrado que hemos mencionado con anterioridad, los cuales en su mayoría han mejorado sus algoritmos. Esta base de conocimientos acerca de los mecanismos de cifrado provee información acerca de cómo funcionan las tecnologías de cifrado en una PKI. La criptografía forma parte importante del proyecto, ya que permite alcanzar el objetivo de confidencialidad e integridad de la información que se requiere alcanzar con la propuesta.

1.7.4. Office 365 Message Encryption

Office 365 Message Encryption (también llamado por sus siglas, OME), es un servicio propietario de Microsoft para su servicio de Office 365. OME está basado en Microsoft

Azure RMS (*Rights Management Service*), el cual es indispensable para aplicar el cifrado de datos y las políticas necesarias para su funcionamiento. Esta tecnología basa su funcionamiento en la creación de reglas de transporte que son definidas para condicionar el cifrado de la información de los correos electrónicos. Además, son definidas por el administrador del servicio de correo electrónico de Office 365 (también llamando Exchange Online). Asimismo, para que un mensaje sea cifrado, debe cumplir con los criterios establecidos en las reglas de transporte, las cuales se aplican luego del envío del mensaje. Es decir, el trabajo de cifrado lo hace el servidor de correos y no el equipo donde se encuentra instalado el cliente de correo.

Cuando un usuario envía un mensaje de correo a través de Exchange Online, que cumpla con una regla de cifrado, este mensaje es enviado con un archivo HTML adjunto. Al ser recibido el mensaje por el destinatario, este abre el HTML adjunto y procede el mecanismo de descifrado mediante el ingreso de un usuario y contraseña asociados al servicio de Office 365 o una cuenta de usuario de Microsoft asociada al correo destinatario.

Figura 13. Diagrama de flujo de un mensaje de correo cifrado por OME. Adaptado de “Office 365 Message Encryption Mail Flow”, por OFFICE365SUPPORT.CA, 2015.

El servicio OME utiliza diversos mecanismos de seguridad avanzados para su funcionamiento. En primer lugar, el algoritmo de cifrado que utiliza es el RSA de 2048 bits, el cual permite el intercambio de llaves asimétricas. Asimismo, utiliza la función hash SHA-256 para asegurar la integridad de la información transmitida. Los mensajes de correo electrónico que pueden ser cifrados por OME, pueden ser de hasta 25MB.

En ese sentido, este servicio ofrecido por Microsoft, para la óptima seguridad de los correos electrónicos, ofrece varias funcionalidades relacionadas con la seguridad de la información, como lo son la Confidencialidad, Integridad y Autenticación. Sin embargo, desde el punto de vista de la seguridad posee algunas deficiencias. El aspecto más importante, debe ser que

OME no es un protocolo de seguridad estándar a ser aplicado en cualquier organización. Incluso, es un servicio adicional ofrecido sobre Office 365. Debido a su complejidad, la cual es básicamente la infraestructura de software que tiene como base para su funcionamiento, este servicio requiere de un alto desarrollo de los sistemas propietarios de Microsoft en la organización. Esto significa, que para implementar el desarrollo de sistema de cifrado de datos en una organización que no posea Office 365, este servicio sencillamente es imposible de aplicar. En contraste a ello, existen otros protocolos estándar como S/MIME (*Secure / Multipurpose Internet Mail Extensions*) que realizan las mismas funciones que OME sin importar la plataforma en donde este alojado el servicio de correo electrónico basado en la nube.

Otro aspecto importante, es que OME es un sistema que funciona en base a reglas de transporte. Estas reglas de transporte son configuradas en la consola de administración de Exchange Online, lo cual supone que el usuario del correo electrónico no posee el privilegio de decidir directamente que mensajes enviar a través del proceso de cifrado de datos y cuáles no. En todo caso, es posible realizar los cambios en su decisión, pero esto debe realizarse a través de una solicitud al administrador del sistema. Las reglas configuradas para la decisión del cifrado de los mensajes son susceptibles a constantes cambios, lo cual hace que la administración de este servicio de cifrado se torne rutinaria a costa del tiempo y costo para el usuario y la organización.

Según lo mencionado anteriormente, debido a que el servicio funciona mediante el uso de reglas, estas reglas son evaluadas siempre en el servidor Exchange Online antes de ser cifradas. En otras palabras, el mensaje enviado a través del servicio OME viaja desde el cliente de correo hasta el servidor de Exchange Online sin ser cifrado. El trabajo de cifrado

de los mensajes de correo electrónico es realizado por el servidor, todo el proceso de intercambio de llaves asimétricas y funciones de resumen es hecho allí, esto causa que el cliente no sea responsable de estas tareas de cifrado que puedan comprometer su rendimiento. Sin embargo, esto cambia el concepto de seguridad por intercambio de llaves asimétricas, ya que el servidor realiza la emisión del certificado y el cifrado en la misma instancia del servicio OME, formando así una figura a la cual podríamos llamar de “juez y parte” en el debido proceso cifrado. Finalmente, la seguridad de la información del correo electrónico es comprometida en este esquema de servicio de cifrado de Office 365, ya que existe una brecha en la cual potenciales amenazas de *ciberataques* como *man-in-the-middle*, *phishing*, entre otros, son fáciles de perpetrar bajo este esquema de seguridad en donde existe un tramo en el recorrido de la información en la cual esta viaja sin ser cifrada.

Figura 14. Diagrama de flujo del servicio OME en la cual se identifica una brecha de seguridad. Adaptado de “Office 365 Message Encryption (& Decryption) – Steps for Purchase, Configuration, Branding and Use – Everything you need to know”, por MICROSOFT.COM, 2014.

Identificada esta deficiencia en la tecnología de OME, se puede hacer un contraste con el protocolo S/MIME que mencionamos antes, el cual opera del lado del cliente, evitando así cualquier brecha de seguridad en el recorrido de la comunicación.

Figura 15. Esquema de funcionamiento del cifrado S/MIME donde se identifica que el cifrado proviene desde el cliente de correo electrónico. Adaptado de “S/MIME Certificate for Email Encryption”, por CYBERSECUREASIA.COM, 2015.

Asimismo, se puede identificar que este servicio no ofrece un mecanismo de firma digital, el cual es importante para complementar la seguridad de la información en el correo electrónico. Esto se debe a que las firmas digitales ofrecen autenticación y no repudio al usuario que envía el mensaje, asimismo, el receptor puede verificar que el usuario que originó el mensaje sea quien dice ser mediante la Entidad Certificadora (CA) que valida la identidad del usuario. Sin embargo, el servicio OME solo proporciona el cifrado de la información en su recorrido, y la autenticación que ofrece se valida mediante el sistema RMS. Este sistema de autenticación usado por OME funciona como un intermediario entre la CA y el usuario que hace uso del certificado. La CA usada por defecto es la del directorio activo (AD) de la infraestructura de servicios de Microsoft, el cual usa los usuarios y contraseñas del directorio para el cifrado y descifrado de la información. Sin embargo, puede

usarse otra CA externa que provea los certificados y valide la identidad de los usuarios, pero esto sería como tener una PKI solo para obtener la autenticación y no repudio que le hace falta al servicio de OME.

Finalmente, esta tecnología investigada, es una de las soluciones de seguridad de la información que existen para el cifrado de los mensajes de correo electrónico en la actualidad. Aunque no contempla la firma digital aplicada a los mensajes, este servicio ofrece en gran manera los mecanismos necesarios para ofrecer un nivel alto de seguridad en el servicio de correo electrónico. Es por ello por lo que esta tecnología ofrece un precedente importante para el desarrollo del proyecto, ya que nos brinda un panorama actual del estado en que se encuentran las soluciones de seguridad al nivel de aplicación en un servicio de correo electrónico.

1.7.5. Caso de Éxito: Planta de Certificación Digital PKI de RENIEC

El Registro Nacional de Identificación y Estado Civil (RENIEC) es un organismo público del estado, el cual vela por la identificación de las personas naturales en el país, manteniendo un registro de la información de todos los peruanos a nivel nacional. La RENIEC mantiene, actualmente, dos grandes bases de datos, la que registra las personas naturales (RUIPN) y la que almacena los registros civiles (RRCC). Para ello, posee de una amplia infraestructura de TI desplegada en todo el país.

Desde que se creó, RENIEC ha venido desarrollando sus tecnologías para la identificación y registros de los datos. Sin embargo, debido a la tendencia en el crecimiento del uso de las tecnologías para actividades cotidianas de las personas, se veía la necesidad de un medio de

identificación en ámbitos no presenciales como internet u otros medios digitales. La necesidad de identificar a las personas en estos medios se hacía más crítica, ya que, en estos ámbitos, no había garantía alguna de identificar que una persona sea quien dice ser por medios físicos como un DNI, Carné de Extranjería, etc. Es por ello, que se conceptualizó la idea de Identidad Digital, la cual busca ser la representación de una persona natural o jurídica dentro de un ámbito digital.

Para que esta identidad digital pueda existir, en el Perú se normó la Ley N° 27269, la llamada Ley de Firmas y Certificados Digitales. En base a esa Ley, RENIEC tomó la iniciativa de crear una infraestructura que pueda soportar la creación y administración de las identidades digitales, las cuales son representadas, según la ley, mediante Certificados Digitales. Esta infraestructura es llamada PKI y fue implementada en el año 2012 en el Perú. Este proyecto desarrolló una planta de certificación digital PKI con una infraestructura de hardware capaz de soportar una cantidad inmensa de usuarios. Esta planta cuenta con la primera Entidad Certificadora (CA) en el Perú, la cual busca ser un beneficio para los peruanos que requieran la emisión de certificados digitales, fomentando así el desarrollo tecnológico del país. Los principales estándares usados para la construcción de esta infraestructura de clave pública son:

1. **X.509 versión 3:** Estándar de la ITU-T que proporciona un marco para la creación de certificados digitales en un PKI.
2. **FIPS 140-2 nivel 3:** Estándar para acreditar los equipos criptográficos HSM adquiridos por la RENIEC.
3. **ISO 27001:2005:** Estándar que brinda un marco de requisitos base para implementar un Sistema de Gestión de la Seguridad de la información.

Figura 16. Infraestructura Tecnológica de la Planta PKI de RENIEC. Adaptado de “Planta de Certificación Digital PKI”, por RENIEC, 2012.

Esta planta que soporta la PKI es un ejemplo de una tecnología *On-Premise* en una Organización, la cual por lo general resulta un costo muy elevado a asumir por una entidad privada, cuyo enfoque de negocio no es ofrecer identidad digital a las personas naturales o jurídicas. Entre los servicios que ofrece la PKI de RENIEC, no existe ninguno que se haya enfocado en brindar seguridad a los correos electrónicos, mediante la emisión de certificados de tipo S/MIME. Sin embargo, este caso de éxito de PKI forma un precedente muy importante para tener en cuenta en el proyecto a desarrollar.

De esta manera, se puede concluir que el actual estado del arte, en el cual buscamos analizar los precedentes y posibles soluciones al problema planteado en el proyecto, se encuentra abierto a nuevas soluciones que ayuden a optimizar la seguridad de la información en los mensajes de correo electrónico en un servicio basado en la nube.

CAPÍTULO II: MARCO TEÓRICO

2.1. Concepto de PKI

2.1.1. Definición de PKI

Una Infraestructura de Clave Pública (PKI) es un sistema diseñado para soportar el uso de certificados digitales, firmas digitales y cifrado de datos para las organizaciones. Asimismo, permite el intercambio de la información de manera segura y privada a través del uso de un par de llaves, pública y privada, las cuales se obtienen a través de una entidad tercera confiable. Este sistema basa su importancia en la seguridad de la información en redes no seguras como internet, debido a que la gran mayoría de aplicaciones, en la actualidad, basan sus operaciones en la nube.

Otros autores definen la PKI como:

“(...) una infraestructura compleja compuesta por hardware, software, bases de datos, redes, procedimientos de seguridad y obligaciones legales.” (INDRA, 2005: 22)

“Una Infraestructura de Clave Pública (PKI) es la plataforma básica de gestión de certificados digitales (credenciales PKI) para la implementación de mecanismos de autenticación y firma electrónica.

Las credenciales PKI basan su fortaleza en el uso de algoritmos criptográficos alcanzando niveles de confianza muy altos, por los que son las adoptadas para infraestructuras de identificación gubernamentales críticas y prestadoras de certificación reconocidos.” (SAFELAYER, 2012)

Como mencionan estas definiciones, la importancia que tiene una PKI y su principal fortaleza recae en los algoritmos criptográficos que utiliza para asegurar que la información estará protegida ante cualquier amenaza externa. Asimismo, provee certificados digitales que ofrecen identidad a personas naturales u organizaciones.

Una PKI controla el uso de la criptografía de clave pública que se emplea en los métodos de autenticación de un emisor de un mensaje enviado a través de internet, así como el cifrado del mismo.

2.1.2. Principios fundamentales de una PKI

El concepto de PKI, en su totalidad, está basado en la Confianza, pues la información que se transmite dentro de la infraestructura está dentro de un marco de confiabilidad entre todas las partes. La confiabilidad es en esencia el principal requisito que se debe tener en una PKI, ya que dentro de toda la infraestructura implementada por la PKI se observa la relación de confianza que existe entre todos sus componentes. Dentro del marco de la confiabilidad que se debe dar en el sistema, existen cuatro principios fundamentales que se deben cumplir en toda PKI.

2.1.2.1. Confidencialidad

La confidencialidad en una PKI se cumple a través del cifrado asimétrico que se maneja con una clave pública y privada en el sistema. Es decir, se logra al permitir que la comunicación de ambas partes, a través de redes inseguras, está protegida de ser leída. Asimismo, otra definición, citando al autor *Vacca*, dice lo siguiente:

“Confidentiality of information assures users that their communications are safe and readable only by the intended recipients. Message encryption using digital certificates assures this confidentiality.” (Vacca 2005: 34)

En esta cita, el autor señala, de manera resumida, cual es el control de seguridad usado para asegurar la confidencialidad en la comunicación. Es así como el uso del cifrado con certificados digitales dentro de una PKI previene totalmente que los documentos o mensajes enviados a través de la red de datos sean observados por personas no autorizadas, evitando así un posible robo de información confidencial a nivel crítico.

2.1.2.2. Integridad

Otro beneficio importante que una PKI ofrece, es la Integridad mediante el uso de certificados digitales y funciones hash, los cuales pueden ser usados para garantizar que los datos no sean manipulados en su transmisión. Asimismo, *Vacca* describe de manera sencilla como una PKI asegura la integridad de los datos que son transmitidos en redes inseguras:

“Integrity of data guarantees that message contents are not altered during the transmission between the originator and the recipient. PKIs provide for digital signatures to ensure the integrity of all transmitted information.” (Vacca 2005: 34)

El autor señala cuán importante es la integridad, indicando que el contenido del mensaje que se transmite entre ambas partes que intervienen en una comunicación no deben ser alteradas. Asimismo, se observa que dentro de una PKI se hace uso de las firmas digitales, los cuales junto con los certificados digitales ayudan a garantizar que

la información permanezca incorruptible, protegiendo así la información corporativa frente a posibles ataques de *Man-in-the-Middle* que traten de alterar el contenido para fines que atenten a la disponibilidad, confiabilidad y prestigio de la organización, lo cual finalmente se traduce en pérdidas monetarias.

La definición de Integridad corresponde a la cualidad de íntegro, lo cual describe que algo no carece de ninguna de sus partes. Así pues, la integridad de la información, dentro del marco de la seguridad de la información, es la cualidad que tiene todo documento o mensaje que no ha sido alterado y que además permite comprobar que no se haya producido alguna manipulación con respecto al documento o mensaje original.

2.1.2.3. Autenticación

La Autenticación o Identidad del origen de la información, la cual se realiza por medio de los certificados digitales y firmas digitales que usa una PKI. Asimismo, *Vacca* también describe de manera sencilla cómo una PKI, por medio de la autenticación frente a un tercero confiable, asegura que la información transmitida realmente corresponda a las partes involucradas en la comunicación:

“User authentication enables systems and applications to verify that users are who they claim they are and have the authority to access the resource. PKIs use digital signatures and user certificates to assure the authentication of all end entities and system resources.” (Vacca 2005: 34)

El autor hace énfasis al beneficio que se obtendrá al asegurar que los participantes (usuarios, sistemas o aplicaciones) de una comunicación bajo la PKI sean realmente quienes dicen ser, mediante los mecanismos de firmas y certificados digitales que son validados por una Autoridad Certificadora (CA). Esto permite que la organización este siempre protegida ante cualquier intento de suplantación dentro de la red interna o externa, y esté libre con accesos no autorizados desde cualquier ubicación de la red.

La definición de Autenticación según la Real Academia Española (RAE) es el efecto de autenticar, el cual acredita como cierto o auténtico a alguien o algo. Sin embargo, dentro de un contexto de seguridad de la información, la autenticidad de la información está relacionada con la autenticación de todas las partes involucradas en un proceso. De manera aplicada, por ejemplo, se refiere a la verificación de la identidad de un usuario. La autenticación se produce cuando el usuario puede, de algún modo, demostrar quien dice ser, a partir de ese entonces se le considera como un usuario autenticado.

2.1.2.4. No Repudio

El No Repudio en una comunicación que se realiza en una PKI se manifiesta mediante el uso de firmas digitales para validar la identidad de ambas partes. Es decir, en el intercambio de mensajes entre ambas partes, ninguno de los dos puede negar la existencia o ejecución del mensaje. Por otro lado, Vacca describe este concepto de la siguiente manera:

“Non-repudiation prevents users of the PKI to deny that they have participated in a transaction or sent a message to another user or

resource. With a legitimate digital signature in hand and the legitimate digital certificate that accompanies it, the chances that a message is forged or originated elsewhere approach zero.” (Vacca 2005: 34)

El autor hace énfasis a destacar que el No Repudio en una PKI previene que los usuarios participantes nieguen ser los originarios de un mensaje enviado. Por otro lado, esto se logra gracias a que la firma digital que se adjunta en los mensajes posee un certificado digital que legitima la identidad del usuario ante una CA que es de confianza entre ambas partes. En consecuencia, este principio de una PKI asegura que las probabilidades de que el mensaje pueda haber sido enviado por otra persona, que no sea dueño del certificado digital, sean cero.

2.1.3. Conceptos de seguridad que aplica

2.1.3.1. Autenticación

La autenticación es un proceso básico de seguridad que verifica la identidad de un usuario. Este es uno de los primeros procesos de control de accesos que se da en un marco de seguridad de la información, el cual acredita que una persona sea quien dice ser. La autenticación se basa en tres factores de identificación, los cuales pueden funcionar uno o los tres la misma vez.

El factor más básico del cual se basa la autenticación es en algo que sabe el usuario. Esta forma de autenticar la identidad ha sido la más básica por mucho tiempo, por lo general consta de pedir al usuario un usuario y contraseña que solo el “conoce”. Sin embargo, a lo largo de los años, ha dejado de ser un método efectivo de autenticar,

debido a la facilidad con la que este método de autenticación puede ser vulnerado por los atacantes. Otro factor que se originó, con la finalidad de fortalecer la autenticación complementando el primer método antes mencionado, es algo que el usuario posee. Esta forma de autenticar se ve en la actualidad en el uso de tarjetas de proximidad, tarjetas inteligentes, *tokens*, etc. Estos métodos de autenticar aún pueden ser falsificados por los atacantes con cierta complejidad. Finalmente, el factor más complejo de autenticación, tanto para su implementación y su vulnerabilidad, es algo que representa lo que el usuario es. Los métodos de autenticación de este tipo son biométricos y la forma más robusta de autenticación. El usuario tiene que validar su identidad con algo que no puede cambiar, como su huella digital, iris de ojos, etc. A pesar de que estas cualidades del usuario no son secretas, son mucho más complicadas de obtener o falsificar.

La combinación de estos 3 factores de autenticación hace que la validación de identidad del usuario sea más robusta. Asimismo, una PKI representa la manera más segura de asociar la representación digital de cada uno de estos 3 factores de autenticación a un certificado digital, el cual identifique al usuario para el control de los accesos no autorizados y la validación de la identidad en cualquier sistema que se beneficie de la autoridad certificadora de una PKI.

Figura 17. Ejemplo de Tarjeta inteligente de autenticación. Adaptado de “Formación PKI – Seminario de Infraestructura de Clave Pública”, por INDRA, 2005.

2.1.3.2. Cifrado asimétrico

El cifrado tradicionalmente usado desde los inicios de la criptografía, fue el cifrado simétrico. Este tipo de cifrado comparte una única llave secreta para cifrar la información y por lo general era enviada por el mismo medio en donde se envía el mensaje. El cifrado simétrico es usado por algoritmos como el DES, los cuales son usados para redes privadas, ya que el uso de este tipo de cifrado no es seguro para redes públicas como internet.

En respuesta a esa oportunidad, nacen los algoritmos de cifrado asimétrico. Este tipo de criptografía asimétrica es usada por las PKI, las cuales se valen de un par de llaves para cifrar la información. Una llave es usada para cifrar la información y la otra es usada para descifrarla. Ambas claves no pueden descifrar por si solas el mensaje y no se puede obtener la otra clave teniendo solo una de ellas. Este tipo de criptografía usada en una PKI funciona de manera más lenta, ya que el intercambio de llaves y el cifrado y descifrado requiere de más procesamiento en comparación a un cifrado tradicional simétrico. Sin embargo, esta desventaja se ha ido mitigando con el tiempo y el

crecimiento de la tecnología, por el contrario, ha permitido obtener un cifrado ampliamente más seguro con el cual se optimiza la seguridad criptográfica de los sistemas. Algunos ejemplos de estos algoritmos de cifrado asimétrico, que son usados en una PKI, son el RSA o el ECDSA.

Figura 18. Comparación entre cifrado simétrico y asimétrico. Adaptado de “Formación PKI – Seminario de Infraestructura de Clave Pública”, por INDRA, 2005.

2.1.3.3. Funciones de resumen

La función de resumen o método hash, es un método para obtener una huella digital virtual de un mensaje dado representado en un código. Este es un código único que se genera a partir de una función de resumen que reduce el tamaño de mensaje a un código representativo y de tamaño único. El código generado por la función hash es usado para validar la integridad de un mensaje mediante los algoritmos de hash que resumen y validan la información. Algunos de estos algoritmos son el MD4, MD5, SHA1, SHA2 y SHA3.

Figura 19. Representación de una función hash. Adaptado de “Public key infrastructure: building trusted applications and Web services”, por VACCA, 2004.

Las funciones de resumen son usadas por las firmas digitales dentro de una PKI. Los códigos generados por los algoritmos son usados para firmar digitalmente el mensaje y este es enviado adjunto con el mensaje en sí mismo con la finalidad de validar la integridad de la firma digital en el lado del receptor.

2.1.3.4. Firma digital

Con el objetivo de lograr la integridad, autenticación y no-repudio de un mensaje, este se firma digitalmente mediante el uso de llaves asimétricas que se manejan en una PKI.

Figura 20. Esquema de firma electrónica. Adaptado de “Formación PKI – Seminario de Infraestructura de Clave Pública”, por INDRA, 2005.

En la *figura 20* se observa el funcionamiento del mecanismo de firmado digital. Como primer paso, se observa que el mensaje que se encuentra en estado natural pasa a ser codificado con una función de hash, el cual hace que la información deje de ser entendible por el ser humano. Luego, para asegurar que esta información no sea interceptada, ni recibida por alguien más que no esté autorizado a leerla o modificarla es que se firma el mensaje con la llave privada del emisor. De esa forma, la información viajará por la red con un cifrado de clave privada del emisor que se dirige a un receptor en particular.

Para entender mejor el funcionamiento, se explicará mediante un ejemplo real en el cual intervienen dos usuarios en una comunicación con firmas electrónicas.

Figura 21. Ejemplo de Integridad de la información con firmas digitales. Adaptado de “Conceptos de Seguridad”, por NORTHSECURE.ES 2013

En el ejemplo de la *figura 21*, se tiene nuevamente la comunicación entre Andrea y Bruno, esta vez con el uso de cifrado y firma digital para su comunicación. En primera

instancia, se observa que Andrea esta vez ha generado una función de resumen del mensaje con una función *hash*, para luego cifrar la función con la clave pública de Bruno y firma su mensaje con su firma digital. Luego, Andrea envía el mensaje cifrado junto con su firma digital, entonces, cuando Bruno recibe el mensaje lo descifra con su clave privada y luego pasa a comparar las funciones de hash. Si la función de hash coincide con la que ha generado Bruno, entonces quiere decir que el mensaje no ha sido manipulado en su recorrido y ha llegado íntegramente al destinatario.

Entonces, se puede argumentar que una PKI ofrece el beneficio de la integridad a través de firmas digitales que pueden ser usadas para probar que el mensaje no ha sido alterado en su transmisión. Además, está el hecho de que el mensaje firmado digitalmente, el cual es enviado a un destino en específico, no puede ser alterado o suplantado, ya que el destinatario espera una firma digital que corresponda a la clave pública que posee para poder descifrar un mensaje, y este solo puede ser enviado de un emisor que posee esa llave privada, con lo cual se estaría evitando que el mensaje sea alterado intencionalmente o enviado desde un emisor que intenta enviar información falseada.

2.1.4. Tecnologías que utilizan una PKI

2.1.4.1. Cryptographic Message Syntax (CMS)

Es un estándar definido por la IETF, el cual establece las pautas de la firma digital, funciones de resumen, autenticación y cifrado de mensajes. Su principal ventaja es que define estructuras de datos y procesa dichas estructuras para el firmado digital y cifrado de datos. Es por ello, que es llamado también como sintaxis de

encapsulamiento. Este estándar es soportado por el estándar X.509, el cual es usado por la PKI que emite certificados digitales como S/MIME, el cual usa esta sintaxis como componente básico en su funcionamiento.

2.1.4.2. SSL

El protocolo SSL (*Secure Sockets Layer*) opera desde la capa de transporte de datos hasta la capa de presentación del modelo OSI. Este por lo general opera con otros protocolos de capas superiores como el HTTP e IMAP. Permite a un servidor y su cliente autenticarse a sí mismos en una comunicación, lo cual les permite establecer una conexión cifrada entre ambos. Este protocolo ha sido adoptado por los servicios web como la manera más segura de autenticar y cifrar la comunicación entre el cliente y el servidor. Asimismo, permite al cliente y al servidor seleccionar los algoritmos de cifrado y de resumen con los que sean compatibles. Además, utiliza el cifrado de clave pública para validar la autenticidad de un servidor mediante los certificados digitales emitidos por una CA que sea de confianza por ambas partes.

2.1.4.3. S/MIME

Es una versión modificada del protocolo MIME (*Multipurpose Internet Mail Extension*) que soporta el cifrado de los mensajes de correo electrónico. Este estándar está basado en la criptografía asimétrica. Asimismo, está basado en el cifrado de clave pública RSA. En el entorno empresarial es de mucho interés el uso de S/MIME para aplicar seguridad a los mensajes de correo, ya que estas ofrecen confidencialidad e integridad que se necesitan por las regulaciones a las que están sometidas. Para usar esta tecnología, en primer lugar, se debe activar en el entorno empresarial el uso de

una PKI básica, la cual provee los certificados digitales y el intercambio de llaves asíncronas que esta requiere.

Para la optimización de la seguridad en el envío de los mensajes de correo electrónico a través de una red insegura como internet, es que se requiere este estándar de cifrado, ya que previene el acceso no autorizado a la información del mensaje o la modificación de esta. Por lo general, las organizaciones que implementan este mecanismo de seguridad en sus comunicaciones de correo electrónico evalúan la implementación de una PKI o la adquisición de un servicio externo de acuerdo con los intereses del negocio.

2.1.4.4. VPN

Una VPN, como ya se describió en el estado del arte, es una tecnología de seguridad que genera una conexión privada entre un punto y otro de la comunicación. Esta conexión es protegida mediante el uso de protocolos de comunicación segura como SSH, los cuales usan mecanismos de cifrado de datos. En ese sentido, las VPN requieren de certificados digitales para realizar el cifrado asimétrico en sus comunicaciones, por lo cual, requieren de una PKI para la emisión de los certificados y el intercambio de llaves. Asimismo, una VPN requiere de una PKI para autenticar las conexiones punto a punto que utilizan, ya que utilizar un certificado autofirmado como se hace actualmente aumenta las probabilidades de los ataques realizados a estos sistemas de cifrado no seguros. Es por ello, que es recomendable el uso de certificados digitales provenientes de una PKI que aplican cifrado asimétrico al canal de comunicación virtual implementado por esta tecnología.

