CIRCULAR
UNA-DTIC-CIRC-012-2020

PARA: Personal Informático de Unidades Académicas, Vicerrectorías, Facultades, Centros y Sedes.

DE: Dirección de Tecnologías de la Información y la Comunicación (DTIC).

ASUNTO: *Apoyo para actualización de software no permitido, software dudoso, y sistemas operativos.*

FECHA: 16 de noviembre de 2020

Estimados señores y señoras:

En complemento a la circular **UNA-DTIC-CIRC-011-2020**, se solicita al personal informático de Unidades Académicas, Vicerrectorías, Centros y Sedes, el apoyo para la desinstalación de software no permitido, software dudoso, y actualización de sistemas operativos en los activos tecnológicos institucionales.

Como parte de las labores de mantenimiento y soporte técnico que habitualmente realizan y considerando que muchos funcionarios y funcionarias han traslado sus equipos informáticos institucionales para realizar teletrabajo desde sus hogares, se requiere el apoyo para desinstalar el software no permitido (ilegal), software dudoso (no soportado o con características insuficientes), así como para mantener instalado en los equipos computacionales un antivirus soportado, y el agente de seguridad de Kaspersky.

Por tal motivo se les solicita el apoyo para desinstalar el software no permitido y actualizar las computadoras de las diferentes instancias que ustedes apoyan, aplicando lo que a continuación se describe:

- Desinstalar Antivirus:
  - MCafee
  - Symantec
  - Malwarebytes
  - Cómodo Security
  - AVAST Software
  - 360 Security Center

Los antivirus soportados por la universidad son el Kaspersky Endpoint Security y el Windows Defender que forma parte integral del sistema operativo Microsoft Windows, por lo que debe desinstalarse cualquier otro antivirus como los indicados en la lista.

- Desinstalar las versiones de Ms-Office sin soporte:
  - MS-Office Enterprise 2007
  - MS-Office Standard 2007
  - MS-Office Standard 2010
  - MS-Office Standard 2013
  - MS-Office Professional Plus 2010 / 2013

Se recuerda que como parte del licenciamiento corporativo que la UNA mantiene con Microsoft, todos los funcionarios tienen acceso al beneficio de Office 365, el cual permite realizar la instalación de diferentes productos entre los cuales se incluye la versión más actualizada de la Suite ofimática (Microsoft Office), por lo cual, no deberían utilizarse versiones anteriores que puedan presentar problemas de seguridad o compatibilidad.

Se les recuerda que para acceder al Office 365 pueden utilizar el siguiente enlace, que puede ser compartido con los usuarios para que realicen la instalación de manera individual.

https://universidadnacional.atlassian.net/wiki/spaces/BDC/pages/82608383/Acceder+Herramientas+de+Microsoft+Office+365?src=search

- Desinstalar herramientas de soporte remoto como:
  - Team Viewer

La instalación de herramientas para el acceso remoto a Windows 10, puede ser realizada mediante la herramienta AnyDesk que está disponible para diferentes plataformas, por lo que se debe desinstalar otros aplicativos con funciones similares.

- Desinstalar herramientas de compresión de archivos
  - WinRAR
  - WinZip

Para la compresión de archivos la alternativa que se recomienda utilizar es 7 Zip.

- Desinstalar programas potencialmente peligrosos:
  - Ask Tool Bars
  - 搜狗高速□□器 8.5.10.31270 Sogou.com
  - Software firmado por “Los creadores” y “El Desaparecido”
  - Avg Secure Browser
  - Avast Secure Browser
  - Brave (*Brave* es un navegador web de código abierto basado en Chromium)
  - Ccleaner Browser
  - UsbFix

  Sobre este tipo de herramientas se recomienda desinstalarlas completamente, debe revisarse en el Panel de Control que ninguna de ellas se encuentra instalada.

- Desinstalar Otros Programas dudosos:
  - Windows Live Essentials
  - Ares, MEGAsync y BitTorrent
  - Amazon
  - Facebook (portal Gameroom para jugar en línea).
  - Ccleaner (Windows Defender marca a CCleaner como "software potencialmente no deseado".

  En el caso de Ccleaner se recomienda sustituir su uso por la herramienta Glary Utilities.
  En general estos aplicativos son obsoletos o representan un riesgo de seguridad para la institución por lo que deben desinstalarse.

Todos los equipos de cómputo de la institución (PC´s y portátiles) deben tener instalado el aplicativo denominado “Agente de Red de Kaspersky Security Center”, el cual es un componente de software (agente) que permite identificar el software instalado en los equipos y realizar tareas de mantenimiento y protección de manera remota. Este es un aplicativo complementario a la solución de antivirus institucional que debe ser instalado en los diferentes equipos computacionales de la institución.

Se aclara que el uso de este software no permite el acceso a los archivos o información de cada dispositivo y su propósito es mejorar los niveles de seguridad de la información para protegerlos ante diferentes amenazas informáticas.

Es responsabilidad del personal informático de cada unidad, colaborar con la instalación de este software en los diferentes equipos de sus instancias, para lo cual deben solicitar previamente mediante iTop un acceso tipo "VPN" que permita la instalación y configuración del agente en los dispositivos de los usuarios que no están conectados a la red institucional.

El manual de instalación de este aplicativo puede ser consultado en la siguiente dirección web: https://universidadnacional.atlassian.net/wiki/spaces/BDC/pages/616923137/C+mo+instalar+el+Antivirus+Kaspersky?src=search, cualquier consulta adicional puede realizarse mediante atención telefónica al 2562-6570, o con el equipo de soporte técnico del CGT, mediante sistema iTop.

Los instaladores del agente Kaspersky se encuentran ubicados en la siguiente dirección: ftp://ftp.una.ac.cr/Pc/Otros/Kaspersky/.

Atentamente,

DIRECCIÓN DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN

Signature not validated

Digitally signed by AXEL ARMANDO HERNANDEZ VARGAS (FIRMA)
Date: 2020.11.16 10:46:11 CST
Location: DTIC

Máster Axel Hernández Vargas
Director General

dms