Proyecto Unidad de Titulación

Danilo José Ninabanda Ocampo

Facultad de Arquitectura e Ingenierías

Tema:

“DISEÑO DE UN MODELO DE COMUNICACIONES SEGURAS BASADO EN RIGHTS MANAGEMENT SERVICES (RMS), BAJO EL DOMINO 10 DE LA NORMA ISO/IEC 27002:2013 APLICADO EN UNA INFRAESTRUCTURA MICROSOFT.”

Agenda

1. Problema
2. Objetivos
3. ISO/IEC 27002:2013
4. Cifrado
5. RMS (Rights Management Services)
6. Herramientas Utilizadas
7. Funcionamiento y Demostración
8. Conclusiones y Recomendaciones

Problema

- Falta de confidencialidad en las comunicaciones dentro de las organizaciones.
- NO existen controles para preservar la integridad de la información.
- Sistemas de seguridad de la información obsoletos.
- Poca gestión sobre la aplicación de controles criptográficos.

Objetivo General

Diseñar un modelo de comunicación segura que impida la pérdida de información valiosa para las empresas, mediante la aplicación de controles criptográficos basados en la Norma ISO/IEC 27002:2013.

Objetivos Específicos

Realizar un estudio bibliográfico de los principales algoritmos criptográficos que se usan para la protección de la información.

Desarrollar una solución para preservar la integridad de la información en base al domino 10 de la norma ISO/IEC 27002:2013 a través de herramientas de software en una infraestructura Microsoft.

Implementar en un ambiente de pruebas el modelo de comunicaciones seguras basado en Rights Management Services (RMS) de Microsoft.

Establecer una comunicación que permita la aplicación de confidencialidad para el servicio de correo electrónico interno aplicando el uso de Microsoft Exchange y RMS de Microsoft.

ISO/IEC 27002:2013

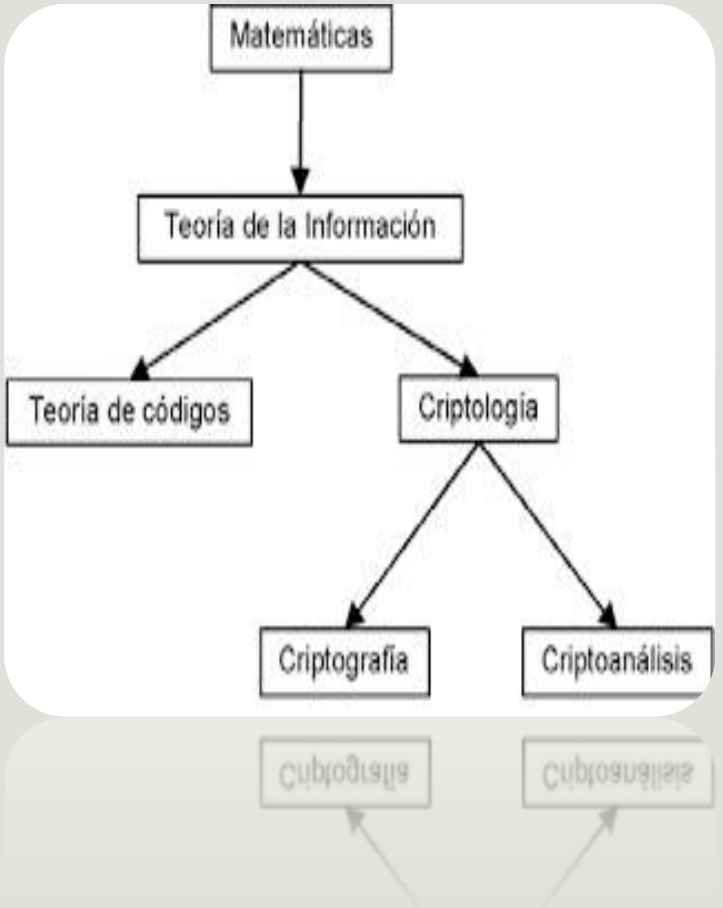
- Desarrolla estándares internacionales que facilitan el comercio internacional.

- Buenas prácticas para mejorar la seguridad de la información.
- Posee 14 Dominios, 35 objetivos de control y 114 controles.

