2023-04-20
0012-258-2023

Señores y Señoras
Junta Directiva
Radiográfica Costarricense S.A.

Señores y Señoras
Consejo de Administración
Compañía Nacional de Fuerza y Luz S.A.

Señores y Señora
Junta Directiva
Gestión de Cobro Grupo ICE S.A.

Sr. Mauricio Barrantes Quesada
Gerente General
Radiográfica Costarricense S.A.

Sr. Christian Gould Ávalos
Gerente General
Gestión de Cobro Grupo ICE S.A.

Sr. José Mario Jara Castro
Gerente General
Compañía Nacional de Fuerza y Luz S.A.

Estimados (as) señores (as):

Asunto: Política Corporativa de Ciberseguridad

Les transcribo el acuerdo emitido por el Consejo Directivo en el artículo 4 del Capítulo III de la Sesión 6569 del 18 de abril del 2023, que textualmente indica:

***"CONSIDERANDO QUE:***

1. *La Estrategia Nacional de Ciberseguridad 2017 establece que las Tecnologías de Información y Comunicación son consideradas herramientas invaluables para el desarrollo del país, lo cual se evidencia en el incremento de los índices de acceso, uso y apropiación de estas. Es imperativo contar con estrategias de ciberseguridad que contemplen las medidas de control que se deben implementar para la protección de las TIC y la información.*

2. *El Poder Ejecutivo, mediante la Directriz 133-MP-MICITT emitida el 21 de abril del 2022, estableció la obligación de ese poder, a través del MICITT de apoyar los programas de transformación y modernización del sector estatal y establecer estrategias relacionadas con la seguridad en las Tecnologías de la Información y la Comunicación en el ámbito del Sector Público costarricense, con el objetivo de alcanzar mayores niveles de eficiencia en los servicios del Estado, contribuir a crear una infraestructura de las tecnologías de la información y la comunicación que potencien al sector productivo nacional y procurar las medidas necesarias para establecer las mejores prácticas y lineamientos en pro de mejorar la ciberseguridad nacional.*

3. *El Protocolo para el Desarrollo de las Acciones que se deben Implementar ante una Amenaza de un Ataque a la Ciberseguridad Nacional", emitido por el MICITT el 06 de mayo del 2022, establece las responsabilidades de las*

Teléfono 2000-7217
Fax 2003-0200
tgonzalez@ice.go.cr

*diferentes instancias involucradas en esta materia y las líneas de acción generales construidas a partir del ente rector y de las instituciones participantes, orientadas a salvaguardar la integridad de la información. La aplicación de este documento va dirigido a la Administración Pública Central, la Administración Pública Descentralizada, las empresas del Sector Público, la Sociedad Civil y al ente rector.*

4. *El Poder Ejecutivo, el 8 de mayo del 2022, mediante el decreto MP-DMP-DVA-DG-CI-2022-0002/Decreto de Emergencia Nacional 43542-MP-MICITT) declaró estado de emergencia nacional debido a los ataques cibernéticos por la necesidad y urgencia que requieren las acciones para contrarrestar el alcance e impacto de los ataques realizados por el grupo cibercriminal Conti, dicha declaratoria permitió gestionar, por la vía de excepción, las acciones y la asignación de los recursos necesarios para atender la emergencia, de conformidad con el artículo 180 de la Constitución Política.*

5. *La Ley 8292 General de Control Interno regula la obligatoriedad de establecer un sistema de control Interno, que debe, entre otros fines, proporcionar seguridad para proteger el patrimonio público y garantizar la confiabilidad y oportunidad de la información, lo cual implica la adopción de medidas técnicas y administrativas adecuadas para preservar la seguridad de la información.*

6. *El artículo 16 de la citada ley, establece la obligación de los entes y órganos de contar con sistemas de información que permitan una gestión documental en el desarrollo de sus actividades, que prevengan cualquier desvío en los objetivos trazados y que estén relacionados con la gestión de la información, en la que deberán contemplarse las bases de datos corporativas y las demás aplicaciones informáticas, las cuales se constituyen en importantes fuentes de la información registrada.*

7. *Las Normas de Control Interno para el Sector Público (N-2-2009-CO-DFOE), en su Capítulo V establecen las regulaciones aplicables al control de los sistemas de información. En el ítem 5.8, dispone que el jerarca y los titulares subordinados, según sus competencias, deben disponer los controles pertinentes para que los sistemas de información garanticen razonablemente la calidad de la información y de la comunicación, la seguridad y una clara asignación de responsabilidades y administración de los niveles de acceso a la información y datos sensibles, así como la garantía de confidencialidad de la información que ostente ese carácter.*

