



Al contestar por favor cite estos datos:
Radicado No. INT-MEMG-00052-2026
2026-05-27 01:21:44 p.m.

1142985

MEMORANDO

Fecha: Bogotá D.C., 27 de Mayo de 2026

Enviar A: Lista de distribución

Para: FUNCIONARIOS, SERVIDORES PÚBLICOS Y COLABORADORES DEL INSTITUTO NACIONAL DE CANCEROLOGÍA

De: **Subgerencia Corporativa**

Asunto: Protocolo para jornada de elecciones presidenciales

En el marco de la jornada de elecciones presidenciales del 31 de mayo de 2026, el INC ha activado un esquema de monitoreo extendido y disponibilidad reforzada de sus sistemas e infraestructura tecnológica. Este contexto electoral representa un período de mayor exposición a amenazas cibernéticas, dado el incremento documentado de ataques dirigidos contra entidades del Estado colombiano durante coyunturas políticas. En consecuencia, el equipo de seguridad de la información estará en operación continua durante la jornada dominical, con vigilancia permanente sobre los activos críticos de la entidad.

Con el propósito de complementar estas acciones institucionales y reducir la superficie de ataque del INC, se solicita a todo el personal acogerse al siguiente protocolo:

1. Todos los usuarios con equipo asignado del INC deben hacer un reinicio programado de su equipo al iniciar o finalizar su jornada laboral. Esto para permitir la ejecución de actualizaciones automáticas necesarias para la mejora del desempeño de la seguridad de los equipos durante la jornada de elecciones.
2. Los usuarios deben dejar apagados los equipos de cómputo, impresoras y dispositivos que no sean necesarios para la operación de la entidad desde el viernes 29 o sábado 30 de mayo, al finalizar su jornada laboral. Esto para reducir la superficie de ataque en el INC durante el desarrollo la jornada de elecciones.
3. Las aplicaciones y sistemas de información que no sean necesarios para la operación de la entidad deben apagarse desde el viernes 29 de mayo al finalizar jornada laboral. Esto para reducir la superficie de ataque en el INC durante el desarrollo la jornada de elecciones. Estos sistemas se deben encender nuevamente el día lunes 1 de junio a las 6am.
4. Todas las VPN con excepción de los administradores de plataformas y personal de soporte técnico, serán suspendidas desde viernes 29 de mayo al finalizar jornada laboral, y serán reactivadas a partir del lunes 1 de junio a las 7am. Las excepciones deben ser autorizadas por las Direcciones Técnicas y/o la Dirección General.

"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-MEMG-00052-2026
2026-05-27 01:21:44 p.m.

5. Para quienes trabajen en domicilio o estén de turno como jurados electorales, deben evitar conectarse a redes WiFi públicas o no confiables con equipos del INC durante la jornada.
6. No abrir correos de procedencia sospechosa o que no se han solicitado, no ejecutar adjuntos ni enlaces embebidos en el mensaje de correo electrónico. Evite abrir y replicar correos, adjuntos, links y mensajes de redes sociales de medios no verificados, relacionados con el tema electoral o afines durante y después de la jornada. Recuerde que los atacantes quieren que su víctima reaccione de manera impulsiva ante mensajes falsos, controvertidos o que apelan a generar alguna emoción.
7. Asegúrese de que su información de su equipo se encuentre sincronizada a su One drive o Microsoft Sharepoint. Si no sabe cómo realizarlo solicite capacitación y soporte a la mesa de ayuda.
8. Le recordamos a todos los usuarios el uso obligatorio de contraseñas robustas, largas y complejas, mantener activo el doble factor de autenticación MFA, al igual que cambiar sus contraseñas periódicamente.
9. En caso de detectar comportamiento inusual en su equipo, intentos de acceso no autorizados o recibir comunicaciones sospechosas, repórtelo de inmediato a la Mesa de Ayuda ext. 7000 o al Oficial de Seguridad de la información via Correo /Teams antes de tomar cualquier acción."

Requerimos a todos los líderes de oficinas y coordinadores de grupo hacer seguimiento de la ejecución del cumplimiento de estas de estas actividades con los integrantes de sus equipos de trabajo.

En caso de cualquier inquietud comunicarse con la Mesa de ayuda extensión 7000 o con Oficial de Seguridad de la información - extensión 3710, |correo: seguridaddigital@cancer.gov.co

Cordialmente,



Lia Margarita Alvarez Puente
Subgerente Corporativa

"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-MEMG-00052-2026
2026-05-27 01:21:44 p.m.

Páginas: 3
Anexos:
Nombre anexos:

Elaboró: Laura Daniela Lamprea Mateus - Auxiliar Administrativo - Grupo Área Gestión de la Tecnología y Sistemas
Revisó: Carlos Andres Guerrero Gonzalez - Profesional Especializado - Grupo Área Sistemas
Revisó: Luis Eduardo Martinez Gonzalez - Coordinador - Grupo Área Gestión de Tecnologías de Información

"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."