10. CIFRADO
10.1 Controles criptográficos
10.1.1 Política de uso de los controles criptográficos
10.1.2 Gestión de claves

Controles Criptográficos

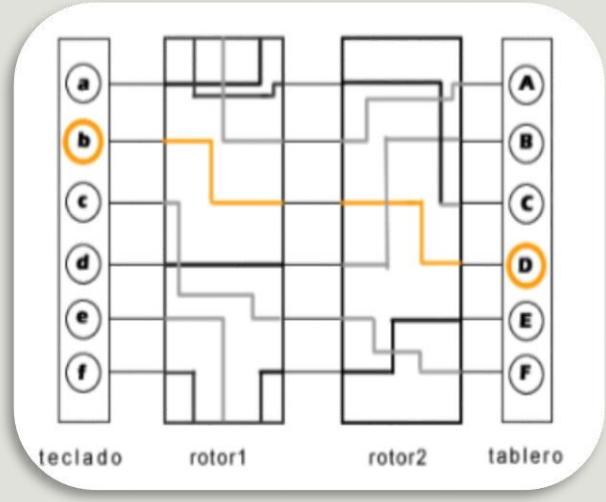
- Protección de la información.
- Garantizar la confidencialidad, autenticidad y la integridad de la información.
- Evitar daños a la imagen empresarial que la información sustraída ilegalmente pueda causar.



Controles Criptográficos

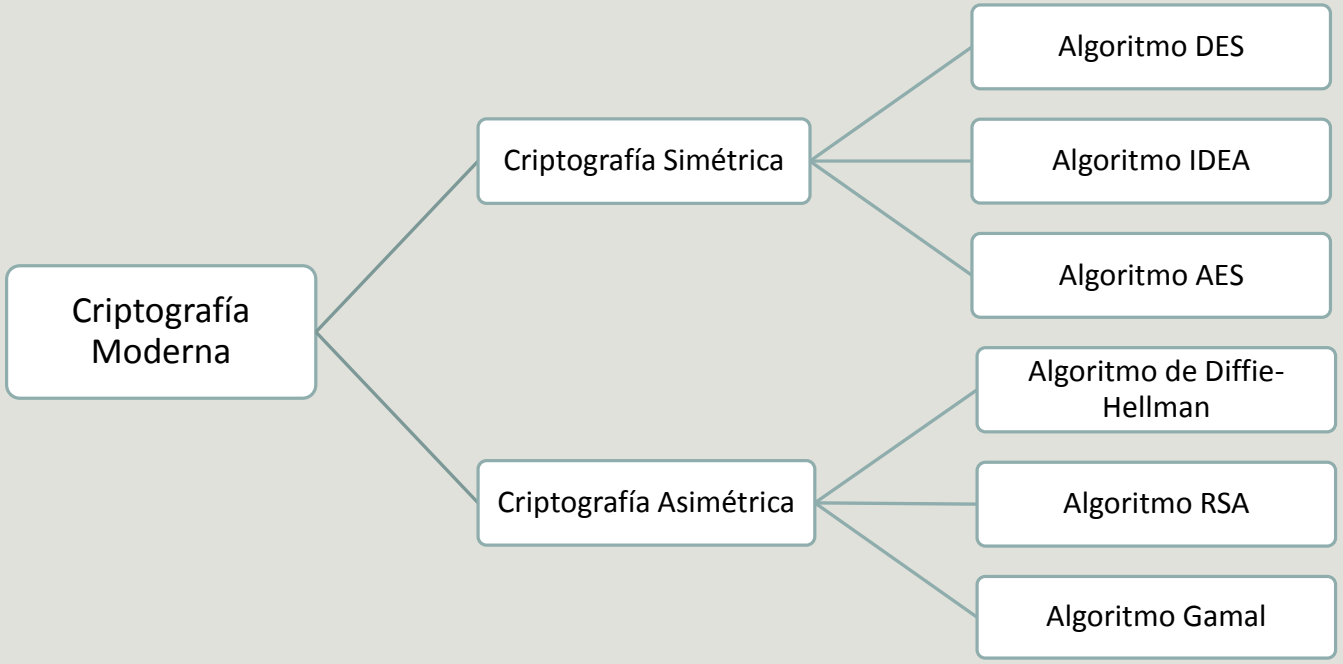
- Criptografía Clásica
  - Cifrado César
  - El disco de Alberti
  - Cifrado Vernam
  - La máquina Enigma