8. *De conformidad con la legislación y la normativa asociada la Institución tiene el deber de disponer de un sistema que garantice la seguridad de la información empresarial mediante la implementación de políticas de*

*acatamiento obligatorio y mecanismos de control, para todo funcionario y trabajador del ICE y sus Empresas, así como para los clientes y terceros.*

9. *El Comité Corporativo, en el artículo 4, inciso a) de la Sesión 6-2022 del 15 de junio del 2022, acordó solicitar a la entonces Gerencia de Transformación Tecnológica, actual Gerencia Tecnología y Servicios Digitales, que en conjunto con la División de Estrategia, trabajara en una Política de Ciberseguridad Corporativa, que promoviera la implementación de mecanismos de seguridad, que garanticen la confidencialidad, integridad, disponibilidad, autenticidad y confiabilidad de la información, tanto en los sistemas utilizados por funcionarios y trabajadores como por las operaciones gestionadas por terceros que prestan servicios. Asimismo, acordó que dicha política incluyera las consecuencias por incumplimiento a la normativa asociada a todas las áreas de Ciberseguridad.*

10. *La División de Estrategia, mediante carta 503-043-2023 del 28 de febrero del 2023, solicitó a las gerencias generales de las empresas del ICE designar representantes para conformar un equipo multidisciplinario a nivel corporativo para elaborar la Política Corporativa de Ciberseguridad. Este equipo elaboró la propuesta y se presentó en la sesión del Comité Corporativo del 17 de marzo del 2023.*

11. *El Comité Corporativo en el artículo 7, incisos a) y b) de la Sesión 17-2023 del 17 de marzo del 2023, conoció la Política Corporativa de Ciberseguridad, y solicitó al equipo técnico afinar el propósito del documento. Asimismo, estableció que la citada política debía ser elevada al Consejo Directivo en un plazo de 15 días naturales. El Comité Técnico conformado al efecto afinó el propósito del documento, según la indicación realizada por el Comité Corporativo.*

12. *La División Jurídica, mediante carta 261-110-2023 del 28 de marzo del 2023, emitió criterio legal sobre la Política Corporativa de Ciberseguridad, e indicó no tener observaciones legales sobre el documento. Asimismo, indicó que conforme con los roles definidos en el Reglamento Corporativo de Organización Sección II, artículo 7, es potestad del Consejo Directivo establecer el direccionamiento estratégico, control corporativo, la gestión de riesgos, la solidez financiera y el modelo de Gobierno Corporativo del ICE y sus empresas, mediante políticas, lineamientos, reglamentos y directrices, entre otros.*

13. *El Reglamento Corporativo de Organización en el artículo 8 inciso 11) establece que corresponde al Consejo Directivo aprobar las políticas corporativas.*

14. *La Estrategia Corporativa 2023-2027 en el apartado Entorno y Macrotendencias de los Negocios establece como parte de los cambios que se deben adoptar en la gestión empresarial, la necesidad de fortalecer la ciberseguridad, asimismo, en el objetivo estratégico 7 se establece consolidar al Grupo ICE como líder de la transformación digital y ciberseguridad.*

15. *La Presidencia Ejecutiva somete a valoración y aprobación del Consejo Directivo la Política Corporativa de Ciberseguridad.*

***POR TANTO, POR UNANIMIDAD DE LOS PRESENTES ACUERDA:***

1. *Aprobar la siguiente Política Corporativa de Ciberseguridad, cuyo texto se detalla a continuación.*

***"Política Corporativa de Ciberseguridad"***

*1* ***PROPÓSITO***

*El ICE y sus Empresas establecen esta Política Corporativa de Ciberseguridad, con el fin de aplicar acciones de ciberseguridad alineadas a la estrategia corporativa, modelos y controles cibernéticos seguros, de acuerdo con las directrices y normativas de cada una de las Empresas, para la protección de la información interna y la información personal entregada por los clientes. De igual manera, la protección de las infraestructuras que soportan los datos, en pro de garantizar un entorno informático seguro y así contar con un alto nivel de madurez en ciberseguridad para responder a las distintas necesidades y amenazas asociadas.*