2.1.4.5. PGP

Es un sistema de cifrado que protege el intercambio de los mensajes de correo, seguridad de archivos y conexiones de red a través de la criptografía de clave pública. Es un programa que protege la privacidad de los archivos y de los correos electrónicos mediante el uso de cifrado asimétrico. Este estándar compite con S/MIME, sin embargo, ambos poseen una gran diferencia. En una organización que hace uso de un PKI para la aplicación del cifrado asimétrico, es el trabajo de la CA la emisión de certificados X.509 para validar a los usuarios. Por otro lado, en una organización que no cuenta con una PKI, este programa genera sus propios certificados que luego deben ser validados por una CA para definir si cumplen o no con el estándar. En conclusión, este sistema ofrece tanto un cifrado simétrico, para mejorar la velocidad de cifrado de la información, como un cifrado asimétrico para asegurar el intercambio de llaves y la autenticidad de los certificados PGP.

2.2. Arquitectura de una PKI

2.2.1. Componentes de una PKI

Una PKI consta de diversos componentes y un modelo que lo soporta para su aplicación:

Figura 22. Componentes de una PKI. Adaptado de “Formación PKI – Seminario de Infraestructura de Clave Pública”, por INDRA, 2005.

En la figura 22 se presentan los diversos componentes de una PKI, los cuales no siempre son implementados en todas las soluciones, ya que esta arquitectura es modular y se implementa dependiendo de las necesidades de la organización.

2.2.1.1. Entidad Certificadora

La Entidad Certificadora o la Autoridad de Certificación (CA) es la entidad de confianza dentro de la infraestructura y se encarga de garantizar, de manera categórica, la identidad asociada a un certificado digital. Además, posee otras funciones, como la de recibir y procesar peticiones de certificación de los clientes, consultar a la Autoridad de Registro (RA) para determinar si se rehúsa o acepta una petición de certificado, emitir el certificado digital una vez se haya aprobado, gestionar la Listas de Revocación de Certificados (CRL) y renovar certificados digitales que hayan expirado por algún motivo.

2.2.1.2. Entidad de Registro

La entidad de registro o Autoridad de Registro (RA) es la encargada de gestionar el registro de los usuarios y sus peticiones de certificación o revocación, este acepta o deniega la creación de un certificado dentro de la PKI. Además, da la orden a la Autoridad de Certificación si se debe emitir un certificado. Asimismo, es el encargado de asociar la clave pública con el titular del certificado y gestionar el ciclo de vida de un certificado digital.

La RA es una entidad opcional en la infraestructura de clave pública, ya que solo funciona como un mediador entre la CA y el suscriptor del certificado. El trabajo de la RA es importante porque reduce la carga de la CA y administra de manera ordenada la solicitud de emisión de certificados. La RA debe estar igualmente autenticada por la CA mediante un certificado especial que la CA emite para las autoridades de registro que existan en la PKI. Cabe resaltar que una CA puede manejar varias RA dentro de la infraestructura.

2.2.1.3. Subscriber

El suscriptor o simplemente titular del certificado digital pueden ser personas naturales, jurídicas o cualquier entidad a la cual se le haya emitido un certificado.

Figura 23. Suscriptor persona natural de un certificado digital. Adaptado de “Firma electrónica y certificados digitales”, por ADLE, 2010.

En la *figura 23*, se observa que el certificado digital le pertenece a una persona natural que se identifica con su documento de identidad, de la misma manera, es posible identificar organizaciones u otras entidades que requieran que su autenticidad sea validada por una CA de confianza.

2.2.1.4. Repositorio

El repositorio proporciona almacenamiento y distribución de los certificados digitales y Listas de Revocación (CRL) a la CA, ya que cuando este emite un certificado digital inmediatamente se almacena en el repositorio. La manera como se acceden luego a estos certificados y las CRL que se encuentran en el repositorio es por medio del protocolo LDAP (X.500); de esta manera, el usuario puede obtener los certificados de

otros usuarios, así como comprobar el estado que tienen actualmente. El directorio en donde se almacenan los certificados digitales y las CRL se suponen de consulta libre para las partes utilizadoras que soliciten información de los mismos.

2.2.1.5. Parte Utilizadora

Existen partes que consultan y confían en los certificados emitidos por una entidad certificadora y usan el certificado para comunicarse y realizar transacciones con sus suscriptores. Asimismo, las partes utilizadoras verifican la firma electrónica que se encuentra dentro del certificado para poder validar su identidad.

Figura 24. Diagrama de Parte utilizadora vs Suscriptor (Servidor Web). Adaptado de “Formación PKI – Seminario de Infraestructura de Clave Pública”, por INDRA, 2005.

En la figura 24, se describe como la parte utilizadora puede ser una aplicación web o un usuario que accederá a dicha aplicación, y a su vez, la aplicación se comunica con el titular del certificado para que valide la legitimidad de la página web y así el usuario que requiere del servicio web pueda navegar de manera segura.

2.2.1.6. Autoridad de Validación

Una autoridad de validación (VA) es una entidad similar a la RA, la diferencia es que esta solo se encarga de recibir las peticiones de información de estado de los certificados digitales. Estas peticiones son realizadas a esta entidad mediante el protocolo OCSP (*Online Certification Status Protocol*) definido por la IETF RFC 6960. La petición del estado de validez de un certificado digital, a diferencia de las Listas de Revocación (CRL) que validan cada vez que se descargan las listas de la CA, se realizan en tiempo real.

2.2.2. Procesos en una PKI

2.2.2.1. Validación

La validación es el proceso en el cual se verifica la información del certificado, si algún dato del certificado ha cambiado o si sigue valido en el tiempo en que se consulta. La validación puede hacerse directamente a la CA o se puede obtener esta información fuera de línea a través de las CRL o mediante el protocolo OCSP para una validación en línea.

2.2.2.2. Revocación

Muy similar al proceso de validación, la revocación es el proceso de informar a los usuarios que la información en un certificado digital ya no es válida. El método más común de validar esta información es mediante las Listas de Revocación de Certificados o CRL, la cual consiste en una lista emitida periódicamente por la CA con los certificados cuya validez ha sido revocada o expirada. En los inicios de las PKI existían problemas con la actualización de las listas, debido a su extenso tamaño y

tiempo en procesarse cada vez más largo. Sin embargo, este problema fue solucionado más adelante por el mismo estándar ITU-T X509, añadiendo un “Delta CRL”, el cual consistía en enviar una lista más pequeña de cambios en vez de enviar la totalidad de la lista de revocación publicada.

2.2.2.3. Autenticación

Como se explicó anteriormente, el proceso de autenticación en el funcionamiento de una PKI tiene que ver con la validación de la identidad del usuario mediante un método de autenticación por contraseña, código PIN, tarjeta inteligente o identificación biométrica, o simplemente la combinación de todos. En este paso, el usuario se identifica en la PKI para poder tener acceso a su clave privada

2.2.2.4. Intercambio de llaves asimétricas

Para asegurar la confidencialidad de la información, la PKI acude al mecanismo de cifrado asimétrico, el cual se caracteriza de la siguiente manera:

Figura 25. Diagrama de cifrado Asimétrico. Adaptado de “Firma electrónica y certificados digitales”, por ADLE, 2010.

La figura 25 muestra como un texto común en formato plano y entendible para una persona, se cifra mediante el uso de una llave pública del destinatario; asimismo, antes de ser cifrado, este mensaje se transforma mediante una función hash de resumen, el cual hace que el mensaje sea codificado a una longitud de caracteres fija. Luego, el mensaje es cifrado en un formato irreconocible para el ojo humano que se envía al receptor, el cual realiza la acción de descifrado del mensaje. Este paso lo realiza con ayuda de la llave privada que el posee el destinatario y que solo él conoce. De esa manera, el mensaje llega a su destino sin que sea visto por terceras personas que traten de acceder indebidamente a la información.

Existen diversos tipos de cifrado asimétrico que pueden ser usados en una PKI, pero:

“(...) Hasta la fecha han aparecido multitud de algoritmos asimétricos, la mayoría de los cuales son inseguros; otros son poco prácticos, bien sea porque el criptograma es considerablemente mayor que el mensaje original, bien sea porque la longitud de la clave es enorme. Se basan en general en plantear al atacante problemas matemáticos difíciles de resolver (...). En la práctica muy pocos algoritmos son realmente útiles. El más popular por su sencillez es RSA, que ha sobrevivido a multitud de ataques, si bien necesita una longitud de clave considerable. Otros algoritmos son los de ElGamal y Rabin” (LUCENA 2010: 171)

Para entender mejor el concepto, se ejemplifica un caso de cifrado de información entre una aplicación de correo electrónico y un usuario:

Figura 26. Ejemplo de cifrado de la información. Adaptado de “Conceptos de Seguridad”, por NORTHSECURE.ES 2013

En el ejemplo, se observa que Andrea quiere enviar un mensaje a Bruno y que solo pueda ser leído por Bruno. Para ello, Andrea usa su cliente de correo con seguridad de cifrado asimétrico, es decir, ella posee dos llaves, una privada que la conoce solo ella y una llave pública que la conoce todo el mundo. Asimismo, Bruno posee dos llaves de la misma forma que Andrea. El primer paso que se efectúa en el cliente de correo de Andrea es que el mensaje que va dirigido a Bruno se cifra con la llave pública de Bruno debido a que todo el mundo la conoce. Luego, Andrea envía el mensaje a través de la red y este es recibido por Bruno, el cual conoce que el mensaje es enviado hacia él y este procede a descifrar el mensaje con su propia clave privada que solo él conoce. Finalmente, el mensaje es leído solo por Bruno ya que nadie más puede tener la clave privada que posee Bruno la cual funciona de manera conjunta con su llave pública para descifrar el mensaje.

2.2.3. Estructura de una PKI

2.2.3.1. Diseño estructural

A continuación, se muestra el modelo o diseño base de la Infraestructura de Clave Pública (PKI):

Figura 27. Diseño base de una PKI. Adaptado de “Formación PKI – Seminario de Infraestructura de Clave Pública”, por INDRA, 2005.

En una comunicación realizada sobre una PKI, entre un cliente y una aplicación o sistema como se muestra en el ejemplo, se efectúan varios controles de seguridad los cuales ayudaran a que la información no sea alterada, vista o suplantada durante todo su recorrido. En una primera instancia, se observa que el usuario debe registrarse por medio de la entidad de registro o RA, luego de ser aceptada por la RA se procede a enviar la solicitud a la CA para que emitir el certificado al usuario. Por último, la CA envía nuevamente a la RA para que este asigne el certificado al usuario. Además, la información de los certificados y las CRL es almacenada en un directorio donde se puede consultar su información. Finalmente, dentro de la infraestructura, se observa

una entidad de validación, la cual es opcional. Esta entidad se encarga de recibir la información de los certificados y las CRL para su consulta por parte de los usuarios en línea (on-line), esta información es consultada mediante el protocolo OCSP en los clientes compatibles con este protocolo.

2.2.3.2. Diseño funcional

Para explicar el funcionamiento funcional de una PKI se puede ejemplificar en un esquema inicial muy sencillo que a continuación se pasará a explicar:

Figura 28. Diagrama de bloques funcionales de una PKI básica. Adaptado de “Public key infrastructure: building trusted applications and Web services”, por VACCA, 2004.

Este diagrama (*figura 28*) muestra el funcionamiento de la infraestructura de clave pública en tres grandes bloques. El primero, llamado CA, es el encargado de los procesos básicos de certificación y generación de listas de revocación en la infraestructura. Es el núcleo del sistema en la cual todos los demás clientes y componentes basan su confianza. Este bloque está compuesto, por lo general, de la Autoridad de Certificación y la autoridad de registro, ya que ambos conforman parte esencial en el proceso.

El segundo bloque, mostrado en la *figura 28* como CS (*Certificate Server*) y CRS (*Certificate Revocation Server*), es donde se realizan los procesos de almacenamiento y administración de los certificados y listas de revocación. Estos no deben tratarse como entidades de confianza, ya que funcionalmente solo se trata de un directorio en donde se administra la distribución de los certificados digitales y las CRL. Este bloque está compuesto por el repositorio y una posible Autoridad de Validación. Eventualmente, podría tener funciones de base de datos en donde se realizan las consultas de datos acerca del estado y la información de los certificados digitales.

Finalmente, el tercer bloque, es en donde se realizan los procesos del lado del Cliente y opera en conjunto con una API que funciona como interface para los servicios de la PKI. El cliente o parte utilizadora utiliza los certificados digitales o listas de revocación de una PKI mediante aplicaciones que son compatibles con los protocolos y estándares de criptografía asimétrica. La principal función de este bloque es utilizar los certificados digitales para brindar seguridad a las aplicaciones y servicios corporativos mediante el uso de cifrado y firmas digitales.

2.3. Estándares de una PKI

2.3.1. Estándar ITU-T X.509

La ITU (*International Telecommunications Union*) es una organización internacional que coordina las telecomunicaciones a nivel mundial. La sección ITU-T es una sección de la organización encargada de investigar y desarrollar estándares de telecomunicaciones. El estándar X.509 está diseñado para definir los lineamientos en el formato de los certificados

digitales y las listas de revocación para una infraestructura de clave pública. Asimismo, dicho estándar define el formato, diseño y funcionamiento de algunos componentes básicos de la PKI, pero no todos los componentes de esta. Según este estándar, el certificado digital que será usado para cifrar la información del correo electrónico y firmar el mismo, debe cumplir con el formato de certificado, el cual incluye los siguientes campos básicos:

Tabla 2

Campos de un Certificado Digital ITU-T X.509 versión 3

Versión
Número de serie
Firma
Emisor
Periodo de validez
Sujeto
Clave pública del sujeto
Extensiones

Nota. Adaptada del estándar ITU-T X.509 - Information technology – Open systems interconnection – The Directory: Public-key and attribute certificate frameworks, por la ITU-T, 2012.

a. Versión:

La versión que se usa en la actualidad es la **versión 3**, pues como se explicó anteriormente, es la que se encuentra en vigencia y todas las implementaciones de PKI deben cumplir con esta versión para asegurar su interoperabilidad con las demás CA a nivel mundial.

b. Número de serie:

El valor de número de serie es un valor numérico entero único definido por la entidad certificadora (CA), este valor no lo define manualmente el administrador de la PKI. Por lo tanto, es un valor aleatorio que se mostrará al momento de que la CA emita un certificado digital S/MIME en base a una de las plantillas.

c. Firma:

Este campo también es llamado “Algoritmo de firma”, el cual puede agregar un campo complementario indicando el algoritmo de hash para la firma. En este campo se definirán los tipos de algoritmo con la cual se creará la firma digital y el algoritmo con el cual se efectuará el intercambio de claves.

d. Emisor:

En este campo se identifica el nombre del emisor con el formato DN (*Distinguished Name*), el cual es un modelo de nombre definido en el estándar ITU-T X.501. Este campo será automáticamente definido por la CA que emite el certificado, ya que este debe identificarse a sí mismo como emisor del certificado.

e. Periodo de validez

Para la definición del periodo de validez, se debe definir antes el ciclo de vida del certificado (el cual veremos más adelante en Definición del ciclo de vida del certificado). En este campo se determina cuál es el periodo de validez que tendrá el certificado. Este campo es de tipo fecha y está dividido en dos campos, **valido desde** y **válido hasta**, el cual, según el estándar X.509 v3, debe estar con el horario UTC (*Coordinated Universal Time*) y bajo el formato *YYMMDDHHMMSS* (año, mes, día,

hora, minutos y segundos). Por lo tanto, este par de campos es necesario para saber la caducidad del certificado.

f. Sujeto:

El campo de sujeto se define según el estándar X.501 con un DN compuesto por los datos del usuario que serán usados para identificarlo y ubicarlo dentro de la organización.

g. Clave pública del sujeto

En este campo se guarda la clave pública del usuario al cual se le ha emitido el certificado digital. La longitud de la clave pública depende del algoritmo que se ha definido para el uso de los certificados digitales. Esta clave se muestra en formato hexadecimal y en la parte de valor se muestra el algoritmo de cifrado asimétrico.

h. Extensiones

Este no es un campo propiamente dicho, sino, un conjunto de campos adicionales que se pueden crear a disposición del administrador de la PKI. Los campos adicionales son opcionales y dependen de la información adicional que se quiera mostrar por parte de la organización. El proveedor de la PKI crea estos campos adicionales, sin embargo, no es un factor clave para el funcionamiento del certificado digital.

2.3.2. Estándar PKCS

Es un estándar desarrollado por los laboratorios de la RSA. Se trata de una serie de especificaciones de carácter público acerca de la criptografía de clave pública desarrollada en conjunto con muchos desarrolladores alrededor del mundo. Dentro de estas especificaciones, hay algunas que son de especial interés para el diseño de una PKI.

La PKCS #10 es el estándar encargado de definir la sintaxis de las peticiones de certificación que hace un suscriptor a una CA o RA. Esta petición es luego respondida por la CA emitiendo un certificado basado en el formato ITU-T X.509. La petición procesada por la RA o CA puede incluir información adicional a ser incluida en el certificado en base a los atributos que fueron enviados en la petición.

La PKCS #12 define el estándar para la sintaxis del intercambio de información personal, la cual especifica el formato que debe cumplir el método de transporte o almacenamiento portable de la clave privada o certificado digital de un usuario. Los sistemas que usan este estándar podrán transferir y almacenar, entre los sistemas, la información privada de un usuario en la infraestructura de manera segura.

La PKCS #7 es el estándar encargado de definir la sintaxis criptográfica de un mensaje. Este provee la sintaxis a la información que haya sido cifrada, por ejemplo, a una firma digital. La sintaxis permite la recursión dentro del sistema, lo cual significa que un mensaje que ya haya sido firmado pueda ser firmado más de una vez. Asimismo, ofrece atributos adicionales como la hora de firmado, la cual permite que el mensaje firmado pueda ser autenticado con su contenido. Este estándar es comúnmente aplicado en certificados digitales S/MIME para el cifrado y firma digital de mensajes de correo electrónico.

2.3.3. Estándar IETF

La IETF es una comunidad internacional conformada por desarrolladores, proveedores, operadores e investigadores que están comprometidos al desarrollo de las tecnologías sobre internet. La IETF trabaja en grupos de trabajo, la cual está definida por especialidades o áreas del conocimiento específicas. Estos grupos se encargan de proponer nuevos estándares y RFC (*Request For Comments*). El grupo que trabaja en el desarrollo de las PKI es la *PKIX Working Group*. Este grupo se encarga de desarrollar estándares que soporten la tecnología PKI basados en los estándares de certificados y CRL de la ITU-T X.509. Gran parte de la información de sus RFC está basada en los estándares de la ITU-T y PKCS, adicionándole especificaciones complementarias a estos estándares previamente mencionados. El grupo de trabajo de la IETF sigue elaborando estándares que establecen directivas para el manejo de una PKI y el uso de esta. La RFC 5280 publicado en mayo del 2008 ofrece especificaciones más claras acerca de los componentes y el funcionamiento de una PKI, siguiendo su base en el estándar ITU-T X.509.

2.4. Certificados Digitales

2.4.1. Definición

Para argumentar que una PKI ofrece la autenticación de las partes involucradas en la comunicación, se debe incurrir al uso de certificados y firmas digitales, asimismo, una entidad tercera confiable que emita y verifique que los certificados digitales emitidos identifiquen al suscriptor. La forma en como la PKI hace uso de los certificados digitales y firmas digitales se explica a continuación:

Antes, se cita un concepto preciso de lo que es un certificado digital:

“El Certificado Digital es un documento firmado por una Autoridad Certificadora (CA). El documento contiene, principalmente, el nombre del sujeto y su clave pública. Si el Certificado es auténtico y confiamos en la CA, entonces, ‘podemos confiar en que el sujeto identificado en el Certificado Digital posee la clave pública que se señala en dicho certificado’” (CNC 2014: 12)

Figura 29. Autenticación por medio de una Autoridad de Certificación. Adaptado de “Infraestructura para la criptografía de clave pública”, por CNC, 2014.

En la figura 29 se observa como el usuario A se está comunicando con el usuario B mediante el uso de su certificado digital que posee su clave pública. En este proceso se observa que interviene la CA como entidad certificadora que valida que los usuarios sean quienes dicen ser y que la comunicación es entre ambos. Por lo cual, si el usuario C quiere participar de esa comunicación no puede, ya que el mensaje no está siendo dirigido hacia él. Por lo tanto, la información que pueda enviar el usuario C, así sea igual, será rechazada, ya que no está

autenticado por la CA que está verificando la identidad de los usuarios que participan en la comunicación.

2.4.2. Estructura del Certificado Digital

Los certificados digitales dentro de una PKI se almacenan bajo un formato establecido por la recomendación de la ITU-T X.509, la versión que está vigente en la actualidad es la 3.

Versión del certificado	Versión 3
Núm. de serie del certificado	Generado por la CA, único
Algoritmo de firma del certif.	sha1withRSAEncryption
Nombre X.500 del emisor	c=ES, o=Empresa, cn= Autoridad de Certificación
Periodo de validez	desde dd/mm/aa hasta dd'/mm'/aa'
Nombre X.500 del sujeto	c=ES, o=Empresa, cn=José Pérez
Clave pública del sujeto	AC:46:90:6D:F9:.....
Uso de la clave	Firma digital, cifrado de clave
Uso de la clave mejorado	Autenticación en W2000
Identificador claves CA	Identifica el par de claves utilizado para firmar el certificado
Identificador claves usuario	Identifica el par de claves asociado a la clave pub. en el certif.
Punto de distribución CRLs	HTTP://servidor/ruta/nombre.crl (publicación en web)
Firma de la AC	Firma del certificado por la CA

Figura 30. Estructura de Certificado Digital X.509 versión 3. Adaptado de “Formación PKI – Seminario de Infraestructura de Clave Pública”, por INDRA, 2005.

Como se puede observar en la *figura 30*, la estructura define los parámetros que define el estándar como información necesaria para identificar a un suscriptor. Existen parámetros que caben resaltar su importancia, como el periodo de validez. Este parámetro establece el tiempo de vida exacto en el cual un certificado mantendrá su usabilidad, por lo general este rango de fechas es de un año, de acuerdo con las buenas prácticas definidas en la industria que hace uso del estándar. Asimismo, el parámetro más importante es la Clave Publica del

sujeto, este campo contiene uno de los pares de llaves que se necesitan para realizar el cifrado asimétrico en todas las funciones para las cuales sea usado este certificado. Este campo es de vital importancia para la generación de las firmas digitales que proveen la autenticación y no repudio en la comunicación.

2.4.3. Tipos de certificación

2.4.1.1. Certificación de Suscriptor

Este tipo de certificación es la razón vital de ser de una PKI, ya que se certifica que una persona natural o jurídica sea identificada en los medios digitales. Este procedimiento es realizado por la CA directamente o mediante la intervención de una autoridad de registro. Este tipo de certificación es el usado para validar la identidad de personas, aplicaciones, compañías, servidores y toda entidad que sea parte sujeto que identificar por el certificado digital.

2.4.1.2. Certificación entre Autoridades (Certificación Cruzada)

Este tipo de certificación es usada de manera exclusiva por las Autoridades de Certificación (CA), ya que en una infraestructura que comprende una innumerable cantidad de las CA en internet se necesita establecer algún tipo de confianza entre ellas. El problema que se generaba entre las CA es la cantidad de certificados que podían almacenar. En una jerarquía de una PKI, no es práctico que todas las CA tengan los mismos certificados almacenados. Por ello, existe un proceso llamado Certificación Cruzada, la cual permite que las CA puedan emitir un certificado especial (*Cross Certificate*), el cual permite que exista confianza entre las CA.

Figura 31. Proceso de validación de la ruta de certificación. Adaptado de “Public key infrastructure: building trusted applications and Web services”, por VACCA, 2004.

Según la figura 31 se puede ver que existe un proceso en el cual las CA se comunican entre ellas para responder a una solicitud de certificado. Este proceso es llamado Ruta de Certificación (*Certification Path*). A través de este proceso, podemos observar que no todas las CA confían una de la otra, por lo cual se puede observar que, para obtener la información del certificado, existe una ruta específica. Así, la CA1 confía en la CA2 y la CA2 confía en la CA3, aunque no directamente, se puede concluir que la CA1 confía en la CA3 de acuerdo con la ruta de certificación gracias a la confianza entre las CA obtenida mediante la certificación cruzada. De esta manera, el sujeto “A” que solicitaba la clave pública del sujeto “B” puede obtener directamente la clave de parte de la CA3 aun siendo la consulta inicial a la CA1.

2.5. Lista de Revocación de Certificados (CRL)

2.5.1. Definición

Las listas de revocación de certificados (CRL) fueron ideadas para comunicar el desuso de uno o varios certificados digitales en toda la PKI. Estos comunicados fueron relacionados al posible peligro de que la seguridad, del par de llaves de un certificado, haya sido comprometida. Bajo este escenario, si un atacante ha logrado obtener la clave privada de un usuario y ha obtenido el certificado digital de este, la identidad del usuario ya no estaría segura en una CA o varias CA de la PKI.

2.5.2. Funcionamiento

Las CRL son emitidas por las CA y poseen un periodo limitado de validez que por lo general consta de 1 año. Estas listas son emitidas con una estructura similar a la de un certificado, sin embargo, poseen otras características que describen la lista de certificados que van a ser revocados. Por otro lado, la actualización de las CRL se realiza constantemente en una PKI, ya que es una buena práctica definir una fecha de expiración a corto plazo para el certificado digital y así evitar posibles ataques a la identidad del usuario. Las CRL publicadas esporádicamente se deben consultar siempre para comprobar que un certificado no haya vencido en su validez. Por otro lado, debido a lo extensa de la información de la lista de certificados, muchas veces estos son divididos en varias partes según los cree conveniente el administrador de la PKI, ya que esto ayuda a reducir el tiempo de verificación de las listas en los usuarios. Así como la longitud de la data suministrada. Asimismo, se proporcionan Deltas CRL para que la información sea incluso más específica en cuanto a los cambios de las CRL, ya que muchas veces se hace pesado enviar varias veces la información de las listas por un simple cambio en un único certificado. Es por ello, que se crearon los Deltas CRL,

los cuales son pequeñas actualizaciones de las listas de revocación, las cuales son reconocidas por los clientes que usan el estándar ITU-T X.509.

Figura 32. Ejemplo de CRL. Adaptado de “Basics of Digital Certificates and Certificate Authority”, por SITES.GOOGLE.COM, 2008.

2.5.3. Estructura de las CRL

La estructura de las listas de revocación está definida en el estándar ITU-T X.509 (CRL versión 2), este posee una estructura similar a la de los certificados digitales y los campos que lo conforman son los siguientes:

- Autoridad de identificadora de llaves.
- Nombre alternativo del emisor.
- Número de CRL

- Indicador Delta de CRL.
- Punto de emisión de los certificados.

Asimismo, posee campos extendidos en las entradas CRL:

- Código de Motivo
- Código de instrucción de almacenamiento
- Fecha de invalidez
- Emisor del certificado

2.6. PKI Gestionada por terceros

2.6.1. Concepto de PKI Gestionada

Para que las organizaciones puedan operar sus aplicaciones corporativas con un alto nivel de seguridad basada en criptografía asimétrica, se requiere de una infraestructura de intercambio de claves públicas que ofrecen dicha seguridad mediante el uso de certificados digitales. Por ello, muchas organizaciones en la actualidad requieren de una PKI para proteger sus aplicaciones mediante el cifrado y firma digital de mensajes de correo electrónico, aplicaciones de comercio electrónico, aplicaciones web bancarias, etc. Teniendo en cuenta la importancia que tiene una PKI para las empresas, se ve necesario el despliegue de esta solución para cumplir con la necesidad de la empresa.

Debido a que el núcleo del negocio de muchas organizaciones no es la emisión de certificados digitales, surge la demanda en el mercado de una PKI gestionada. Este tipo de PKI, es un servicio ofrecido por compañías terceras cuyo negocio es rentar su infraestructura de clave pública para la emisión de certificados digitales. Asimismo, las organizaciones que

adquieren este tipo de PKI, obtienen certificación por parte de una CA que es de confianza a nivel mundial. Por otro lado, el proveedor de PKI gestionada se compromete a dar la administración, soporte, alta disponibilidad y seguridad de la PKI que está siendo rentada. La principal ventaja de este tipo de servicio prestado por un tercero es el costo implementación y mantenimiento. Esto se debe a que una PKI significa un alto costo de inversión en su implementación y mantenimiento, dado que existen muchos componentes involucrados en su desarrollo. Sin embargo, una PKI gestionada por un tercero, ofrece un costo muy bajo en su implementación y un costo bajo en su mantenimiento, de la misma manera, existen otras ventajas que solo una PKI gestionada por terceros podría ofrecer a nivel de seguridad de la información. Dado que el núcleo del negocio de muchas organizaciones no es mantener una PKI implementada en hardware para una tarea básica como es la emisión de certificados digitales, se justifica aún más la necesidad de este tipo de servicios de PKI gestionada para alinear las tecnologías adquiridas a los intereses del negocio.

2.6.2. Proveedores de PKI gestionada

En la actualidad existen muchos proveedores de este tipo de servicios de PKI gestionados.