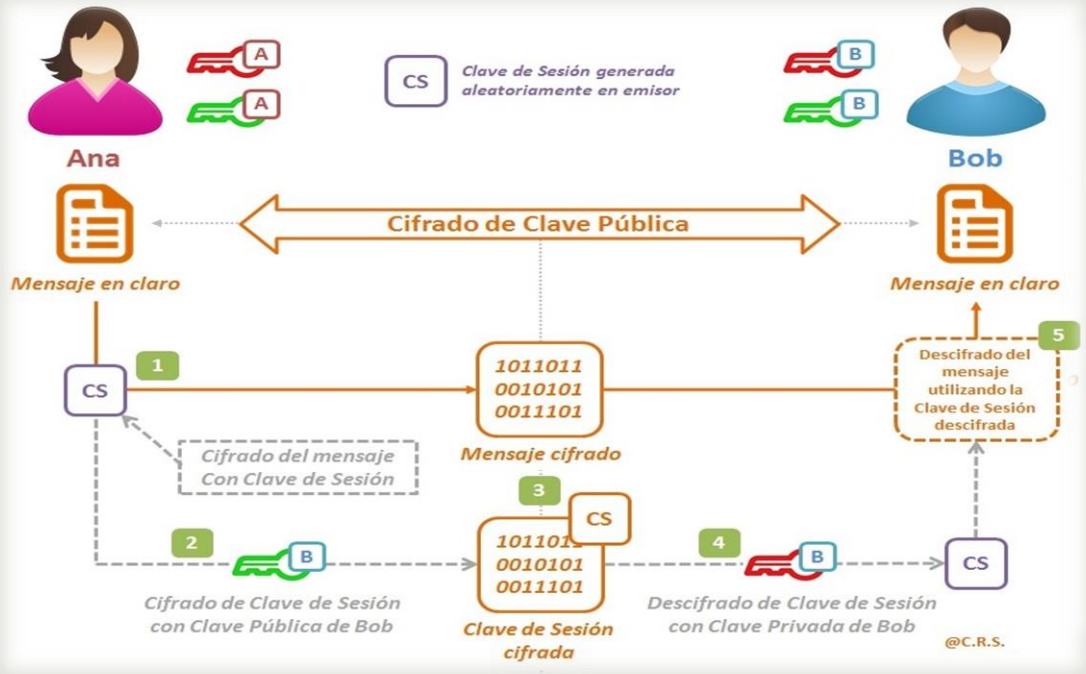
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V



Criptograma	11010	00000	01010	10110	10100	10101	10010
Clave	10100	00110	00111	11100	10111	11100	01010
Mensaje	01110	00110	01101	01010	00011	01001	11000
	C	I	F	R	A	D	O

