DGTIC UNAM CERT

Active Directory Rights Management Services sobre la plataforma Windows Azure

Ricardo Carmona

Lilia González

Agenda

- Introducción
  - Objetivo del Proyecto
  - Windows Azure
  - ¿Qué es AD RMS?
- Funcionamiento General
- Diseño de la infraestructura
- Implementación
- Prueba funcional
- Costo
- Ventajas y Limitantes
- Opciones de crecimiento

Objetivo del Proyecto

- Implementar AD RMS en la plataforma Windows Azure para la distribución y restricción de permisos en el material desarrollado por la CSI, que permita una administración centralizada, sin que sea difundido o distribuido a terceros no autorizados.

Windows Azure

- Servicio PaaS (Platform as a Service)
- Entorno flexible para desarrollar aplicaciones y servicios
- Reduce tiempo de lanzamiento de productos
- Facilita la adaptación por la demanda

Active Directory Rights Management Services

- Rol en un servidor Windows
- Permite administrar permisos a archivos de manera individual
  - Gestiona permisos a través de plantillas
  - Facilita la restricción de usos (copiar, imprimir, visualizar, editar, etc.)

Funcionamiento General

Cliente RMS (Creación de Contenido)

1. Adquiere un Client Licensor Certificate (CLC)
2. Cifra el documento con el CLC (AES 128 bits)
3. Crea y firma la Licencia de Publicación (PL)
4. Liga una copia de la PL al documento, lo que restringe el uso del documento, incluso si sale de la organización.

Cliente RMS (Consumir Contenido Protegido)

1. Determina si el usuario se ajusta a las políticas de la licencia de publicación.
2. Descifra con el Right Account Certificate (RAC) la licencia de uso, para con ésta, descifrar el documento protegido.
3. Garantiza que el usuario cumpla con las condiciones de la licencia de usuario final.
4. Protege los documentos según lo previsto por las plantillas.