A continuación, se nombran los más destacados:

2.6.2.1. Symantec

Symantec es una compañía internacional que ofrece servicios de seguridad. Su producto de PKI gestionada es llamado: *Symantec Managed PKI Service*. Este servicio fue implementado por Symantec a partir de la compra de la sección del negocio de autenticación de la compañía *Verisign*, la cual era dueña de una de las más

grandes infraestructuras de PKI en el mundo. Ahora toda esa tecnología y conocimiento de *Verisign* es ofrecido por Symantec como servicio de PKI gestionada.

2.6.2.2. DigiCert

DigiCert es una compañía internacional que principalmente ofrece servicios de seguridad SSL. Asimismo, otro de sus productos es la PKI gestionada, la cual tienen orientada a dos sectores empresariales. La solución para pequeñas y medianas empresas es llamada: ***Managed PKI CertCentral***. Esta es una plataforma en la cual se ofrece un portal en donde la empresa administra sus certificados digitales. Por otro lado, para grandes empresas ofrecen un servicio llamado ***DigiCert Private PKI***, la cual es una infraestructura virtual privada proporcionada por DigiCert que funciona como una IaaS.

2.6.2.3. Entrust

Entrust es una compañía internacional que cuenta con amplia experiencia en el mercado. Su producto de PKI gestionada es llamado ***Managed PKI Service***. De igual manera que DigiCert, ofrecen una infraestructura basada en la nube de la PKI. Este producto ofrece características como alta disponibilidad, redundancia, monitoreo constante y una solución de backups con recuperación de desastres.

2.6.2.4. Globalsign

GlobaSign es una compañía internacional que ofrece servicios de seguridad por autenticación. El producto de PKI gestionada que ofrece, tanto para las PYMES y las grandes compañías, es el ***Managed PKI Platform***. Este producto ofrece una plataforma

de SaaS que brinda todas las funcionalidades de administración de una PKI. Además, soporta múltiples entidades que pueden ser gestionadas por el administrador de manera centralizada.

2.7. Amenazas a las PKI

Las Autoridades de Certificación (CA) dentro de una PKI son un blanco muy atractivo para los atacantes y existen diversas maneras de poder perpetrar estos ataques. Estos pueden provenir desde elementos que se encuentran dentro de la misma infraestructura interna en donde se almacenan las claves privadas y los certificados digitales, hasta de manera externa mediante el uso de herramientas y métodos para aprovechar las vulnerabilidades de la Infraestructura.

2.7.1. Ataques Internos a las CA

Como se sabe, la infraestructura de hardware de una PKI consta de varios niveles de seguridad. Esta seguridad va desde el nivel físico de control de accesos a los centros de datos hasta la seguridad perimetral de la red y el hardware en donde se almacenan las llaves privadas de cada certificado digital. Esta seguridad es desplegada y puede ser controlada mediante estándares como el SGSI, los cuales ayudan a mantener la seguridad de la PKI en constante vigilancia. Sin embargo, existen factores internos que no tienen que ver con la tecnología usada para la seguridad, sino con el personal operativo a cargo de operarla. Los ataques internos pueden ser perpetrados por aquellos quienes son responsables de cuidar la seguridad de las llaves privadas, ya que son un objetivo atractivo para lucrar con ellos. Para reducir las probabilidades de ataques internos al mínimo, los accesos a las CA deben ser restringidos al máximo posible al personal que opera con ellas. El hardware en donde se

almacenan las llaves privadas (Criptocajas) debe estar sujetos a medidas ultra seguras. Estas cajas que contienen estas claves deben estar en constante monitoreo por cámaras de video, controles de acceso biométrico a varios niveles, detección de intrusos y poseer todas las medidas de alta disponibilidad y respuesta ante desastres. Estas medidas reducirán significativamente el posible riesgo de que surja un ladrón de información dentro del personal que opera en las instalaciones del centro de datos.

2.7.2. Ataques Externos a las CA

Los ataques externos a las CA se producen desde fuera de la infraestructura de hardware de la PKI. Estas usan computadoras localizadas fuera de las instalaciones de donde se encuentra la CA, usando mecanismos especializados para dichas tareas. Estos pueden provenir desde internet, mediante malware proveniente desde un dispositivo de almacenamiento externo o algún otro método que le dé acceso al atacante a la red privada local en donde se encuentra la CA. Estos ataques son perpetrados por lo general explotando vulnerabilidades de los sistemas operativos del hardware usado en la CA o cualquier otro componente de la PKI que mantenga confianza con la CA. Los objetivos de estos ataques pueden ser dar de baja el servidor o hardware en donde se encuentran las llaves privadas y los certificados, el robo de las llaves privadas o intentar modificar el normal funcionamiento de la PKI.

2.7.3. Seguridad para las CA

Teniendo en cuenta que el núcleo en donde reside la confianza de una PKI es la CA, es fundamental proteger al máximo este elemento central en la infraestructura. El tener la CA comprometida por un ataque interno o externo puede ser perjudicial no solo para el proveedor, sino para todas las compañías cuya seguridad y confianza, en internet, depende

de ella. En respuesta a esta necesidad de seguridad máxima para las CA, se han establecido una serie de recomendaciones en la industria, las cuales se presentan a continuación:

1. El uso de módulos criptográficos HSM en una PKI es básico para garantizar una seguridad óptima en el almacenamiento de los certificados y las llaves. Ya que los servidores CA implementados por Software son un grave riesgo para la administración de los certificados y llaves. Asimismo, para generar la llave privada de la CA raíz con la cual se deben distribuir las relaciones de confianza entre las demás CA de la infraestructura, debe utilizarse un módulo de seguridad FIPS 140-2 nivel 3 o superior.
2. La llave privada de la CA raíz no debe existir almacenada en texto plano en ningún otro medio que no sea el módulo criptográfico HSM bajo el estándar FIPS 140-2 nivel 3 o superior. Esta llave debe ser el elemento más protegido dentro de la CA, ya que de este depende que la CA raíz no sea *hackeada* y así no se comprometa la seguridad de toda la infraestructura.
3. El control de acceso, tanto físico como digital, al módulo en donde se encuentra almacenada la llave de la CA raíz, debe contar con los más altos estándares de control de acceso. No se debe escatimar en esfuerzos para asegurar lo máximo posible a este módulo criptográfico vital.
4. Las tareas de *backup* de la CA raíz y su llave no debe comprometer la exposición de su llave privada. Estos deben estar sometidos a los mismos controles de seguridad a los cuales están sujetos el módulo criptográfico de la CA.
5. En caso de un ataque físico o atentado realizado a las instalaciones en donde se encuentra el módulo criptográfico de la CA raíz, deben deshabilitarse todas las funciones criptográficas del servicio y destruir toda la información de las llaves privadas y sus certificados digitales. De esta manera se evita que esta información sea utilizada por los atacantes en un futuro y que la información o equipos sustraídos les sean inservibles.

Finalmente, proveer la máxima seguridad a una PKI frente a los ataques internos o externos depende de mucho del tipo de hardware en donde se base el funcionamiento de la PKI. Como se observa, el uso de módulos criptográficos HSM un mayor nivel de seguridad que las soluciones basadas en software. Por lo cual, es vital exigir a nuestros proveedores de PKI gestionada que cuenten con todas estas recomendaciones para contar con la máxima seguridad y confianza en la CA y su infraestructura, la cual gestiona nuestros certificados digitales y llaves privadas.

2.8. Normativa nacional de las PKI

La normativa nacional para la regulación de las PKI en nuestro país consta de varias leyes y decretos que modifican dichas leyes. Estas fueron creadas para regular las implementaciones PKI que fuesen realizadas en el país y definir las entidades del estado que fiscalizan estas implementaciones. El ejemplo más claro a nivel nacional se dio con la PKI implementada por la RENIEC, la cual fue regulada por estas normativas. A continuación, se describen las normativas:

2.8.1. Ley N° 27269 de Firmas y Certificados Digitales

Esta Ley fue promulgada para por el Congreso de la Republica en el año 2000. El objetivo principal de esta ley es regular el uso de la firma electrónica como medio de identificación digital, otorgándole la misma validez y eficacia jurídica que una firma manuscrita. La firma digital otorga la manifestación de voluntad por parte del individuo a dar verificar su identidad como medio de autenticación en medios digitales. La ley regula, entre otras cosas, el uso de la firma digital representada por un símbolo en los distintos medios digitales posibles. Asimismo, regula las características que debe tener un certificado digital que es usado para identificar a un usuario en los medios digitales ante una entidad de certificación confiable. Este certificado forma parte del proceso de firma digital.

Para esta ley, existe una modificación en el artículo 11, la cual fue decretada con la **Ley N° 27310**. Esta ley modifica el artículo 11 de la Ley 27269, resumiéndola de manera que permita el reconocimiento de las entidades de certificación extranjeras. Esta permite la validez de los certificados que son emitidos por las entidades de certificación extranjeras, siempre y cuando

sean reconocidas por la Autoridad Administrativa del estado encargada de la regulación de las normas (INDECOPI).

2.8.2. Ley N° 27291 que Modifica el Código Civil

La Ley N° 27291 fue promulgada el mismo año que fue promulgada la ley de Firmas y Certificados Digitales. Esta ley estaba dirigida a modificar el Código Civil permitiendo que un individuo pueda manifestar su voluntad e identificarse mediante una firma digital. Esto se especifica para los casos en los cuales el individuo requiera utilizar recursos digitales del estado o privados y para ello necesite manifestar su voluntad mediante una firma digital. De esta manera, se aprueba la validez de este tipo de transacciones realizadas en medios digitales en las cuales intervengan los certificados y firmas digitales.

2.8.3. Decreto Supremo N°052-2008-PCM

Este es un decreto supremo que se promulgo el año 2008 para establecer el Reglamento para la Ley N° 27269 de Firmas y Certificados digitales. Este reglamento está basado en la primera ley N° 27269 promulgada en el año 2000, estableciendo las regulaciones en un panorama más amplio que tiene que ver no solo con las firmas y certificados digitales, sino con todas las especificaciones que debe cumplir una PKI en el Perú. De esta manera, toda entidad pública o privada debe cumplir con los lineamientos de este decreto para la implementación de una PKI ya sea implementada en sus instalaciones o rentada a un proveedor externo ya sea nacional o extranjero.

2.8.4. Decreto Supremo N°070-2011-PCM

Este decreto supremo se promulgo el año 2011 para actualizar el decreto supremo del 2008 que se describió con anterioridad. En este decreto se modificaban el contenido y la vigencia de los certificados digitales de la firma electrónica. Asimismo, se designó a INDECOPI como la IOFE (Infraestructura Oficial de Firma Electrónica) para cumplir la función de autoridad administrativa encargada de administrar el registro de certificados digitales y creación de su respectiva firma digital. Por otro lado, se especificó finalmente que los documentos oficiales del estado puedan ser firmados digitalmente con este tipo de identificación digital. Finalmente, se decretó que las entidades públicas del estado que hayan mantenido el uso de certificados digitales emitidos por entidades certificadoras con Web Trust realicen el remplazo de sus certificados a los que son emitidos por la RENIEC a través de su planta de certificación digital PKI.

2.9. Servicio de correo electrónico Office 365

2.9.1. Exchange Online

Uno de los servicios de correo electrónico basado en la nube que se ha popularizado en los últimos años es el servicio de Exchange Online que viene incluido dentro de la suite de Office 365. Para describir mejor de que se trata la solución, se cita la siguiente descripción extraída de la web del mismo fabricante:

“Microsoft Exchange Online es una solución de mensajería hospedada que brinda las características de Microsoft Exchange Server como un servicio basado en la nube. Les brinda a los usuarios acceso a correo electrónico, calendario, contactos y tareas del equipo, la red y dispositivos móviles con solo iniciar sesión. Se integra

completamente con Active Directory, lo que permite a los administradores usar directivas de grupo, como también otras herramientas de administración, para administrar características de Exchange Online en el entorno.

Las organizaciones que se suscriben a Exchange Online mantienen el control de los servicios de mensajería que ofrecen a los usuarios, pero no tienen la carga operativa del software de servidor local. Con los planes hospedados de Exchange Online que se describen en este documento, el correo electrónico está hospedado en servidores que admiten varios clientes simultáneamente. Estos servidores se hospedan en centros de datos de Microsoft y los usuarios tienen acceso a los mismos mediante un amplio rango de dispositivos desde una red corporativa o mediante Internet.”

(MICROSOFT 2015)

Dicho de otra manera, el servicio de Microsoft Exchange Online está diseñado para las organizaciones que busquen obtener la flexibilidad que les brinda un servicio de correo alojado en la nube, sin necesidad de sacrificar las características de un servidor Microsoft Exchange Server, ya que, finalmente, este servicio en la nube está basado en la misma tecnología de Microsoft Exchange Server, la cual es ampliamente utilizada a nivel corporativo en la actualidad. Asimismo, para no perder las ventajas administrativas que provee un servidor Exchange *On-Premises*, este brinda amplias herramientas administrativas muy similares, las cuales son basadas en una interface web para la administración en línea.

2.9.2. Ventajas

A continuación, se presenta un cuadro cuya fuente es del fabricante Microsoft, en la cual se especifica de manera detallada cuales son las ventajas de la solución.

Tabla 3

Cuadro de ventajas de Exchange Online

Ventaja	Descripción
Costo	<p>Microsoft Exchange Online administra el hardware para reducir el costo total de propiedad del sistema de correo, lo cual incluye actualizaciones y soporte telefónico las 24 horas del día, los 7 días de la semana.</p> <p>Sin embargo, es importante destacar que la incorporación a Exchange Online, dentro de Office 365, no significa que ya nunca tendrá que administrar el hardware. El servicio es tan flexible que permite a las organizaciones hacer uso de sus <i>Active Directory</i> a nivel local, con la posibilidad de mantener la sincronización de AD con Office 365, así como con ADFS (<i>Active Directory Federation Services</i>).</p>
Alta disponibilidad	<p>La alta disponibilidad y la redundancia constituyen una de las características más importantes que posee Exchange Online. El servicio consta de un contrato de nivel de servicio del 99,9 % avalado financieramente para Exchange Online.</p>
Administración y control	<p>Exchange Online se maneja desde una sola interfaz administrativa basada en web, que contiene herramientas avanzadas de administración y muy fáciles de usar.</p>
Almacenamiento	<p>Exchange Online cuenta con 50 GB de almacenamiento de manera predeterminada para los buzones por usuario.</p>
Funciones contra el correo no deseado y el malware	<p><i>Exchange Online Protection</i> (EOP) es la solución que ofrece Exchange Online para el filtrado de correo electrónico no deseado entrante y saliente, de creación de informes, de seguimiento de mensajes y de configuración del flujo de correo y la protección contra malware de</p>

	varios motores. EOP incorpora muchas mejoras a diferencia de su predecesor FOPE, una de las más notables es la administración, que está totalmente integrada en el Centro de administración de Exchange (EMC).
Seguridad, privacidad y cumplimiento normativo	La seguridad y la privacidad son sumamente importantes y más si se trata de un servicio alojado en la nube. Exchange Online junto con Office 365 cumple con muchas normas internacionales del sector, entre las cuales se incluyen la ISO-27001 y la FISMA.
Movilidad	Gracias a la naturaleza del servicio en la nube, la movilidad en el servicio de Exchange Online se hace sencillo, ya que los usuarios pueden tener acceso a correo electrónico, calendario, contactos y tareas desde cualquier dispositivo móvil como tabletas, laptops, teléfonos inteligentes, etc. Asimismo, las plataformas de las cuales se pueden acceder al servicio van desde Windows y Macintosh desde cualquier navegador web, así como aplicaciones de Android, IOS y Windows Phone como cliente de correo.

Nota. Fuente: Recuperado de “Descripción del servicio Exchange Online”, de Microsoft, recuperado de MICROSOFT TECHNET, 2015.

Figura 33. Diagrama funcional de Exchange Online servicio de correo de Office 365. Adaptado de “Diagrama básico de red corporativo de un servicio Exchange Online”, elaboración propia.

2.10. Estándar NIST SP 800-57

Este estándar brinda recomendaciones para las buenas prácticas en el uso de los algoritmos para una PKI. La NIST (*National Institute of Standards and Technology*) SP 800-57 parte 1, publicada en enero de 2016, se hace referencia al estándar FIPS 140-2 y se muestra una matriz de análisis comparativo de la fortaleza que tienen los algoritmos de cifrado simétrico o asimétrico y cuales están recomendados para su uso en la actualidad.

Para ello, la recomendación NIST propone un análisis realizado en base a prospectivas de mecanismos y tecnologías para vulnerar la seguridad de una clave, de acuerdo con su fortaleza de seguridad en bits a lo largo del tiempo. El valor de la llave descrita como

“Fortaleza de Seguridad” es un valor referencial que se compara a los otros tamaños de las llaves de los otros algoritmos de cifrado simétrico o asimétrico que no necesariamente son del mismo tamaño debido al tipo de ataques que son hechos a ciertos algoritmos.

Tabla 4

Comparativa de la fortaleza de los algoritmos de cifrado

Security Strength	Symmetric key algorithms	FFC (e.g., DSA, D-H)	IFC (e.g., RSA)	ECC (e.g., ECDSA)
≤ 80	2TDEA ²¹	$L = 1024$ $N = 160$	$k = 1024$	$f = 160-223$
112	3TDEA	$L = 2048$ $N = 224$	$k = 2048$	$f = 224-255$
128	AES-128	$L = 3072$ $N = 256$	$k = 3072$	$f = 256-383$
192	AES-192	$L = 7680$ $N = 384$	$k = 7680$	$f = 384-511$
256	AES-256	$L = 15360$ $N = 512$	$k = 15360$	$f = 512+$

Nota. Recuperada de NIST SP-800-57 pt.1, de la NIST, Copyright 2016 de NIST.

Observando el análisis de la *tabla 4*, se puede observar que los algoritmos de clave asimétrica posibles son EL Diffie-Hellman, RSA y ECDSA (de curva elíptica). Sin embargo, el uso de los algoritmos 192 y 256 bits de fortaleza para RSA y Diffie-Hellman no son recomendados por problemas identificados en la interoperabilidad y deficiencia en sus procesos de cifrado.

Tabla 5

Fortaleza de las claves a lo largo del tiempo

Security Strength		Through 2030	2031 and Beyond
< 112	Applying	Disallowed	
	Processing	Legacy-use	
112	Applying	Acceptable	Disallowed
	Processing		Legacy use
Security Strength		Through 2030	2031 and Beyond
128	Applying/Processing	Acceptable	Acceptable
192		Acceptable	Acceptable
256		Acceptable	Acceptable

Nota. Recuperada de NIST SP-800-57 pt.1, de la NIST, Copyright 2016 de NIST.

Por otro lado, la parte 3 de la NIST SP-800-57 recomienda cuales de estos algoritmos funcionan de manera óptima en aplicaciones específicas. A continuación, se presenta una tabla extraída del estándar, la cual determina que algoritmos son los más adecuados para una PKI dependiendo la seguridad que quiera aplicarse.

Tabla 6

Algoritmos recomendados y sus tamaños de llave

Key Type	Algorithms and Key Sizes
Digital Signature keys used for authentication (for Users or Devices)	RSA (2048 bits) ECDSA (Curve P-256)
Digital Signature keys used for non-repudiation (for Users or Devices)	RSA (2048 bits) ECDSA (Curves P-256 or P-384)
CA and OCSP Responder Signing Keys	RSA (2048 or 3072bits) ECDSA (Curves P-256 or P-384)
Key Establishment keys (for Users or Devices)	RSA (2048 bits) Diffie-Hellman (2048 bits) ECDH (Curves P-256 or P-384)

Nota. Recuperada de NIST SP-800-57 pt.3, de la NIST, Copyright 2016 de NIST.

Por otro lado, el estándar indica que función hash es recomendada a usar en conjunto con los algoritmos de criptografía asimétrica para las firmas digitales.

Tabla 7

Algoritmos Hash recomendadas para una PKI

Public Key Algorithms and Key Sizes	Hash Algorithms	Padding Scheme
RSA (2048 or 3072 bits)	SHA-256	PKCS #1 v1.5, PSS
ECDSA (Curve P-256)	SHA-256	N/A
ECDSA (Curve P-384)	SHA-384	N/A

Nota. Recuperada de NIST SP-800-57 pt.3, de la NIST, Copyright 2016 de NIST.

La función hash emplea el algoritmo SHA-256, el cual posee 256 bits de longitud en su módulo de salida luego de aplicar la función al mensaje en texto plano y convertirlo a una cadena alfanumérica de tamaño fijo. Esta función se detalla en el estándar FIPS 202 como estándar SHA-3, la cual reemplaza el estándar SHA-1 y SHA-2 aplicando funciones de *Array* más complejos para el resumen del mensaje. La función usada por el algoritmo SHA3-256 es la KECCAK que usa un módulo de 512 bits. En el estándar NIST FIPS-202 se muestra una comparativa entre los algoritmos de hash que son recomendados para su uso, según el factor de fortaleza en la seguridad medida en bits:

Tabla 8*Comparativa de funciones hash SHA*

Function	Output Size	Security Strengths in Bits		
		Collision	Preimage	2nd Preimage
SHA-1	160	< 80	160	$160 - L(M)$
SHA-224	224	112	224	$\min(224, 256 - L(M))$
SHA-512/224	224	112	224	224
SHA-256	256	128	256	$256 - L(M)$
SHA-512/256	256	128	256	256
SHA-384	384	192	384	384
SHA-512	512	256	512	$512 - L(M)$
SHA3-224	224	112	224	224
SHA3-256	256	128	256	256
SHA3-384	384	192	384	384
SHA3-512	512	256	512	512
SHAKE128	d	$\min(d/2, 128)$	$\geq \min(d, 128)$	$\min(d, 128)$
SHAKE256	d	$\min(d/2, 256)$	$\geq \min(d, 256)$	$\min(d, 256)$

Nota. Recuperada de NIST FIPS 202, de la NIST, Copyright 2016 de NIST.

2.11. Metodología del Plan de Pruebas

Para tener la seguridad de que la propuesta planteada en el proyecto es viable por parte del cliente, se deben realizar las pruebas necesarias para obtener los resultados requeridos en el proyecto. Para ello, se elabora un Plan de Pruebas, el cual debe ser aplicado a cada objetivo específico del proyecto. Para desarrollar este plan de pruebas se plantea una metodología que paso a paso nos guiará al cumplimiento de los objetivos. Por otro lado, la metodología del plan de pruebas se realizará tomando como referencia un Plan de Pruebas o Ensayos de Software adecuado a una solución de Seguridad de la información. El método de validación varía con el desarrollo del Plan de Pruebas y depende de lo que se validará en el objetivo específico. A continuación, se detallan los pasos del Plan de Pruebas:

Figura 34. Diagrama de Flujo del Plan de Pruebas. Adaptado de “Business Continuity Planning y la Gestión de Ensayos”, por ALBERTO G, 2017.

2.11.1. Información Resumen

Como primer paso, se realizará un resumen con toda la información que es importante para tener en cuenta en el proceso de pruebas. Esta información se presenta en una tabla con la información que se ha presentado en los anteriores capítulos, como lo son los aspectos introductorios y el planteamiento del problema.

2.11.2. Definir el alcance de la prueba

El primer paso en la ejecución es definir el alcance al cual llegarán las pruebas para alcanzar el logro del objetivo específico. En este apartado se definen los elementos que compondrán las pruebas y que herramientas serán requeridas para probarlas.

2.11.3. Recursos necesarios para la prueba

Luego de definir el alcance, se debe listar cuales son los requerimientos de hardware y/o software que serán necesarios para realizar las pruebas de la solución. Asimismo, se definen las herramientas que serán utilizadas para las pruebas, si existieran, así como el personal requerido para realizar las pruebas de en un entorno de preproducción.

2.11.4. Definir el método de prueba

Se debe definir el método de prueba que será utilizado para validar los resultados. Este método de pruebas verifica que el sistema o la solución que se está proponiendo para el proyecto cumplan con los objetivos específicos del proyecto.

2.11.5. Definir el caso de prueba

Parte principal de las pruebas, es definir el caso o escenario de la prueba que serán requeridos para comprobar que el objetivo del proyecto se cumpla. De esta manera, se estaría evidenciando el cumplimiento del objetivo específico en la propuesta del proyecto. Cada caso de prueba debe estar correctamente identificado y documentado.

2.11.6. Ejecución del caso de prueba

Finalmente, se debe ejecutar el caso de pruebas utilizando las herramientas o métodos de pruebas necesarios para medir el logro del objetivo específico, el cual brindará los resultados necesarios para concluir si este cumple con los objetivos específicos del proyecto.

CAPÍTULO III: DEFINICIÓN DEL PROBLEMA

3.1. Definición del Problema

3.1.1. Análisis de la problemática

La problemática identificada en el capítulo uno se encuentra en un contexto en donde el servicio de correo electrónico alojado en la nube posee deficiencias en la seguridad de la información que se transmite a través de internet desde la red interna de la compañía. Asimismo, existen problemas que son causados por factores internos y externos. Es decir, amenazas internas y externas que podrían comprometer la confidencialidad, integridad, autenticación y no repudio de la información que los usuarios envían en el contenido de sus mensajes de correo electrónico.

Para realizar el análisis de la problemática, se presenta una matriz en la cual se realiza un diagnóstico de las posibles causas de los problemas identificados con anterioridad. Luego, se tiene un pronóstico de las causas, los cuales son los problemas identificados en la organización y las posibles consecuencias que se podrían dar a si no son tomadas las medidas necesarias para la solución del problema.

Tabla 9

Matriz de análisis de la problemática actual.

	DIAGNÓSTICO (POSIBLES CAUSAS)	PRONÓSTICO (PROBLEMAS)	CONSECUENCIAS (POSIBLES CONSECUENCIAS)
ANÁLISIS INTERNO	<ul style="list-style-type: none"> • El total de mensajes de correo electrónico enviados usa firma escrita al final del mensaje. • La organización no orienta un presupuesto para el cifrado de la información de los mensajes de correo electrónico. 	<p>El servicio de correo electrónico no posee mecanismos de identificación digital para la seguridad de la información de los mensajes enviados.</p>	<ul style="list-style-type: none"> • Suplantación de identidad. • Ataques de spoofing a los usuarios de correo electrónico. • Desconfianza entre las partes de la comunicación.
	<ul style="list-style-type: none"> • La mayoría de los usuarios no son instruidos en prácticas de seguridad de la información. • Negligencia por parte de los usuarios en el manejo de su información confidencial. 	<p>Los usuarios de correo electrónico no están conscientes de las buenas prácticas en la seguridad de la información confidencial que les es otorgada.</p>	<ul style="list-style-type: none"> • Comparten contraseñas de manera escrita u oral. • Acceso no autorizado a información confidencial del usuario y de la organización. • Ataques de ingeniería social.
ANÁLISIS EXTERNO	<ul style="list-style-type: none"> • La organización usa el correo electrónico corporativo de Office 365 al ajustarse a sus necesidades de negocio. • El servicio de correo de Office 365 ofrece características de cifrado básicas. 	<p>El servicio de correo electrónico basado en Office 365 posee un riesgo intrínseco en la seguridad de la información que es transmitida a través de internet, el cual no cuenta con un mecanismo de cifrado para asegurar la confidencialidad e integridad de los mensajes de cliente a cliente.</p>	<ul style="list-style-type: none"> • Se puede producir un ataque <i>man-in-the-middle</i>, en la cual la información del mensaje pueda ser filtrada o modificada en su recorrido desde el cliente al servidor de Exchange Online de Office 365.
	<ul style="list-style-type: none"> • Información de carácter pública de los altos ejecutivos de Toyota. • Empresa líder en el sector automotriz del Perú. • Riesgos no identificados en la seguridad de la información. 	<p>La organización posee alta probabilidad de ataques externos a las cuentas de correo electrónico de los altos ejecutivos de un servicio basado en Office 365.</p>	<ul style="list-style-type: none"> • Ataques direccionados a las cuentas de correo a los altos ejecutivos de la compañía. • Incremento de activos de información vulnerables a amenazas externas. • Incremento de ataques externos con cada vez nuevas herramientas, lo cual trae como consecuencia la inversión en equipos de seguridad modernos y costosos.

Nota. Se ha realizado un análisis interno y externo de los problemas teniendo como referencia el modelo de análisis FODA. Adaptado de “La matriz de análisis DAFO (FODA)”, por robertoespinoza.es, 2013.

