Modelo de infraestructura común para el Servicio de correo electrónico para la Comunidad RedIRIS

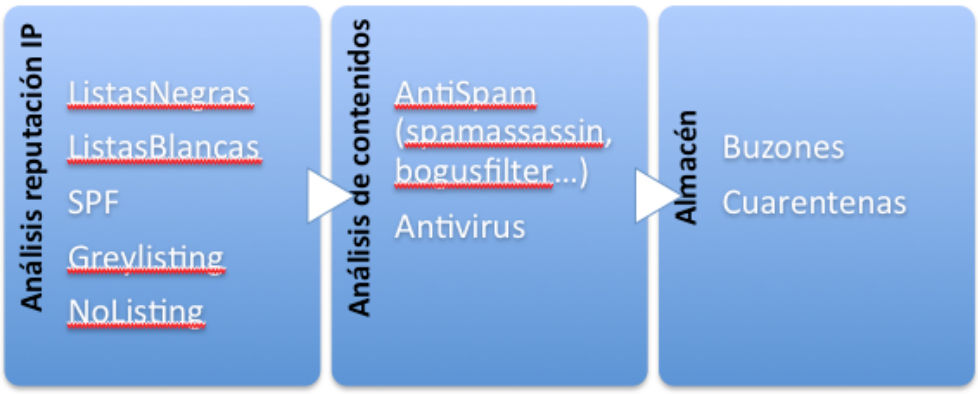
Octubre 2008

1. Situación actual

Actualmente el correo electrónico junto con el web y la red son servicios imprescindibles para las actividades diarias de las instituciones RedIRIS. El correo electrónico es una tecnología estable pero cuya gestión y recursos continua incrementándose en detrimento de los necesarios para abordar nuevos retos y servicios. La amplia implantación del correo electrónico provoca que sus infraestructura sufran continuos ataques para hacer llegar información no deseada al usuario final, complicando la selección del correo bueno del malo. Los actuales servicios de correo electrónico requieren de muchos recursos para sus correcto mantenimiento:

- Actualizaciones y reconfiguraciones de software
- Estudio, evaluación y configuración de nuevas tecnologías y/o productos que aparecen en el mercado.
- Licencias de Antivirus y Antispam
- Actualización y aumento de los recursos de hardware.

La mayor parte de los servicios de correo disponen de dos barreras defensivas donde se concentran todos los esfuerzos: **Análisis de la reputación** de IP que establece conexión SMTP con nuestro servidores y **análisis de contenidos**.



Esquema general de los servidores de correo en RedIRIS

Estos esfuerzos vienen produciendo resultados satisfactorios haciendo que el 85% aproximadamente del correo sea interceptado como basura. Actualmente el mayor problema en la lucha contra el spam es la contención del alto incremento de conexiones SMTP que sufren los servidores lo que implica un aumento de los recursos. En resumen se aumentan los recursos para bloquear grandes cantidades de basura y buscar los mensajes buenos, por el contrario

se mantienen o reducen los recursos para investigar y mejorar nuevos servicios o mejorar interfaces webmail , aumentar almacenamiento, dispositivos móviles etc. u otros servicios nuevos.

Por otro lado cada institución dispone de su propio servidor lo que implica una amplia dispersión de políticas de recepción y entrega de correo así como diferentes niveles de recursos necesarios para operar el servicio o evaluar e implantar nuevas soluciones tecnológicas de forma coherente.

Para ayudar a las instituciones RedIRIS viene ofreciendo servicios como RACE con auditorias y recomendaciones tecnológicas , así como otros que ayudan a mejorar la efectividad de la lucha contra el spam, como el Servicio IRISRBL y Lista Blanca.

2. Objetivos

El objetivo de esta propuesta es evaluar la posibilidad de ofrecer desde RedIRIS una plataforma unificada de correo con el objeto de:

- Reducir en las instituciones los recursos necesarios para frenar el spam
- Mejorar la efectividad de las medidas anti-spam
- Disponer de políticas comunes en RedIRIS que ayudarían a:
    - Definir una línea única y coherente de actuación frente al spam
    - Mejorar y simplificar el soporte
    - Mejorar la experiencia del usuario final ante incidencias relativas al filtrado de mensajes.
    - Ajustar los requisitos a los requerimientos de las instituciones
    - Disponer de una política de coherencia en el servicio de correo electrónico
- Ofrecer un modelo viable económicamente asi como de gestión y operación
- Definir un plataforma tecnológica avanzada cuya definición y experiencia sería pionera en Europa
- Establecer colaboración tecnológica con la industria española del sector

3. Modelo propuesto

3.1 Introducción

El modelo propuesto podría asemejarse al modelo típico de encaminamiento de red como podría ser el del backbone de RedIRIS. En este modelo existe una política de intercambio de rutas que permite a los routers asegurar el encaminamiento de paquetes o determinar la ruta que debe tomar un paquete de datos.

