

## INDICE

### ACTA SESIÓN ORDINARIA N°2238

*Martes 3 de setiembre del 2019*

#### **CAPÍTULO I**

#### **APROBACIÓN DEL ACTA**

- 1° Aprobación del acta de la sesión ordinaria N°2237 del 27 de agosto del 2019

#### **CAPÍTULO II**

#### **ASUNTOS DE LA GERENCIA GENERAL**

- 2° Sustento jurídico que respalda el derecho de registrar la reserva legal como un gasto deducible antes del impuesto de la renta
- 3° Política Continuidad del Negocio
- 4° Política Seguridad de la Información
- 5° Reglamento para el reconocimiento económico de los servicios móviles a los colaboradores de RACSA
- 6° Operador Móvil Virtual “fullmóvil” Informe mensual. Confidencial

#### **CAPÍTULO III**

#### **ASUNTOS DE JUNTA DIRECTIVA**

- 7° Oportunidades de negocio con el ICE. Oficio del Comité de Vigilancia

#### **CAPÍTULO IV**

#### **COMENTARIOS Y PROPOSICIONES**

- 8° Gobernanza Empresarial

### ACTA DE LA SESIÓN ORDINARIA N°2238

Celebrada por la Junta Directiva de Radiográfica Costarricense, Sociedad Anónima, en su domicilio legal, en la intersección de la Calle Primera y Avenida Quinta, San José, a partir de las diecisiete horas del martes tres de setiembre del dos mil diecinueve. Presentes: la Presidenta, señora Hazel Valverde Richmond; el Vicepresidente, señor Gabriel Viquez Jiménez; el Secretario, señor Hans Jiménez Láscarez; y el Tesorero, señor José Alberto Retana Reyes. Por la Asesoría Jurídica, la señora Illiana Rodríguez Quirós.

Ausente por asuntos personales, la Vocal, señora Agnes Paniagua Cubero.

Por la Gerencia General, el señor Francisco Calvo Bonilla; por la Dirección Administrativa Financiera, la señora Patricia Chavarría Lizano; por la Dirección Comercial, el señor Marco Meza Altamirano; por la Dirección de Operaciones, la señora Suzeth Rodríguez Solís y el señor Vladimir Sequeira Cole; por la Asesoría Jurídica, el señor Óscar Talavera Villalobos.

#### **CAPÍTULO I**

#### **APROBACIÓN DEL ACTA**

##### Artículo 1°

##### Aprobación del acta de la sesión ordinaria N°2237 del 27 de agosto del 2019:

La Presidenta, señora Hazel Valverde Richmond, somete a aprobación de los señores Directivos que estuvieron presentes el acta de la sesión ordinaria N°2237 del 27 de agosto del 2019.

Los señores Directivos se manifiestan conformes con el contenido del acta y la dan por aprobada.

## **CAPÍTULO II ASUNTOS DE LA GERENCIA GENERAL**

### **Artículo 2º Sustento jurídico que respalda el derecho de registrar la reserva legal como un gasto deducible antes del impuesto de la renta:**

La Presidenta, señora Hazel Valverde Richmond, señala que la Gerencia General en cumplimiento a lo requerido por la Junta Directiva en las sesiones N°2230 del 2 de julio del 2019 y N°2235 del 13 de agosto del 2019, somete a consideración el documento de referencia GG-998-2019, mediante el cual aporta el criterio emitido por la Asesoría Jurídica de la Empresa, sobre los elementos que sustentan el derecho de registrar la reserva legal como un gasto deducible antes del impuesto de la renta.

Ingresan a la sala el Gerente General, señor Francisco Calvo Bonilla y por la Asesoría Jurídica, el señor Óscar Talavera Villalobos, quienes indican que con el propósito de atender el requerimiento planteado por la Junta Directiva sobre este tema, mediante la nota de referencia AJ-529-2019 del 19 de agosto, se presenta el análisis de la creación de la reserva legal en la Empresa, el concepto de deducibilidad y su relación con la reserva patrimonial, el fundamento de la reserva patrimonial y el tratamiento fiscal, lo que permite concluir que la reserva patrimonial establecida en el artículo 4 inciso d) de la Ley N°3293, según lo dispuesto en el párrafo tercero de la Ley N°7722, es una de las reservas deducibles del impuesto sobre la renta, siempre y cuando sean útiles y pertinentes para la actividad comercial de la Empresa y que produzca utilidades y así pueda ser plenamente comprobado ante una eventual fiscalización de la Administración Tributaria.