3.1.2. Problemas por Resolver

Siguiendo el análisis realizado en la *tabla 9*, se procede a definir los problemas que serán planteados en el proyecto, para los cuales serán tomadas las medidas necesarias para dar una solución teniendo como organización objetivo a Toyota del Perú. A continuación, se definen los problemas a resolver:

1. Los usuarios de correo electrónico no poseen un mecanismo de identificación digital como una firma digital en sus mensajes, el cual realmente identifique al usuario, ya que los métodos convencionales de “firma escrita” al final del mensaje pueden ser fácilmente suplantados o falsificados.
2. Los usuarios de correo electrónico no están concientizados en las buenas prácticas de seguridad para el manejo de la información confidencial que les es otorgada, lo cual puede causar accesos no autorizados, ataques de ingeniería social y ataques de *spoofing* que afectan a los activos de información de la organización.
3. El riesgo que corren los mensajes de correo electrónico, que viajan a través del servicio de Office 365 en la nube, al ser interceptados por un atacante especializado en ataques *man-in-the-middle*. Debido a que, no se cuenta con un mecanismo de cifrado para los mensajes de correo electrónico que son enviados desde un cliente de correo hacia otro (punto a punto).
4. Riesgo medio-alto de amenazas de ataque a las cuentas de correo electrónico, sobre todo a los altos ejecutivos de una compañía como Toyota que es de interés público por su valor económico.

3.2. Evaluación del Impacto del Problema en la Organización

3.2.1. Impacto Tecnológico

El impacto tecnológico del problema vendría a afectar a la infraestructura tecnológica de la empresa. Más concretamente, el problema de mantener vulnerabilidades en el servicio de correo electrónico significaría que la empresa estaría propensa a amenazas de ataques que comprometan a la disponibilidad del servicio. Otro de los riesgos que suponen los problemas identificados es la posibilidad de que, mediante un ataque efectuado al servicio de correo electrónico para obtener credenciales, se puedan escalar privilegios en la infraestructura de

red de la compañía. De esa manera, el atacante podría obtener más que la información del mensaje, ya que podría obtener documentación privada importante que se encuentra almacenada en la infraestructura de la red corporativa.

3.2.2. Impacto Legal

De acuerdo con la normativa legal del Perú a la que se encuentra sujeta Toyota, existen leyes como la Ley N° 29733 – Ley de Protección de datos personales, la cual establece ciertos lineamientos que se tienen que cumplir en las empresas peruanas. Una de las finalidades más resaltantes de esta ley, es que no debe permitirse la difusión de la información personal de un usuario sin su consentimiento. Por lo cual, el más mínimo riesgo de un ataque que permita la filtración de esta información de los usuarios de correo sin su consentimiento impactaría de manera legal y financiera a la empresa. Esto se debe a que la normativa aplica multas administrativas a las empresas que caigan en el incumplimiento de estas normas.

3.2.3. Impacto Económico

El impacto económico del problema viene en consecuencia de la inversión realizada en la adquisición y mantenimiento de los activos tecnológicos de la empresa, al ocurrir un impacto tecnológico, es inevitable que haya gastos en la pérdida de la información a causa los incidentes de seguridad. Este impacto puede ser incalculable si se perdió información vital para la empresa. Por el lado legal, el impacto económico suele ser significativo, ya que la normativa establece multas administrativas con montos fijos de acuerdo con el alcance de la infracción.

3.3. Definición de Requerimientos

Para realizar el análisis y definición de los requerimientos del proyecto, en primer lugar, se deberán identificar los interesados del proyecto. Luego, se definirán los requerimientos funcionales que serán propuestos para el proyecto.

3.3.1. Registro de Interesados del Proyecto

Para establecer una línea clara en la toma de requerimientos, el primer paso es identificar y registrar los interesados (*stakeholders*) del proyecto. A continuación, se presenta un cuadro con los interesados del proyecto y sus diferentes niveles de interés e influencia

Tabla 10

Matriz de Registro de Interesados del Proyecto

Interesado	Organización a la que pertenece	Rol	Interés (Bajo, Medio, Alto)	Influencia (Bajo, Medio, Alto)
Gerente de TI	Toyota Perú	Patrocinador	Alto	Alto
Clientes destinatarios de correos electrónicos.	Terceros	Cliente	Bajo	Medio
Jefes de áreas	Toyota Perú	Usuario	Medio	Medio
Gerentes	Toyota Perú	Usuario	Medio	Alto
Gerente General	Toyota Perú	Alta Dirección	Alto	Alto
Indecopi	Estado Peruano	Entidad reguladora	Bajo	Medio
Proveedor de PKI basado en la nube	Proveedores	Proveedor	Medio	Alto

Interesado	Organización a la que pertenece	Rol	Interés (Bajo, Medio, Alto)	Influencia (Bajo, Medio, Alto)
Jefe de Sistemas	de Toyota Perú	Director Proyecto	Alto	Alto
Analistas de Sistemas	de Toyota Perú	Miembro proyecto	Alto	Medio

Nota. Adaptado de “10.1 Identificar los interesados”, por PM-DEVICES, 2012.

Una vez identificados y establecidos los interesados del proyecto, se procede a realizar una matriz de Poder-Interés, en la cual se definirá cual es el tratamiento que se le da a cada parte interesada en el proyecto. Finalmente, este gráfico servirá como base para la definición de las características de los requerimientos.

Figura 35. Matriz de Poder-Interés del proyecto. Adaptado de “10.1 Identificar los interesados”, por PM-DEVICES, 2012.

3.3.2. Requerimientos Funcionales

Estos son los requerimientos que deberá cumplir la solución que se va a proponer en el proyecto. Básicamente, son las especificaciones o funciones con las que debe contar la solución para cumplir con las necesidades de los *stakeholders* del proyecto. Se brinda la información detallada de las especificaciones de la solución en un lenguaje técnico que no necesariamente debe ser entendido por todos los Interesados del proyecto, ya que estos requerimientos funcionales representan una base para el desarrollo del proyecto.

A continuación, se muestra un cuadro en donde se listan los requerimientos funcionales, los cuales toman como referencia los problemas definidos con anterioridad. Asimismo, se puede observar que estos requerimientos tienen una parte interesada a la cual están relacionados, lo cual indica cual es la prioridad que se le dará al requerimiento.

Tabla 11

Matriz de Toma de Requerimientos Funcionales.

Nº	Requerimiento Funcional	Interesados	Prioridad (Según matriz de Poder-interés)
1	Un usuario, como un jefe de área o gerente, debe poseer un método de autenticación y de no repudio como lo es la firma digital. La firma digital debe ser aplicada a los mensajes de correo electrónico enviados a ciertos destinatarios especificados por él emisor.	Jefe de Sistemas, jefes de área, Gerentes.	Alta
2	La propuesta debe ofrecer un método de autenticación en la cual los mensajes que son		Media

	enviados por un usuario sean auténticamente enviados por él. Esto sin la necesidad de depender de los métodos de autenticación tradicionales de la cuenta de correo electrónico.	Jefe de Sistemas, jefes de área, gerentes, Clientes destino.	
3	Se debe asegurar la integridad y confidencialidad de todo el flujo de correos electrónicos que son enviados por los usuarios, jefes de área y gerentes, a través del servicio de Office 365 en la nube.	Jefe de Sistemas, Proveedor PKI	Alta
4	Se debe proponer una PKI como mecanismo de criptografía asimétrica, la cual reduzca al mínimo el riesgo de amenazas que puedan tener acceso a la información de certificados digitales necesarios para el cifrado y firma digital de los correos electrónicos.	Jefe de Sistemas, Proveedor PKI, Indecopi	Media
5	El cifrado y firma digital debe operar desde el cliente de correo electrónico del emisor hasta el cliente del receptor. Ofreciendo así, seguridad de punto a punto de la comunicación.	Jefe de Sistemas, jefes de área, Gerentes, Clientes destino.	Media

Nota. Se ha realizado este cuadro para el ordenamiento de los requerimientos con sus interesados y de prioridad según matriz poder-interés, de elaboración propia.

3.1. Estructura Desglosable de Trabajo (EDT)

CAPÍTULO IV: PLANTEAMIENTO DE LA SOLUCIÓN PROPUESTA

4.1. Modelo de arquitectura de integración de una PKI y un servicio de correo electrónico Office 365

Figura 36. Modelo de arquitectura de integración de una PKI y un servicio de correo electrónico Office 365, elaboración propia.

4.2. Especificaciones

Teniendo en cuenta los requerimientos definidos en el capítulo tres y que estos deben ser redactados en actas aprobadas por las partes interesadas, se definen las especificaciones de una PKI basada en la nube integrada a un servicio de correo electrónico basado en Office 365 para el cifrado y firma digital de los mensajes. Estas especificaciones deben cumplir con los requerimientos previamente establecidos, los cuales buscan solucionar los problemas planteados en el proyecto. A continuación, se definen las especificaciones según el modelo presentado en el diagrama del punto 4.1 (*figura 36*).

4.2.1. Definición de los algoritmos de cifrado y firma digital

Es importante especificar, en primer lugar, qué algoritmos se han de emplear para la emisión de los certificados digitales que serán usados para el cifrado y firma digital de los mensajes de correo electrónico. Esta especificación cubre parte de los requerimientos 1, 2 y 3 definidos en el capítulo 3 del proyecto.

4.2.1.1. Algoritmo de cifrado asimétrico

Para definir el algoritmo de cifrado a usar se recomienda seguir las recomendaciones de la NIST SP 800-57. Para ello, para sustentar la elección de uno o varios algoritmos de cifrado que sean válidos para la solución propuesta, primero se debe descartar que algoritmos no son recomendados para su uso en la actualidad. Según la *tabla 5*, del marco teórico, se demuestra que las claves de un tamaño menor a 112 bits ya no son recomendados en su uso. Asimismo, se observa que hasta el año 2030 será aceptable el uso de una clave de 112 bits, sin embargo, a partir de ese año el uso de ese tamaño de clave referencial ya no estará permitida. Asimismo, se observa que las claves con

una longitud de 128 bits en adelante serán aceptadas a lo largo del tiempo, por lo cual, se buscará un algoritmo que posea una longitud de clave mayor o igual a una fortaleza de seguridad de 128 bits teniendo como referencia la lista de algoritmos de la *tabla 4*.

Finalmente, como se nota en la *tabla 6* de recomendaciones, los mejores algoritmos para la aplicación de firmas digitales son el RSA y ECDSA. Ahora, como se observa en la *tabla 6*, para el algoritmo RSA se opta por una clave de 2048 bits y no de 3072 bits, debido a que la capacidad computacional requerida para cifrar y descifrar es muy alta con una clave de 3072 bits. Por lo tanto, para mejorar la velocidad del proceso criptográfico asimétrico es recomendado el uso del RSA de 2048 bits. En el caso del algoritmo asimétrico ECDSA, posee rangos de longitud de claves menores y que ofrecen la misma seguridad que el algoritmo RSA. Por ello, es recomendable el uso del rango de las claves de 256-383 bits que reduce un poco la velocidad del proceso criptográfico, pero brinda mayor seguridad por la longitud de sus claves. Sin embargo, el anterior rango de 224-255 bits ofrece mayor velocidad del proceso criptográfico, pero por la longitud menor de sus claves hace que este al límite del rango no permitido de 160-223 bits.

Entonces, teniendo en cuenta el análisis realizado, se concluye que los algoritmos de cifrado asimétrico a usar en la solución pueden ser el **RSA de 2048 bits o el ECDSA de factor P-256**. Sin embargo, como se verá en la especificación del tipo de certificado a usar, el algoritmo óptimo para el cifrado asimétrico de los mensajes de correo electrónico es el **RSA de 2048 bits**.

4.2.1.2. Función Hash de resumen para firma digital

Teniendo en cuenta la recomendación de la NIST SP-800-57 parte 3, se procede a analizar que funciones hash cumplen con el nivel de seguridad requerido para las firmas digitales usando el algoritmo RSA. Para ello, en la *tabla 7*, encontramos que la función hash recomendada para el algoritmo RSA-2048, es la SHA-256.

Asimismo, según el análisis de la *tabla 8*, del marco teórico, se concluye que la función hash recomendada para su uso en la actualidad, teniendo en cuenta que la fortaleza de bits mínima es de 128, lo cual corresponde a una función hash SHA-2 o SHA-3 de 256 bits o mayor. Por ello, se recomienda utilizar la función de 256 bits de módulo, ya que el nivel de procesamiento criptográfico es más rápido para su uso en firmas digitales en los servicios de correo electrónico. Además, teniendo en cuenta que un servicio de correo electrónico basado en la nube como Office 365 posee deficiencias en la velocidad de sus transacciones de envío y recepción de mensajes, es necesario no aumentar demasiado el tiempo de latencia entre estos. Por ello, se recomienda el uso de **SHA-256** como función de resumen.

4.2.1.3. Algoritmo de cifrado de contenido

Como especificación adicional en la definición de los algoritmos a usar, se define el algoritmo de cifrado simétrico para el cifrado del contenido del mensaje de correo electrónico. Este algoritmo no guarda relación con la PKI de manera directa, ya que este usa una sola clave para cifrar y descifrar el mensaje. Como se observa en la *tabla 4* del NIST SP-800-57, el algoritmo de clave simétrica tomado como referencia para aplicaciones que utilicen una PKI es el AES.

También se muestra el algoritmo 3TDEA como opción válida, sin embargo, en el mismo documento se define su validez como estándar seguro de cifrado y descifrado de contenidos. Este estándar era válido hasta el año 2015, a partir del 2016 se recomienda el uso de AES como estándar de cifrado de contenido, el cual cifra el contenido en bloques de 128 bits. Asimismo, el estándar NIST FIPS 140-2 recomienda el uso de los algoritmos AES y HMAC considerados está dentro del estándar. Por lo tanto, los algoritmos de cifrado del contenido que pueden ser utilizados son el **AES-128, AES-192, AES-256**.

4.2.2. Compatibilidad con Certificados Digitales S/MIME

El estándar de criptografía de clave pública S/MIME es el que será usado para el cifrado y firma de los mensajes enviados por el servicio de correo electrónico a través del servicio de Exchange Online. Es por ello, que la solución a proponer debe cumplir con la emisión de certificados digitales S/MIME necesarios para los procesos de criptografía en el mensaje de correo electrónico. Esta especificación cubre parte de los requerimientos 2 y 5 definidos en el capítulo 3 del proyecto.

4.2.2.1. Algoritmos recomendados por el estándar

La solución PKI basada en la nube debe seguir las especificaciones recomendadas por el estándar S/MIME, el cual se especifica en el IETF RFC 5751 (*S/MIME Version 3.2 - Message Specification*). En la sección 2 del estándar se brindan las recomendaciones de los algoritmos óptimos para el uso de los certificados S/MIME, tanto para el envío como para la recepción de los mensajes se muestra la siguiente jerarquía.

Receiving agents:

- MUST support RSA with SHA-256.
- SHOULD+ support DSA with SHA-256.
- SHOULD+ support RSASSA-PSS with SHA-256.
- SHOULD- support RSA with SHA-1.
- SHOULD- support DSA with SHA-1.
- SHOULD- support RSA with MD5.

Figura 37. Algoritmos recomendados por el IETF RFC 5751. Adaptado de “Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.2 - Message Specification”, por IETF RFC 5751, 2010.

Por lo tanto, los algoritmos recomendados por el estándar S/MIME están dentro de los algoritmos que se especificaron como válidos para la solución PKI. De esta manera, se puede determinar que el conjunto de algoritmos óptimos para las firmas digitales sería el **RSA-2048** junto a **SHA-256**.

Por otro lado, el estándar define que el algoritmo de cifrado de intercambio de llaves asimétricas óptimo para un certificado digital S/MIME es el **RSA** y para cifrar el contenido de los mensajes de correo electrónico el algoritmo óptimo es el **AES-128** o superior.

4.2.2.2. Compatibilidad con X.509 v3

La Autoridad de Certificación de la PKI basada en la nube debe emitir certificados digitales configurados con las especificaciones del estándar IETF RFC 5750, los cuales están estructurados de acuerdo con el estándar X.509 v3 con las

configuraciones y procesos requeridos para la integración del cifrado y firma digital en los mensajes de un correo electrónico enviado y recibido en formato MIME.

Los certificados digitales emitidos deben ser válidos para operar con el servicio de correo de Microsoft Exchange Online junto con los clientes de correo de Microsoft Outlook u OWA (Online Web Access). El cliente de correo Microsoft Outlook se encuentra habilitado para para la configuración de certificados digitales S/MIME con el formato X.509 v3.

4.2.3. Configuración de los certificados digitales S/MIME

La configuración de los certificados digitales que serán emitidos por la CA debe estar claramente definidos y estandarizados dentro de la organización. Por lo cual, en el presente apartado, se busca dar las pautas necesarias para la definición del formato de la plantilla a usar para la emisión de los certificados digitales S/MIME de los usuarios de correo electrónico. Se definirán los algoritmos de cifrado, longitud de claves y el ciclo de vida que tendrán. Todas estas características, serán establecidas siguiendo la estructura del estándar ITU-T X.509 versión 3, el cual brinda las recomendaciones necesarias para la emisión de un certificado digital por la CA dentro de una PKI.

Para la organización objetivo, Toyota del Perú, se determinarán los perfiles de certificados a usar dentro de la solución. Para desarrollar la propuesta, se pondrá como premisa el caso de una organización con 100 usuarios, los cuales estarán distribuidos en tres jerarquías o niveles de confidencialidad. El primer nivel y el más confidencial, serán los gerentes y directores de la organización. El segundo nivel, lo conformaran los jefes de área o

supervisores. El tercer nivel estará compuesto por el resto de los empleados de la organización. Sin embargo, el tercer nivel solo se planteará de manera referencial y no se tomará en cuenta en la propuesta del proyecto, ya que, de acuerdo con el alcance establecido en la primera parte del proyecto, la propuesta de seguridad de la información mediante el cifrado y firma digital de los mensajes de correo electrónico tienen como alcance a los gerentes, directores y jefes de área. Esta especificación cubre parte de los requerimientos 1, 2 y 3 definidos en el capítulo 3 del proyecto.

4.2.3.1. Definición de plantillas de los certificados

Antes de empezar con la definición de las plantillas, se debe mencionar que la solución debe ser compatible con la emisión de certificados X.509 v3. Además, debe proveer un mecanismo de definición de plantillas que facilita la creación de los certificados digitales. Para este caso, se definirán tres tipos de plantillas de certificados una para cada nivel de confidencialidad de la organización.

- **Correo Nivel 1:** Plantilla de certificados digitales para los usuarios de correo que sean directores o gerentes dentro de la organización.
- **Correo Nivel 2:** Plantilla de certificados digitales para los usuarios de correo que sean jefes de área o supervisores a cargo de personal dentro de la organización.
- **Correo Nivel 3 (referencial):** Plantilla de certificados digitales para los usuarios de correo que formen parte del resto de empleados de la organización.

4.2.3.2. Configuración del campo *Subject*

Este es un campo importante que definir en la estructura del certificado digital, ya que es donde se identificará al dueño del certificado digital. En principio, el dueño del certificado

digital será el usuario de correo electrónico, por lo cual se ingresará la información que la organización requiere que se muestre del usuario.

Tabla 12

Cuadro de campos definidos en las plantillas de certificados para el campo Subject.

Campo	Alias	Descripción
Nombre Común	CN	En este campo se recomienda ingresar la dirección de correo electrónico del usuario dueño del certificado.
Unidad Organizativa	OU	En este campo se recomienda ingresar el área a la cual pertenece el usuario dentro de la organización.
Nombre propio	CN	En este campo se recomienda ingresar los nombres de la persona dueña del certificado.
Apellidos	CN	En este campo se recomienda ingresar los apellidos de la persona dueña del certificado.
Cargo	O	En este campo se recomienda ingresar el cargo que ocupa el usuario dentro de la organización.
Organización	O	En este campo se recomienda ingresar el nombre legal de la organización (razón social o nombre oficial de la entidad organizativa)
Calle	STREET	En este campo se recomienda ingresar la dirección de la ubicación del usuario. Estas direcciones serán por lo general las oficinas de la organización en donde laboran los usuarios.
Localidad	L	En este campo se recomienda ingresar la localidad, departamento o provincia en la cual se encuentra la Calle previamente definida.
País	C	En ese campo se recomienda ingresar el país a donde pertenece la localidad previamente definida.

Nota. Se ha realizado este cuadro para describir los campos dentro del campo Subject del certificado digital, de elaboración propia. Adaptado de ITU-T X.500, por ITU-T X.500, 2012.

Como se observa en la *tabla 12*, la información del usuario de correo se debe ingresar en formato DN (*Distinguished Names*) según lo indica el estándar ITU-T X.501. De esta manera, se tiene la información del usuario de correo organizado y compatible las CA a nivel mundial.

4.2.3.3. Configuración de algoritmos y longitud de claves

Como parte esencial de la configuración de los certificados digitales, es necesario definir qué algoritmos y longitud de claves serán configurados. Además, cuál es el nivel de seguridad que cada uno de ellos ofrece, para así alinearlos con el cifrado y el firmado requerido de los correos electrónicos que serán enviados por los usuarios a través del servicio de correo Exchange Online.

Para definir el tipo de algoritmo de firma digital, se tiene en cuenta el nivel de confidencialidad de la organización. Además, en la sección de definición de los algoritmos, solo se recomienda usar el algoritmo **SHA-256**. A continuación, se muestra un cuadro en el cual se describe la asignación por tipo de plantilla según la importancia de los usuarios de la organización:

Tabla 13*Cuadro de niveles de confidencialidad*

Nivel de Confidencialidad	Algoritmo de firma	Descripción
Correo Nivel 1	SHA-256 con cifrado RSA	Para los directores y gerentes, los cuales manejan información mucho más confidencial, es más seguro usar la función hash SHA-256. Y el algoritmo RSA para el cifrado de la información con claves asimétricas.
Correo Nivel 2	SHA-256 con cifrado RSA	Para los jefes de área y supervisores, también es requerido la función SHA-256. Y el cifrado RSA para el cifrado de la información con claves asimétricas.
Correo Nivel 3 (referencial)	SHA-1 con cifrado RSA	De manera referencial, se propone la función SHA-1 para los usuarios de correo comunes, la cual posee 160 bits de salida. Es usado en la actualidad, sin embargo, ya no se recomienda su uso, debido a que posee vulnerabilidades descubiertas. Asimismo, el cifrado RSA para el intercambio de claves asimétricas.

Nota. Se han definido los niveles de confidencialidad para el uso de los algoritmos de cifrado y función de resumen, de elaboración propia.

Por otro lado, la longitud de clave a usar por cada uno de los tres tipos de plantillas también debe ser considerada teniendo en cuenta ciertos aspectos de seguridad. Cada uno de los niveles de confidencialidad o jerarquía va a tener un tipo de longitud de clave tal como se muestra en el siguiente cuadro:

Tabla 14

Longitud de clave pública a definir por cada plantilla de certificado.

Plantilla	longitud de clave	Descripción
Correo Nivel 1	2048 bits	Para los directores y gerentes, los cuales manejan información mucho más confidencial, se debe usar una longitud de clave de 2048 bits, ya que estas claves son mucho más seguras y difíciles de descifrar con el algoritmo RSA.
Correo Nivel 2	2048 bits	Para los jefes de área y supervisores, es recomendable también una clave de 2048 bits. Esto se debe a que los usuarios de este nivel no envían gran cantidad de tráfico de correos y se requiere un nivel de seguridad superior.
Correo Nivel 3 (referencial)	1536 bits	Para los usuarios de correo comunes, de manera referencial, es suficiente con una longitud de clave de 1536 bits la cual asegure un nivel de seguridad bueno. Sin embargo, el algoritmo RSA con esta longitud de clave no está recomendado para su uso.

Nota. Se han definido los niveles de confidencialidad para establecer la longitud de las claves del algoritmo de cifrado RSA, de elaboración propia.

De esa manera, se puede observar que el cifrado en cada plantilla en la organización es similar y requiere de un tipo de seguridad específico. Es por ello, que se determina el tipo de algoritmo, función hash y longitud de clave requeridos para cada uno de ellos. Luego de definir la configuración que tendrán los tres tipos de plantilla, se pasa a definir el ciclo de vida de los certificados para complementar la configuración de los certificados digitales.

4.2.3.4. Definición del ciclo de vida de los certificados

Finalmente, se debe definir el ciclo de vida que tendrá cada certificado digital S/MIME de acuerdo con dos factores previamente definidos: La longitud de las claves y la confianza en el usuario certificado. Estos factores, nos ayudaran a tener una idea de la duración que debe tener cada tipo de certificado digital, creándose así un posterior cronograma de renovaciones de certificados de acuerdo con su ciclo de vida.

A continuación, se muestra un cuadro en donde se definen los ciclos de vida a considerar por cada tipo de certificado:

Tabla 15

Cuadro del ciclo de vida de las plantillas de certificados

Plantilla	longitud de clave	Confiabilidad en el usuario	Ciclo de vida	Descripción
Correo Nivel 1	2048 bits	Alta	2 años	Para los directores y gerentes se plantean 2 años. Debido a que su longitud de clave es de 2048 bits, es una clave difícil de descifrar. Asimismo, la confiabilidad de los usuarios que se encuentran en esta plantilla es alta, por lo cual se puede confiar que los usuarios no divulgaran su clave privada fácilmente.
Correo Nivel 2	2048 bits	Media	1 año	Para los jefes de área y supervisores se plantea 1 año. Esto debido a que su longitud de clave es de 2048 bits, lo cual la hace una clave difícil de descifrar. Por otro lado, la confiabilidad en el usuario

				es media, por lo cual se recomienda que el certificado del usuario tenga una validez de 1 año como máximo.
Correo Nivel 3 (referencial)	1536 bits	Baja	6 meses	Para los usuarios de correo comunes se plantean 6 meses. Esto debido a que la longitud de su clave es de 1536 bits, lo cual la hace una clave compleja pero menos difícil de descifrar. Por otro lado, se define que para un usuario empleado se debe emitir un certificado digital con 6 meses de validez, ya que su grado de confiabilidad es muy bajo.

Nota. Se ha definido el ciclo de vida de los certificados digitales según el nivel de confidencialidad, de elaboración propia.

Según se observa en el cuadro, no todos los certificados digitales deben tener el mismo ciclo de vida, como medida de seguridad se debe limitar la validez de un certificado digital. La mejor manera de definir este tiempo es tomar en cuenta los factores correctos, como lo son en este caso la longitud de la clave y la confiabilidad en el usuario. Pueden existir otros factores adicionales, lo cuales podrían ser evaluados por las organizaciones, sin embargo, para el caso de Toyota se proponen estos.

Finalmente, se concluye que la configuración de los certificados digitales debe ser correctamente planeada y analizada, para así determinar un estándar interno en la organización, el cual ayude a administrar mejor los certificados digitales. Por otro lado, es importante definir los parámetros de tiempo y criptografía utilizada en los certificados digitales, para así establecer niveles de seguridad requeridos en la organización, los cuales estén acordes al servicio de correo electrónico sobre el cual se van a integrar para utilizar el

cifrado y firma digital. Asimismo, la determinación de las mejores prácticas aplicadas a los certificados digitales debe registrarse en una CP (*Certificate Policy*) que defina toda la gestión y configuración de los certificados en la CA a detalle, el cual debe exceder las capacidades de organizaciones que operan con una PKI On-Premise.

4.2.4. PKI basada en la nube

La propuesta de solución del proyecto basa su funcionamiento en una PKI basada en la nube. Se propone esta solución debido a que es una solución más acorde a los requerimientos de la organización. Esta especificación cubre el requerimiento 4 definido en el capítulo 3 del proyecto. A continuación, se especifican los componentes que están dentro de este bloque de la PKI basada en la nube tal como se muestra en el modelo de arquitectura propuesto.

4.2.4.1. Modelo de Confianza de las CA

El núcleo central de la PKI basada en la nube está basada en la relación de confianza entre las CA que la componen. Para la propuesta, la CA que emitirá los certificados digitales S/MIME debe pertenecer a una infraestructura del modelo jerárquico, el cual es ampliamente usado en la actualidad y está compuesto por un gran número de CA, las cuales están divididas en tres tipos. Es importante que la jerarquía de las CA sea de gran tamaño y está distribuida de manera geográfica en distintas partes del mundo, ya que esto ayuda a mejorar la velocidad de respuesta a las consultas de estado de los certificados (OCSP) y la alta disponibilidad de los certificados digitales.

Figura 38. Jerarquía de las CA que forman parte de la PKI. Adaptado de “Building and Managing a PKI Solution for Small and Medium Size Business”, por SANS.ORG, 2013.

- **CA Raíz:** Esta CA es la encargada de emitir los certificados digitales a las demás CA que componen la jerarquía. Existe una relación de confianza directa entre ellas y las CA intermediarias, mas no con las CA emisoras.
- **CA Intermediaria:** Estas CA son subordinadas de la CA raíz y son las encargadas de emitir certificados a las otras CA de la jerarquía. Asimismo, pueden emitir certificados digitales a otras CA y a usuarios finales que requieran de una suscripción.
- **CA Emisora:** Esta CA es la encargada de emitir el certificado digital a los usuarios finales. Es decir, esta CA será la que emita los certificados digitales S/MIME que serán usados para el servicio de correo electrónico.