Controles Criptográficos



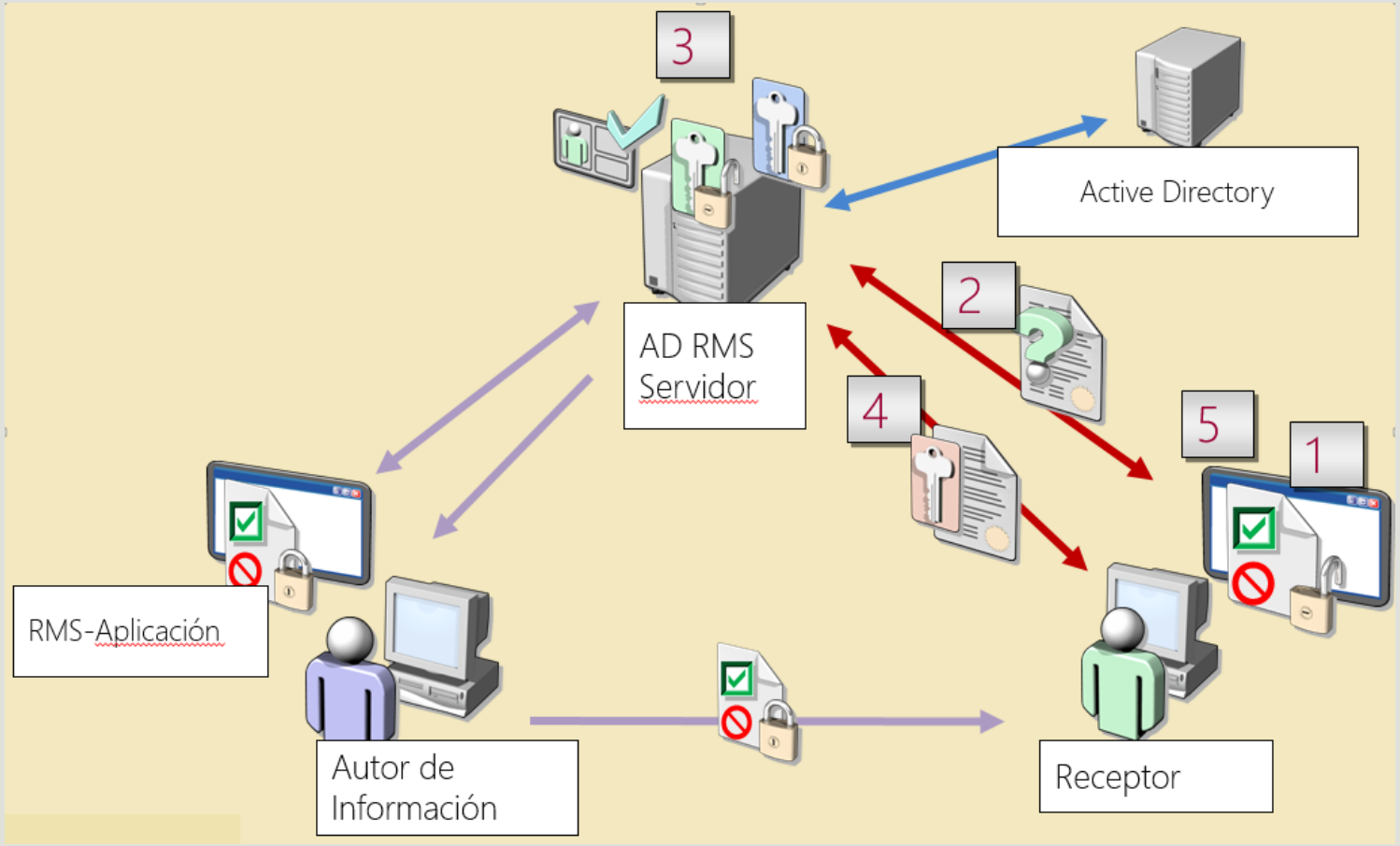


RMS (Rights Management Services)

Cifrado + **Políticas:**

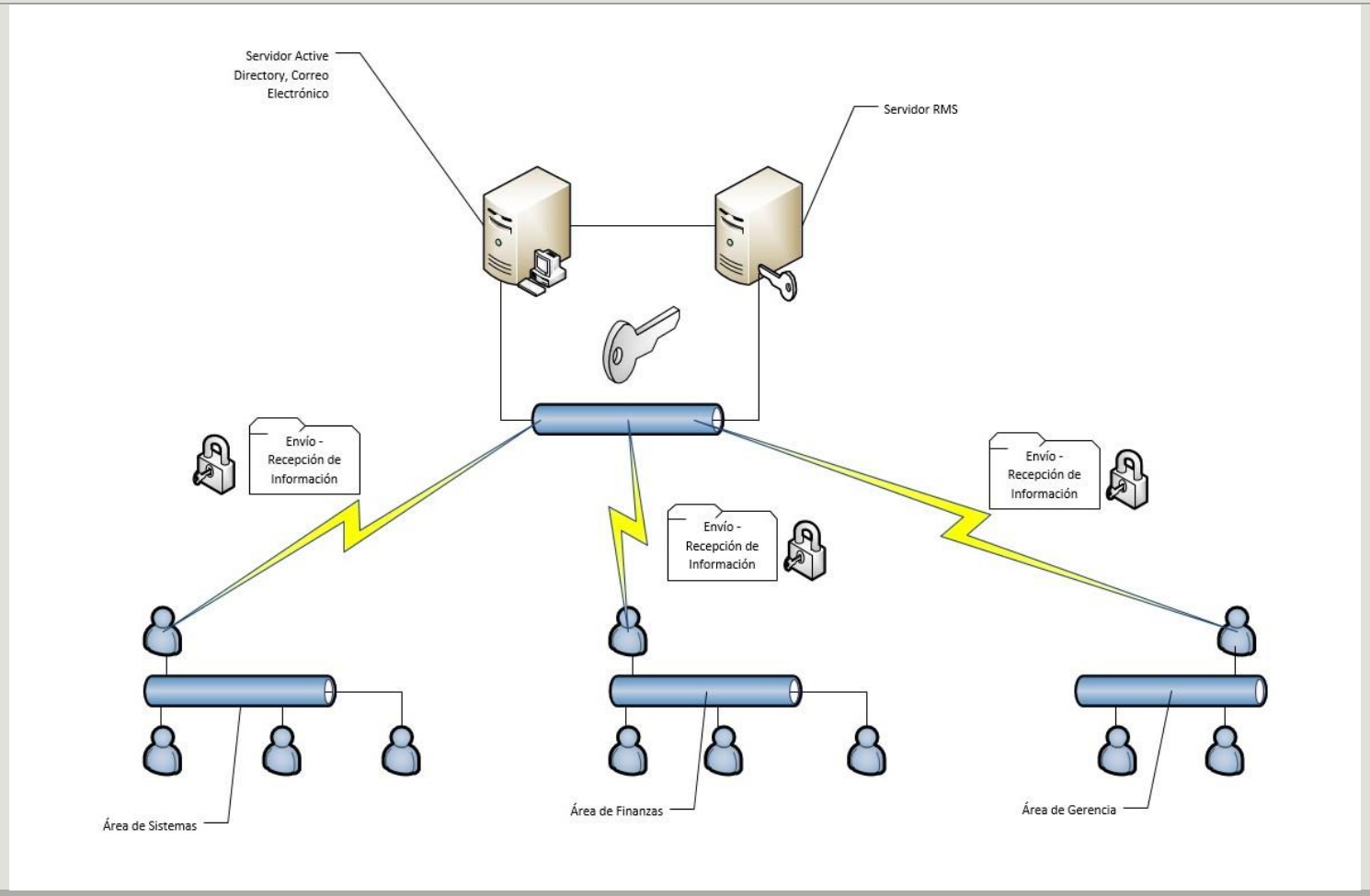
- **Permisos de acceso**
- **Derechos de uso**

