



CIRCULAR

646243

Bogotá D.C., 1 de julio de 2021

Para: FUNCIONARIOS Y SERVIDORES PUBLICOS DEL INSTITUTO NACIONAL DE
CANCEROLOGÍA EMPRESA SOCIAL DEL ESTADO

Asunto: Aplicación de controles complementarios sobre usos de redes sociales, nubes de colaboración, almacenamiento y transferencias de archivos en la nube, y cierre de puertos de dispositivos de almacenamiento

En el marco de cumplimiento de la Norma técnica ISO 27001:2013; de las actividades de mejora continua registradas en el plan PMR-20-00009 producto de auditoria de seguridad de la información; en el desarrollo del plan de seguridad y privacidad de la información del INC GTI-P01-PL-01; y de las recomendaciones realizadas debido a la activación del Puesto de Mando Unificado (PMU CIBER) por parte de 07 entidades gubernamentales, en el marco del desarrollo de las protestas sociales que se están llevando a cabo desde el 28 de abril de 2021.

Me permito comunicar que a partir del martes 6 de julio de 2021 se empezarán a aplicar controles complementarios sobre uso de redes sociales, nubes de colaboración, correos electrónicos de tipo personal, almacenamiento en la nube de tipo personal, sitios de transferencia de archivos de gran volumen, y se producirá el cierre de puertos de dispositivos de almacenamiento externo en todos los equipos de cómputo de la entidad, los cuales fueron aprobados debidamente por cada una de las subdirecciones.

El manejo de excepciones sobre estos nuevos controles requiere de la justificación mediante formato GTI-P01-F-21 SOLICITUD DE EXCEPCIÓN DE CONTROLES, y de la evaluación y aprobación del mismo por parte del Subdirector General correspondiente y el Oficial de Seguridad de la Información. Les recordamos el uso obligatorio de las diferentes herramientas ofimáticas de uso corporativo que el INC a adquirido y desplegado con gran esfuerzo, y que deben consolidarse como las herramientas oficiales para realizar la comunicación, la colaboración, el almacenamiento seguro, la transferencia y compartido de información, entre las cuales encontramos:

Suite de ofimática Microsoft Office 365- Suite de Word, Excel, Power Point
Correo electrónico Outlook 365 - Correo institucional @cancer.gov.co
Microsoft One Drive - Almacenamiento y colaboración segura de archivos y documentos, backup y sincronización de documentos en Nube Privada Microsoft.

"El presente documento ha sido firmado electrónicamente para garantizar su plena validez jurídica y probatoria. El original del documento es generado en formato electrónico y su firma se pueden consultar en TMS. Toda impresión se entenderá como copia del mismo y debe hacerse sólo si es necesario."





Microsoft Teams - Nube de trabajo basado en Video llamada, Chat corporativo, y colaboración de los equipos de trabajo

Microsoft SharePoint –Colaboración en la nube por área, para la gestión documental, el trabajo en equipo, y la colaboración de información hacia otras entidades de manera segura.

Microsoft Forms – Creación y aplicación de Encuestas, formularios, cuestionarios personalizados y registros, con resultados exportables

Microsoft Sway: - Creación y elaboración de presentaciones web interactivas, compatibles en múltiples dispositivos.

Para aquellos funcionarios y colaboradores que requieran acceso temporal o justificado sobre alguno de los servicios restringidos de uso personal, se dispone de una red WIFI BYOD para conexión de dispositivos móviles, la cual se encuentra por seguridad totalmente aislada de los recursos de servidores, compartidas y equipos en la red del INC. Este acceso de conexión WIFI BYOD para dispositivos móviles debe ser justificado y autorizado vía correo electrónico por el Coordinador de Grupo Área correspondiente, y por la Coordinación del Grupo Hardware y Redes (jdgutierrez@cancer.gov.co , josorio@cancer.gov.co). Una vez autorizado el usuario debe llevar su equipo móvil a la mesa de ayuda para la conexión correspondiente, entregando la dirección MAC del dispositivo.

Antes de solicitar la conexión de su dispositivo personal en la red WIFI BYOD móvil, debe realizar el cumplimiento con los siguientes requisitos de seguridad:

1. Que el móvil cuente con cualquier antivirus instalado. En los mercados de aplicaciones móviles hay varias opciones gratuitas, ubique las de mejor puntuación.
2. El dispositivo móvil debe tener algún tipo de bloqueo configurado (PIN, patrón de bloqueo, biométrico, reconocimiento facial, otros)
3. El dispositivo móvil debe tener instaladas las últimas actualizaciones de su sistema operativo.
4. Debe tener configurado el borrado remoto en el dispositivo móvil, en caso de pérdida o robo de este.

Por último, les recordamos que el acceso de proveedores y visitantes del Instituto se realiza también en redes WIFI aisladas (WIFI INVITADOS) con conexión únicamente a internet, y que, en caso de requerir acceso a servicios corporativos de la red institucional, deben realizarlo mediante el servicio de VPN del INC.

Cualquier inquietud sobre los nuevos controles favor comunicarse por Microsoft Teams o telefónicamente a la Ext. 3710 - Carlos Andrés Guerrero / Oficial de seguridad de la información, o con la Mesa de ayuda ext. 7000

Atentamente,

"El presente documento ha sido firmado electrónicamente para garantizar su plena validez jurídica y probatoria. El original del documento es generado en formato electrónico y su firma se pueden consultar en TMS. Toda impresión se entenderá como copia del mismo y debe hacerse sólo si es necesario."





Al contestar por favor cite estos datos:
Radicado No. INT-CIR-00069-2021
2021-07-01 03:14:05 p.m.



Carolina Wiesner Ceballos
Directora General
DIRECCION GENERAL

Páginas: 3
Anexo:
Nombre anexos:

Elaboró: Yury Nathaly Celis Patiño - Auxiliar Administrativo
Revisó: Carlos Andres Guerrero Gonzalez - Profesional Especializado I
Revisó: Luis Eduardo Martinez Gonzalez - Coordinador Grupo Área Gestión de Tecnologías de Información
Revisó: Juan José Pérez Acevedo - Subdirector General de la Gestión Administrativa y Financiera

"El presente documento ha sido firmado electrónicamente para garantizar su plena validez jurídica y probatoria. El original del documento es generado en formato electrónico y su firma se pueden consultar en TMS. Toda impresión se entenderá como copia del mismo y debe hacerse sólo si es necesario."

NIT: 899.999.092-7
Calle 1ª # 9-85 · PBX: 3905012
www.cancer.gov.co
Bogotá D.C., Colombia