Servidor RMS

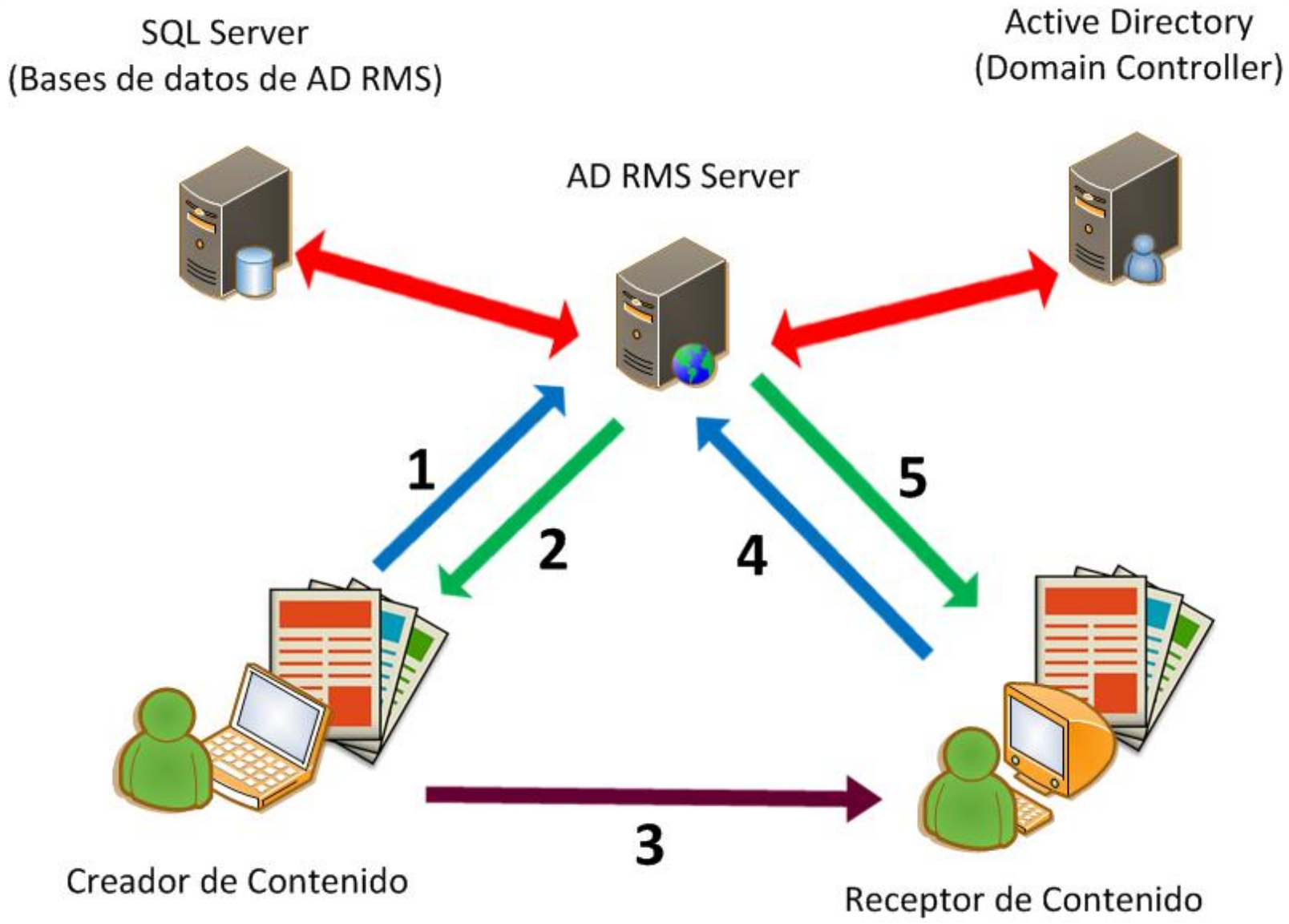
- Conjunto de servicios web que se ejecutan en Internet Information Services (IIS)

