

**RECOMENDACIONES SEGURIDAD
ANTI - MALWARE**



Política de Anti - Malware

Preparado para:



por:

Wilver Avendaño

RECOMENDACIONES SEGURIDAD ANTI - MALWARE



Tabla de Contenido

1.	Objetivo	3
2.	Descripción del Problema	3
3.	Recomendaciones SE	3

RECOMENDACIONES SEGURIDAD ANTI - MALWARE



1. **Objetivo**

Debido a la problemática que se tiene en las secretarías, debido a las reglas permisivas configuradas para su normal operación, se requiere implementar una política de seguridad que regule la utilización y uso indebido del acceso a Internet y en particular el manejo del Antivirus a nivel de correo

2. **Descripción del Problema**

Los equipos de las secretarías constantemente reportan problemas de contagio con Virus, Worms, Troyanos y demás Malware, lo cual genera pérdida de operatividad de la secretaria para diferentes servicios en Internet como correo, web, etc.

3. **Recomendaciones SE**

Para tratar de tener una red sana, libre de Malware (virus, Troyanos, Worms , etc), Global Crossing recomienda las siguientes acciones para que sean tomadas por cada SE, en caso que no lo estén aplicando.

Deberá ser norma de la secretaria:

1. **Programas automáticos**

Contar con una buena herramienta de anti malware (antivirus, antispyware, etc) la cual deberá ser actualizada constantemente para prevenir y eliminar las consecuencias de la acción de los virus informáticos. Los programas deben ser instalados por el área de Sistemas, en los equipos centralizados de procesamiento y en las estaciones de trabajo de modo residente para que estén activados durante su uso.

2. **Actualizaciones**

Se deben actualizar periódicamente las versiones de los programas Anti-Malware y dicha situación debe estar reflejada en los contratos con el proveedor.

4. **Archivos enviados y recibidos**

Los programas de Anti-Malware (Anti-Virus, Anti-Spyware, etc), deben permitir la detección de malware en archivos enviados y recibidos vía el servicio de correo electrónico y detección sobre aplicaciones HTTP, FTP, SMTP y POP3 desde otras redes de datos / internet.

RECOMENDACIONES SEGURIDAD ANTI - MALWARE



5. Otras Medidas Complementarias

- ✓ *No abrir correos de remitentes desconocidos*
- ✓ *No tratar de abrir archivos ejecutables que vengan anexos a correos*
- ✓ *Realizar escaneos de malware en los PC por lo menos una vez por semana.*
- ✓ *Tener una herramienta adicional de Anti-Malware, con la cual se debe realizar una verificación, de los PC de los usuarios, por lo menos una vez cada 6 meses*

Wilver Avendaño V.
Service Secure Specialist
Global Crossing