La Junta Directiva expresa satisfacción por el criterio jurídico sobre este tema, agradecen la participación de los representantes de la Administración quienes abandonan la sala a partir de este momento.

### **Artículo 3º Política Continuidad del Negocio:**

La Presidenta, señora Hazel Valverde Richmond, señala que la Gerencia General como parte del esfuerzo de actualización de la normativa empresarial bajo el concepto de Gobierno Corporativo, somete a consideración de la Junta Directiva el documento de referencia GG-996-2019 del 22 de agosto del 2019, la propuesta para la definición de una política de continuidad del negocio.

Ingresan a la sala, el Gerente General, señor Francisco Calvo Bonilla, la Directora de Operaciones, la señora Suzeth Rodríguez Solís y por el Área de Seguridad y Continuidad del Negocio, el señor Vladimir Sequeira Cole, quienes explican que el objetivo de esta gestión es que la Empresa disponga de un instrumento que establece la visión empresarial, el alcance y los principios que regirán la gestión de la continuidad del negocio, con el fin de garantizar a los clientes y al país la estabilidad y calidad necesaria en los servicios críticos ante eventos disruptivos imprevistos y sorpresivos. Con el apoyo de una presentación, explican el alcance del instrumento, la metodología del sistema de gestión, los principales ejes y las disposiciones finales entre las que destaca el enfoque estratégico en los procesos críticos, el compromiso en la formación de capacidad empresarial para la gestión de continuidad, la

definición de prioridades de recuperación ante desastres, la participación de personal clave en el desarrollo e implementación del sistema de gestión, la definición de la estructura empresarial y el impulso a la asignación de recursos.

La Junta Directiva sobre la propuesta presentada por la Administración señalan que sería conveniente definir un protocolo para la atención de los eventos con una delimitación clara de la responsabilidad a través de este instrumento y en términos generales recomiendan revisar la propuesta para que exista concordancia entre las responsabilidades y el articulado para mantener consistencia en la integralidad del documento. Asimismo, recomiendan mantener vigilancia sobre el cumplimiento de las actividades que se han definido para la implementación del plan de continuidad empresarial. Finalmente, manifiestan interés de conocer al cierre del proceso un informe sobre el resultado obtenido en cuanto al impacto en los principales procesos, en lo que respecta a tiempos de recuperación, compromisos, niveles de criticidad así como los elementos de mejora de cara al negocio.

Los representantes de la Administración procederán a revisar la propuesta conforme a las observaciones planteadas y abandonan la sala a partir de este momento.

**La Junta Directiva, basada en el contenido de la información aportada y en los argumentos expuestos, resuelven:**

**Considerando que:**

- a) **RACSA no cuenta con una Política de Continuidad de Negocio en donde se establezca el propósito, el contexto, alcance y gobernanza del Plan de Continuidad de Negocio Empresarial, para mantener en operación los servicios críticos ante eventos disruptivos, imprevistos y sorpresivos.**
- b) **De conformidad con las Normas Técnicas para la Gestión y el Control de las TI de la Contraloría General de la República es imperativo para RACSA alinearse con dicha normativa a fin de contar con una base regulatoria para la continuidad de sus operaciones.**
- c) **Se ha utilizado como documentos de referencia y fundamento técnico la norma internacional ISO22301-2012, así como lo señalado en los “Lineamientos de Mejores Prácticas” dictado por el Business Continuity Institute (BCI).**
- d) **La Asesoría Jurídica, por medio del oficio AJ-546-2019 del 22 de agosto de 2019, otorga el visto bueno a la propuesta de la Política de Continuidad del Negocio de RACSA.**
- e) **La Gerencia General mediante el oficio de referencia GG-996-2019 del 22 de agosto del 2019, avala y eleva a aprobación de la Junta Directiva la propuesta de la Política de Continuidad del Negocio de RACSA.**
- f) **Conforme a lo establecido en los artículos 181 del Código de Comercio y 9.4 del Reglamento de Junta Directiva de RACSA, corresponde a la Junta Directiva, aprobar las políticas generales para el garantizar a los clientes y al país la estabilidad y calidad necesaria en los servicios.**