Servidor RMS

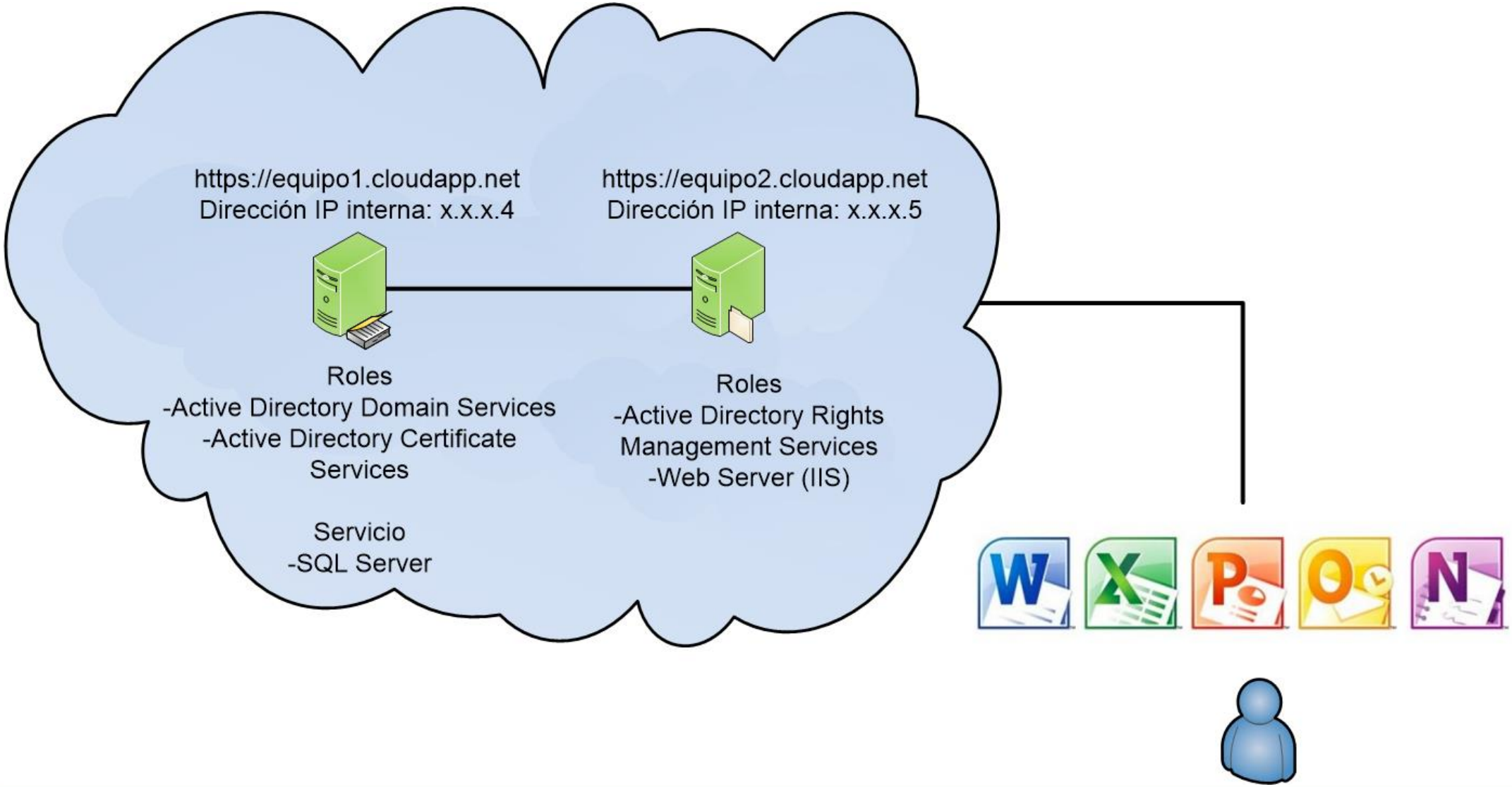
Administration	• Aloja el sitio web de administración para manejar AD RMS.
Account Certification	• Crea certificados de equipo y de derechos de cuenta permitiendo identificar usuarios y equipos.
Licensing	• Expide licencias de usuario final.

Servidor RMS

Publishing	• Crea licencias de emisión definidas en las políticas, que se enumeran en una licencia de usuario final.
Precertification	• Permite a un servidor solicitar un certificado RAC en nombre del usuario.
Service Locator	• Provee la URL de la cuentas de certificación y servicios de publicación, así como el licenciamiento, permitiendo a los clientes descubrir los servidores AD RMS.


SQL Server
(Bases de datos de AD RMS)
Active Directory
(Domain Controller)
AD RMS Server
1
2
3
4
5
Creador de Contenido
Receptor de Contenido

