ACUERDO No. 16-CNR/2021. El Consejo Directivo del Centro Nacional de Registros, sobre lo tratado en el **punto número seis: Dirección de Tecnología. Subdivisión seis punto dos: Solicitud aprobación de Controles Generales de los Recursos Informáticos del CNR;** de la sesión ordinaria número dos, celebrada en forma virtual y presencial, a las siete horas con treinta minutos del veintiocho de enero de dos mil veintiuno; punto expuesto por el Director de Tecnología de la Información ingeniero Fernando Edward Calderón y el Oficial de Seguridad Informática, ingeniero Juan Rivas Ángel,

CONSIDERANDO:

I. Que se somete, para aprobación del Consejo Directivo, la Actualización de Documento Normativo Controles Generales de los Recursos Informáticos; constituyendo la base legal las **Normas Técnicas de Control Interno Específicas del CNR** (Diario Oficial Tomo No. 391, Número 84, jueves 5 de mayo de 2011); las que en su acápite "Definición de Políticas y Procedimientos de los Controles Generales y Específicos de los Sistemas Informáticos" que incluye al artículo 28, regula: El Consejo Directivo, aprobará la Política de Tecnología de Información, en la que se establecerán y documentarán las políticas y procedimientos sobre los controles generales y específicos aplicables a todos los sistemas informáticos. Será responsabilidad de la Dirección de Tecnología de Información, la formulación de dichas políticas y procedimientos; así como la aplicación de los referidos controles. Para la mitigación de riesgos informáticos, se tomará como base el código de buenas prácticas para la gestión de la seguridad de la información del estándar internacional ISO 27002. Igualmente, el **Reglamento para el Uso y Control de las Tecnologías de Información y Comunicación en las Entidades del Sector Público** (Decreto No. 24 de la Corte de Cuentas de la República) publicado en el Diario Oficial Tomo No. 404, Número 125, del 8 de julio de 2014, regla en su artículo 5 que la Unidad de TIC deberá proponer a la máxima autoridad la adopción de mejores prácticas (estándares abiertos) y controles para la gestión de las TIC, que se requiera para el logro de los objetivos.

II. Que los Controles Generales de los Recursos Informáticos se derivan de la Política de Tecnologías de Información y Telecomunicación, siendo aplicables a los procesos de negocio del CNR que son usuarios de tecnología. La actualización del documento se origina a raíz de los cambios en la infraestructura tecnológica institucional implementados a partir de 2017, la actualización de normativas internas de tecnología, la incorporación de controles de seguridad informática, las oportunidades de mejora y recomendaciones generadas por la Unidad de Auditoría Interna y los cambios en el marco regulatorio de tecnología (NTCI, el referido decreto 24 y la Ley Especial contra los de Delitos Informáticos y Conexos, entre otros.

III. Que se informa que *fueron actualizados* los siguientes capítulos: Normativa para la utilización de recursos y servicios informáticos, Normativa de seguridad para claves de acceso a los servicios informáticos del CNR, Normativa de uso del servicio de internet provisto por el CNR, Normativa del uso de correo electrónico institucional del CNR. Son *nuevos los capítulos siguientes*: Normativa de acceso remoto, Normativa de medios extraíbles. Los capítulos *que no sufren cambios* son: Normativa para el

Procedimiento para la Adquisición de Tecnología Informática, Sanciones, Divulgación y Vigencia. Con la incorporación de la Normativa de acceso remoto, se definen reglas y requisitos para conectarse a la red de datos del CNR desde cualquier computadora. Estas reglas y requisitos están diseñados para minimizar la posible exposición al CNR por daños que puedan resultar del uso no autorizado de los recursos del CNR; los daños incluyen la pérdida de datos sensibles o confidenciales de la institución, propiedad intelectual, daños a la imagen pública y daños a los sistemas internos críticos del CNR. De igual importancia es señalar que la regulación de la Normativa de medios extraíbles, se tiene: Normar el uso de dispositivos extraíbles para minimizar el riesgo de pérdida o exposición de información sensible mantenida por el CNR y reducir el riesgo de adquirir infecciones de malware en equipos informáticos.

IV. Que los artículos que se actualizan dentro del capítulo I denominado Normativa para la utilización de recursos y servicios informáticos, se tienen: El artículo 3 Uso de equipo, artículo 4 Control de computadoras portátiles, artículo 5 Acceso a la información, artículo 6 Uso de software. Las disposiciones actualizadas, dentro del Capítulo II denominado: Normativa de seguridad para claves de acceso a los servicios informáticos del CNR, se tiene: El artículo 11 Creación de claves de acceso, artículo 12 Cambio de contraseñas, artículo 13 Protección de la contraseña, artículo 14 Directrices de construcción de contraseñas, artículo 15 Mantenimiento de claves de acceso. Al igual, en el capítulo III llamado: Normativa de uso del servicio de internet provisto por el CNR, se actualizaron los artículos: 18 Uso de recursos, 19 Uso permitido, 20 Prohibiciones, 21 De la administración y monitoreo. Dentro del capítulo IV, denominado: Normativa de uso de correo electrónico institucional del CNR, se actualizaron los artículos: 22 Objeto, 24 Uso del correo electrónico, 25 Prohibiciones, 27 Excepciones.

En razón a lo expuesto, conforme a la normativa relacionada solicita al Consejo Directivo: La aprobación de la actualización del Documento Normativo Controles Generales de los Recursos Informáticos.

Por tanto, el Consejo Directivo, conforme a lo explicado y a las normativas relacionadas:

ACUERDA: I) Aprobar la actualización del Documento Normativo Controles Generales de los Recursos Informáticos. **II) Comuníquese**. Expedido en San Salvador, dos de febrero de dos mil veintiuno.

Licenciada Tanya Elizabeth Cortez Ruiz

Secretaria del Consejo Directivo

CENTRO NACIONAL DE REGISTROS - SECRETARIO DE CONSEJO DIRECTIVO - EL SALVADOR, C.A.