RMS (Rights Management Services)



Herramientas Usadas

Funcionamiento y Demostración



Funcionamiento y Demostración

Conclusiones

Se puede concluir que con el estudio de los diferentes algoritmos criptográficos queda abierto un amplio panorama para que en la actualidad se pueda usar estas técnicas valiosas para preservar la confidencialidad de toda la información no solo que se maneja en las redes de las empresas, sino también en la información que maneja cada persona en sus diversos entornos.

El modelo de comunicaciones seguras diseñado en base al dominio 10 de la norma ISO/IEC 27002:2013, además de brindar la confidencialidad por medio de algoritmos criptográficos en las comunicaciones que se generen con el servicio de correo electrónico Microsoft Exchange, garantiza la integridad de todos los documentos electrónicos que se encuentren en las empresas por medio de la función Hash que forma parte de los algoritmos criptográficos aplicados junto al servicio de RMS.

En la implementación sobre el ambiente de pruebas de este proyecto se pudo llegar a la conclusión que algunos de los pre-requisitos para el funcionamiento de RMS, como por ejemplo Active Directory mejoran la gestión de usuarios y todos los recursos como por ejemplo: archivos electrónicos, que una empresa posee y se encuentran vinculadas al dominio de la misma. Además este servicio presta una importante ayuda en cuanto a la gestión de claves, que es muy indispensable para cumplir con protección de la información.

Conclusiones

El diseño del modelo de comunicaciones seguras realizado con RMS de Microsoft y que usa los servicios de Microsoft Exchange, ha demostrado ser una solución que impide la pérdida de información para cualquier empresa que lo implemente ya que todo el contenido que se crea, almacena e intercambia en la empresa se encuentra cifrado; así los documentos que salgan de manera ilegal de la empresa no podrán ni siquiera ser visualizados por los intrusos.

En este proyecto se ha mencionado sobre la importancia de la información y el valor que tiene para el funcionamiento de las empresas; así que se pudo llegar a la conclusión que la implementación de RMS y el uso de la criptografía darán la pauta para que las empresas empiecen a utilizar alternativas de seguridad poco comunes que complementarían a sus sistemas de seguridad ya implantados disminuyendo considerablemente el riesgo de perder documentos electrónicos importantes y conservar la integridad de los mismos.

Se puede concluir que con el uso de este modelo de comunicaciones seguras basadas en RMS se puede evitar la fuga de información o documentos electrónicos de las empresas los cuales pueden registren pérdidas económicas, daños al nombre de la marca, incluso la interrupción en la continuidad del negocio.

Recomendaciones

En base al estudio del dominio 10 de ISO/IEC 27002:2013, para la implementación de este modelo de comunicaciones seguras, se recomienda que para tener un mejor resultado en cuanto a la protección de los documentos electrónicos, se implementen algunos dominios más con sus respectivos controles con el fin de aumentar la protección en dichos documentos.

Se recomienda a todas las personas encargadas del área de tecnologías de la información de las empresas que deseen aplicar las herramientas y servicios expuestos en este trabajo, que deberán realizarlo primero en un ambiente de pruebas con el modelo de su infraestructura, para así evitar cualquier error al momento de realizar la implementación.

Recomendaciones

Para complementar la implementación de RMS, se recomienda también la creación de políticas de gestión de claves que es muy importante para que el modelo de comunicaciones seguras no quede expuesto ante el uso de técnicas de criptoanálisis.

Se recomienda la creación de suficientes políticas de gestión de documentos electrónicos mediante RMS con el fin de proteger la mayor cantidad de información de personal no autorizado.