Diseño de la Infraestructura



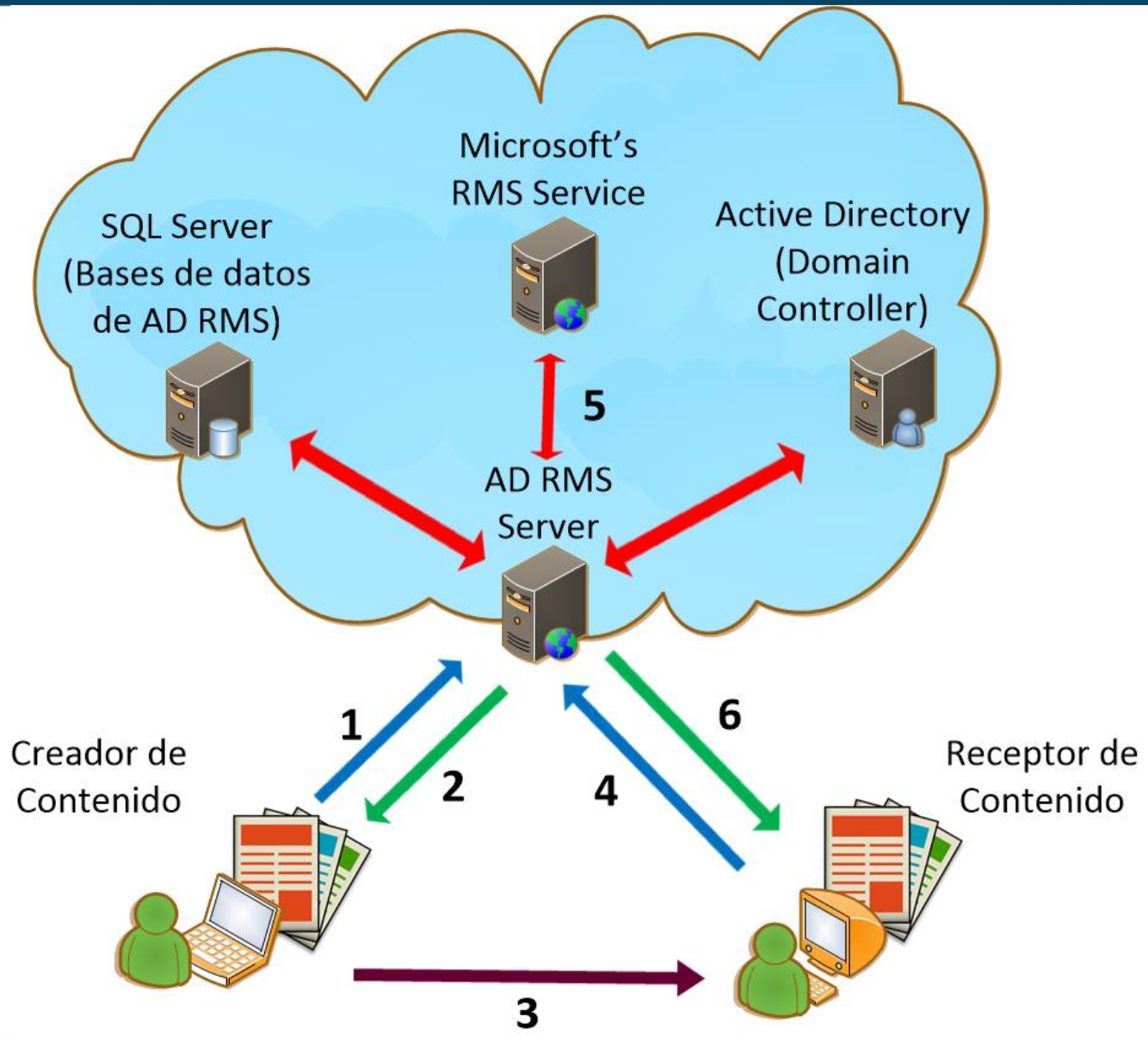
Implementación

Plantillas

- Definir permisos a un grupo de correos Windows ID (outlook, Hotmail o live)
- Los permisos no necesariamente son los mismos para todos los usuarios

Permisos individuales

- Definir permisos sobre un documento sin hacer uso de una plantilla
- Usuarios con registro de último minuto.


Microsoft's
RMS Service
SQL Server
(Bases de datos
de AD RMS)
Active Directory
(Domain
Controller)
5
AD RMS
Server
1
2
4
6
Creador de
Contenido
Receptor de
Contenido
3

Prueba Funcional

Costo

Máquinas virtuales Windows

Basic | Standard

Serie A

A0 | A1 | A2 | A3 | A4

1 núcleo, 1,75 MB de RAM

2

MXN$1.347,78
MXN$1,812/hr

SQL Server

Basic | Standard

A0 | A1 | A2 | A3 | A4 SQL Server Standard

1 núcleo, 1,75 MB de RAM

1

MXN$4.316,51
MXN$5,802/hr

MXN$5.664,29/mes

Moneda:

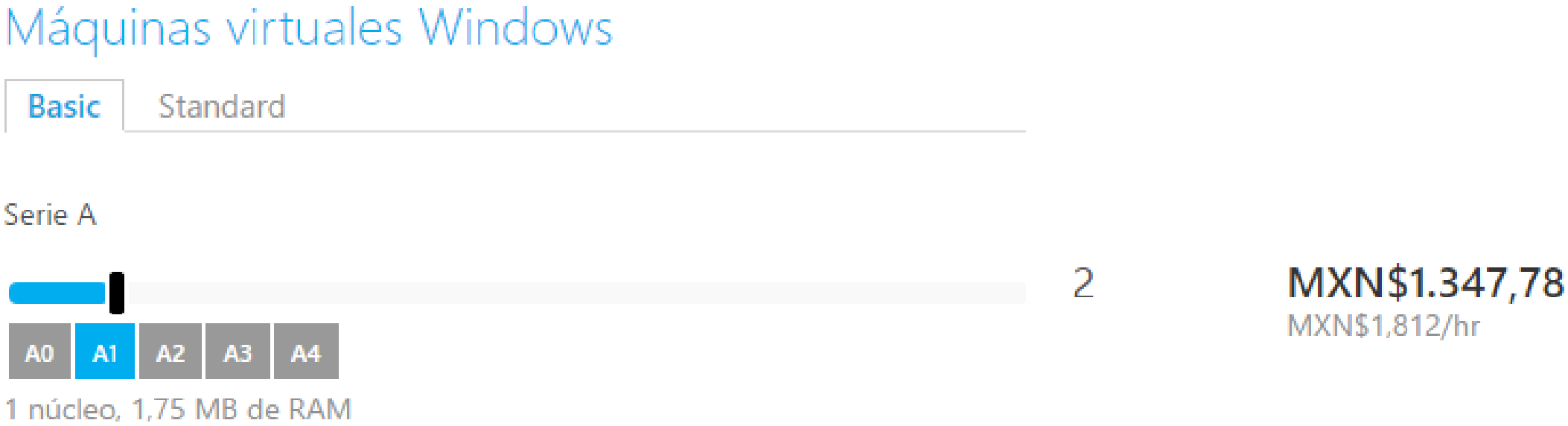
Peso mexicano (MXN$)

Precio estimado

Pago por uso

Coloquio de proyectos de Becarios en Seguridad Informática 3er

Costo


Máquinas virtuales Windows
Basic
Standard
Serie A
A0
A1
A2
A3
A4
1 núcleo, 1,75 MB de RAM
2
MXN$1.347,78
MXN$1,812/hr

Ventajas

Asignar permisos a múltiples usuarios una sola vez

Permite elegir el tipo de administración de cuentas

Diferentes permisos para diferentes usuarios

Bloquea capturas de pantalla

No permite múltiples sesiones para un usuario

Permite asignar permisos individuales

Alta disponibilidad

Limitantes

Es necesario un equipo con Windows (Vista o superior) y Office para su uso.

Requiere una relación de confianza con Microsoft para usar la aplicación móvil.

Precio

Requiere soluciones de terceros para protección de archivos PDF

Solo funciona con cuentas de dominio o cuentas de correo de Microsoft (hotmail, outlook, live)

Actualización de plantillas cada 7 días

Requiere conexión a Internet

Opciones de Crecimiento

- Implementar la infraestructura en equipos bajo el control de la CSI en un ambiente federado.
- Compatibilidad con la aplicación móvil de RMS.
- Añadir soporte para archivos PDF.
- Ofrecerlo como alternativa para proteger documentos en otras áreas de DGTIC, e incluso, otras dependencias de la UNAM.

Gracias

Ricardo Carmona

ricardo.carmona@cert.unam.mx

Lilia González

lilia.gonzalez@cert.unam.mx

56228169