Por tanto, acuerda:

- 1) Aprobar la Política de Continuidad de Negocio de acuerdo con el siguiente texto:

**“Política de Continuidad del Negocio de RACSA**

**1. OBJETIVO**

Establecer la visión empresarial, el alcance y los principios que regirán la gestión de la continuidad de negocio de RACSA, con el fin de garantizar a los clientes y al país la estabilidad y calidad necesaria en los servicios críticos ante eventos disruptivos, imprevistos y sorpresivos.

**2. ALCANCE**

La presente política alcanza los procesos, subprocesos, actividades, plataformas y elementos que sean identificados como críticos y muy críticos de acuerdo con: el Análisis de Impacto de Negocio del Sistema de Gestión de Continuidad de Negocio de conformidad con la norma ISO22301-2012; las Normas Técnicas para la Gestión y el Control de las TI de la Contraloría General de la República; así como todo el personal de RACSA involucrado en la atención de los mismos.

**3. ABREVIATURAS**

**BIA: Business Impact Analysis (Análisis de Impacto de Negocio).**

**COBIT: Control Objectives for Information and related Technology (Objetivos de Control para Información y Tecnologías Relacionadas).**

**ERI: Estructura de Respuesta de Incidente.**

**ICE: Instituto Costarricense de Electricidad.**

**ISO: International Organization for Standardization. (Organización Internacional de Normalización).**

**MBCO: Minimum Business Continuity Objective (Objetivo Mínimo de Continuidad de Negocio).**

**MTPD: Maximum Tolerable Period of Disruption (Máximo Tiempo de Interrupción Permisible).**

**PCN: Plan de Continuidad de Negocio.**

**RACSA: Radiográfica Costarricense S.A.**

**RTO: Recovery Time Objective (Tiempo de Recuperación Objetivo).**

**SGCN: Sistema de Gestión de Continuidad de Negocio.**

#### 4. DEFINICIONES

**Análisis de impacto del negocio: (Business Impact Analysis –BIA-).** El BIA, es un proceso sistemático para determinar y evaluar los efectos potenciales de la interrupción de una actividad de proceso o de un elemento funcional de infraestructura operativa, como resultado de un incidente o circunstancia no planeada. El BIA además determina los tiempos máximos permisibles para una interrupción (MTPD –Maximum Time Period of Disruption) y los plazos de recuperación objetivo (-RTO-Recovery Time Objective) de cada actividad o elemento identificado como crítico. El BIA es la base de inicio para la etapa de análisis de riesgos de continuidad que es la siguiente de desarrollo en un Sistema de Gestión de Continuidad de Negocio (SGCN) según ISO 22301.

**Continuidad de negocio:** conjunto de mejores prácticas aplicadas al establecimiento de lineamientos de identificación, mitigación de riesgos, atención funcional, evaluación y mejora de la gestión empresarial ante la aparición de eventos disruptivos no planeados que puedan afectar los elementos críticos para la marcha del negocio.

**Estructura de respuesta de incidentes:** estructura organizacional responsable de la atención de un incidente que afecte la continuidad.

**Plan de continuidad de negocio:** documento que define las estrategias de atención de los procesos e infraestructuras por parte de las ERI, los procesos de prevención y mitigación de amenazas.

**Resiliencia:** capacidad empresarial de recuperación ante procesos de crisis, situaciones adversas o eventos disruptivos sorpresivos que afectan la continuidad de las operaciones empresariales.

**Sistema de gestión de continuidad de negocio:** conjunto de procesos tendientes a la configuración de un modelo empresarial permanente que busca la continuidad de negocio y su mejora continua, tiene por objetivo establecer la administración adecuada de los incidentes imprevistos que pueden afectar las actividades o elementos críticos para el funcionamiento empresarial.

#### 5. RESPONSABILIDADES

##### Junta Directiva

- Aprobar la presente política, así como las modificaciones que se le incorporen.