*Según la visión estratégica, se ha definido que la gestión corporativa de ciberseguridad para el ICE y sus empresas se basan en 3 principios clave; esto según marcos de referencias y mejores prácticas en cuanto a redes de tecnologías de información IT y redes operativas OT; dichos principios son, sin importar el orden:*

- *Confidencialidad*
- *Integridad*
- *Disponibilidad*

*2* ***ALCANCE***

*Este documento es de acatamiento obligatorio para todo el personal del ICE y sus Empresas, de acuerdo con los roles y áreas respectivas.*

## 3 DOCUMENTOS APLICABLES

| Código | Título |
|---|---|
| *Ley 8292* | *Ley General de control Interno* |
| *Ley 8454* | *Ley de certificados firmas, digitales y documentos electrónicos* |
| *Ley 8642* | *Ley General de Telecomunicaciones* |
| *Ley 8660* | *Ley de Fortalecimiento y Modernización de las Entidades Públicas del Sector Telecomunicaciones. Art. 35* |
| *Ley 8968* | *Ley de Protección de la Persona frente al Tratamiento de sus Datos Personales* |
| *Ley 7975* | *Ley de Información no Divulgada* |
| *Directriz 133-MP-MICITT* | *Dirigida a la Administración Pública Central y Descentralizada sobre las mejoras en materia de Ciberseguridad para el Sector Público del Estado.* |
| *NA* | *Protocolo para el desarrollo de las acciones que se deben implementar ante una amenaza de un ataque a la ciberseguridad nacional, de fecha de 06 de mayo del 2022.* |
| *NA* | *Estrategia Nacional de Ciberseguridad Costa Rica 2017-2021. (ciberseguridad política gubernamental Costa Rica 2. Seguridad en computadoras 3. Redes de computadoras - medidas de seguridad 4. Tecnología de información Medidas de Seguridad)* |
| *NA* | *Normas técnicas para la gestión y control de las Tecnologías de Información MICITT* |
| *36.00.001.2009* | ** Reglamento para la utilización de recursos de usuario final: hardware, software y servicios de comunicación* |
| *38.04.001.2008* | **Política Empresarial de Seguridad de la Información* |
| *38.00.002.2013* | *Política Corporativa de Confidencialidad de la Información* |
| *38.00.002.2016* | **Lineamientos de Seguridad de la Información* |
| *NA* | ***Política de Seguridad de la Información de la CNFL* |
| *NA* | ***Directriz para la asignación de roles y responsabilidades en la gestión de seguridad de la información* |
| *DGP-PT-001* | **** Política de Seguridad de la Información de RACSA* |
| *DGP-LN-001* | **** Lineamiento de Uso de Recursos Informáticos de RACSA* |

**Normativa aplicable únicamente al ICE.*
***Normativa aplicable únicamente al CNFL.*
**** Normativa aplicable únicamente a RACSA.*

## *4 TÉRMINOS, ABREVIATURAS Y SIGLAS*

*Ataque Informático: Es toda aquella conducta abusiva en la cual se hace un uso malintencionado de los sistemas informáticos, con el fin de provocar un perjuicio a la organización de manera directa con dicha conducta o juntamente con otras acciones delictivas, encaminadas a vulnerar un bien jurídico tutelado penalmente.*

*Activo de información: Por Activo se entiende cualquier componente (sea humano, tecnológico, software, etc.) que sustenta uno o más procesos de negocios de una unidad o área de negocio, es decir, todo aquello que tiene valor para su empresa.*

*Activo de soporte (infraestructura crítica): Activo o elemento que soporta el ingreso, generación, transporte, procesamiento, almacenamiento, publicación, distribución y eliminación de la información, tales como hardware, software, base de datos, elementos de red, instalaciones, personal y terceros involucrados.*

*Activo tecnológico: Es todo componente de Tecnologías de Información (Sistemas, Comunicación e Informática) que, integradas por medio de una arquitectura, soportan servicios corporativos y complementan los principales negocios de Telecomunicaciones, Infocomunicaciones y Electricidad. Comprende activos tangibles e intangibles como software, licencias, soporte, hardware de red, plataformas, etc.*

*Ciberataque: Un ciberataque es un conjunto de acciones dirigidas contra sistemas de información y las infraestructuras que lo soportan, como pueden ser bases de datos o redes computacionales o afectación de un elemento operativo del negocio, con el objetivo de perjudicar a personas, instituciones o empresas. Este tipo de acción puede atentar tanto contra los equipos y sistemas que operan en la red, anulando sus servicios, como contra bases que almacenan información, siendo esta espiada, robada o incluso, utilizada para extorsionar.*