En el caso del correo electrónico, en lugar de paquetes se encaminarían piezas de correo electrónico. El router o relay es definido por el registro MX del correspondiente dominio. Actualmente cada institución dispone de su router o

relay final que gestiona las conexiones SMTP entrantes. El objetivo de esta propuesta es centralizar hardware especializado las conexiones SMTP en un modelo virtualizado lo que implicaría ahorrar costes a las instituciones. Este modelo permitiría a las instituciones gestionar determinados parámetros opcionales

El modelo de distribuido permitiría desplegar varias plataformas redundantes y balanceadas para disponer de la máxima disponibilidad en caso de fallo. En principio la idea sería un solo nodo centralizado y ubicado en RedIRIS. Un solo punto de fallo es algo que habría que evitar.

3.2. Requisitos

Los requisitos necesarios para desplegar un servicio de estas características

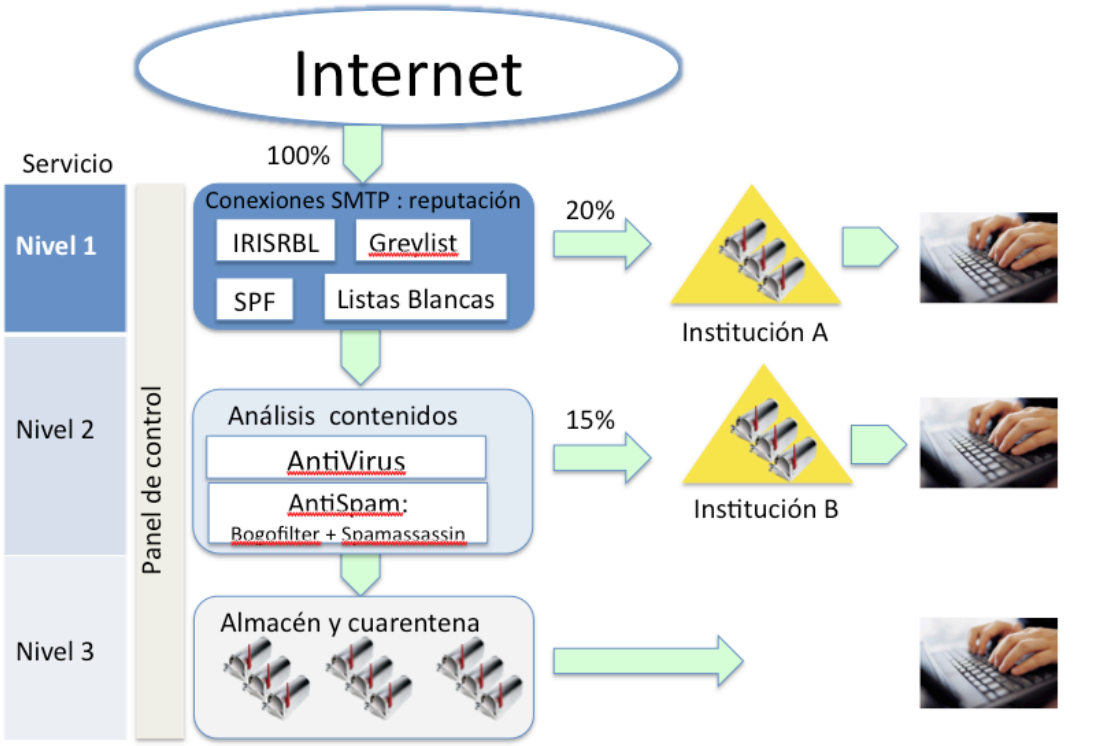
- Ubicado en las instalaciones de RedIRIS
- Hardware necesario para soportar gran carga de conexiones SMTP y tiempos de respuesta eficientes
- Módulos de reputación eficientes
- Módulos de análisis de contenidos (opcional)
- interface de gestión para cada institución.