Como se ve en la figura de arriba, existe una relación de confianza jerárquica entre las CA de la PKI, para poder intercambiar la información de los certificados digitales y las CRL que almacenan sus repositorios locales. Las CA Emisoras que conforman esta jerarquía serán las encargadas de emitir los certificados S/MIME para los usuarios de correo. Asimismo, si una

CA emite el certificado, este será replicado en las otras CA de la infraestructura. Cada CA Emisora de tercer nivel tiene una RA (autoridad de registro) y un repositorio que interactúan de manera directa entre sí.

Funciones de la CA en la PKI:

- Recibir las peticiones de emisión de certificados de los usuarios suscriptores.
- Interactuar con la RA para aprobar la emisión de un certificado.
- Emitir un Certificado Digital de acuerdo con la información proveída por la RA.
- Administrar las CRL.
- Renovar Certificados Digitales.

4.2.4.2. Autoridad de Registro

Dentro de la PKI basada en la nube cada CA Emisora posee asociada una RA. La función de la RA es de gestionar cada una de las peticiones para emisión de certificados y CRL. Se propone que cada usuario suscriptor debe tramitar la emisión de su certificado digital S/MIME mediante el “Administrador de PKI” definido en la propuesta. Este administrador es el único encargado con acceso a la interfaz de administración que brinde el proveedor de PKI basada en la nube. Cada petición de certificado S/MIME será tramitado con documentación interna entre el administrador PKI y el usuario de correo. Una vez definida la información del usuario que será definida en el certificado, de acuerdo con el estándar X.509 v3, el Administrador PKI hará de intermediario entre la RA de la PKI a través de la interface de administración.

Funciones de la RA en la PKI:

- Envío de las solicitudes de emisión de certificados S/MIME a la CA de la PKI.
- Registro en la DB local de la RA de las solicitudes de emisión de certificados.
- Gestionar el ciclo de vida de los certificados digitales para establecer la creación de las CRL que serán descargadas por los usuarios o consultadas a la Autoridad de Validación mediante el protocolo OCSP.
- Descargar y enviar los certificados S/MIME emitidos por la CA a los usuarios de correo electrónico. Esta acción la hace el Administrador PKI para luego instalar los certificados en los clientes de correo.
- Gestionar el envío de la clave privada de manera segura al usuario de correo electrónico.

Figura 39. Funcionamiento interno de la RA en la PKI basada en la nube. Adaptado de “Modelo de arquitectura de integración entre una PKI y un servicio de correo electrónico basado en Office 365”, elaboración propia.

4.2.4.3. Autoridad de Validación

La Autoridad de Validación (VA) tiene como principal objetivo el responder a las solicitudes que consultan acerca del estado de un certificado digital. La VA que forma parte de la PKI basada en la nube, es la encargada de responder a las consultas acerca de la validez de los certificados digitales en nombre de la CA. La VA obtiene esta información de la CA cada vez que se realiza el proceso de emisión, renovación o revocación de un certificado digital. Luego, esta almacena esta información en su BD local para luego responder a las consultas mediante el protocolo OCSP. La información de los estados es en tiempo real, ya que la CA actualiza esta información en la VA cada vez que existe un cambio en la validez de los certificados digitales. Como se observa en el diseño, estas consultas serán efectuadas por los clientes de correo electrónico S/MIME para validar los certificados digitales que contienen las claves públicas de los destinatarios.

Figura 40. Funcionamiento de la VA en la PKI basada en la nube. Adaptado de “Modelo de arquitectura de integración entre una PKI y un servicio de correo electrónico basado en Office 365”, elaboración propia.

4.2.4.4. Almacenamiento y Distribución del par de claves

Otra especificación muy importante por considerar en la PKI es la administración del almacenamiento y la distribución de las claves o llaves que han de ser parte fundamental para el cifrado y firma de los mensajes de correo. Por lo cual se requiere que el servicio PKI demuestre que emplea mecanismos de seguridad avanzados para su cuidado y distribución.

Repositorio HSM

El almacenamiento de las claves privadas y públicas dentro de la PKI se realiza en la CA junto con el repositorio y estos deben cumplir con el nivel de seguridad requerido por el estándar **NIST FIPS 140-2** cifrando el par de llaves e impedir el acceso no autorizado a ellas. Los dispositivos que cumplen estas funciones criptográficas son llamados Hardware de Módulos de Seguridad (HSM). Para el almacenamiento de las claves criptográficas a un nivel alto de seguridad no suele usarse software, pues estas soluciones son muy propensas a vulnerabilidades, manipulación o uso indebido de la información. Por ello, el repositorio donde se almacenan los certificados digitales y el par de claves deben estar basados en módulos HSM y son los que deben ser utilizados por el servicio de PKI basado en la nube que se escoja para proteger las claves almacenadas en la PKI.

El almacenamiento en estos módulos HSM, al no ser por software, utilizan conjuntos de circuitos integrados o chipsets que ofrecen almacenamiento físico de las claves generadas por la CA. Para cumplir con las características óptimas de seguridad de la información, se recomienda utilizar el nivel 3 de seguridad que ofrece el estándar FIPS 140-2 para las especificaciones del almacenamiento y distribución de las claves.

Almacenamiento en el equipo cliente

Por otro lado, para el almacenamiento de las claves privadas en los certificados digitales almacenados como archivos se usan las extensiones “.p12” o “.pfx” definidas por el estándar PKCS #12. Asimismo, el estándar **NIST 800-57** provee recomendaciones para la administración, almacenamiento y distribución de las claves dentro y fuera de la PKI. En los clientes de correo electrónico en donde se instalarán los certificados digitales deben ser soportados estas extensiones de archivos aceptados a nivel mundial por su interoperabilidad.

Distribución de los certificados

Las claves privadas que son almacenadas en unidades de almacenamiento “*offline*” en la CA o repositorio usan cifrado de datos sobre las mismas unidades de almacenamiento y para acceder a la distribución de la clave almacenada se debe pasar por múltiples autorizaciones para la autorización de entrega de la clave, siendo todos estos procesos auditados. Los métodos de distribución de las claves privadas pueden ser mediante tarjetas inteligentes, token USB o un dispositivo HSM móvil el cual debe permanecer con el usuario de manera segura. Asimismo, la clave puede ser distribuida para un usuario mediante una comunicación segura mediante su portal de administración PKI.

4.2.5. Servicio de correo electrónico Office 365

Dentro de la red corporativa de Toyota, ya sea del Perú o de otra sede internacional, se encuentran los clientes de correo electrónico que harán uso de los certificados digitales para el cifrado y firma digital. Asimismo, es en donde opera el servicio de correo electrónico

basado en la nube Office 365. En esta red se encuentran los usuarios que harán uso del servicio de cifrado y firma digital sobre sus correos, estos usuarios son los Gerentes y jefes de área que manejan la información más crítica en la organización. Por otro lado, se observa el Administrador de la PKI que gestiona todo lo relacionado con los certificados digitales que serán emitidos para el funcionamiento del cifrado y firma digital. A continuación, se describe el propósito de cada elemento del diseño dentro de la red corporativa de Toyota, así como, su funcionamiento dentro de la solución. Esta especificación cubre parte de los requerimientos 3 y 5 definidos en el capítulo 3 del proyecto.

4.2.5.1. Cliente de Correo Office 365

El cliente de correo electrónico está configurado con el servicio Exchange Online de Office 365. Este servicio es accedido a través de la nube (Internet) por los usuarios de la red corporativa de Toyota del Perú. Los usuarios de correo electrónico acceden a sus cuentas a través del cliente Microsoft Outlook que está instalado de manera local en las computadoras personales de los usuarios. Según el alcance del proyecto, el medio por el cual los usuarios podrían enviar correos electrónicos firmados y cifrados digitalmente sería a través de estos equipos de cómputo personales que estarán configurados con los certificados digitales S/MIME. Para ello, el servidor Exchange Online debe tener habilitado el protocolo S/MIME, sin embargo, cabe resaltar que por defecto el soporte del protocolo se encuentra habilitado en el servicio de Office 365 contratado por Toyota.

El cliente de correo electrónico se integra con la PKI basada en la nube mediante la instalación de los certificados digitales S/MIME en el cliente Microsoft Outlook. El cliente de Microsoft Outlook almacena los certificados digitales con la clave pública de los usuarios

de correo electrónico destinatarios, estos certificados se asocian a sus cuentas de correo de correo dentro de la información del contacto.

Como se observa en la propuesta, El cliente de correo Office 365 “A” posee el certificado digital con su clave privada y el certificado digital con la clave pública del cliente de correo “B”, asimismo, de manera inversa en el cliente de correo Office 365 “B”. Según la propuesta, el funcionamiento es el siguiente:

- El usuario “A” envía un correo electrónico firmado electrónicamente con su clave privada para que el usuario “B” pueda validarlo con la clave pública del usuario “A”.
- El usuario “A” envía un correo electrónico cifrado con la clave pública del usuario “B” para que solo el usuario “B” con su clave privada pueda descifrar el mensaje enviado por el usuario “A”.

De esta manera, todos los mensajes de correo electrónico enviados viajan de manera segura a través de internet, pasando por el servidor Exchange Online, y llegando finalmente a sus destinatarios. Como se mencionó previamente, el destinatario puede tener su cuenta de correo electrónico abierto en varios dispositivos, pero los mensajes cifrados y firmados digitalmente solo podrán ser leídos en la computadora personal con el cliente Microsoft Outlook en donde se tienen instalados los certificados digitales emitidos por la PKI.

4.2.6. Administrador de PKI

Esta especificación cubre parte del requerimiento 2 definido en el capítulo 3 del proyecto.

El Administrador de la PKI representa al área de TI de Toyota del Perú, más específicamente, son los analistas de sistemas especializados en el manejo de la PKI basada en la nube. El

administrador posee los conocimientos necesarios para la administración de los certificados digitales y la configuración de la PKI. Estos conocimientos son brindados, mediante capacitaciones del proveedor de la PKI basada en la nube, a los analistas de sistemas. Asimismo, estos deberán contar con los conocimientos teóricos y normativos acerca del funcionamiento de una PKI de manera general.

El Administrador de PKI opera el sistema mediante una interfaz gráfica o panel de administración que es proporcionado por el proveedor de la PKI. A través de esta interfaz, se realizarán las tareas de solicitud de emisión de un certificado digital S/MIME para los usuarios de correo electrónico, dicha solicitud será efectuada, de manera interna, mediante un formulario en el cual el usuario de correo electrónico registrará la información que necesita el Administrador de la PKI para gestionar la emisión de su certificado a la RA de la PKI.

Solicitud de Emisión de Certificado Digital para Correo Electrónico

Razón Social Toyota del Perú S.A.
 Fecha de Solicitud:
 Cierre de inscripción:
 Código:

La información contenida en el presente formulario será mantenida confidencial y sólo será utilizada para la Emisión del Certificado Digital a través de la Entidad de Certificación.

Datos del Usuario

Nombre	<input style="width: 90%;" type="text"/>		
Apellido	<input style="width: 90%;" type="text"/>		
Área/Gerencia	<input style="width: 40%;" type="text"/>	DNI	<input style="width: 50%;" type="text"/>
Cargo	<input style="width: 90%;" type="text"/>		
Teléfono/Celular	<input style="width: 90%;" type="text"/>		
Correo Electrónico	<input style="width: 90%;" type="text"/>		
Domicilio	<input style="width: 90%;" type="text"/>		

Información del Certificado Digital S/MIME

Usuario	<input style="width: 60%;" type="text"/>		
Fecha de Emisión	<input style="width: 20%;" type="text"/>	Fecha de Vto.	<input style="width: 70%;" type="text"/>
Unidad Organizativa	<input style="width: 90%;" type="text"/>		
Datos Adicionales	<input style="width: 90%;" type="text"/>		
Firma del Usuario	<hr style="border: 0; border-top: 1px solid black; width: 100%;"/>		
Firma del Jefe de TI	<hr style="border: 0; border-top: 1px solid black; width: 100%;"/>		

Figura 41. Propuesta de Formulario de Solicitud de Certificado Digital. Adaptado de “Un formulario de inscripción estándar”, elaboración propia.

Este formulario es un Pre-Registro que será llenado por el usuario de correo electrónico. Luego, el administrador PKI tramita la Emisión del certificado digital con la información llenada en el registro, el registro es hecho a la RA a través del panel de administración de la PKI basada en la nube. Finalmente, una vez emitido el certificado digital S/MIME, el administrador de la PKI se encarga de descargar e instalar el certificado digital en el cliente de correo electrónico Microsoft Outlook que utilizan los usuarios.

4.3. Evaluación y Selección de Recursos

Luego de haberse detallado las especificaciones y características técnicas que tendrá la PKI basada en la nube, se debe realizar una evaluación de las alternativas de solución que se tienen en el mercado. Para ello, se han establecido tres productos de diferentes proveedores, los cuales se evaluarán teniendo como criterio el cumplimiento de las especificaciones y sus características técnicas detalladas con anterioridad. A continuación, se presenta una matriz de evaluación propuesta, la cual dispone del siguiente método de valoración:

- Es 0 (cero) cuando el producto No cumple con la característica.
- Es 1 (uno) cuando el producto Cumple deficientemente con la característica.
- Es 2 (dos) cuando el producto Cumple medianamente con la característica.
- Es 3 (tres) cuando el producto Cumple perfectamente con la característica.

Tabla 16

Evaluación de especificaciones en productos MPKI basada en la nube

#	Especificación técnica	Producto		
		Symantec MPKI	DigiCert MPKI	GlobalSign MPKI
1	Emplea el algoritmo criptográfico asimétrico RSA con una clave de 2048 bits para el firmado de los certificados digitales y el cifrado de datos.	3	3	3
2	Emplea el algoritmo SHA-256, el cual posee 256 bits de longitud en su salida.	3	3	3
3	El algoritmo de cifrado simétrico para cifrar el contenido del mensaje es el AES-256 que usa una llave de 256 bits para el cifrado y descifrado del contenido del mensaje de correo electrónico.	3	3	3
4	La Autoridad de Certificación emite certificados digitales para las aplicaciones de correo que utilicen	3	3	3

	S/MIME, siguiendo el estándar X.509 v3 para la estructura de los certificados digitales.			
6	Los certificados digitales emitidos son válidos para operar con el servicio de correo de Microsoft Exchange Online, en conjunto con los clientes de correo de Microsoft Outlook u OWA (Online Web Access) bajo los navegadores de internet más populares como Mozilla Firefox, Google Chrome, Internet Explorer o Safari.	3	3	3
8	El Administrador de la PKI debe identificarse continuamente con métodos de autenticación múltiple antes de ejecutar operaciones críticas de seguridad como el cambio de la política de seguridad, cambio de contraseñas, etc.	2	1	1
11	La solución ofrece un único portal de administración centralizado para la gestión de todas las tareas de la PKI.	3	2	2
18	El almacenamiento y distribución de claves cumple con el nivel de seguridad requerido por los estándares FIPS 140-2, PKCS (#7, #10 Y #12) y NIST 800-57	3	3	2
19	La solución determina unas CP (Certificate Policy) que definen toda la gestión de los certificados en la PKI a detalle, el cual debe exceder las capacidades de organizaciones que operan una PKI On-Premise.	3	3	3
20	El almacenamiento de la solución debe estar basado en módulos de hardware criptográfico (HSM) para proteger las claves almacenadas en los repositorios de la PKI.	3	3	3
21	Las claves privadas son almacenadas en unidades de almacenamiento “offline” usando cifrado de datos sobre las mismas unidades de almacenamiento.	3	3	2
22	Los métodos de distribución de las claves privadas pueden ser mediante tarjetas inteligentes, token USB o un dispositivo HSM móvil. Por otro lado, la clave también puede ser distribuida a través de una	2	2	1

comunicación segura mediante el portal de administración.

28	La PKI soporta el algoritmo RSA y con una longitud de las claves de 1536 y 2048 bits.	3	3	3
29	La PKI soporta la función hash o de resumen SHA-2 con una longitud de salida de 256 bits	3	3	3
30	La duración mínima de los certificados digitales que la PKI ofrece es de 6 meses.	3	0	0
Puntaje Total:		43	38	35

Nota. Se ha elaborado siguiendo las especificaciones de cada producto extraído de las páginas de Symantec, Digicert y Globalsign indicado en la comparativa, elaboración propia.

Finalmente, luego de evaluar cada especificación en las tres propuestas de PKI *Cloud-based*, el producto MPKI basada en la nube con mayor puntaje es la de *Symantec Managed PKI* con **43 puntos**. Por lo cual, se sugiere el uso de este producto para la propuesta de PKI para la emisión de certificados digitales S/MIME. Asimismo, cabe recalcar que la corporación Symantec es uno de los líderes en tecnologías de cifrado para la seguridad de la información.

4.4. Evaluación de Costos

Los costos que la solución supone implementar y mantener a lo largo del tiempo son evaluados en este apartado, para ello, se toman en cuenta el CAPEX (inversión inicial o capital inicial para el despliegue de la solución) y el OPEX (costo de la operatividad de la solución). En consecuencia, se evalúan los costos involucrados en la solución, los cuales están basados a una la lista de precios oficial de Symantec² tomada como referencia. Este

² Cfr. Ver enlace a la lista de precios en la bibliografía: KERNELSOFTWARE.COM

análisis esta realizado teniendo como referencia comparativa a una solución de PKI *On-Premise*. Por otro lado, el análisis de la evaluación de costos está basado en un total de 100 usuarios de certificado digital aproximadamente por administrar en Toyota. A continuación, se presentan los análisis realizados para el CAPEX y el OPEX del proyecto:

Tabla 17

Cuadro de CAPEX del proyecto

Licencia de Servicio				
Ítem	Descripción	Cantidad	Costo Unit.	Costo Total
1	Setup de la cuenta Managed PKI (MGD PKI ACCT SETUP EXPRESS BAND F)	1.00	\$ 1,222.97	\$ 1,222.97
Total				\$ 1,222.97
Personal				
Ítem	Descripción	Cantidad	Costo Unit.	Costo Total
1	Capacitación básica del Administrador PKI	1.00	\$ 200.00	\$ 200.00
Total				\$ 200.00
Total CAPEX:				\$ 1,422.97

Nota. Resumen de los costos que son tomados al inicio del proyecto, elaboración propia.

En la *tabla 17* se puede observar que el producto de Symantec MPKI casi no genera costos de implementación. Solo se cuenta con una licencia inicial para la configuración de la cuenta, el cual es un pago único al momento de contratar el servicio. Por otro lado, se requiere de una capacitación básica para el administrador de PKI, ya que la administración de la PKI fácil de usar y requiere de conocimientos básicos. Además, no existe ningún costo por implementación de una infraestructura de hardware, pues se trata de un servicio que está alojado en la nube y es accesible desde cualquier parte en donde se tenga acceso a internet.

Tabla 18*Cuadro de OPEX del proyecto*

Licencia de Servicio				
Ítem	Descripción	Cantidad	Costo Unit.	Costo Total
1	Cuota anual por el servicio PKI administrado.	1	\$ 17,000.00	\$ 17,000.00
2	Cuota anual por certificado (seat) digital (MGD PKI U SEATS HS SUB EXPRESS BAND F 1YR)	100	\$ 27.59	\$ 2,759.00
3	Soporte anual GOLD (MGD PKI SUP GOLD VPA 1YR)	100	\$ 2.06	\$ 206.00
Total				\$ 19,965.00
Infraestructura				
Ítem	Descripción	Cantidad	Costo Unit.	Costo Total
1	Conexión a internet para la administración web del servicio Symantec PKI Manager (mensual)	12	\$ 80.00	\$ 960.00
Total				\$ 960.00
Personal				
Ítem	Descripción	Cantidad	Costo Unit.	Costo Total
1	Administrador de la PKI	1	\$ 15,000.00	\$ 15,000.00
2	Asistente	1	\$ 5,000.00	\$ 5,000.00
Total				\$ 20,000.00
Total				\$ 40,925.00
OPEX:				

Nota. Resumen de los costos operativos que, mensual o anualmente, se aplican a la solución, elaboración propia.

En la *tabla 18* se observa que uno de los costos más altos que supone implementar la solución de Symantec es la inversión que se realiza anualmente para mantener operativa la solución en el licenciamiento del servicio. Por otro lado, existe un pago anual por cada certificado digital contratado para cada usuario de correo electrónico a utilizar y un pago anual de soporte por licencia de certificado digital adquirido. Para la infraestructura de hardware, se observa que Symantec no genera costos adicionales, más si es necesario considerar un pago anual por la conexión a internet que se necesita para acceder al portal de administración de la PKI (Symantec PKI Manager) Finalmente, el personal necesario para administrar la solución comprender de un administrador y un asistente, los cuales no necesitan ser expertos en la tecnología PKI.

Tabla 19

Cuadro de Análisis Financiero de la solución Symantec MPKI

ANALISIS FINANCIERO DEL PROYECTO

		12	4
Tasas	Anual	Mensual	Trimestral
Tasa Promedio Ponderado de Costo de Capital (WACC)	15%	1.17%	3.56%

	año 00	año 01	año 02	año 03	año 04	año 05
(+) Mantenimiento de Software		25,000.00	25,000.00	25,000.00	25,000.00	25,000.00
(+) Mantenimiento de Infraestructura		10,000.00	10,000.00	10,000.00	10,000.00	10,000.00
(+) Personal y Servicios de terceros		55,000.00	55,000.00	55,000.00	55,000.00	55,000.00
Costo de Solucion On-Premises	270,000.00	90,000.00	90,000.00	90,000.00	90,000.00	90,000.00
(-) Licenciamiento del Servicio (x100 usuarios)		-19,965.00	-19,965.00	-19,965.00	-19,965.00	-19,965.00
(-) Conexión a Internet		-960.00	-960.00	-960.00	-960.00	-960.00
(-) Costo de Personal		-20,000.00	-20,000.00	-20,000.00	-20,000.00	-20,000.00
Costo Operativo de Symantec MPKI (OPEX)		-40,925.00	-40,925.00	-40,925.00	-40,925.00	-40,925.00
Flujo Económico de Operación (FEO)		49,075.00	49,075.00	49,075.00	49,075.00	49,075.00
Denominador		1.15	1.32	1.52	1.75	2.01
División		42,673.91	37,107.75	32,267.61	28,058.79	24,398.95
Inversion Neta de Capital (CAPEX)	1,522.97					
Totales	271,522.97	49,075.00	49,075.00	49,075.00	49,075.00	49,075.00

NPV o VAN en 1 año	41,150.94
NPV o VAN en 5 años	162,984.04

ROI en 1 año	100.55%
ROI en 5 años	398.25%

Nota. Análisis de los costos implicados en el CAPEX y OPEX de la solución propuesta en comparativa a una solución On-Premises, Adaptado de una tabla de análisis financiero presentada en el curso de Finanzas para las operaciones, por UPC, 2014.

Para realizar el análisis financiero del proyecto, fue necesario definir la tasa de Promedio Ponderado de Costo per Cápita (WACC) usado en proyectos de TI, la cual nos ayuda a hallar el costo promedio de la solución por año a evaluar. Además, se calcularán valores como el VAN, que trae el costo de inversión a futuro a su valor actual presente neto, y el ROI, el cual indicará una tasa que demuestra si la inversión es justificada.

El análisis toma una tasa de WACC de 15% para obtener mayor margen al momento de realizar la evaluación. Extrayendo todos los datos del CAPEX y OPEX se desarrolla un flujo de caja a futuro de la solución de Symantec. Por otro lado, los ingresos dentro del flujo vienen definidos con los precios estándar que implicaría una solución PKI interna (*On-Premises*) con prestaciones básicas necesarias para Toyota del Perú.

Se observa que la solución cumple con un retorno de la inversión mayor al 100% al año de ser implementado, por lo cual esta solución es sumamente viable y recomendable para la implementación de una PKI basada en la nube que brinde certificados digitales para su uso en firmas digitales y cifrado en los mensajes de correo electrónico de Toyota.

CAPÍTULO V: PRUEBAS, RESULTADOS Y VALIDACIÓN DE LA PROPUESTA

5.1. Desarrollo del Plan de Pruebas por O.E.

Siguiendo la metodología definida en el capítulo 2 (punto 2.11), se proceden a desarrollar los planes de pruebas de cada objetivo específico definido en el proyecto.

5.1.1. Ejecución del plan de pruebas O.E. “a”

5.1.1.1. Información general

Organización	Toyota del Perú
Fecha de preparación	22-12-2017
Objetivo Especifico	Determinar los principales riesgos que podrían afectar a la seguridad de la información y los costos que implican los incidentes de seguridad que podrían presentarse en un servicio de correo electrónico basado en Office 365.
Servicio analizado	Correo Office 365
Año de análisis de datos	2016
Líder de proyecto	Jefe de TI
Líder de las pruebas	Analista de Seguridad de TI

5.1.1.2. Alcance de prueba

Se medirán los riesgos cuyas amenazas impactan a los activos de información relacionados con el servicio de correo electrónico. Además, se utilizarán las métricas de porcentaje a la exposición de los riesgos y el monto del costo que implican los incidentes de seguridad que afectan al servicio de correo electrónico de una organización como Toyota del Perú.

5.1.1.3. Recursos necesarios

Los recursos necesarios para las pruebas son los siguientes:

1. Amenazas que impactan a la seguridad de la información en un servicio de correo electrónico basado en la nube.
2. Activos de información que son impactados en caso de ataques al servicio de correo electrónico y cuál es su valoración ante algún incidente que impacte dicho activo.
3. Valor de ventas anual que tuvo Toyota del Perú el año 2016 (proyectado).

5.1.1.4. Método de prueba

El método de prueba a usarse en el objetivo específico “a” es una matriz de análisis de riesgos de seguridad de la información. Este método será aplicado al servicio de correo electrónico teniendo en cuenta las amenazas que impactan su seguridad y los activos de información que serían afectados al producirse una incidencia de seguridad.

5.1.1.5. Definición del Caso de Prueba

Tabla 20

Formato de la definición del Caso de Prueba del O.E. A

Matriz de análisis y evaluación de riesgos de seguridad de la información	Código:	CP-A01
	¿Prueba de despliegue?	No
Descripción:		
<p>Este caso de prueba se realiza un análisis y evaluación de riesgos para determinan los principales riesgos podrían afectar a la seguridad de la información que afecte a los activos de información y los costos por los incidentes de seguridad que podrían suscitarse en la organización. Asimismo, los resultados de las pruebas obtenidas mediante el uso de este método se medirán por el porcentaje de exposición al riesgo y los costos por incidente de seguridad, lo cual brindará un panorama de la cantidad de riesgos a los que se está expuesto sin dar una solución al problema y su impacto económico en la compañía.</p>		
Prerrequisitos:		
<ol style="list-style-type: none">1. Realizar un inventario de activos de información que reúna los principales activos que son afectados en un servicio de correo electrónico basado en Office 365.2. Definir la valoración de los activos de información que serían impactados en caso de ataques al servicio de correo electrónico basado en Office 365.3. Definir el índice máximo de pérdidas económicas permitidas por Toyota del Perú con respecto a las ventas anuales.		
Pasos:		
<ol style="list-style-type: none">1. Se establece la probabilidad de que ocurra una amenaza a la seguridad de la información del servicio de correo electrónico en Toyota del Perú.		

-
2. Se establece el impacto del daño que podría causar el ataque de una de estas amenazas a uno de los elementos de la información.
 3. Se calcula el porcentaje a la exposición de riesgos altos y medios más allá del límite aceptable de la organización.
 4. Se calcula el costo por pérdida debido a un incidente de seguridad teniendo como referencia las ventas anuales de Toyota del Perú y un valor referencial promedio de lo que cuesta cada incidente en la compañía.
-

Resultado esperado:

1. El resultado esperado de esta prueba es validar que el porcentaje de riesgos altos y medios no supere más allá del límite aceptable por la organización.
 2. El otro resultado esperado es que la suma total de costos por incidentes de seguridad no supere el índice del porcentaje de ventas permitido por Toyota del Perú.
-

Nota. Adaptado de “Planes de pruebas funcionales”, de Junta de Andalucía, 02/12/2017, recuperado de <http://www.juntadeandalucia.es/servicios/madeja/node/1249>.

5.1.1.6. Ejecución del caso de prueba

Luego de haber definido el caso de prueba, se procede a su ejecución. En este caso se trata de un solo caso de prueba para el **O.E. “a”**, el cual se procede a detallar a continuación.

Caso de Prueba 1 (CP-A01)

Para realizar el caso de prueba 01, primero se desarrollan los prerequisites necesarios para realizar el análisis y evaluación de riesgos. Para ello, primero se realiza el inventario de activos, el cual enumera los activos de información impactados ante un posible ataque.