*Ciberespacio: Entorno complejo que resulta de la interacción de personas, software y servicios en internet por medio de dispositivos y redes de tecnología conectados a éste, los que no existen en forma física.*

*Ciberriesgo: Ataques y riesgos que se sufren al hacer uso de la tecnología. Es decir, es cualquier amenaza que pueda afectar a la tecnología de una empresa, así como al conjunto de datos que se agrupan en la misma.*

*Ciberseguridad: Conjunto de herramientas tecnológicas, políticas, directrices, conceptos de seguridad cibernética digital, concientización, mejores prácticas que pueden utilizarse para proteger los activos de la organización y sus usuarios finales.*

*Concienciación o Concientización: Las dos formas, concienciar y concientizar, son correctas, en América se prefiere concientizar. Concienciar: "adquirir conciencia de algo" o "hacer que alguien sea consciente de algo". Concientizar: sinónimo de concienciar usado en el español de América.*

*Confidencialidad: Propiedad de la información de no estar disponible ni ser revelada a individuos, entidades o procesos no autorizados.*

*Custodio de información: Se refiere al funcionario o trabajador que funge como custodio en posesión física o lógica de la información del ICE y sus Empresas o de la información que se le ha confiado a estas.*

*Delitos computacionales: Es un delito tradicional cuya ejecución se da por medios informáticos (electrónicos y digitales).*

*Delitos Informáticos: Conducta típica, antijurídica y culpable que tenga como elemento distintivo el uso de equipos o aplicaciones programáticas de computación, como herramienta para la comisión del hecho delictivo o bien, como destino final de la conducta ilegítima.*

*Disponibilidad: Propiedad de ser accesible y utilizable por solicitud de una entidad autorizada.*

*Estrategia de Ciberseguridad: Una estrategia de ciberseguridad es un conjunto de planes, políticas y procedimientos diseñados para proteger los sistemas informáticos, las redes y los datos contra amenazas cibernéticas como virus, malware, hackers, phishing y otros ataques cibernéticos.*

*Impacto cibernético: Gravedad del resultado de un ataque cibernético, pueden ocasionar pérdidas de dinero o resultar en el robo de información personal, financiera o médica, suspensión e impedimento de brindar los servicios a los clientes.*

*Integridad: Cualidad de salvaguardar la exactitud y estado completo de los activos.*

*Sistema de información: Se refiere a un conjunto independiente de recursos de información organizados para la recopilación, procesamiento, mantenimiento, transmisión y difusión de información según determinados procedimientos, tanto automatizados como manuales.*

*Responsable de la información: Persona física o jurídica, que, en el ejercicio de un rol asignado por el ICE o alguna de sus empresas, tiene a su cargo la gestión de la información, desde su creación hasta su eliminación una vez cumplida la vigencia legal-administrativa (ciclo de vida de la información), rigiéndose por la normativa vigente y leyes relacionadas.*

*Seguridad Perimetral: La seguridad perimetral corresponde a la integración de elementos y sistemas, tanto electrónicos como mecánicos, para la protección de perímetros físicos, detección de tentativas de intrusión y/o disuasión de intrusos en instalaciones especialmente sensibles. Entre estos sistemas destacan los radares tácticos, video sensores, vallas sensorizadas, cables sensores, barreras de microondas e infrarrojos, sirenas, etc.*

*Usuario de la información: Persona física o jurídica, proceso o sistema, que, en el ejercicio de un rol asignado por el ICE o alguna de sus empresas, debe gestionar la información, a la cual accede de forma autorizada, de acuerdo con lo indicado por el responsable, rigiéndose por la normativa vigente y leyes relacionadas. El nivel de acceso es designado por el responsable de la información. La información empresarial, como recurso controlado por el ICE o alguna de sus empresas, será valorada mediante los criterios de confidencialidad, integridad y disponibilidad con el fin de determinar los controles a establecer para su gestión y preservación.*

## *5 RESPONSABILIDADES*

### *5.1 Consejo Directivo*

- *Aprobar la presente política.*
- *Instruir a la Presidencia Ejecutiva para establecer una estrategia de ciberseguridad conforme a la normativa interna del ICE y sus empresas.*
- *Dar seguimiento al cumplimiento de la presente política mediante los informes de rendición de cuentas correspondientes.*

