CIRCULAR
UNA-R-CIRC-053- 2022
UNA-DTIC-CIRC-011-2022

FECHA: 24 de junio de 2022

PARA:
Vicerrectores(as)
Decanos(as)
Directores (as) de Unidades Académicas y Administrativas

ASUNTO: Cumplimiento Circular UNA-R-CIRC-034-2022 UNA-DTIC-CIRC-002-2022 y solicitud de información relacionada.

Estimados(as) señores(as):

Considerando la situación de emergencia nacional establecida mediante Decreto N°43542-MP-MICITT, publicado en el Alcance N°94 a la Gaceta N°86 del 11 de mayo del año en curso, mediante el cual se declara Estado de Emergencia Nacional en todo el Sector Público del Estado Costarricense, debido a los cibercrímenes acontecidos en las distintas instituciones del país, y en apoyo a las acciones que ha venido realizando la Universidad Nacional para fortalecer las capacidades de ciberseguridad de la plataforma tecnológica institucional, y en seguimiento a la circular UNA-R-CIRC-034-2022 - UNA-DTIC-CIRC-002-2022, del 25 de abril de 2022, en la que se solicita la implementación de acciones específicas para fortalecer la ciberseguridad y proteger los activos de información institucionales, se informa que de acuerdo con las herramientas de monitoreo, muestreos presenciales y plataformas de gestión de los activos tecnológicos, se ha identificado que dichas acciones no han sido implementadas de manera efectiva en las diferentes instancias universitarias.

Por lo anterior, y considerando la importancia que implica la implementación de estas acciones, así como los continuos ataques que recibe el país, **se instruye** a cada Vicerrectoría, Facultad, Centro, Sede y Biblioteca y Unidades Administrativas con personal informático a cargo, a implementar las siguientes acciones:

1. Realizar la instalación del software de seguridad institucional (Kaspersky), y activación del firewall de Windows o de Kaspersky.
2. Aplicar los parches de seguridad disponibles, al sistema operativo de computadoras (Windows Update), y dispositivos móbiles institucionales (tabletas).
3. Desactivación del protocolo RDP (compartir escritorio), en todas las computadoras institucionales.
4. **Completar el formulario adjunto,** considerando al menos la siguiente información relacionada a los activos institucionales en uso:

    a. Cantidad de computadoras, que cuentan con sistema operativo Windows 8 o anteriores a dicha versión. Para estos casos es necesario que se informe a la DTIC vía iTop el detalle del numero de activo, tipo de computadora (desktop o laptop) y responsable de cada activo, para valorar la posibilidad

de sustituir estos equipos de acuerdo con la disponibilidad institucional. Se debe utilizar el servicio de "**Soporte Técnico**" y la Subcategoria de "**Valoracion de equipo para solictar renovación**".

b. Cantidad de computadoras con Windows 10 o superior.
c. Cantidad de computadoras que se encuentran actualizadas (que se les aplica de forma continua las actualizaciones o parches de software y sistema operativo disponibles).
d. Cantidad de computadoras con software de seguridad institucional instalado, a saber Kaspersky Endpoint Security.
e. Cantidad de computadoras con software de Firewall activo (Windows firewall o Kaspersky).
f. Cantidad de computadoras con el protocolo RDP activo (compartir escritorio), si no se tiene una justificación, debe deshabilitarse.
g. Cantidad de tabletas o dispositivos móviles institucionales.

Se solicita **completar el formulario** por Vicerrectoría, Centro, Sede y Biblioteca y remitir la información relacionada, antes del **12 de agosto de 2022**. Esta información debe completarse con el **apoyo del personal informático** destacado en la Vicerrectoría, Facultad, Centro, Sede o Biblioteca, y comunicarse a la Rectoría con copia a la DTIC. La información será analizada en el Comité Estratégico de Tecnologías (CETI) para valorar las siguientes acciones.

Para las computadoras de uso personal que se conectan a la red institucional, se recomienda al personal informático, asesorar a los propietarios de estos equipos, en el procedimiento de actualización del sistema operativo, y de la solución nativa de antivirus (Windows Defender), de tal forma que estos equipos se mantengan actualizados y con el menor nivel de riesgo posible.

Agradecemos la colaboración y comprensión en la atención de estas medidas de seguridad que fortalecen la seguridad de la información y nos permiten protegernos ante los ataques que continuamente estamos enfrentando.

Como referencia técnica para realizar las acciones solicitadas, se comparten las siguientes guías técnicas:

- Deshabilitar RDP - https://universidadnacional.atlassian.net/wiki/spaces/BDC/pages/2669019137/Desactivar+protocolo+RDP+Remote+Desktop
- Actualizar sistema operativo (Windows, Android y MacOS) - https://universidadnacional.atlassian.net/wiki/spaces/BDC/pages/2613149697/Como+Actualizar+mi+Sistema+Operativo
- Instalación de Kaspersky - https://universidadnacional.atlassian.net/wiki/spaces/BDC/pages/616923137/C+mo+instalar+el+Antivirus+Kaspersky

Cualquier consulta adicional puede remitirse al correo dtic@una.ac.cr.

AdjuntoUNA-R-CIRC-034-2022_UNA-DTIC-CIRC-002-2022 - https://agd.una.ac.cr/share/s/rQM8dfpBTQ6974r9ZXqWTA

Formulario: https://docs.google.com/forms/d/e/1FAIpQLSdvRUM8ErvHo-91uEPdGsAE6LpYAFHgb8hrahFvdakh62vhzg/viewform?usp=sf_link

Atentamente,

Firmado por AXEL ARMANDO HERNANDEZ VARGAS (FIRMA)
PERSONA FISICA, CPF-01-0968-0694.
Fecha declarada: 24/06/2022 02:39 PM
Lugar: DTIC

Axel Hernández Vargas, M.Sc.
Director General DTIC

FRANCISCO JOSE GONZALEZ ALVARADO (FIRMA)
PERSONA FISICA, CPF-02-0451-0487.
Fecha declarada: 24/06/2022 04:35:06 PM
Razón: Rector
Lugar: UNA - Heredia

M.Ed. Francisco González Alvarado
Rector

C. Señores Consejo Universitario