MINISTERIO CULTURA Y JUVENTUD
DIRECCIÓN GENERAL DEL ARCHIVO NACIONAL

Resolución CNSED-01-2022

Comisión Nacional de Selección y Eliminación de Documentos. San José a las trece horas con treinta minutos del seis de mayo del dos mil veintidós.

CONSIDERANDO QUE:

1º—De conformidad con el artículo 2 de la Ley N° 7202, Ley del Sistema Nacional de Archivos, esta resolución es de aplicación para los órganos del Sistema Nacional de Archivos y de los Archivos de los poderes Legislativo, Judicial y Ejecutivo, y de los demás entes públicos, cada uno con personalidad jurídica y capacidad de derecho público y privado.

2º—El artículo 3 de la ley supra citada establece que todos los documentos con valor científico cultural son bienes muebles y forman parte del patrimonio científico cultural de Costa Rica; y que la determinación del valor científico-cultural de los documentos corresponderá a la Comisión Nacional de Selección y Eliminación de Documentos.

3º—El artículo 31 de la Ley N° 7202, establece que la Comisión Nacional de Selección y Eliminación de Documentos, en adelante CNSED, es el Órgano de la Dirección General del Archivo Nacional, encargado de dictar las normas sobre selección y eliminación de documentos, de acuerdo con su valor científico cultural.

4º—El artículo 35 de la Ley N° 7202 establece que todas las instituciones a que se refiere el artículo 2° de esa misma ley, incluida la Dirección General del Archivo Nacional, estarán obligadas a solicitar el criterio de la CNSED, cada vez que necesiten eliminar algún tipo documental. También deberán considerar las resoluciones que al respecto emita la Comisión Nacional, las que serán comunicadas por escrito, por medio del Director General del Archivo Nacional.

5º—El artículo 10 del Reglamento Ejecutivo a la Ley del Sistema Nacional de Archivos, dado por Decreto N° 40554-C de 29 de junio de 2017, dispone que una de las funciones de la CNSED es dictar normas sobre valoración de los documentos que producen las instituciones mencionadas en el artículo 2 de la Ley N°7202, sean las instituciones que forman parte del Sistema Nacional de Archivos.

6º—El artículo 24 del Reglamento Ejecutivo de cita, establece que las entidades productoras podrán hacer sus consultas a través de la tabla de plazos de conservación, valoraciones parciales o cualquier otro instrumento que la CNSED determine. Asimismo, establece que las instituciones consultantes pueden eliminar los tipos o series

www.archivonacional.go.cr
archivonacional@dgan.go.cr
Tel: (506) 2283-1400
Fax: (506) 2234-7312
Curridabat, 900 mts sur y
150 mts oeste de Plaza del Sol

documentales que no posean valor científico cultural, una vez que caduque su vigencia administrativa y legal, sin consultar nuevamente a la CNSED.

7º—El artículo 26 del Reglamento Ejecutivo a la Ley N° 7202, dispone que las tablas de plazos de conservación, deben someterse a una revisión, tanto del Cised como de la CNSED, cuando se presente alguna de las siguientes circunstancias: a- Producción de nuevos tipos o series documentales. b- Cambios sustanciales en las funciones de las unidades que conforman la estructura organizativa. c- Cambios en la estructura orgánica del ente productor. d- Variaciones en los soportes de la información o de los plazos de vigencia administrativa y legal de los tipos o series documentales que cuentan con declaratoria de valor científico cultural. e- Cuando el Cised lo considere necesario.

8°—En uso de las facultades conferidas en los artículos 140 incisos 3) y 18) y 146 de la Constitución Política; artículos 25 inciso 1) y 28 inciso 2.b), 99 y 100 de la Ley N° 6227, “Ley General de la Administración Pública”, publicada en el En el Alcance n° 90 al Diario Oficial La Gaceta nº 102 del 30 de mayo de 1978; artículos 4 y 100 de la Ley N° 7169, del 26 de junio de 1990, “Ley de Promoción del Desarrollo Científico y Tecnológico”, publicada en el Alcance n° 23 al Diario Oficial La Gaceta n° 144 del 01 de agosto de 1990 y sus reformas; artículo 281 de la Ley 7594, del 10 de abril de 1996, “Código Procesal Penal”, publicado en el Alcance n° 31 al Diario Oficial La Gaceta n° 106 del 04 de junio de 1996 y el Decreto N.º 37052-MICIT, del 9 de marzo del 2012, “Crea Centro de Respuesta de incidentes de Seguridad Informática CSIRTCR”, publicado en el Diario Oficial La Gaceta Nº 72 del 13 de abril del 2012.