Tabla 21*Inventario de Activos*

Código	Nombre	Descripción	Responsable	Tipo	Ubicación	Nivel de Valoración
ISC_00 1	BD local de correo electrónico.	Es la base de datos almacenada localmente en el equipo de cómputo donde se encuentra el cliente de correo electrónico del usuario.	Usuario de correo electrónico	Datos	PC de usuario	Medio
ISC_00 2	Buzón de correo del Servicio de correo electrónico de Office 365	BD en donde se almacena la información del buzón de correos electrónicos de los usuarios en la nube.	Dpto. de TI	Servicio	Servicio externo en la nube	Alto
ISC_00 3	Flujo de información en los mensajes de correo electrónico por internet.	Es la información que es transmitida en los mensajes de correo electrónico a través de internet.	Dpto. de TI	Datos	Internet	Alto
ISC_00 4	PC del usuario de correo electrónico.	Equipo de procesamiento de datos personal que es asignado al usuario para sus labores, en la cual una de ellas es el envío de mensajes	Usuario de correo electrónico	PC	Área física de pertenencia del usuario	Bajo

			de correo electrónico.					
ISC_00	Información	Es toda información	Usuario de Datos	PC	de Medio			
5	personal del usuario.	personal o laboral que almacena el usuario en su PC personal, siendo esta confidencial.	correo electrónico	usuario				
ISC_00	Usuario de correo electrónico (Gerentes y jefes de área).	Es el usuario que hace uso de la información y genera nueva información. Asimismo, posee información confidencial de la organización.	Usuario de correo electrónico	Person al	Área física de pertenencia del usuario	Medio		
6								

Nota. Adaptado de “Taller de implementación de la norma ISO 27001”, por ONGEI, 02/02/2018, adaptado de <https://www.slideshare.net/zerobar/si-semana11-iso27001v011>

Como se observa en la matriz de activos de información, existe un nivel de valoración que posee cada activo, el cual es un valor determinante para el análisis y evaluación de riesgos. Para ello, se elabora previamente una matriz de valoración de activos, en la cual se determina cual es el valor económico que tendrá de acuerdo al impacto que tiene el activo con respecto al problema planteado. El valor del “% de valor de incidente de seguridad estándar” será determinado de acuerdo al valor económico, según las estadísticas del mercado latinoamericano, que tiene un incidente de seguridad.

Tabla 22*Valoración de los Activos de Información*

Nivel de Valoración	Impacto del problema (Tecnológico, Económico y Legal)	Descripción	% del costo de un incidente de seguridad
Bajo	El activo aplica 1 impacto	El riesgo del activo puede impactar económicamente, tecnológicamente o legalmente.	30%
Medio	El activo aplica 2 impactos	El riesgo del activo puede impactar en dos ámbitos al mismo tiempo. Entre económico-legal, económico - tecnológico o tecnológico-legal.	70%
Alto	El activo aplica 3 impactos	El riesgo del activo puede impactar a los 3 ámbitos de la problemática al mismo tiempo.	100%

Nota. Se definió una escala de 3 niveles de valoración de acuerdo con los 3 tipos de impacto que pueden causar los problemas definidos, elaboración propia.

Luego de definir los prerequisites en las *tablas 21 y 22*, se procede a realizar el análisis y evaluación de los riesgos que son involucrados por cada activo de información. Para ello se describen las amenazas y vulnerabilidades que pueden afectar a los activos. Asimismo, se define el impacto que causan las amenazas ante la ausencia de un mecanismo de cifrado con una PKI, según los 4 principios de seguridad de la información (Confidencialidad, Integridad, Autenticación y No Repudio), que afectan a los activos de información. Por otro lado, se define la probabilidad de ocurrencia de las amenazas, con la cual calculamos el riesgo (IxP) que afecta al activo de la información. Finalmente, se calcula la clasificación final del riesgo, teniendo en cuenta el valor del activo y el nivel del riesgo del activo previamente calculado.

Tabla 23

Matriz de análisis y evaluación de riesgos

Activos	Amenazas	Vulnerabilidades	Impacto				Probabilidad	Riesgo IxP	Valor del Activo	Clasificación
			Confidencialidad	Integridad	Autenticación	No Repudio				
							Alto Medio Bajo	Alto Medio Bajo	Alto Medio Bajo	Alto Medio Bajo
BD local del cliente de correo electrónico (PST).	- Acceso no autorizado - Robo de información	- Un solo método de autenticación de acceso a la BD de correo local.	M	M	B	B	B	Bajo	Medio	Bajo
Buzón de correo electrónico del servicio de Office 365	- Malware, Phishing, Ransomware, etc. - Acceso no autorizado	- Filtro de Spam deficiente. - Robo de credenciales de acceso al servicio.	B	M	M	B	M	Medio	Alto	Medio
Flujo de información en los mensajes de correo electrónico por internet.	- Falta de encriptado. - Ataques Man-in-the-middle. - Spoofing.	- Ausencia de cifrado en los mensajes de correo electrónico.	A	A	B	B	M	Medio	Alto	Medio
PC del usuario de correo electrónico.	- Pérdida de información. - Robo de la PC en físico.	- PC Portable.	A	M	B	B	B	Bajo	Bajo	Bajo
Información personal del usuario.	- Malware, Phishing, Ransomware, etc. - Alteración de información. - Spoofing.	- Seguridad anti-malware deficiente. - Canal de comunicación no cifrado. - Usuarios no identificados digitalmente.	A	A	M	B	M	Medio	Medio	Medio
Usuario de correo electrónico (Gerentes y jefes de área).	- Manejo inadecuado de contraseñas. - Ingeniería Social	- Personal no concientizado en buenas prácticas de seguridad de la información.	B	B	A	M	M	Medio	Medio	Medio

Nota. Adaptado de “Taller de implementación de la norma ISO 27001”, por ONGEI, 02/02/2018, adaptado de <https://www.slideshare.net/zerobar/si-semana11-iso27001v011>

La matriz de análisis y evaluación de riesgos determina, a base de los activos de información, que amenazas son los más probables de ocurrir. Estas amenazas han sido tomadas como referencia de los estudios de INTECO-CERT³, Microsoft Office⁴ y *Last Line*⁵, en cuyos reportes se identifican las amenazas más importantes que se presentan en un servicio de correo electrónico. Asimismo, en consecuencia, se han determinado cuales son las vulnerabilidades que pueden ser explotadas por estas amenazas.

5.1.2. Resultados del plan de pruebas O.E. “a”

Para medir los resultados del O.E. “a” se usan dos métricas. La primera de ellas es el porcentaje de riesgos altos y medios más allá del límite aceptable definido por la organización y el segundo es la suma de costos, en dólares, perdidos por la posible ocurrencia de los incidentes de seguridad. Ambas métricas están basadas en las unidades de medición definidas en el anexo B.5 (*Risk Exposure*) y B.8 (*Security Incident Cost*) del estándar ISO/IEC 27004:2016.

5.1.2.1. Medida de exposición al riesgo

Para obtener los resultados de esta medida primero se debe definir el límite aceptable de riesgos altos y medios que puede asumir una organización como Toyota. Para ello, se tomará como referencia la publicación “*Determining Your Organization’s Information Risk Assessment and Management*” realizada por la ENISA⁶ (Agencia

³ Cfr. Ver bibliografía INTECO-CERT, Pág. 12-15

⁴ Cfr. Ver bibliografía OFFICE.COM

⁵ Cfr. Ver bibliografía LASTLINE.COM

⁶ Cfr. Ver bibliografía ENISA

de la Unión Europea para la seguridad de red y de la información), en la cual se detallan 14 modelos de segmentos empresariales en donde se diferencian los requerimientos de seguridad en la evaluación de riesgos de cada organización de acuerdo a la exposición a las amenazas y vulnerabilidades, así como, el impacto a las amenazas y vulnerabilidades. De acuerdo a los segmentos descritos en esta publicación, se puede estimar que el servicio de correo electrónico de Toyota del Perú está acorde con el segmento 8 (Alguna exposición al riesgo e impacto significativo al riesgo), de acuerdo a las características de la organización expuesta en este segmento. Según el Proceso 13 de Aceptación al Riesgo, que tiene este tipo de organizaciones, es de 2 de una escala del 0 al 3.

0 = 76% a 100% de riesgos aceptados

1 = 51% a 75% de riesgos aceptados

2 = 26% a 50% de riesgos aceptados

3 = 0% a 25% de riesgos aceptados

Es decir, según la escala presentada, se podría decir que una organización del segmento 8 como Toyota puede aceptar o tolerar del 26% al 50% de los riesgos identificados.

5.1.2.2. Medida del costo por incidente de seguridad

Según la matriz de análisis y evaluación de riesgos, se puede observar que cada activo de información posee un valor económico ante el impacto de una amenaza de seguridad. Para calcular el costo por el índice de seguridad, se debe entonces tomar

como referencia dicho valor y sumar los porcentajes de valor por índice de seguridad estándar. Para ello, se muestra el siguiente cuadro:

Tabla 24

Matriz de valoración de los activos de información

Activo de Información	Riesgo del activo	% del costo de un incidente de seguridad
BD local del cliente de correo electrónico (PST).	Bajo	30%
Buzón de correo electrónico del servicio de Office 365	Medio	70%
Flujo de información en los mensajes de correo electrónico por internet.	Medio	70%
PC del usuario de correo electrónico.	Bajo	30%
Información personal del usuario.	Medio	70%
Usuario de correo electrónico (Gerentes y jefes de área).	Medio	70%
Total:		340%

Nota. Análisis de la suma de porcentajes de costos por incidentes de seguridad por cada activo de información identificado como en riesgo, elaboración propia.

Como se observa en la matriz de valoración de los activos de información cada activo tiene un valor monetario, en este caso, se identificará con respecto al índice o valor monetario de un incidente de seguridad, el cual en este caso está de acuerdo con el impacto que causaría el incidente en la organización (Tabla de Valoración de activos de información). Entonces, los resultados obtenidos, que serán necesarios para

validar el objetivo con la métrica definida, indican que la suma de los costos por los incidentes de seguridad que podrían suscitarse en los activos de información que tienen que ver con el servicio de correo electrónico es del 340% del valor del costo que supone un incidente de seguridad de la información.

5.1.3. Validación del plan de pruebas O.E. “a”

5.1.3.1. Medida de exposición al riesgo

Para la medida de exposición al riesgo se evaluaron las métricas propuestas y se validó con respecto al porcentaje del límite de riesgos altos y medios permitidos que previamente se definió en un rango de 26% a 50%. Entonces, según los resultados de la matriz de evaluación de riesgos, se tiene lo siguiente:

$$B = \# \text{ Activos de Información} = 6$$

$$A = \# \text{ Activos con riesgos medios y altos} = 4$$

$$C = \% \text{ de riesgos altos y medios} = (A / B) * 100 = (4 / 6) * 100 = 66.67\%$$

Finalmente, se valida que el porcentaje de riesgos altos y medios que se tienen identificados en el servicio de correo electrónico de una organización como Toyota es de aproximadamente 67%. Por lo tanto, este porcentaje no está dentro del rango de riesgos aceptables del 26% al 50%.

Es decir, se identifica que la situación en la que podría estar Toyota en cuanto a la seguridad de la información de su servicio de correo electrónico basado en Office 365 sobrepasa el límite permitido por la organización, no cumpliendo así con el

objetivo de la medida de la exposición al riesgo del objetivo específico “a”. Por lo tanto, se valida la necesidad de una solución que ayude a reducir el riesgo para cumplir con el objetivo de la métrica.

5.1.3.2. Medida del costo por incidente de seguridad

Para validar la medida del costo por incidente de seguridad se toman los valores obtenidos en el resultado de la suma por de los incidentes de seguridad de acuerdo a su probabilidad de ocurrencia.

Asimismo, es necesario saber el porcentaje de un presupuesto estándar de seguridad de la información en una empresa de Latinoamérica, el cual se define de acuerdo con un estudio de ISACA.ORG⁷ donde se indica que el presupuesto de seguridad de la información es del 4% del presupuesto de TI.

Entonces:

A = Suma del % de costos por un incidente de seguridad probable = 340%

B = % Presupuesto de seguridad de la información = 4%

C = % del presupuesto de seguridad que asume un incidente de seguridad = 32%

*D = # de incidentes de seguridad que representan el presupuesto de seguridad =
(100 * 1) / 32 = 3.125*

*E = # de incidente de seguridad que equivale la suma de costos por incidentes de seguridad probables = (340 * 1) / 100 = 3.4*

⁷ Cfr. ISACA.ORG 2016: Diapositiva 34

Por lo tanto, en primer lugar, se valida que la suma del porcentaje de costos por incidentes de seguridad probables para el servicio de correo electrónico equivale a la ocurrencia de 3.4 incidentes de seguridad en los 6 activos de información identificados. En segundo lugar, se puede determinar que el presupuesto de seguridad de una organización en Latinoamérica puede alcanzar a cubrir la ocurrencia de 3.125 incidentes de seguridad. Por lo tanto, si los 3.125 incidentes de seguridad de posible ocurrencia representan al 4% del presupuesto de seguridad en TI, los 3.4 incidentes de seguridad representan al 4.35% del presupuesto de TI.

Se concluye entonces, que la medida de los costos ocasionados por los incidentes de seguridad sobrepasa en la actualidad al 4% del presupuesto de TI para la seguridad de la información. Por ello, se valida la necesidad de una solución para reducir los costos por los incidentes de seguridad para cumplir con la métrica del objetivo “a”.

5.1.4. Ejecución del plan de pruebas O.E. “b”

5.1.4.1. Información general

Organización	Toyota del Perú
Proyecto	Propuesta de una PKI para el uso de cifrado y firma digital en los mensajes de correo electrónico de un servicio basado en Office 365.
Objetivo Especifico	Elaborar las especificaciones técnicas requeridas para una Infraestructura de Clave Pública (PKI) basada en la nube, siguiendo los estándares internacionales para el cumplimiento de las buenas

prácticas de la industria, que permitan el uso de cifrado y firmas digitales en los mensajes de correo electrónico de un servicio basado en Office 365.

Fecha de preparación	04-12-2017
Campo de Acción en la Organización	Directores, Gerentes y Jefes de Área.
Líder de proyecto	Jefe de TI
Líder de las pruebas	Analista de Seguridad de TI

5.1.4.2. Alcance de la prueba

Las especificaciones definidas en el capítulo cuatro del proyecto son las que serán evaluadas en esta prueba. Cada una de las 6 especificaciones, que a su vez poseen características específicas, serán tomadas en cuenta como criterio de evaluación para el *checklist* a realizarse en contraste a los controles del marco de auditoria del estándar *Webtrust for CAs* basado en el ISO 21188:2006.

5.1.4.3. Recursos necesarios

Los recursos necesarios para las pruebas son los siguientes:

1. Listado de las especificaciones técnicas del producto seleccionado como la PKI basada en la nube.
2. Marco de referencia de auditoria *Webtrust for CAs* (ISO 21188:2006).
3. Formato de Lista de Comprobación.

5.1.4.4. Método de prueba

El método de prueba o ensayo a aplicar para el plan de pruebas del O.E. “b” es la **lista de comprobación**. Este método permitirá validar que las especificaciones elaboradas en el proyecto cumplan con los controles definidos en el marco de auditoria del estándar propuesto como referencia. De esa manera, se podrá medir el grado de cumplimiento de las especificaciones sobre los controles que aplican a una PKI basada en la nube para el uso de cifrado y firma digital en el servicio de correo electrónico de Office 365.

5.1.4.5. Definición del Caso de Prueba

Tabla 25

Formato de la definición del Caso de Prueba 1

Lista de comprobación de especificaciones del proyecto	Código:	CP-B01
	¿Prueba de despliegue?	No
Descripción:		
Este caso de prueba se realiza para analizar el cumplimiento de las especificaciones elaboradas para la PKI con respecto al marco de auditoria <i>WebTrust for CAs</i> , el cual está basado en el estándar ISO 21188:2006.		
Prerrequisitos:		
<ol style="list-style-type: none">1. Elaboración de especificaciones del proyecto.2. Formato de Lista de Comprobación con los criterios establecidos en el marco de auditoria <i>WebTrust for CAs</i>.		
Pasos:		
<ol style="list-style-type: none">1. Se evalúan las especificaciones planteadas en el proyecto con respecto al marco de referencia propuesto bajo un formato de Lista de comprobación.		

Resultado esperado:

El resultado esperado de esta prueba es validar que el porcentaje de cumplimiento de las especificaciones con respecto al estándar sea del 85% o más.

Nota. Adaptado de “Planes de pruebas funcionales”, de Junta de Andalucía, 02/12/2017, recuperado de <http://www.juntadeandalucia.es/servicios/madeja/node/1249>

5.1.4.6. Ejecución del caso de prueba

Luego de haber definido el caso de prueba, se procede a su ejecución. En este caso se trata de un solo caso de prueba para el **O.E. “b”**, el cual se procede a detallar a continuación.

Caso de Prueba 1 (CP-B01)

Tabla 26

Lista de comprobación de auditoría a las especificaciones de la PKI propuesta

CONTROLES DE WEBTRUST FOR CA (BASADOS EN EL ISO 21188:2006) EN COMPARACION A LAS ESPECIFICACIONES DEL PROYECTO

Controles inspeccionados: 7 GRUPOS DE CONTROLES CON Fecha: 05/01/2018
CRITERIOS APLICABLES A UNA PKI PARA EMITIR
CERTIFICADOS DIGITALES S/MIME

Especificaciones: **1** **2** **3** **4** **5** **6** **Inspector: Daniel Ramos**

CONTROL 1.0 y 2.0: Prácticas Comerciales de la CA	Especificaciones	Calificación
--	-------------------------	---------------------

La CA divulga sus prácticas comerciales que incluyen, pero no se limitan a, los temas enumerados en RFC 3647 en su Declaración de Prácticas de Certificación (CPS).		☐ SI ☒ NO
---	--	--

La CA divulga sus prácticas comerciales que incluyen, pero no se limitan a, los temas enumerados en RFC 3647 en su Política de Certificados (CP).	3	☒ SI ☐ NO
---	---	--

CONTROL 3.0: Controles Ambientales de la PKI	Especificaciones	Calificación
<p>La CA mantiene controles para proporcionar una seguridad razonable de que:</p> <ul style="list-style-type: none"> • La seguridad está planificada, administrada y respaldada dentro de la organización. • Los riesgos de seguridad son identificados y gestionados. • La seguridad de la información de un suscriptor y de las partes que confían en la PKI se mantienen cuando la responsabilidad de las subsunciones de la CA ha sido subcontratada a otra organización o entidad. • Eventos importantes de CA ambiental, gestión de claves y gestión de certificados son con precisión y apropiadamente registrado. • Se mantiene la confidencialidad e integridad de los registros de auditoría actuales y archivados. • Los registros de auditoría son revisados periódicamente por personal autorizado. • Eventos importantes de la CA, gestión de claves y gestión de certificados son apropiadamente registrados. • Se mantiene la confidencialidad e integridad de los registros de auditoría actuales y archivados. • Los registros de auditoría son revisados periódicamente por personal autorizado. 		☐ SI ☒ NO
CONTROL 4.0: Controles de gestión del ciclo de vida de la CA	Especificaciones	Calificación
La CA mantiene controles para proporcionar una seguridad razonable de que los pares de claves se generan en de acuerdo con los procedimientos definidos en estándares internacionales.	4	☒ SI ☐ NO
La CA mantiene controles para proporcionar una seguridad razonable de que las claves privadas de la CA permanecen confidenciales y mantienen su integridad. Las claves privadas de la CA están respaldadas,	4	☒ SI ☐ NO

almacenadas y resguardadas por personal autorizado de confianza, usando control de múltiples personas en un entorno físicamente seguro.

La CA mantiene un control para una seguridad razonable de la integridad y la autenticidad de las claves públicas de la CA y sus parámetros asociados son mantenidos en su distribución inicial y posterior.	4	☒ SI ☐ NO
---	---	--

La CA mantiene controles para proporcionar una seguridad razonable de que:	4	☒ SI ☐ NO
--	---	--

- Dispositivos utilizados para el almacenamiento y recuperación de claves privadas, y las interfaces con estos dispositivos son probados antes del uso para asegurar su integridad.
 - El acceso al hardware criptográfico de la CA (módulos HSM) está limitado a personal autorizado de confianza, usando controles múltiples.
 - El hardware criptográfico CA funciona correctamente.
-

CONTROL 5.0: Controles del ciclo de vida de la clave del suscriptor	Especificaciones	Calificación
--	-------------------------	---------------------

La CA mantiene controles para proporcionar una seguridad razonable de que:	4, 6	☒ SI ☐ NO
--	------	--

- Las claves del suscriptor generadas por la CA (o RA) se generan dentro de un entorno seguro mediante un dispositivo criptográfico con bajo riesgo de ataques.
 - Las claves de suscriptor generadas por la CA (o RA) se distribuyen de forma segura al suscriptor. De forma segura es entregando este par de claves junto con el certificado al suscriptor. La CA puede hacer esto para ciertos tipos de certificados como S/MIME.
-

La CA mantiene controles para proporcionar una seguridad razonable de que:	1, 4	☒ SI ☐ NO
--	------	--

- Las claves privadas del suscriptor almacenadas por la CA son confidenciales y mantienen su integridad.
-

- Las claves privadas del suscriptor son archivadas y custodiadas por la CA son confidenciales.
- Las claves privadas del suscriptor son almacenadas por la CA y se destruyen por completo al final de su ciclo de vida.

La CA mantiene controles para proporcionar una 4 ☒ SI ☐ NO
seguridad razonable de que:

- Los requisitos para la protección de las claves del suscriptor se comunican a los suscriptores.
- Cualquier herramienta de administración de claves de suscriptor proporcionada por la CA respalda los requisitos de buenas prácticas de la CA.

CONTROL 6.0: Gestión del ciclo de vida del certificado **Especificaciones** **Calificación**

La CA mantiene controles para proporcionar una 3, 4, 6 ☒ SI ☐ NO
seguridad razonable de que:

- Las solicitudes de certificados de los suscriptores son precisas, autorizadas y completas.

La CA mantiene controles para proporcionar una 3 ☒ SI ☐ NO
seguridad razonable de que las solicitudes de nuevas peticiones de certificado digital, incluidas las solicitudes posteriores a la revocación o caducidad del certificado, son precisas, autorizadas y completas.

La CA mantiene controles para proporcionar una 2, 3 ☒ SI ☐ NO
seguridad razonable de que los certificados se generan y emiten de acuerdo con los estándares internacionales.

La CA mantiene controles para proporcionar una 3,4 ☒ SI ☐ NO
seguridad razonable de que, una vez emitidos, los certificados completos y precisos estén disponibles para los suscriptores y las entidades de confianza de acuerdo con los estándares internacionales.

La CA mantiene controles para proporcionar una 3 ☒ SI ☐ NO
seguridad razonable de que los certificados son revocados, basado en solicitudes de revocación de

certificados autorizadas y validadas dentro del marco de tiempo en de acuerdo con las prácticas sugeridas por el estándar.

La CA mantiene controles para proporcionar la seguridad de que la información del estado de un certificado digital se obtenga en tiempo real, completa y precisa (incluidas las listas de revocación de certificados y otros mecanismos de estado de certificado), y se pone a disposición de las entidades pertinentes (suscriptores).	4	☒ SI ☐ NO
---	---	--

CONTROL 7.0: Controles del ciclo de vida de la CA subordinada	Especificaciones	Calificación
--	-------------------------	---------------------

La CA mantiene controles para proporcionar una seguridad razonable de que:	E4	☒ SI ☐ NO
<ul style="list-style-type: none"> • las solicitudes de las CA subordinadas son precisas, autenticadas y aprobadas; • Las solicitudes de sustitución de las CA subordinadas y certificación cruzada son exactas, autorizadas, completas. • certificados de CA y certificados secundarios nuevos, renovados y revisados. • En el momento de la emisión, están disponibles Certificados de CA subordinados y certificados cruzados a las entidades relevantes (Suscriptores y entidades de confianza). • La CA subordinada y certificados cruzados son revocados en base a solicitudes de revocación de certificados autorizadas y validadas. • Información sobre el estado del certificado es oportuna, completa y precisa (mediante CRL y OCSP). 		

Nota. Adaptado de “Webtrust for Certification Authorities”, de CPA Canada, 12/12/2017, recuperado de <http://www.webtrust.org/principles-and-criteria/docs/item85228.pdf>.

5.1.5. Resultados del plan de pruebas O.E. “b”

5.1.5.1. Medida del grado de cumplimiento del marco de auditoria

Para medir los resultados del O.E. “b” se toma como referencia la medida del grado de cumplimiento del marco de auditoria. La métrica usada en este caso es el porcentaje de cumplimiento, el cual medirá las especificaciones que se definieron en el capítulo cuatro del presente proyecto estén presentes en una proporción mayor o igual al 90% de los controles aplicables del estándar *WebTrust for CAs* (ISO 21188:2006).

Tabla 27

Resumen de resultados de auditoria a las especificaciones de la PKI propuesta

Grupo de Controles de <i>Webtrust for CAs</i>	Criterios	Especificaciones	Criterios
	Aplicables	Aplicadas	Cumplidos
1.0 y 2.0: Prácticas Comerciales de la CA	2	E3	1
3.0: Controles Ambientales de la PKI	1		0
4.0: Controles de gestión del ciclo de vida de la CA	4	E4	4
5.0: Controles del ciclo de vida de la clave del suscriptor	3	E1, E4, E6	3
6.0: Gestión del ciclo de vida del certificado	6	E2, E3, E4, E6	6
7.0: Controles del ciclo de vida de la CA subordinada	1	E4	1
Total	17		15

Nota. Resumen de los resultados evaluados en la tabla 26, en donde se obtienen los criterios aplicables y los cumplidos en comparativa, elaboración propia.

5.1.6. Validación del plan de pruebas O.E. “b”

5.1.6.1. Medida del grado de cumplimiento del marco de auditoria

Para validar que el objetivo específico “b” se haya cumplido se calcula el porcentaje de cumplimiento del marco de auditoria *Webtrust for CAs* (ISO 21188:2006), en base a los resultados obtenidos en el punto anterior, para determinar el grado de las especificaciones.

Por lo tanto, se determina que de los 17 criterios seleccionados que conforman los 7 controles del marco de auditoria *Webtrust for CAs* las especificaciones y sus características técnicas cumplen con 15 de ellas. Entonces se tiene lo siguiente:

$$A = \# \text{ Criterios aplicables} = 17$$

$$B = \# \text{ Criterios aplicados} = 15$$

$$C = \% \text{ Grado de cumplimiento} = (B / A) * 100 = 88 \% (\text{redondeado})$$

Finalmente, se valida y concluye que el grado de cumplimiento de las especificaciones y sus características técnicas cumplen con los controles y criterios seleccionados del marco de auditoria *Webtrust for CAs* (ISO 21188:2006) para evaluar una PKI (CA) que emite certificados digitales S/MIME para el cifrado y firma digital de los mensajes de un servicio de correo electrónico.

5.1.7. Ejecución del plan de pruebas O.E. “c”

5.1.7.1. Información general

Organización	Toyota del Perú
Proyecto	Propuesta de una PKI para el uso de cifrado y firma digital en los mensajes de correo electrónico de un servicio basado en Office 365.
Objetivo Especifico	Elaborar un modelo de arquitectura, que integre una Infraestructura de Clave Pública (PKI) basada en la nube sobre un servicio de correo electrónico basado en Office 365, el cual aplique cifrado y firma digital en los mensajes de correo electrónico con el fin de reducir las vulnerabilidades que puedan poner en riesgo la seguridad de los activos de información en la organización objetivo.
Fecha de preparación	04-12-2017
Campo de Acción en la Organización	Directores, Gerentes y Jefes de Área.
Patrocinador principal	Gerente de TI
Líder de proyecto	Jefe de TI
Líder de pruebas de la solución	Analista de seguridad de TI

5.1.7.2. Alcance de la prueba

El servicio de *Symantec Managed PKI* es una solución completa que emite certificados digitales para diversas tecnologías que usan criptografía asimétrica para asegurar las aplicaciones de negocio. Entre los tipos de certificados que emite están los usados por el protocolo SSL para los servicios web, IPSec para el cifrado en las conexiones VPN, los utilizados para firmar digitalmente documentos PDF, S/MIME para los servicios de correo electrónico seguro y entre otras aplicaciones que sean compatibles con el estándar de certificados X.509. Sin embargo, el alcance de las pruebas solo constará en el uso de la

emisión de certificados digitales S/MIME con todas las funcionalidades y configuraciones que ofrece la solución.

En cuanto al servicio de correo electrónico basado en la nube, se usa el servicio de Exchange Online con unas cuentas de correo configuradas de manera estándar. El alcance serán dos cuentas de correo con las cuales se harán pruebas de envío y recepción de mensajes para los casos de prueba.

5.1.7.3. Recursos necesarios

Los recursos requeridos que serán usados dentro del ambiente de pruebas (preproducción) son los siguientes:

Hardware:

- 1 computadora personal desde donde se administra la solución PKI.
- 2 computadoras personales para los clientes de correo.

Software:

- 2 licencias de prueba de Office 365 para los clientes de correo.