### *5.2 Presidencia Ejecutiva*

- *Proponer al Consejo Directivo las actualizaciones que correspondan a la presente política.*
- *Instruir a la Gerencia General del ICE que coordine con las Gerencias Generales de las Empresas ICE, el establecimiento de la política corporativa de ciberseguridad.*
- *Proveer los recursos necesarios para su desarrollo.*

### *5.3 Gerencia General*

- *Gestionar y ejecutar las acciones asociadas a la presente política y los proyectos que deriven para la operacionalización de esta.*
- *Velar por el control y seguimiento de la implementación de la presente política.*

### *5.4 Gerencia Tecnología y Soluciones Digitales*

- *Aplicar la presente política.*

- *Definir los enlaces que estarán trabajando en la identificación e implementación de los controles necesarios para proteger la información del ICE y de sus clientes.*
- *Velar por el control y seguimiento de la implementación de la presente política*
- *Establecer la Política Corporativa de Ciberseguridad en coordinación con las demás Gerencias del ICE y Gerencias Generales de las Empresas ICE, así como la elaboración de mecanismos y de los procedimientos asociados para su implementación, ejecución y actualización.*
- *Ejecutar en coordinación con las demás Gerencias del ICE y Gerencias Generales de las Empresas ICE, la normativa y acciones necesarias para la gestión de seguridad de la información.*
- *Dar seguimiento a las acciones que se implementen acorde a la Política Corporativa de Ciberseguridad establecida.*
- *Realizar actividades de concientización y comunicación a nivel corporativo en temas de ciberseguridad.*

*5.5 Gerencias del ICE*

- *Aplicar la presente política.*
- *Definir los enlaces que estarán trabajando en la identificación e implementación de los controles necesarios para proteger la información del ICE y de sus clientes.*
- *Velar por el control y seguimiento de la implementación de la presente política*

*5.6 Gerencias Generales de las Empresas*

- *Aplicar la presente política.*
- *Definir los enlaces relacionados a temas de ciberseguridad de cada empresa que estarán trabajando en conjunto para la identificación e implementación de todos los controles necesarios para proteger la información del ICE y sus empresas, así como la de sus clientes.*
- *Gestionar y ejecutar las acciones asociadas a la presente política y los proyectos que deriven para la operacionalización de esta; así como proveer los recursos necesarios para su desarrollo.*
- *Velar por el control y seguimiento de la implementación de la presente política.*

*5.7 Titulares subordinados del ICE y sus empresas.*

- *Acatar en todos sus extremos la presente política.*
- *Ejecutar las acciones para operacionalizar esta política.*
- *Funcionarios y personal*

- *Acatar e implementar la presente política.*
- *Contribuir en lo que corresponda en su operacionalización.*

## *6 DESCRIPCIÓN DE LA POLÍTICA*

*El ICE y sus empresas gestionan acciones estratégicas corporativas relacionadas a ciberseguridad de forma proactiva y con el objetivo de promover la implementación oportuna de mecanismos de seguridad, que garanticen la confidencialidad, integridad y disponibilidad de la información sin importar el orden de estas, para el óptimo desempeño de las operaciones y la correcta protección de los datos e información del ICE, sus empresas y sus clientes.*

*En consideración de lo anterior, el ICE y sus empresas deben acatar los siguientes principios rectores:*

- *Mantener un inventario de sus activos de información como elemento estratégico para la ejecución de sus operaciones.*
- *Clasificar la información, esto con el fin de proteger la misma de acuerdo con su naturaleza y mitigar los riesgos de fuga de datos u otros relacionados.*
- *Establecer las medidas de protección de los equipos y dispositivos a fin de evitar la materialización de ataques u eventos que puedan impactar la seguridad de la información.*
- *Velar para que en las relaciones con terceros ya sea los prestadores de servicios, proveedores y empresas con las que se guarda relación, adopten normativa, procedimientos y controles de ciberseguridad compatibles con los riesgos que implica la prestación de los servicios a los clientes, preservando además la continuidad de las operaciones y negocios.*
- *Establecer mecanismos y controles lógicos y físicos para que el acceso a los sistemas, servicios y ambientes, se limiten a las personas identificadas y autorizadas.*
- *Comunicar mediante los canales oficiales del ICE y sus empresas cualquier incidencia relacionada con la información de clientes, personal, funcionarios o empresarial.*
- *Establecer una cultura de ciberseguridad, mediante la concienciación, principios y directrices de este tema a través de programas de capacitación para funcionarios y grupos de interés social.*
- *Asegurar el alineamiento a las normas y buenas prácticas de seguridad establecidas en el ICE y sus empresas por parte de los procesos de desarrollo, implementación, operación y mantenimiento de los sistemas de servicios corporativos y comerciales.*