9°—En La Gaceta n° 78 del 29 de abril del 2022 se publicó la Directriz n° 133-MP-MICITT “Dirigida a la Administración Pública Central y Descentralizada sobre las mejoras en materia de ciberseguridad para sector público del Estado”

10º—Desde el 18 de abril de 2022, varios sistemas operados por las instituciones gubernamentales de Costa Rica fueron atacados con un ataque de “ransomware” en instituciones como la Caja Costarricense de Seguro Social (CCSS), el Ministerio de Hacienda y el Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones (Micitt), la Junta Administrativa del Servicio Eléctrico de Cartago (Jasec), entre otras; a fin de extraer vulnerabilidades del sistema de explotación de datos confidenciales con amenaza de atacar a las grandes empresas de Costa Rica. Estos eventos interrumpieron sistemas operativos, incluida la infraestructura crítica, afectando seriamente el servicio público de las instituciones afectadas.

11º—La Directriz N° 133- MP-MICITT obliga a todos los organismos gubernamentales a informar al Centro de Respuesta de Incidentes de Seguridad Informática (CSIRT-CR) de Costa Rica sobre los incidentes que ocurran en sus instituciones que afecten la confidencialidad, disponibilidad e integridad de servicios disponibles al público. Además, se ordena a todas las agencias cambiar contraseñas, deshabilitar servicios y puertos de

red no necesarios y monitorear la infraestructura de red. Se establece el coordinador de la ciberseguridad nacional que se refiere a ciberseguridad y seguridad de la información.

Por lo tanto,

Con base en las facultades que le confieren los artículos 31 y 35 de la Ley del Sistema Nacional de Archivos y los artículos 10 y 24 de su Reglamento Ejecutivo, la Comisión Nacional de Selección y Eliminación de Documentos, mediante acuerdo 12, tomado en la sesión 13-2022 de 06 de mayo de 2022, acordó emitir la siguiente norma:

01.2022 Declarar con valor científico cultural el 100% de la producción de documentos, en las instituciones que conforman el Sistema Nacional de Archivos (SNA) y que estén relacionados con ciberseguridad y la seguridad de la información, de todas aquellas acciones que se hayan tomado, para restablecer sistemas que hayan sido vulnerados y atacados, así como de los daños e impacto que esto ha ocasionado; independientemente del productor, soporte, la clase y tipo de documento que se produzca, custodie o reciba relacionado con este trascendental tema para Costa Rica y el mundo, por las siguientes razones:

a) La protección de los datos y los sistemas, a fin de que se reduzca la probabilidad de que ocurran ataques cibernéticos, minimizando además, el impacto ocasionado en las instituciones que conforman el SNA, cuando ocurran contingencias derivadas de ataques deliberados y que pongan en riesgo los documentos patrimoniales del país.

b) El enfoque de gestión de riesgos integrado en todas las instituciones públicas que ayuda a garantizar que la tecnología, los sistemas y la información estén protegidos de la manera más adecuada.

c) El análisis de tecnologías, análisis en seguridad y de riesgos existentes ante la vulneración de sistemas, y como impactaría un ciberataque en las organizaciones, son necesarios para crear una cultura en las organizaciones, dirigida hacia el entendimiento y el desarrollo de una seguridad cibernética positiva, que permita adoptar una cultura de integridad centrada en el compromiso y la capacitación continua, situando no solo a los sistemas como eje central de la estrategia de seguridad, sino también a las personas. Desarrollo, implementación y controles sobre políticas relacionadas con la ciberseguridad y la seguridad de la información.