Servicios:

- 1 versión de prueba de *Symantec Managed PKI Service Test Drive* con acceso a la emisión de 1000 certificados digitales validos por 180 días.

5.1.7.4. Método de prueba

El método de prueba usado es la **Simulación** a través de las Pruebas Funcionales del sistema, ya que se trata de una PKI ofrecida como servicio por un tercero. Este servicio es adquirido como un IaaS (Infraestructura como Servicio), la cual ofrece una interfaz de administración de la PKI a la cual se le realizarán las pruebas funcionales cuando este sea integrado al servicio de correo electrónico basado en la nube.

Lo primero es definir el caso de prueba y los ensayos que se realizarán. Luego, se ejecutan los casos de pruebas que se han definido. En los siguientes procesos del plan de pruebas se detallará el desarrollo de cada uno de estos casos de pruebas.

5.1.7.5. Definición de los Casos de Pruebas

Tabla 28

Formato de la definición del Caso de Prueba 1

Envío de mensaje de correo electrónico sin cifrado y firma digital	Código:	CP-C01
	¿Prueba de despliegue?	No
Descripción:		
Este caso de prueba se realiza para analizar el nivel de seguridad que posee un mensaje de correo electrónico enviado por un usuario de Office 365 en Toyota del Perú. Esta prueba de envío se realiza previo a la integración del certificado digital S/MIME con el cliente de correo electrónico. Es decir, no cuenta con la solución de cifrado y firma digital propuesta. El objetivo principal de esta prueba es tener una referencia para comparar con el segundo caso de prueba.		

Prerrequisitos:

1. 2 clientes de correo electrónico Outlook configurados con cuentas de Office 365.
2. 2 computadoras para los clientes de correo Outlook conectadas a internet

Pasos:

1. Elaboración del mensaje de correo electrónico de prueba, con un texto de asunto y cuerpo de prueba.
2. El receptor recibe el mensaje de correo electrónico sin cifrar y sin firma digital.

Resultado esperado:

El resultado esperado de esta prueba es validar y evidenciar, en la información de la *metadata* del mensaje de correo electrónico enviado, la ausencia de cifrado y firma digital.

Nota. Adaptado de “Planes de pruebas funcionales”, de Junta de Andalucía, 02/12/2017, recuperado de <http://www.juntadeandalucia.es/servicios/madeja/node/1249>

Tabla 29

Formato de la definición del Caso de Prueba 2

Envío de mensaje de correo electrónico cifrado y	Código:	CP-C02
firmado digitalmente con S/MIME	¿Prueba de despliegue?	Si

Descripción:

Esta prueba tiene como objetivo contrastar el nivel de seguridad con la primera prueba. Aquí se muestra el envío de un mensaje de correo electrónico luego de realizar la integración de los certificados digitales S/MIME con el cliente de correo electrónico Outlook en el equipo de cada uno de los usuarios de prueba. Asimismo, se procederá a realizar la prueba de envío de correo electrónico cifrado y firmado mediante el uso de los certificados instalados.

Prerrequisitos:

-
1. 2 clientes de correo electrónico Outlook configurados con cuentas de Office 365.
 2. 2 computadoras para los clientes de correo Outlook conectadas a internet.
 3. Emisión de 2 certificados digitales de prueba S/MIME de Symantec MPKI.
-

Pasos:

1. Redactar el mensaje de correo electrónico con un texto de asunto y contenido de prueba.
 2. Aplicar la opción de cifrado y firma digital al mensaje seleccionando la opción en el cliente de correo.
 3. El usuario que recibe el mensaje debe validar su identidad usando su clave privada para descifrar el mensaje que ha sido enviado usando su clave pública.
 4. Al abrir el mensaje se observa que el mensaje también se encuentra firmado digitalmente por el usuario remitente.
-

Resultado esperado:

El resultado que se espera obtener, en la *metadata* del mensaje de correo electrónico enviado, es la validación de que el contenido del mensaje ha sido cifrado con los algoritmos definidos en las especificaciones y que la firma digital confirme la identidad del remitente.

Nota. Adaptado de “Planes de pruebas funcionales”, de Junta de Andalucía, 02/12/2017, recuperado de <http://www.juntadeandalucia.es/servicios/madeja/node/1249>

5.1.7.6. Ejecución de los casos de pruebas

Para la ejecución de los casos de pruebas, se debe realizar un paso previo que consiste en la instalación, en ambiente de pruebas, de la versión *Trial* del producto *Symantec Managed PKI Services* que fue seleccionada en el capítulo cuatro en la evaluación de recursos. Por ello, este proceso se muestra en el anexo “A” del presente documento, el cual detalla paso a paso el proceso de instalación y configuración del servicio de *Symantec Managed PKI*

Services y la instalación de los certificados digitales S/MIME en el cliente de correo electrónico para el cifrado y firma digital de los mensajes.

Luego de tener el ambiente de pruebas listo. Se procede a realizar la prueba que validará el cumplimiento del **O.E. “c”** del proyecto.

Caso de Prueba 1 (CP-C01)

1. En primer lugar, se procede a redactar un correo electrónico con un contenido y asunto de prueba en formato de texto. El remitente de correo es el usuario Josué Alarcón y el destinatario es el usuario Hernán Ramos que dentro del ámbito de pruebas forman parte de la misma organización:

Figura 42. Prueba de envío de correo sin cifrado y firma digital. Adaptado de “Prueba de envío de correo electrónico de un cliente de correo electrónico Office 365 desde Outlook 2013”, elaboración propia.

2. Entonces, en el lado del receptor se observa que el mensaje llega de manera normal, sin ningún mecanismo de firma digital o de cifrado, simplemente con la identificación del nombre de contacto y la firma al pie del mensaje del usuario que remite.

Figura 43. Recepción del correo sin cifrado y ni firma digital. Adaptado de “Prueba de envío de correo electrónico de un cliente de correo electrónico Office 365 desde Outlook 2013”, elaboración propia.

3. En la *figura 43*, podemos observar que los mensajes de correo electrónico que son enviados comúnmente desde el servicio de correo de Office 365 no son firmados ni cifrados por ningún método de criptografía asimétrica. El contenido del mensaje puede ser fácilmente interceptado por los atacantes en su recorrido u obtenido del lado del receptor del mensaje mediante los métodos de autenticación tradicionales. El resultado aquí es la ausencia de cifrado de la información y firma digital en el mensaje. Asimismo, se puede observar en la *metadata* mostrada en la *figura 44*, que el parámetro (**dkim**, según el estándar MIME) que lleva la información de la firma digital posee el atributo de **none** y adicionalmente menciona (**message not signed**). Esto significa que el mensaje no está siendo firmado digitalmente en todo su recorrido.

Figura 44. Detalle de la cabecera del correo enviado, sin cifrado y firma. Adaptado de “Prueba de envío de correo electrónico de un cliente de correo electrónico Office 365 desde Outlook 2013”, elaboración propia.

Caso de Prueba 2 (CP-C02)

1. Primero, se debe redactar el mensaje de prueba a enviar al destinatario, al igual que el caso anterior se usan los usuarios Josué Alarcón y Hernán Ramos como remitente y receptor respectivamente. Sin embargo, cabe señalar que para este caso ya se debe tener instalado el certificado digital del receptor Hernán Ramos para el cifrado del mensaje con su clave pública. Asimismo, en la pestaña de **Opciones** del mensaje en el cliente Outlook, se deben seleccionar las opciones de Cifrado (*Encrypt*) y Firma Digital (*Sign*). Al seleccionar estas opciones se indica al cliente de correo que el mensaje debe ser enviado cifrado con el certificado digital de Hernán Ramos (usando su clave pública) y firmado con el certificado digital de Josué Alarcón (usando su clave privada).

Figura 45. Envío de correo cifrado y firmado desde Outlook 2013. Adaptado de “Prueba de envío de correo electrónico cifrado y firmado desde un cliente de correo electrónico Office 365 con Outlook 2013”, elaboración propia.

2. Al terminar de redactar el correo, al momento de **Enviar** el correo electrónico, se solicitará la clave PIN del equipo para acceder al uso del certificado digital que contiene la clave privada de Josué Alarcón, el cual está administrado por el **Symantec PKI Client**.
3. Una vez enviado el correo cifrado y firmado por Josué Alarcón, este será recibido en el buzón de Hernán Ramos como un mensaje seguro. Cuando el usuario Hernán Ramos quiera abrir el correo electrónico recibido, se le solicitará el PIN de su equipo para hacer uso de su certificado digital que contiene su clave privada con la cual podrá descifrar el mensaje que el remitente Josué Alarcón envió con la clave pública de Hernán Ramos.

Figura 46. Recepción del correo cifrado y con firma digital. Adaptado de “Prueba de envío de correo electrónico cifrado y firmado desde un cliente de correo electrónico Office 365 con Outlook 2013”, elaboración propia.

4. Como se muestra en la figura 46, al abrirse el mensaje, se pueden observar dos iconos que indican que el mensaje recibido ha sido cifrado y firmado digitalmente mediante el protocolo S/MIME.
5. Luego, se observa la información del **Cifrado** en el detalle de la *metadata* del mensaje. Para ello, ir al enlace del **candado azul** y se mostrarán las siguientes propiedades del cifrado de acuerdo con los parámetros del certificado S/MIME.

Figura 47. Ventana de Propiedades de Cifrado en Outlook 2013. Adaptado de “Prueba de envío de correo electrónico cifrado y firmado desde un cliente de correo electrónico Office 365 con Outlook 2013”, elaboración propia.

6. En la información que se ve en la *figura 47*, se puede ver que el mensaje fue cifrado para el usuario de correo electrónico de Hernán Ramos usando los algoritmos RSA de 2048 bits para la criptografía asimétrica con la PKI y el contenido fue cifrado usando el algoritmo AES de 256 bits.
7. Por otro lado, también se pueden observar los parámetros de la **firma digital** aplicada al correo, los cuales también concuerdan con el certificado digital emitido para el usuario. Para ello seguimos el enlace del icono de **insignia roja** para ver la metadata del mensaje.

Figura 48. Ventana de Propiedades de Firma Digital en Outlook 2013. Adaptado de “Prueba de envío de correo electrónico cifrado y firmado desde un cliente de correo electrónico Office 365 con Outlook 2013”, elaboración propia.

8. Finalmente, en la *figura 48* se puede observar que el mensaje fue firmado digitalmente por el usuario de correo electrónico de Josué Alarcón usando el algoritmo RSA de 2048 bits para el intercambio de llaves asimétricas con la PKI y el algoritmo hash SHA256 de 256 bits de longitud en la función de resumen (en la figura se muestra una prueba con un SHA1, lo cual fue un error y no es recomendado).

5.1.8. Resultados del plan de prueba O.E. “c”

Para medir los resultados del O.E. “c” se usa la métrica del porcentaje de activos de información que reducirían sus vulnerabilidades y amenazas que afectan a la integridad, confidencialidad, autenticación y no repudio de la información sensible de los mensajes de correo electrónico. Esta métrica está basada en la unidad de medición definida en el anexo B.29 (*Pentest and vulnerability assessment*) del estándar ISO/IEC 27004:2016.

5.1.8.1. Medida de la evaluación de vulnerabilidades

Para obtener los resultados de esta medida, primero se debe obtener la cantidad de activos de información que se identificaron en el inventario de activos. Luego, teniendo en cuenta la matriz de análisis y evaluación de riesgos realizada para el primer objetivo específico (O.E. a), se puede extraer la cantidad de riesgos medios y altos cuyas vulnerabilidades serían reducidas con la propuesta de PKI.

Tabla 30*Evaluación de riesgos de vulnerabilidades.*

Activos de Información	Clasificación del Riesgo	
	Actualmente	Con propuesta PKI
BD local de correo electrónico.	Bajo	Bajo
Buzón de correo del Servicio de correo electrónico de Office 365	Medio	Medio
Flujo de información en los mensajes de correo electrónico por internet.	Medio	Bajo
PC del usuario de correo electrónico.	Bajo	Bajo
Información personal del usuario.	Medio	Bajo
Usuario de correo electrónico (Gerentes y jefes de área).	Medio	Medio
Cant. De Riesgos medios y altos	4	2
% de riesgos medios y altos	67%	33%

Nota. La solución reduce los riesgos en 2 activos de información que poseen amenazas por falta de cifrado y firma digital, elaboración propia.

5.1.9. Validación del plan de prueba O.E. “c”

5.1.9.1. Medida de la evaluación de vulnerabilidades

Para la evaluación de vulnerabilidades se usaron las métricas propuestas por la medida B.29 definida en el estándar ISO 27004:2016, la cual propone la siguiente escala de porcentajes para establecer si las vulnerabilidades que afectan a la seguridad de la información de los elementos o sistemas de información cumplen con el estándar:

Verde = 100%

Naranja $\geq 75\%$

Rojo $< 75\%$

Según los resultados obtenidos, no existe ningún riesgo alto identificado para los activos de información, lo cual significaría un problema de seguridad crítico según el estándar ISO/IEC 27004. Por lo tanto, el objetivo específico “c” se cumple al no existir riesgos críticos identificados en la matriz de evaluación de vulnerabilidades sobre los 6 activos de información identificados, lo cual significaría un valor de 100% para la métrica del objetivo.

Asimismo, se concluye que la propuesta de solución de cifrado y firma digital con una PKI reduce el riesgo de seguridad en los activos de información que poseen vulnerabilidades relacionadas al cifrado e identificación digital del usuario de correo electrónico. La solución propuesta reduce las vulnerabilidades de 2 de los 4 activos de información que tenían riesgo medio a riesgo bajo. Es decir, se reduce en un 50% la cantidad de riesgos medios de seguridad de información que afectaban al servicio de correo electrónico mediante el cifrado y firma digital de los mensajes que se envían por la organización.

CONCLUSIONES

- Para tener un claro panorama previo de las tecnologías que brindan seguridad de la información a un servicio de correo electrónico basado en la nube, se detallaron estas en el estudio del estado del arte. Además, el caso de éxito de implementación de una PKI en el Perú por RENIEC fijo precedentes importantes para el desarrollo del trabajo.
- Se procedió a elaborar una investigación profunda acerca de las características de una PKI. La investigación describe la importancia de los componentes relacionados con la infraestructura, principios criptográficos de seguridad de la información que intervienen, y las mejores prácticas y normativas que permiten tener una solución regulada y segura. El desarrollo de esta investigación comprende un paso fundamental para el entendimiento del trabajo y la propuesta elaborada.
- Se identificaron los principales problemas que afectaban a la seguridad de la información en la organización objetivo. Asimismo, se planteó una problemática a resolver en el proyecto, teniendo en cuenta el impacto tecnológico, legal y económico que estos ocasionan en la actualidad, se buscó dar la solución a esta problemática al finalizar el trabajo consiguiendo un grado aceptable de satisfacción.
- Para tener una solución más a la medida de la organización objetivo, se procedió a definir requerimientos, los cuales mediante un análisis a fondo pudieron convertirse en requerimientos funcionales que son la base para el establecimiento de las especificaciones que se elaboraron más adelante en el trabajo.

- Las especificaciones del proyecto están orientadas a las necesidades que tienen las organizaciones para implementar una Infraestructura de Clave Pública (PKI) de acuerdo con los estándares internacionales y buenas prácticas de esta tecnología. De esta manera, se han establecido 8 especificaciones, cada una con sus características técnicas, que buscan ser una guía para las organizaciones que requieran de un marco de referencia para sus proyectos o anteproyectos de seguridad de la información para sus aplicaciones mediante la implementación de una PKI basada en la nube.
- Se propone una arquitectura modelo de la integración de una PKI basada en la nube y un servicio de correo electrónico Office 365. Este modelo ofrece la funcionalidad de cifrado y firma digital a los mensajes de correo electrónico que son enviados desde el servicio de Office 365. Dicha integración se realiza mediante el protocolo S/MIME, el cual utiliza los certificados digitales emitidos por la CA para aplicar funciones criptográficas a la información transmitida por el servicio de correo electrónico.
- Asimismo, es importante señalar que para validar la propuesta como económicamente factible, se realizó una evaluación de costos al producto elegido para la propuesta de PKI basada en la nube. Con esta evaluación, se determinaron los costos del capital necesario para implementar la solución propuesta y los costos operativos que implicarían mantener esta tecnología funcionando a lo largo del tiempo. De manera satisfactoria mediante un análisis se concluyó, que los costos de la solución traídos al presente (VAN) en un año significarían un índice de retorno de la inversión (ROI) del 100%, lo cual indica que la solución propuesta de PKI basada en la nube es muy rentable en comparación a una PKI On-Premises.

- La metodología del plan de pruebas utilizada en el proyecto es necesaria para determinar que cada objetivo específico presentado en el proyecto se cumpla. Por lo tanto, se desarrolló cada paso de la metodología por cada objetivo específico, desde la ejecución del plan de pruebas para obtener los resultados deseados y la validación de que el objetivo de las métricas definidas por cada objetivo específico se haya cumplido.

RECOMENDACIONES PARA TRABAJOS FUTUROS

- Si bien es cierto, el trabajo completo está orientado a la seguridad de la información de un servicio de correo electrónico. Se puede lograr desarrollar una propuesta similar a esta para el cifrado y firma digital de documentos electrónicos. De esta manera, muchos más activos de información estarán correctamente protegidos ante cualquier amenaza del exterior que se propaga al transmitir datos en la nube.
- Se podrían fijar más objetivos específicos y medidas que ayuden a validar la importancia de la seguridad de la información en un servicio de correo electrónico basado en la nube, las cuales ayuden a concientizar sobre el grado de riesgos a los que están expuestos sus sistemas y así controlar los riesgos residuales que permanecen en la organización.
- En cuanto a la arquitectura de la propuesta, podría considerarse en un trabajo futuro, la integración del directorio activo de la organización que maneja el servicio de correo electrónico Office 365 a la PKI basada en la nube, para así almacenar los certificados digitales en el directorio activo local de la organización. Sin embargo, esto podría traer sus desventajas en lo que respecta a la seguridad de la información de los certificados digitales que son almacenados en lugares no seguros.
- Finalmente, para la metodología del plan de pruebas, se recomendaría incluir un plan de mejoras por cada objetivo específico planteado, el cual permita tomar medidas correctivas o de cambio para mejorar el rendimiento de los objetivos de la organización y el índice de las métricas que se usan para medir los logros que se van obteniendo con el tiempo.

BIBLIOGRAFÍA

AGENCIA DE DESARROLLO LOCAL Y EMPLEO (ADLE) (2010) Firma electrónica y certificados digitales (consulta: 28 de julio de 2017) (http://www.google.com.pe/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&cad=rja&uact=8&ved=0CB0QFjAB&url=http%3A%2F%2Fwebs.um.es%2Fdanielsm%2Fmiwiki%2Flib%2Fexe%2Ffetch.php%3Fid%3Dinicio%26cache%3Dcache%26media%3Dceeic_-firma_electronica_y_certificados_digitales.pdf&ei=d_XU-rUNYrKsQS01oLABA&usg=AFQjCNGuSThYx_4HTUrvD9D0gmoVUb3UYA&bvm=bv.71778758,d.cWc)

ALBERTO G. Alexander (2017) Business Continuity Planning y la Gestión de Ensayos. Lima: EGP (www.eficienciagerencial.com)

BLOGSPOT.PE (2011) Estado del Arte (Consulta: 07 de octubre de 2017) (<http://formandoinvestigadores-gft.blogspot.pe/2011/01/estado-del-arte.html>)

CARAT (2000) *Guidelines for Constructing Policies Governing the Use of Identity Based Public Key Certificates* (consulta: 27 de Julio de 2017) (http://civics.typepad.com/files/carat_final_011400-1-1.pdf)

CENTRO NACIONAL DE COMPUTO (CNC) (2014) Infraestructura para la criptografía de clave pública (consulta: 27 de julio de 2017) (<http://www.cnc.una.py/cms/cnc/content/pki.pdf>)

CISCO.COM (2011) Cisco RV042 Dual WAN VPN Router (consulta: 23 de setiembre de 2017) (https://www.cisco.com/c/en/us/products/collateral/routers/rv042-dual-wan-vpn-router/data_sheet_c78-501225.html)

CYBERSECUREASIA.COM (2015) *S/MIME Certificate for Email Encryption* (consulta: 25 de setiembre de 2017) (<https://www.cybersecureasia.com/blog/smime-certificate-for-email-encryption>)

DENNING, Elizabeth (1982) *Cryptography and Data Security*. USA: Addison-Wesley Publishing Company

ECURED.CU (2014) PKI (consulta: 09 de setiembre de 2017) (<http://www.ecured.cu/index.php/PKI>)

ENISA (2008) *Determining Your Organization's Information Risk Assessment and Management*. (Consulta: 21 de febrero de 2018) (<https://www.enisa.europa.eu/publications/archive/determining-your-organization2019s-information-risk-assessment-and-management>)

ETAPA.NET.EC (2016) Cortafuegos (informática) (consulta: 09 de setiembre de 2017) (<http://www.etapa.net.ec/Portals/0/Productos%20y%20Servicios/Cortafuegos%20o%20Firewall.pdf>)

IETF RFC 5280 (2008) Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile (consulta: 19 de noviembre de 2017) (<https://tools.ietf.org/html/rfc5280>)

IETF RFC 5750 (2010) Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.2 - Certificate Handling (consulta: 19 de noviembre de 2017) (<https://tools.ietf.org/html/rfc5750>)

IETF RFC 5751 (2010) Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.2 - Message Specification (consulta: 19 de noviembre de 2017) (<https://tools.ietf.org/html/rfc5751>)

INDRA (2005) Formación PKI – Seminario de Infraestructura de Clave Pública (consulta: 13 de julio de 2017) (<https://es.scribd.com/document/127971489/Formacion-PKI>)

INTECO-CERT (2011) Riesgos y Amenazas en Cloud Computing (consulta: 13 de febrero de 2018) (https://www.incibe.es/extfrontinteco/img/File/intecocert/EstudiosInformes/cert_inf_riesgos_y_amenazas_en_cloud_computing.pdf)

ISACA.ORG (2016) Estudio de la seguridad de la información en México 2017 (consulta: 09 de enero de 2018) (<https://www.isaca.org/chapters4/Mexico-City/Documents/Estudio%20de%20la%20Seguridad%20de%20la%20Informaci%C3%B3n%20en%20M%C3%A9xico%202017.pdf>)

ISO/IEC 27004 (2016) Information technology – security techniques – information security management – Monitoring, measurement, analysis and evaluation. Suiza: ISO/IEC

ITU-T X.509 (2012) Information technology – Open systems interconnection – The Directory: Public-key and attribute certificate frameworks. EEUU: TELECOMMUNICATION STANDARDIZATION SECTOR

ITU-T X.500 (2012) Information technology – Open Systems Interconnection – The Directory: Overview of concepts, models and services. EEUU: TELECOMMUNICATION STANDARDIZATION SECTOR

ITU.INT (2006) La seguridad de las comunicaciones y las tecnologías de la información (consulta: 23 de setiembre de 2017) (https://www.itu.int/dms_pub/itu-t/opb/hdb/T-HDB-SEC.03-2006-PDF-S.pdf)

KASPERSKY.COM (2016) Reporte: Midiendo el impacto financiero de la seguridad informática en los negocios. (Consulta: 05 de enero de 2018) (<https://latam.kaspersky.com/blog/reporte-midiendo-el-impacto-financiero-de-la-seguridad-informatica-en-los-negocios/7711/>)

KERNELSOFTWARE.COM (2017) SYMANTEC Price List as of 29 May 2017 (consulta: 30 de noviembre de 2017) (<http://www.kernelsoftware.com/products/catalog/symantec.html>)

LASTLINE.COM (2017) Top 10 Malicious Email Threats (consulta: 15 de febrero de 2018) (<https://www.lastline.com/blog/top-10-malicious-email-threats/>)

LUCENA LOPEZ, Manuel J. (2010) Criptografía y Seguridad en Computadores. (Consulta: 27 de julio de 2017) (<http://sertel.upc.edu/tdatos/Libros/Lucena.pdf>)

MICROSOFT TECHNET (MICROSOFT TECHNET) (2015) Descripción del servicio Exchange Online (consulta: 24 de setiembre de 2017) <https://technet.microsoft.com/es-es/library/exchange-online-service-description.aspx>

MAPS.COM.MX (2017) Soluciones Fortinet (consulta: 23 de setiembre de 2017) (<http://www.maps.com.mx/index.php/fortinet>)

MICROSOFT.COM (2014) *Office 365 Message Encryption (& Decryption) – Steps for Purchase, Configuration, Branding and Use – Everything you need to know* (consulta: 25 de setiembre de 2017) (<https://blogs.technet.microsoft.com/compilations/2014/04/29/office-365-message-encryption-decryption-steps-for-purchase-configuration-branding-and-use-everything-you-need-to-know/#.Wl6azq7ibDf>)

MINJUS.GOB.PE (2000) LEY N° 27269 - Ley de Firmas y Certificados Digitales (<https://www.minjus.gob.pe/wp-content/uploads/2014/03/Ley27269.pdf>)

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (FIPS140-2) (2001) FIPS PUB 140-2: Security Requirements for cryptographic modules. (Consulta: 01 de noviembre de 2017) (<http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf>)

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (FIPS140-2A) (2014) Annex A – Approved Security Functions for FIPS PUB 140-2 (consulta: 01 de noviembre de 2017) (<http://csrc.nist.gov/publications/fips/fips140-2/fips1402annexa.pdf>)

NIST SP-800-57 Part 1 (2016) Recommendation for Key Management Part 1: General (<http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-57pt1r4.pdf>)

NIST SP-800-57 Part 2 (2016) Best Practices for Key Management Organization (<http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-57p2.pdf>)

NIST SP-800-57 Part 3 (2016) Application-Specific Key Management Guidance (<http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-57Pt3r1.pdf>)

NORTHSECURE.ES (2013) Conceptos de Seguridad (Consulta: 20 de setiembre de 2017) (<http://northsecure.es/conceptos-de-seguridad/>)

NORTHWARE.MX (2012) Técnicas efectivas para la toma de requerimientos (consulta: 16 de noviembre de 2017) (http://www.northware.mx/tecnicas_efectivas_toma_requerimientos/)

O'REILLY, Charlie Scott, Paul Wolfe, Mike Erwin (1999) Virtual Private Networks, Second Edition. USA: O'Reilly

OFFICE.COM (2016) *5 commonly overlooked security threats*. (Consulta: 15 de febrero de 2018) (<https://blogs.office.com/en-us/2016/01/28/overlooked-email-security-threats/>)

OFFICE365SUPPORT.CA (2015) Office 365 Message Encryption Mail Flow. (Consulta: 16 de noviembre de 2017) (<http://office365support.ca/setup-and-enable-office-365-message-encryption/>)

PM-DEVICES.COM (2012) Identificar a los interesados – Proyecto técnico (consulta: 16 de noviembre de 2017) (http://www.pm-devices.com/Documentos_Tecnico/Grupo%20Iniciacion/10.1.%20Identificar%20los%20interesados%20-%20Iniciaci%C3%B3n.pdf)

PMOINFORMATICA.COM (2014) Plantilla del plan de pruebas de software (consulta: 19 de noviembre de 2017) (<http://www.pmoinformatica.com/2014/05/plan-de-pruebas-de-software.html>)

REAL ACADEMIA ESPAÑOLA (RAE) (2014) Diccionario de la lengua española (consulta: 29 de julio de 2017) (<http://www.rae.es/recursos/diccionarios/drae>)

RENIEC.GOB.PE (2014) Planta de Certificación Digital PKI (consulta: consulta: 09 de septiembre de 2017) (<http://www.reniec.gob.pe/portal/plantaPKI.htm>)

SAFELAYER (2012) Infraestructura de Clave Pública (consulta: 29 de julio de 2017) (<http://www.safelayer.com/es/soluciones/infraestructura-de-clave-publica>)

SANS.ORG (2013) Building and Managing a PKI Solution for Small and Medium Size Business. (Consulta: 15 de noviembre de 2017) (<https://www.sans.org/reading-room/whitepapers/certificates/building-managing-pki-solution-small-medium-size-business-34445>)

SITES.GOOGLE.COM (2008) Basics of Digital Certificates and Certificate Authority. (Consulta: 29 de octubre de 2017) (<https://sites.google.com/site/ddmwsst/digital-certificates#TOC-Further-Reading>)

SYMANTEC CORPORATION (SYMANTEC-CORP) (2011) Whitepaper: Securing Your Business Applications with Managed PKI (Consulta: 05 de octubre de 2017) (https://www4.symantec.com/mktginfo/whitepaper/user_authentication/21195758_WP_GA_ManagedPKISecuringYourBizApps_062311.pdf)

SYMANTEC MPKI (2013) Integrating S/MIME Certificates with Microsoft Outlook® (consulta: 26 de noviembre de 2017) (https://adgrafics.net/docs/symantec/pki/MPKI_SMIME.pdf)

SYMAUTH.COM (2015) Symantec PKI Manager Test Drive (consulta: 15 de febrero de 2015) (<https://testdrive-pki-manager.symauth.com/pki-manager/>)

TESIS PUCP (2012) Plan estratégico del sector automotriz del Perú (consulta: 05 de enero de 2018)

http://tesis.pucp.edu.pe/repositorio/bitstream/handle/123456789/4614/BARANDIARAN_CALDERON_CHAVEZ_COELLO_AUTOMOTRIZ_PERU.pdf?sequence=1)

THENEWPM (2009) *Another look at requirements* (consulta: 15 de noviembre de 2017) (<http://thenewpm.blogspot.pe/2009/06/another-look-at-requirements.html>)

TOYOTA.COM.PE (2017) Pagina web comercial de Toyota del Perú – Visión, Misión, Valores (consulta: 5 de setiembre de 2017) (<https://www.toyotaperu.com.pe/>)

UNM.EDU (2002) *A History and Survey of Network Firewalls* (consulta: 09 de septiembre de 2017) (<https://www.cs.unm.edu/~treport/tr/02-12/firewall.pdf>)

VACCA, John R. (2004) *Public key infrastructure: building trusted applications and Web services*. Washington D.C.: Auerbach Publications

VILAS, Jorge (2001) Infraestructura de Clave Pública (PKI) y sus aplicaciones en el mundo real. (Consulta: 18 de julio de 2017) (<http://www.salvador.edu.ar/jhvdcolodrero.pdf>)

WEBTRUST.ORG (2017) WEBTRUST PRINCIPLES AND CRITERIA FOR CERTIFICATION AUTHORITIES (consulta: 20 de diciembre de 2017) (<http://www.webtrust.org/principles-and-criteria/docs/item85228.pdf>)

WIKIPEDIA.ORG (2004) Maquina de Crackeado DES. (Consulta: 22 de noviembre de 2017) (https://es.wikipedia.org/wiki/Data_Encryption_Standard#/media/File:Board300.jpg)

WORDPRESS.COM (2011) Matriz para el análisis de riesgos (consulta: 6 de diciembre de 2017) (https://protejete.wordpress.com/gdr_principal/matriz_riesgo/)

GLOSARIO

- **Cifrado:** Es un procedimiento de seguridad informática que se utiliza para proteger la información confidencial, codificando el mensaje mediante una clave secreta. Finalmente, este mensaje cifrado no puede ser leído con lenguaje humano.
- **Nube:** En la actualidad, es el nombre con el cual se le conoce a la Internet. Es comúnmente usado contextos informáticos para describir servicios que son ofrecidos por terceros alojados en internet.
- **Entidades Certificadoras:** Son entidades de confianza reconocidas mundialmente por validar, mediante certificados digitales, la autenticidad de personas, aplicaciones, sitios web, documentos, etc.
- **Criptografía Asimétrica:** Es un método de criptografía el cual usa un intercambio de dos llaves o claves para el cifrado de la información. Una clave es pública y la otra es privada.
- **Claves Públicas:** Dentro de la criptografía asimétrica, la clave pública es un conjunto de caracteres que es conocido por todo el mundo y que puede ser usado para enviarle mensajes encriptados al dueño de la clave.
- **Claves Privadas:** Dentro de la criptografía asimétrica, la clave pública es un conjunto de caracteres secreto, el cual solo es conocido por el dueño del certificado o firma digital.
- **Exchange Online:** Es una tecnología de servicio de correo propietaria de Microsoft basada en la tecnología On-Premise de Microsoft Exchange Server, la diferencia es que el servicio es alojado por Microsoft en sus centros de datos en la nube.
- **Office 365:** Es un producto de Microsoft que consiste en servicios de correo electrónico, Word, Excel, Power Point, mensajería instantánea, colaboración y almacenamiento en la nube. Este es adquirido como un servicio pagado en plazos mensuales o anuales según el adquiriente.
- **Firma Digital:** Es un mecanismo de seguridad usado en criptografía para validar la autenticidad del emisor de un mensaje, asegurando que este venga desde el dueño del mensaje y no desde una fuente no autorizada.