- Integración y desarrollo por parte de alguna empresa
- Debe implicar una disminución de recursos económicos, hardware y software por parte de las instituciones asi como una mejora de la efectividad
- Que la plataforma sea igual o mas efectiva que las individuales
- Que se disponga de un servicio de atención a usuarios (CAU)
- Que se viable económicamente

3.3. Propuesta

El desarrollo de esta propuesta pasaría por la colaboración con alguna empresa como socio tecnológico para su desarrollo. En la propuesta no se ha tenido en cuenta un posible estudio previo de potenciales clientes que sería conveniente a la hora de colaborar con la Empresa.

La propuesta de los diferentes niveles de servicio intenta conjugar el desarrollo, recursos necesarios asi como viabilidad económica para el despliegue de de esta plataforma que sería incorporada como Servicio de RedIRIS a sus instituciones. La propuesta incluye tres niveles de servicio, el de Nivel 1 se pretende fuera gratuito para las instituciones interesadas, los otros niveles serían ofrecidos y facturados directamente a la institución interesada por la Empresa que actuara de socio tecnológico.



Propuesta de modelo de plataforma común de correo electrónico

Nota: los porcentajes % son aproximados

La propuesta consistiría de un Servicio con 3 niveles:

Servicio Nivel 1.

Funciones: El correo al dominio que solicita el servicio sería encaminado a esta plataforma ubicada en las instalaciones de RedIRIS . Analizaría las IPs origen que establecen conexión SMTP en función de unos criterios comunes en RedIRIS, tomaría acciones de bloquear, aceptar y encaminar los mensajes hacia el servidor de la institución donde se localizan los buzones.

Características: La plataforma estaría ubicada en las instalaciones y conectada a RedIRIS. Se ofrecería gratuitamente a las instituciones afiliadas que lo solicitaran. Sería necesario modificar el registro MX hacia el servidor de esta plataforma.

Modelo de desarrollo:

- RedIRIS dispondrá de las maquinas
- RedIRIS contrataría a una Empresa para:
  - Instalación, configuración, mantenimiento y optimización del software de los módulos de Análisis de reputación de IPs.
  - Desarrollo y puesta a punto de la interface de gestión
- La Empresa pondría un servicio de atención de incidentes exclusivamente para técnicos (postmaster)

Oferta del servicio:

- Gestión de flujos SMTP y análisis de reputación de IP para correo destinado al dominio declarado por la institución: IRISRBL, Greylist
- Panel de control vía web para analizar logs, estadísticas o parámetro de configuración
- Personalización de chequeos
- Soporte 8x5 a cargo de la Empresa
- Chequeo de existencia usuarios vía LDAP u otros
- Almacenamiento en caso de caída del servidor destino
- Cobertura de política homogénea para toda la comunidad RedIRIS: acciones, errores, tamaño máximo mensaje etc

Módulos para el análisis de reputación de IPs:

1. RBLs por definir: publicas o comerciales. Integración de RBL de RedIRIS (IRISRBL)
2. Integración de Listas Blancas de RedIRIS.
3. Greylisting opcional para el cliente
4. Chequeos SPF, DKIM

I**nterface de gestión** requiere:

1. Análisis de trazas de sus dominio
2. Posibilidad de seleccionar
   2.1 Greylist
   2.2 Marcado de mensajes

Servicio Nivel 2.

Funciones: Desarrollaría las funciones del **Servicio de Nivel 1** pero se añadiría un análisis de contenidos con escaneo de mensajes con módulos Antivirus y Antispam para después ser encaminado el mensaje al servidor de la institución y almacenado en sus buzones

Modelo de desarrollo:

La plataforma estaría ubicada en las instalaciones de RedIRIS. Este Servicio Nivel 2 sería de pago con **contrato y facturación** entre la Institución que lo desee y la Empresa. Seria gestionado por la Empresa.

Oferta del servicio:

- Las ofertadas en el Servicio de Nivel 1
- Escaneo de contenido de mensajes con varios sistemas Antivirus y Antispam
- Bloqueo y/o marcaje de mensajes interceptados. **No habría cuarentena**
- Soporte técnico a cargo de la Empresa

Servicio Nivel 3.

Funciones: Desarrollaría las funciones del Servicio de Nivel 2 añadiendo la posibilidad de **almacenamiento de buzones.**

Modelo de desarrollo:
La plataforma estaría ubicada en las instalaciones de RedIRIS. Este Servicio Nivel 3 sería de pago con **contrato y facturación** entre la Institución que lo desee y la Empresa. Seria gestionado por la Empresa.

Oferta del servicio:

- Las ofertadas en el Servicio de Nivel 2
- Almacenamiento de buzones
- Interface de acceso al correo para los usuarios
- Soporte técnico a cargo de la Empresa