TABLA DE CONTENIDO

1 PROPÓSITO 2
2 ALCANCE 2
3 DOCUMENTOS APLICABLES 2
4 TÉRMINOS, ABREVIATURAS Y SIGLAS 4
5 RESPONSABILIDADES 5
6 DESCRIPCION DE LA POLITICA 7
7 VIGENCIA 8
8 REVISIONES y ACTUALIZACIONES 8
9 CONTROL DE CAMBIOS 9
10 CONTROL DE ELABORACIÓN, REVISIÓN Y APROBACIÓN 9

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 N° 8292	Ley General de control Interno
Ley N° 8454	Ley de certificados firmas, digitales y documentos electrónicos
Ley N° 8642	Ley General de Telecomunicaciones
Ley N° 8660	Ley de Fortalecimiento y Modernización de las Entidades Públicas del Sector Telecomunicaciones. Art. 35
Ley Nº 8968	Ley de Protección de la Persona frente al Tratamiento de sus Datos Personales
Ley N° 7975	Ley de Información no Divulgada
Directriz No. 133-MP-	Dirigida a la Administración Pública Central y Descentralizada sobre

©Documento Normativo Propiedad del ICE, prohibida su reproducción total o parcial sin autorización.

MICITT	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 de 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.*

©Documento Normativo Propiedad del ICE, prohibida su reproducción total o parcial sin autorización.

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).

©Documento Normativo Propiedad del ICE, prohibida su reproducción total o parcial sin autorización.

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.

©Documento Normativo Propiedad del ICE, prohibida su reproducción total o parcial sin autorización.

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.

©Documento Normativo Propiedad del ICE, prohibida su reproducción total o parcial sin autorización.

5.7 Titulares subordinados del ICE y sus empresas.

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

5.8 Funcionarios y personal

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

6 DESCRIPCION DE LA POLITICA

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.

©Documento Normativo Propiedad del ICE, prohibida su reproducción total o parcial sin autorización.

- 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.

©Documento Normativo Propiedad del ICE, prohibida su reproducción total o parcial sin autorización.

9 CONTROL DE CAMBIOS

NA

10 CONTROL DE ELABORACIÓN, REVISIÓN Y APROBACIÓN

ELABORÓ	DEPENDENCIA	FECHA
Felix Araya Martínez	División de Estrategia	17-03-2023
Edith Guevara Espinoza Mike Zamora González Erick Obregón Navarro	Seguridad de la Información -GTSD	17-03-2023
Pablo López Aguilar	Dirección Estrategia Digital	17-03-2023
Leslie Calvo Arroyo	GTSD	17-03-2023
Fausto Roldán Gamboa Vladimir Sequeira Cole	RACSA	17-03-2023
Marcial Solís Rodríguez Sergio Méndez Fernández	CNFL	17-03-2023
Oscar Quesada Umaña	Gestión de Cobro	17-03-2023

REVISÓ	SESIÓN	FECHA
Comité Corporativo	artículo 7, incisos a y b Sesión 17-2023 del 17 de marzo de 2023	17-03-2023

APROBÓ[1]	SESIÓN	FECHA
Consejo Directivo	artículo 4 del Capítulo III de la Sesión 6569	18 de abril del 2023

[1] De conformidad al artículo 4, del Capítulo III, de la Sesión 6569 del 18 de abril del 2023, esta normativa entra en vigencia a partir de su publicación, la cual se llevó a cabo en el ALCANCE N° 82 de La GACETA N° 80 del martes 9 de mayo del 2023.

©Documento Normativo Propiedad del ICE, prohibida su reproducción total o parcial sin autorización.