- **Texto Plano:** Es el modo en que son enviados los mensajes de correo electrónico por defecto. Es llamado así, porque estos pueden ser leídos por cualquier herramienta de análisis de red.
- **Sniffer:** Es una herramienta de análisis de red especializada en el análisis de los paquetes de datos que fluyen a través de la red.
- **Función Hash:** Llamada también función de resumen. Son funciones basadas en métodos matemáticos para resumir un mensaje, sin importar su tamaño, a un mensaje codificado y de longitud fija. Esta función necesita de una llave o clave con la cual será codificada.
- **Algoritmo de cifrado:** Operación o función matemática que se utiliza en combinación con una o par de claves que se aplica a un texto plano y permite obtener un texto cifrado (o descifrarlo) garantizando la confidencialidad e integridad de la información contenida. Existen dos tipos de cifrado, estos son el cifrado simétrico y cifrado asimétrico.
- **Pendrive:** Es un dispositivo de almacenamiento portátil, por lo general son dispositivos que se conectan mediante la interfaz USB a las computadoras compatibles con dicha interfaz.
- **Token de seguridad:** Este dispositivo se usa para el almacenamiento de llaves criptográficas para cualquier proceso de validaciones de la identidad dentro de una PKI.
- **Backup:** Es una copia de seguridad que realizan las organizaciones para resguardar la información de los archivos o aplicaciones contenidas en un servidor. Ello para tener un respaldo ante cualquier desastre que ocasione la pérdida de la información.
- **Cloud-based:** Este es un término inglés usado para referirse a algo basado en la nube, o que alguna aplicación o servicio está alojada en un centro de datos externo y se acceden a estos recursos a través de internet.
- **On-Premise:** Este es un término inglés usado para referirse a algún servicio o software que funciona en las mismas instalaciones o infraestructura de la organización o persona que lo usa.

SIGLARIO

- **PKI:** *Public Key Infrastructure* o en el español, Infraestructura de Clave Pública.
- **SGSI:** Sistema de Gestión de Seguridad de la Información.
- **RAE:** Real Academia Española
- **VAI:** Valor Actual de Ingresos totales netos
- **VAC:** Valor Actual de los Costos de inversión
- **VAN:** Valor Actual Neto
- **ROI:** Retorno de Inversión
- **DRP:** *Disaster Recovery Plan* o en el español, Plan de Recuperación ante Desastres.
- **OCSP:** *Online Certificate Status Protocol* o en el español, Protocolo de Estado de un Certificado en Línea.

ANEXOS

Anexo A:

El punto de inicio de este proceso es desde el ingreso al portal de administración de la PKI que ofrece la versión de prueba de Symantec (*Symantec Management PKI Service Test*

Drive) hasta la configuración de los certificados digitales S/MIME en los clientes de correo electrónico, el cual es requisito indispensable para ejecutar los casos de prueba definidos.

Ingreso al portal de administración

- a. El primer paso es ingresar al portal de administración de *Symantec PKI Manager*, para ello se debe ingresar al enlace proporcionado por el proveedor Symantec, el cual puede ser de esta manera:

<https://testdrive-pki-manager.symauth.com/pki-manager/>

- b. Para ingresar, el navegador mostrará una ventana solicitando el PIN de seguridad que autentica la computadora en donde está instalado el certificado, la cual valida que el equipo desde donde se ingresa al portal de administración sea seguro:

Figura 49. Ventana de solicitud de PIN. Adaptado de “Symantec PKI Manager Test Drive”, por SYMAUTH.COM, 2015.

- c. Luego, se abrirá la ventana principal de administración la cual se muestra de la siguiente manera en la figura 50:

Figura 50. Ventana de administración principal: PKI Manager. Adaptado de “Symantec PKI Manager Test Drive”, por SYMAUTH.COM, 2015.

Creación de perfiles de certificados

- a. Continuando con el proceso, se procede a crear el perfil de los certificados de correo electrónico, que serían las tres plantillas de certificados que se propusieron. Para ello,

se despliega el menú de configuraciones y se selecciona la opción “Administrar perfiles de certificados”:

Figura 51. Opción de Administrar perfiles de certificados. Adaptado de “Symantec PKI Manager Test Drive”, por SYMAUTH.COM, 2015.

- b. Luego, en la parte superior, al elegir la opción **Agregar perfiles de certificado** aparecerá una ventana con cuatro pasos para crear el perfil, se selecciona el **Modo Producción** y clic en **Continuar**:

Crear perfil: **Seleccionar modo** Seleccionar plantilla Personalizar opciones Personalizar servicios

¿Cómo desea usar este perfil?
 Seleccione el modo para este perfil.

☐ **Modo de prueba**
 Este perfil se usará para fines de pruebas únicamente. Es posible mover el perfil y todos los certificados a producción más tarde.
Nota: Los certificados emitidos son válidos en modo de prueba. Sea cuidadoso al emitir certificados de modo de prueba.

☒ **Modo de producción**
 Este perfil se usará para administrar los usuarios y los certificados activos.

Figura 52. Ventana de creación de perfil, selección de modo. Adaptado de “Symantec PKI Manager Test Drive”, por SYMAUTH.COM, 2015.

- c. En el segundo paso, para seleccionar una plantilla, se elige la opción **Correo electrónico seguro** para que por defecto se carguen las configuraciones necesarias para un certificado S/MIME y clic en **Continuar**:

☒ Correo electrónico seguro (Versión de prueba)	Usuario	Para soporte de S/MIME. Habilita el cifrado y la firma digital correos electrónicos.
--	---------	--

Atrás Cancelar Continuar

Figura 53. Selección de plantilla, opción Correo electrónico seguro. Adaptado de “Symantec PKI Manager Test Drive”, por SYMAUTH.COM, 2015.

- d. A continuación, se mostrará una ventana de personalización de opciones para el certificado digital S/MIME. Este paso es muy importante, ya que se definen las características que se le darán al perfil de certificado. Para ello, se debe ingresar un nombre para el perfil o plantilla, en este paso es donde se configuran los parámetros descritos en la definición de las plantillas de los certificados. Para el ejemplo, se define la creación del perfil “**Correo Nivel 1**”, ya que es uno de los tres perfiles que se proponen para la organización:

Figura 54. Creación de perfil, Personalización de certificado. Adaptado de “Symantec PKI Manager Test Drive”, por SYMAUTH.COM, 2015.

- e. En opciones de certificado principales se debe elegir el método de inscripción **PKI Client** para que los usuarios de correo electrónico reciban un mensaje de inscripción a su buzón al momento en que el certificado digital les sea emitido:

Figura 55. Creación de perfil, Personalización de certificado. Adaptado de “Symantec PKI Manager Test Drive”, por SYMAUTH.COM, 2015.

- f. En cuanto a las demás opciones de certificado principales, el **método de autenticación** debe ser por **Código de inscripción**, ya que la inscripción y manejo

de certificados digitales instalados será mediante un PIN de seguridad que será solicitado por el **PKI Client** de Symantec. El **almacén de los certificados** será en el **Equipo**, ya que estos serán instalados y almacenados por el sistema operativo en donde se encuentra instalado el cliente de correo Outlook, asimismo, serán administrados por el **PKI Client**. Finalmente, el **nivel de seguridad de la clave privada** debe definirse como **Medio**, ya que la clave privada será instalada en el equipo y deberá proveerse del PIN de seguridad para su uso en cada transacción en la cual se haga uso de la clave privada:

Figura 56. Opciones de certificado, nivel de seguridad medio. Adaptado de “Symantec PKI Manager Test Drive”, por SYMAUTH.COM, 2015.

- g. Luego, se deben definir las características, por defecto, que tendrá el certificado digital S/MIME. Para el campo **Subject** del certificado digital se pueden editar los datos que este contendrá, el cual se configura con la información requerida por cada usuario de acuerdo con el estándar ITU-T X.509.

Figura 57. Opciones de certificado, configuración de campos. Adaptado de “Symantec PKI Manager Test Drive”, por SYMAUTH.COM, 2015.

- h. Por último, se deben configurar las opciones adicionales del certificado digital. Las cuáles serán definidas de acuerdo con uno de los tres perfiles a crear. En estas opciones se configurarán los parámetros de **algoritmo de firma digital, tamaño de clave** y el **periodo de validez** del certificado, los cuales son parámetros variables que dependerán del perfil de certificado digital a crear. A continuación, se muestra la configuración de ejemplo para el perfil “**Correo Nivel 1**”, los cuales variarán para el perfil de “**Correo Nivel 2**”:

Opciones adicionales del certificado

Período de validez: 730 Días

Custodia de clave: Symantec

Publicar en directorio público: Sí

Ventana de renovación: 15 Días

Eliminar certificados inactivos: No

Algoritmo de firma: SHA256 con cifrado RSA

Tamaño de clave: 2048

Tamaño de clave: 2048

El tamaño de clave predeterminado se recomienda para obtener seguridad y compatibilidad óptimas, a menos que las políticas de seguridad o el entorno de red requieran otro tamaño de clave.

Recomendaciones:

- Seleccione un tamaño de clave más grande solamente si sus políticas lo requieren y si los dispositivos y los usuarios pueden admitirlo.
- Seleccione un tamaño de clave más pequeño si los dispositivos y los usuarios no pueden admitir el tamaño de clave predeterminado.

Atrás Cancelar Vista previa Guardar

Figura 58. Configuraciones personalizadas del certificado digital. Adaptado de “Symantec PKI Manager Test Drive”, por SYMAUTH.COM, 2015.

- i. Finalmente, se guarda el perfil de certificado digital. Si se presenta un mensaje de confirmación, clic en **Continuar**. De la misma manera, se realizan estos pasos para la creación del perfil de **Correo Nivel 2** y opcionalmente se puede crear el perfil de Correo Nivel 3 para tenerlo de manera referencial. Los perfiles de certificados digitales S/MIME que se usaran como plantillas para la emisión de los certificados digitales por usuario se muestran como la *figura 59*:

Todas las perfiles de certificado

Operaciones de búsqueda:

Buscar por: Mostrar todo

Especificar criterios: Mostrar todo

☐ Incluir perfiles de certificado ocultos

Buscar

4 perfiles de certificado

Correo Nivel 1
Correo electrónico seguro (V... Producción)

Correo Nivel 2
Correo electrónico seguro (V... Producción)

Correo Nivel 3
Correo electrónico seguro (V... Producción)

Figura 59. Administración de perfiles de certificado (plantillas). Adaptado de “Symantec PKI Manager Test Drive”, por SYMAUTH.COM, 2015.

Emisión del certificado digital para un usuario de correo electrónico

- a. Luego de tener definida en plantillas la configuración de los certificados se pasa a emitir certificados digitales para los usuarios de correo electrónico. En el PKI Manager, se selecciona la opción **Administrar usuarios**:

Figura 60. Barra de opciones de PKI Manager. Adaptado de “Symantec PKI Manager Test Drive”, por SYMAUTH.COM, 2015.

- b. Aparecerá la ventana de Administrar usuarios y se selecciona **Agregar usuarios**:

Figura 61. Ventana de administración de usuarios. Adaptado de “Symantec PKI Manager Test Drive”, por SYMAUTH.COM, 2015.

- c. En la siguiente ventana, se ingresa el **ID del puesto** (*Seat ID*), el cual será la dirección de correo electrónico del usuario al cual se le emitirá el certificado digital y continuamos con el procedimiento:

Agregar usuarios a esta cuenta

Agregar:

☒ Un solo usuario

☐ Varios usuarios

Escriba la información del usuario que desea agregar.

* Id. de puesto (el identificador único para este usuario):

josue.alarcon@zaralu.onmicrosoft.com ?

* Información necesaria

Cancelar Continuar

Figura 62. Agregar usuario con la dirección de correo electrónico. Adaptado de “Symantec PKI Manager Test Drive”, por SYMAUTH.COM, 2015.

- d. Luego, se proporcionará la información de **Nombre, Apellidos** y la **dirección de correo**, la cual automáticamente será considerada la del ID del puesto previamente ingresado. Asimismo, es importante marcar el *check* que indica “**Deseo inscribir a este usuario para que obtenga un certificado**” y continuamos con el procedimiento tal como se muestra en la *figura 63*.

El usuario no está en el sistema. Escriba la información del usuario a continuación.

Agregar usuarios a esta cuenta

* Id. de puesto:

josue.alarcon@zaralu.onmicrosoft.com

* Nombre:

Josue

* Apellidos:

Alarcon

* Correo electrónico:

josue.alarcon@zaralu.onmicrosoft.com

☒ Deseo inscribir a este usuario para que obtenga un certificado.

* Información necesaria

Cancelar Atrás Continuar

Figura 63. Ventana agregar usuarios, configuración de nombres y correo. Adaptado de “Symantec PKI Manager Test Drive”, por SYMAUTH.COM, 2015.

- e. Al crearse el usuario, el cual será llamado Josué Alarcón, se mostrará un mensaje de confirmación y se solicitará inmediatamente la selección de un perfil a asignar para la creación del certificado. Para el ejemplo, se asignará al usuario el perfil “**Correo Nivel 1**” para que este pueda heredar todas las características de básicas del perfil y completar la información personalizada para el usuario.

Figura 64. Ventana de inscripción para obtener el certificado digital. Adaptado de “Symantec PKI Manager Test Drive”, por SYMAUTH.COM, 2015.

- f. En seguida, se le solicitará ingresar la información que fue definida en el perfil “**Correo Nivel 1**” para el **Subject** del usuario. Y al final del formulario, debe marcar el *check* “**¿El sistema envió el correo electrónico de inscripción al usuario?**” para que el usuario pueda recibir el mensaje de inscripción y el Administrador PKI pueda instalar el certificado digital en su equipo y cliente de correo Outlook.

Introducir información adicional

Esta inscripción requiere información adicional.

Id. de puesto:
josue.alarcon@zaralu.onmicrosoft.com

* Departamento:
Ventas

* Nombre propio:
Josue

* Apellidos:
Alarcon

* Cargo:
Gerente de Ventas

Figura 65. Ventana de inscripción de usuario, información adicional. Adaptado de “Symantec PKI Manager Test Drive”, por SYMAUTH.COM, 2015.

- g. Después de completar el registro con información adicional del usuario, el *PKI Manager* generará un código de inscripción el cual se debe tener en cuenta al momento de descargar e instalar el certificado digital en el equipo del usuario. Debe tenerse especial cuidado en la manera como se maneja este código de inscripción por parte del Administrador PKI, por motivos de seguridad, se recomienda que este no sea enviado por ningún mecanismo a través de internet, lo recomendable es que el Administrador PKI lleve el código escrito en físico al momento de su instalación en el equipo del usuario de correo electrónico.

Figura 66. Ventana de inscripción de usuario, código de inscripción. Adaptado de “Symantec PKI Manager Test Drive”, por SYMAUTH.COM, 2015.

Obtención e Instalación del certificado digital

- a. Luego de emitido el certificado digital S/MIME, el Administrador PKI verifica que en el buzón de correo electrónico del usuario haya recibido un mensaje de parte del *Symantec Enterprise PKI Team* con el enlace para la verificación. Asimismo, se debe tener listo el código de inscripción que se generó para el usuario de correo electrónico.

Figura 67. Correo de solicitud de inscripción del Enterprise PKI Team. Adaptado de “Symantec PKI Manager Test Drive”, por SYMAUTH.COM, 2015.

- b. Al seguir el enlace, en el navegador se mostrará la siguiente ventana en la cual confirmaremos la dirección de correo electrónico del usuario y continuamos con el procedimiento tal como se muestra en la *figura 68*.

Figura 68. Web de Inscripción al certificado asignado (Symantec). Adaptado de “Symantec PKI Manager Test Drive”, por SYMAUTH.COM, 2015.

- c. Luego, se introduce el **código de inscripción** el cual fue proporcionado al Administrador PKI responsable del registro del certificado digital en la PKI para así validar la inscripción.

Figura 69. Web de Inscripción al certificado asignado, código de inscripción. Adaptado de “Symantec PKI Manager Test Drive”, por SYMAUTH.COM, 2015.

- d. Luego, antes de descargar el certificado digital, Symantec requiere instalar una extensión o complemento de *Symantec Authentication Client*. Este complemento se instala en el navegador desde el cual se abrirá el portal de administración, para proporcionar un canal seguro con certificados digitales.

Instalar extensión del complemento de Symantec Authentication Client

Antes de poder inscribirse en el certificado, deberá instalar la extensión del complemento de Symantec Authentication Client. La extensión de complemento de Symantec Authentication Client permite que el navegador se comunique con Symantec PKI Client para administrar los certificados.

Descripción general de la instalación de la extensión del complemento de Symantec Authentication Client.

- 1 Descargue la extensión del complemento de Symantec Authentication Client.
Haga clic en **Descargar**. Si se le indica, haga clic en **Agregar** para agregar la extensión al navegador. A continuación, haga clic en **Ejecutar**.
- 2 Instale la extensión del complemento de Symantec Authentication Client.
Siga las indicaciones para instalar la extensión del complemento.
[Haga clic](#) aquí para obtener más detalles sobre la extensión del complemento del cliente de autenticación de Symantec.
- 3 Si se le indica, instale PKI Client.
Siga las indicaciones para instalar PKI Client.
- 4 Inscribese para obtener un certificado.
Después de instalar PKI Client, será necesario reiniciar el sistema. Una vez reiniciado el sistema, busque el mensaje de correo electrónico de inscripción y haga clic en el vínculo para volver a comenzar el proceso de inscripción.

Figura 70. Instalación de complemento Symantec Authentication Client. Adaptado de “Symantec PKI Manager Test Drive”, por SYMAUTH.COM, 2015.

- e. Para instalar el complemento en el navegador, se debe realizar la instalación según el tipo de navegador use el usuario. Los navegadores validos son Internet Explorer, Mozilla Firefox, Safari y Google Chrome. Una vez el navegador lo haya guiado correctamente en la instalación del complemento, la página de inscripción al certificado usará el complemento del navegador para validar la identidad del equipo. A continuación, se muestra la ventana de confirmación:

✓
Identidad confirmada.

Verifique su información

Verifique que la información asociada con el certificado sea correcta y que se hayan completado los campos obligatorios.

Correo electrónico	josue.alarcon@zaralu.onmicrosoft.com
Nombre	Josue
Apellidos	Alarcon
Departamento	S/MIME
Departamento	Ventas
Compañía	Symantec Corporation
Cargo	Gerente de Ventas
Nombre propio	Josue
Apellidos	Alarcon
Calle	Av. Arequipa 3512
Localidad	Lima
País	PE
Apodo del certificado	<input style="width: 80%;" type="text" value="Correo Nivel 1"/> ?

Figura 71. Confirmación de identidad a través del navegador web. Adaptado de “Symantec PKI Manager Test Drive”, por SYMAUTH.COM, 2015.

- f. Después de haberse validado la identidad del usuario, se le solicitará la instalación del cliente encargado de administrar los certificados instalados en el equipo, el *Symantec PKI Client*. Este es un cliente ligero que remplazará el administrador de certificados nativo de Windows o Mac. Descargamos el archivo de instalación y lo ejecutamos siguiendo todos los pasos por defecto:

Figura 72. Descarga de Symantec PKI Client en la PC del usuario. Adaptado de “Symantec PKI Manager Test Drive”, por SYMAUTH.COM, 2015.

- g. Luego, se procederá a instalar el certificado digital en el equipo. Para ello, el último paso que se muestra en la página de inscripción es la Instalación del certificado:

Figura 73. Instalación del certificado en la PC del cliente. Adaptado de “Symantec PKI Manager Test Drive”, por SYMAUTH.COM, 2015.

- h. Después, se solicitará ingresar un PIN de seguridad para instalar el certificado en el equipo. Este PIN identificará al equipo y será solicitado cada vez que se requiera instalar un nuevo certificado. Si es la primera vez, debe crear un nuevo PIN, si no, se le solicitará ingresar el PIN previamente configurado:

Figura 74. Solicitud de creación de PIN para la PC cliente (única vez). Adaptado de “Symantec PKI Manager Test Drive”, por SYMAUTH.COM, 2015.

- i. En seguida, se mostrarán varios mensajes de confirmación para la instalación del certificado en el equipo, tanto por parte del SO Windows y de Symantec *PKI Client*, a los cuales se aceptan los mensajes de advertencia:

Figura 75. Ventana de Instalación del certificado S/MIME. Adaptado de “Symantec PKI Manager Test Drive”, por SYMAUTH.COM, 2015.

- j. Finalmente, se muestra un mensaje de confirmación para instalar el certificado digital S/MIME con el perfil **Correo Nivel 1** tal como se solicitó. Luego, se mostrará un mensaje indicando la instalación del certificado digital correctamente.

Figura 76. Ventana de confirmación inscripción de certificado completa. Adaptado de “Symantec PKI Manager Test Drive”, por SYMAUTH.COM, 2015.

Configuración del cliente de correo electrónico para el uso de los certificados digitales S/MIME

El cliente de correo que se tomará como ejemplo a continuación es Microsoft Outlook 2013, ya que es el cliente de correo electrónico recomendado por el servicio de Microsoft Exchange Online de Office 365. En esta sección se describirá detalladamente como configurar el certificado instalado en el paso anterior sobre un cliente de correo Outlook 2013 que es el mismo que utiliza en la actualidad la organización objetivo.

- a. En primer lugar, en el equipo donde se encuentra instalado el cliente de correo Outlook se configurará el uso del certificado digital S/MIME previamente descargado. Para ello, se selecciona **Archivo**, luego clic en **Opciones**, **Centro de confianza** y luego **configuraciones de centro de confianza**. En esa ventana emergente, ir a la sección de **seguridad de correo** (en la imagen de abajo se muestra en inglés) y luego seleccionar el botón **Import/Export** de la sección de **Digital IDs**:

Figura 77. Ventana de confirmación de correo en Microsoft Outlook 2013. Adaptado de “Configuración para el envío de correo electrónico cifrado y firmado desde un cliente de correo electrónico Office 365 con Outlook 2013”, elaboración propia.

- b. En la siguiente ventana, se debe importar el certificado instalado en el equipo. Para ello, primero se debe exportar el certificado a un archivo que pueda ser leído por el cliente de correo mediante la opción de **Exportar el ID digital a un archivo**. Elegir en **Digital ID** mediante el botón “*Select...*” el certificado digital instalado “**Correo Nivel 1**”, luego, en **Filename** (“*Browse...*”) se indica en que ubicación del equipo se exportará el certificado y finalmente se ingresa una **contraseña** para proteger el certificado digital a exportar.

Figura 78. Ventana de Importación y Exportación de certificado. Adaptado de “Configuración para el envío de correo electrónico cifrado y firmado desde un cliente de correo electrónico Office 365 con Outlook 2013”, elaboración propia.

Figura 79. Selección de Certificado Correo Nivel 1. Adaptado de “Configuración para el envío de correo electrónico cifrado y firmado desde un cliente de correo electrónico Office 365 con Outlook 2013”, elaboración propia.

Figura 80. Archivo de certificado digital exportado a usar en el cifrado y firma digital de los mensajes de correo. Adaptado de “Configuración para el envío de correo electrónico cifrado y firmado desde un cliente de correo electrónico Office 365 con Outlook 2013”, elaboración propia.

- c. Luego, en la ventana de **Import/Export Digital ID**, importar el certificado digital exportado e ingresar la contraseña previamente definida.

Figura 81. Selección del archivo de certificado a instalar en Outlook 2013. Adaptado de “Configuración para el envío de correo electrónico cifrado y firmado desde un cliente de correo electrónico Office 365 con Outlook 2013”, elaboración propia.

- d. Para habilitar el cifrado y firmado de los mensajes con el certificado ya configurado, se procede a ingresar a **Archivo > Opciones > Centro de confianza > Configuraciones de centro de confianza**. En la ventana, dirigirse a la sección de **Seguridad de correo** y en las opciones de Correo cifrado, seleccionar las opciones “**Cifrar contenido y adjuntos para los mensajes salientes**” (*Encrypt contents and attachments for outgoing messages*) y “**Agregar firma digital para los mensajes salientes**” (*Add digital signature to outgoing messages*)

Figura 82. Habilitación de Cifrado y Firmado digital de los correos. Adaptado de “Configuración para el envío de correo electrónico cifrado y firmado desde un cliente de correo electrónico Office 365 con Outlook 2013”, elaboración propia.

- e. Por otro lado, se pueden establecer configuraciones personalizadas para el uso de los certificados digitales para el cifrado y firma de los correos electrónicos mediante el protocolo S/MIME. Para ello, ingresamos a **Configuraciones** (*Settings...*) para ver las configuraciones por defecto, los cuales deberían mostrar los algoritmos que definimos en el perfil del certificado digital **Correo Nivel 1** (RSA-2048, Hash SHA-256 y Cifrado de Contenido AES-256).

Figura 83. Ventana de configuraciones de seguridad S/MIME en Outlook. Adaptado de “Configuración para el envío de correo electrónico cifrado y firmado desde un cliente de correo electrónico Office 365 con Outlook 2013”, elaboración propia.