##### Gerente General

- Elevar ante la Junta Directiva la propuesta de Política de Continuidad de Negocio para su valoración y aprobación.

- Promover y apoyar una cultura de orientación hacia las mejores prácticas en continuidad de negocio.
- Acoger las recomendaciones necesarias para la implementación y operación de los instrumentos: Análisis de impacto del negocio, Análisis de riesgo de continuidad; Análisis de planes de continuidad del negocio y estrategias de recuperación del Sistema de Gestión de Continuidad de Negocio de RACSA y de la presente Política.
- Recibir y aprobar los entregables del plan de trabajo para las distintas fases de implementación del Sistema de Gestión de Continuidad de Negocio.
- Apoyar la mejora del Sistema de Gestión de Continuidad de Negocio y el destino de recursos financieros, humanos y materiales para una efectiva implantación empresarial.

#### Direcciones

- Destinar recursos financieros y de personal para garantizar en procesos críticos que tengan a cargo, la continuidad del negocio según el modelo de gestión.
- Aprobar y poner en ejecución los procedimientos, prácticas y documentación normalizada de las distintas fases del Sistema de Gestión de Continuidad de Negocio.
- Participar activamente en la promoción y apoyo de la formación del personal orientada a las mejores prácticas en continuidad de negocio.
- Participar activamente en los ejercicios prácticos según sea su rol –cuando aplique- en las estructuras de respuesta de incidentes de los planes de recuperación.
- Asumir el rol definido en las Estructuras de Respuesta de Incidentes ante activación del Plan de Continuidad.

#### Jefaturas responsables de procesos críticos identificados

- Participar activamente en las diferentes fases de implementación del Sistema de Gestión de Continuidad de Negocio bajo la guía del personal del Área de Seguridad y Continuidad de RACSA y los Gestores de Continuidad de cada Dirección.
- Cumplir en tiempo y forma con la información que se solicite para las fases de implementación del Sistema de Gestión de Continuidad de Negocio.
- Participar activamente en los ejercicios prácticos de acuerdo con el rol que posea en las estructuras de respuesta de incidentes.
- Asumir el rol definido –cuando aplique- en las Estructuras de Respuesta de Incidentes ante activación del Plan de Continuidad.

#### Área de Seguridad y Continuidad de Negocio

- Elaborar la Política de Continuidad de Negocio de RACSA.
- Velar por el cumplimiento de la Política de Continuidad de Negocio.
- Proponer los manuales o procedimientos por los cuales se materialice la Política de Continuidad del Negocio coordinado con las

áreas funcionales de la Empresa y los Gestores de Continuidad de las Direcciones.

- Guiar a la Empresa en el proceso de incorporación e implementación del Sistema de Gestión de Continuidad de Negocio a partir de la norma ISO 22301.
- Capacitar y formar a los Gestores de Continuidad en cuanto a las fases de implementación del Sistema de Gestión de Continuidad de Negocio.
- Homologar según sea pertinente, los lineamientos y prácticas que se definen en el Grupo ICE, a través del Equipo Sectorial de Continuidad de Negocio.
- Revisar el Sistema de Gestión de Continuidad de Negocio cada vez que se presenten cambios importantes a nivel de procesos u orientaciones estratégicas de la Empresa.
- Estudiar y analizar las estrategias de recuperación de los procesos críticos de las distintas áreas, para establecer su participación en la atención de incidentes, según se defina en los planes de continuidad.
- Coordinar externamente con el equipo Sectorial de Continuidad del Negocio de la Gerencia de Telecomunicaciones del ICE, el aprovisionamiento de recursos extraordinarios en caso de incidentes de alto impacto, según se requiera.
- Coordinar internamente en la verificación de cumplimiento de los lineamientos descritos en los planes de continuidad del negocio.
- Asumir el rol definido en las ERI cuando sea requerido.
- Responsable de coordinar el Comité Interno de Continuidad de Negocio.

#### **Gestores de Continuidad designados por las direcciones**

- Asegurar el cumplimiento en tiempo y forma de los requerimientos de información del Área de Seguridad y Continuidad.
- Participar activamente en las distintas fases del proceso de implementación interno de cada Dirección del Sistema de Gestión de Continuidad de Negocio.
- Apoyar el proceso de formación del personal clave de la Dirección a cargo en cuanto a la Gestión de la Continuidad.
- Participar del Comité Interno de Continuidad del Negocio, coordinado por el Área de Seguridad y Continuidad.

