NO-09 PREVENCIÓN, DETECCIÓN Y ELIMINACIÓN DE MALWARE

1. Normatividad Relacionada

PO-05 Comunicaciones Electrónicas

PO-08 Normas, Procedimientos Operativos y Documentación

PO-11 Responsabilidad de los Servidores Públicos

2. Objetivo

Establecer los controles necesarios para la prevención, detección y eliminación de malware en los componentes tecnológicos de la UAEAC.

3. Alcance

Esta norma aplica a los usuarios de los componentes tecnológicos de la UAEAC.

4. Descripción

Prevención

- Los usuarios deben adoptar en forma permanente medidas preventivas para evitar la presencia de Malware en los computadores de la UAEAC y deben estar entrenados en el uso del software antimalware definido por la UAEAC. La Dirección de Informática es responsable del entrenamiento de los usuarios en el uso del software antimalware.

- Todos los usuarios deben estar alerta sobre el riesgo de malware que se transmiten a través de Internet, por correo electrónico, desde otro computador de la red o desde los dispositivos de almacenamiento extraíbles (USB, discos externos, teléfonos móviles, entre otros).

- Cuando se autorice la instalación de software de libre distribución, antes de ser instalado en los computadores o servidores de la UAEAC, debe ser revisado y certificado como libre de malware, por el servidor público Responsable del Componente Tecnológico.

- Todos los documentos recibidos a través de la red de datos de la UAEAC, deben ser revisados por el antimalware antes de ser abiertos o almacenados en los computadores.

- El servidor público Responsable del Componente Tecnológico será el único autorizado para descargar software desde Internet, dando cumplimiento a la normatividad establecida en el Modelo de Seguridad y Privacidad de la Información.

- La instalación de software en los computadores y servidores de la UAEAC solamente podrá ser realizada por el servidor público Responsable del Componente Tecnológico o por personal previamente autorizado por la Dirección de Informática.

- El software antimalware debe estar instalado en todos los servidores y computadores de la UAEAC y debe ser actualizado y distribuido de manera automática desde los servidores de red.

- Los servidores y computadores tendrán residente en memoria el antimalware seleccionado por la entidad y debe estar configurado de tal forma que se active cuando se encienden los computadores.

- Deben existir procedimientos y mecanismos para garantizar que el antimalware esté permanentemente actualizado, activo y configurado para realizar la detección y eliminación de malware.

- Los cambios a la configuración del antimalware son responsabilidad exclusiva del personal de Soporte Informático y ningún usuario debe intentar modificar dicha configuración.

- Cualquier inactivación temporal del software antimalware realizada por terceros para instalación de software en los servidores o computadores de la UAEAC debe ser reportada al Administrador del Antimalware.

- Los usuarios son responsables de la eliminación de archivos o mensajes de correo recibidos cuyo origen sea sospechoso o desconocido y asume la responsabilidad por las consecuencias que pueda ocasionar su apertura o ejecución. Los mensajes sospechosos o de origen desconocido no se deben abrir ni reenviar a otros usuarios, el usuario debe enviarlo como mensaje de correo adjunto a Línea-3000 con asunto “correo sospechoso”.

- En los computadores y servidores de la UAEAC únicamente debe estar instalado el antimalware autorizado por la Dirección de Informática, el cual cumple con los requerimientos técnicos y de seguridad. En casos estrictamente necesarios, se podrá instalar o ejecutar otro antivirus, previa autorización de la Dirección de Informática, con el fin de erradicar la presencia de malware.

Detección de Malware.

- Los usuarios de los componentes tecnológicos de la UAEAC deben reportar a Línea-3000 o al personal de Seguridad Informática la presencia de cualquier malware.

- Los usuarios de los componentes tecnológicos de la UAEAC deben conocer los procedimientos de detección y eliminación de virus informáticos.

- Todos los registros de detección de malware serán examinados por el Administrador del Antimalware con el fin de evitar reincidencias.

Eliminación de Malware.

- Cualquier computador o servidor en el que se detecte la presencia de malware, debe ser desconectado inmediatamente de la red de datos de la UAEAC y solo será puesto en servicio cuando el Administrador del Antimalware certifique que el malware ha sido eliminado.

- Cuando un malware no pueda ser eliminado, a pesar de haber aplicado los mecanismos disponibles para tal fin, se debe conformar un Comité de Decisión integrado por el Coordinador del Grupo Soporte Informático, el Administrador del Antimalware, el Coordinador del Grupo Seguridad de la Información y el responsable de Soporte Informático Línea-3000 quienes deben elaborar un plan de acción para atender el incidente y erradicar el malware.