d) Asegurarse de que los datos, sistemas y servicios estén protegidos contra el acceso, la modificación o la eliminación no autorizada, lo que implica garantizar que los datos estén protegidos en reposo, en uso, en tránsito y al final de su vida útil; para lo cual se requiere de controles robustos de autenticación y autorización de usuarios; la colaboración con proveedores y asociados; asegurar que las interfaces que permiten el acceso a datos confidenciales estén bien definidas y expongan solo la funcionalidad necesaria para reducir la oportunidad de que un atacante abuse de ellos; y que las

medidas de seguridad esenciales y relevantes, deben incluir el mantenimiento de copias de seguridad fuera de línea, aisladas y actualizadas de tal manera que se garantice la restauración de manera segura.

e) El monitoreo de seguridad para accesos de registro a datos, consultas inusuales, comportamiento inusual del sistema, intentos de exportación masiva de datos y acceso administrativo ayuda a detectar posibles compromisos y eventos que podrían considerarse un incidente de seguridad.

f) Un enfoque sistemático y disciplinado para evaluar y mejorar la eficacia de los procesos de gestión, control y gobierno de riesgos.

g) Arquitectura y configuración sana de sistemas que garanticen que la seguridad cibernética robusta, esté integrada en los sistemas y servicios desde el principio, y que esos sistemas y servicios puedan mantenerse y actualizarse para adaptarse de manera efectiva a las amenazas y riesgos emergentes.

h) Evaluación de sistemas, mantenimiento y gestión de vulnerabilidades; mediante la revisión periódica, para garantizar que todos los sistemas funcionen correctamente y cumplan sus objetivos a lo largo de su ciclo de vida.

i) Los incidentes cibernéticos pueden tener un grave efecto en las organizaciones, en términos de costos, productividad, continuidad de negocio y reputación. Sin embargo, una buena gestión de incidentes ayudará a reducir el impacto ocasionado cuando sucedan. Contar con la capacidad para detectar y responder rápidamente a las contingencias que se presenten, ayudará a minimizan daños, que de otro modo serían irreversibles y que comprometerían a las organizaciones y a su capacidad operativa. Un plan bien elaborado y desarrollado, ayuda a tomar decisiones correctas y fortalece la comunicación en toda la organización, ante un incidente real. Es necesario extraer lecciones aprendidas, identificar brechas y analizar la capacidad de respuesta ante un futuro que se presenta incierto, con respecto a los ciberataques cada vez más presentes y frecuentes en el mundo.

j) Desarrollo e implementación de políticas y prácticas de seguridad de datos, ciberseguridad y políticas relacionadas con la seguridad de la información. Las políticas relacionadas con la seguridad de la información generalmente tienen tres categorías: política de seguridad de toda la organización, una política de seguridad específica del problema y una política de seguridad específica del sistema. Las políticas cubren las responsabilidades de seguridad, detallan la estructura de la seguridad de la información, el uso adecuado de la tecnología como el correo electrónico, Internet, dispositivos portátiles, almacenamiento en la nube, así como los procedimientos utilizados para la configuración y el mantenimiento de los sistemas.

k) Proteger las instituciones y los sistemas gubernamentales, es una tarea incuestionable, que requiere recursos y capacidad para implementar soluciones técnicas preventivas y

paliativas; es evidente por los hechos acaecidos recientemente, que enfrentamos retos, que trascienden a las necesidades particulares de cada una de las organizaciones, y que demandan del desarrollo y puesta en marcha de acciones colectivas. Es imperativo entender que, una eficiente seguridad de la información en las organizaciones, garantizará una mejor protección de los documentos en todas las instituciones que conforman el SNA. ~~L~~a acción dedicada e integral de las instituciones, con respecto a la seguridad de la información, es necesaria y debería ocupar una posición prioritaria, en la estrategia de negocio de las organizaciones.

Cabe señalar que los documentos declarados con valor científico cultural, forman parte del patrimonio cultural de Costa Rica, son de interés público y deben ser custodiados en los diversos archivos administrativos públicos del país; posteriormente, una vez cumplidos los plazos de remisión, deberán ser transferidos a la Dirección General del Archivo Nacional, donde se conservarán de forma permanente, de acuerdo con los artículos 3, 4 y 5 de Ley N° 7202.

La presente norma rige a partir de su publicación en el Diario Oficial La Gaceta.

Comuníquese.

Susana Sanz Rodríguez-Palmero

Presidente