- *Evaluar los controles destinados a la prevención y tratamiento de incidentes a ser adoptados por los proveedores de servicios que manejen datos o información sensible o que sean relevantes para el desarrollo de las actividades operativas. Las incidencias relevantes relacionadas con la información almacenada o procesada por el proveedor deben ser reportadas a través de los canales oficiales establecidos en el ICE y sus empresas.*
- *Implementar procesos para restaurar cualquier tipo de repositorio de datos registrados en los sistemas de información y servidores de archivos, de manera integral, redundante y confiable.*
- *Implementar herramientas y controles de defensa para proteger de forma proactiva y predictiva la infraestructura, los sistemas y la información. Los eventos lógicos de los sistemas y servicios deben ser debidamente registrados y monitoreados.*
- *Realizar los análisis de riesgos tecnológicos de ciberseguridad respectivos a toda la infraestructura crítica y/o sensible, en procura de establecer la evaluación eficaz del riesgo cibernético a los cuales se podrían enfrentar el ICE y sus empresas.*
- *Priorizar las acciones para la implementación de controles a fin de mitigar el apetito del riesgo cibernético establecido por el Marco Corporativo para la Administración Integral de Riesgos en el Grupo ICE.*
- *Implementar, en apego de las mejores prácticas, los modelos o acciones estratégicas de ciberseguridad corporativas enfocado en la aplicación de la confidencialidad, integridad y disponibilidad de la información sin importar el orden de las mismas y las infraestructuras críticas que la soportan para así establecer un entorno cibernético corporativo seguro.*
- *Establecer e implementar procesos de monitoreo y control de la infraestructura crítica, en procura de reducir las vulnerabilidades de ataques informáticos en software, equipos y redes del ICE y sus empresas.*
- *Adoptar, implementar y asegurar la aplicación de la normativa de ciberseguridad del ICE y sus empresas, a través de una coordinación corporativa con entes rectores en apego al ordenamiento jurídico y regulatorio relacionado.*
- *Fortalecer las medidas de ciberseguridad para garantizar la legitimidad, auditabilidad y trazabilidad en los entornos digitales y tecnológicos del ICE y sus empresas.*

## *7 VIGENCIA*

*Esta Política de Ciberseguridad Corporativa entra en vigor a partir de su publicación en el Diario Oficial La Gaceta.*

*8* ***REVISIONES y ACTUALIZACIONES***

*La revisión y actualización de la presente política se realizará por parte de la División de Estrategia en coordinación con el ICE y sus empresas, acorde a las pautas normativas nacionales e internacionales y los requerimientos de aseguramiento nacidos en el seno de cada empresa."*

2. *Instruir al ICE y sus empresas, para que, en el plazo máximo de 3 meses, elaboren el plan de implementación, asignen los recursos, el plan de inversión y otras consideraciones necesarias para la oportuna puesta en marcha de los controles asociados a esta política.*

3. *Instruir al ICE y sus empresas, para que procedan a ajustar la normativa interna vinculada con la política aprobada en la presente sesión.*

4. *Instruir a la División de Estrategia para que publique la política aprobada en la presente sesión en el Diario Oficial La Gaceta.*

5. *Instruir a la División de Estrategia que ingrese este documento en el sitio de normativa oficial, una vez publicada en el Diario Oficial La Gaceta y le dé publicidad mediante los mecanismos internos.*

6. *Instruir a la Secretaría del Consejo Directivo comunicar el presente acuerdo a las Juntas Directivas, Consejo de Administración y Gerencias Generales del ICE y sus empresas. Acuerdo firme."*

*Atentamente,*
***Secretaría Consejo Directivo***
**TERESITA GONZALEZ VILLEGAS (FIRMA)**
Firmado Digitalmente
Fecha: 20/04/2023 09:25:00 CST
Localización: Costa Rica
***Teresita González Villegas***
***Secretaria***

*TGV/icm*
*: Archivo*
*X: Consejo Directivo/Acuerdos por Sesión/6569*