#### **Área de Comunicación**

- Liderar el desarrollo de la estrategia de comunicación empresarial de la presente política y del proceso de Gestión de Continuidad de Negocio.
- Coordinar los aspectos técnicos y administrativos para el lanzamiento de campañas, comunicados y otros medios para la comunicación de la Gestión de Continuidad de Negocio.
- Asumir el rol definido en las ERI cuando sea requerido.

## Departamento de Gestión Estratégica y Desempeño Empresarial

- Revisar, desde el ámbito de sus competencias, la creación o modificación de esta política.
- Custodiar la última versión oficial aprobada del documento e incluirla en el sitio web oficial intranet.

## 6. REFERENCIAS Y DOCUMENTOS APLICABLES

- INTE/ISO 22301-2012 Seguridad de la Sociedad, Sistemas de Gestión de Continuidad de Negocio.
- Normas Técnicas para la Gestión y el Control de las TI de la Contraloría General de la República (N-2-2007-CO-DFOE).
- COBIT: Control Objectives for Information and related Technology.

## 7. ALINEAMIENTO DE LA POLÍTICA DE CONTINUIDAD DE NEGOCIOS

### 7.1. Alineamiento Corporativo

El Sistema de Gestión de Continuidad de Negocio de RACSA estará alineado con la Estrategia Corporativa del Grupo ICE, a través del Equipo Sectorial de Continuidad de Negocio y su coordinación.

### 7.2. Alineamiento Estratégico

El Sistema de Gestión de Continuidad de Negocio estará alineado en todo momento con la estrategia, planes de negocio y de soporte al negocio que se encuentren vigentes.

## 8. POLÍTICA GENERAL DE CONTINUIDAD DEL NEGOCIO

La Política de Continuidad de Negocio se apoya en conjunto con los vínculos citados en el apartado 7 y sus compromisos, que se presentan a continuación:

**Artículo 1.** La implementación y operación del Sistema de Gestión de Continuidad de Negocio de RACSA es una prioridad empresarial y es de aplicación obligatoria en todas las unidades funcionales de la Empresa, de tal forma que se atiendan todos los procesos críticos identificados y actualizados en el Análisis de Impacto de Negocio desarrollado por cada Dirección, bajo la supervisión y guía del personal del Área de Seguridad y Continuidad de RACSA.

**Artículo 2.** La Gerencia General se compromete a mantener los servicios, procesos y elementos críticos que sean definidos en el Análisis de Impacto de Negocio de las Direcciones funcionales de RACSA, dentro de parámetros predefinidos de operación y tiempo de recuperación, como parte de un Sistema de Gestión de Continuidad de Negocio que se rige por



las mejores prácticas de la norma ISO 22301 vigente, en atención de eventos disruptivos imprevistos; buscando el mayor nivel de calidad en la prestación de los servicios para la satisfacción de nuestros clientes y demás partes interesadas.

**Artículo 3.** La Dirección de Operaciones se compromete a asignar y formar al personal clave en las mejores prácticas de continuidad de negocio, buscando que se fortalezca con el tiempo el Sistema de Gestión y su mejora continua, con la firme convicción y compromiso de cumplir con la normativa vigente.

**Artículo 4.** La Gerencia General velará por la protección y seguridad de las personas como objetivo prioritario, tanto en situaciones de normalidad, como en incidentes sorpresivos e imprevistos.

**Artículo 5.** La Dirección de Operaciones garantizará de manera prioritaria la continuidad, calidad y eficiencia a nuestros clientes en la prestación de los servicios, tanto en situación normal como en situación de crisis derivada de un evento sorpresivo e imprevisto, manteniendo el orden conforme al análisis de priorización de actividades críticas elaborado por las jefaturas con procesos críticos identificados.

**Artículo 6.** Las Direcciones de la Empresa nombrarán los representantes de las distintas áreas con la debida experiencia y conocimiento, para que participen activamente en las fases de implementación y posterior mantenimiento del Sistema de Gestión de Continuidad de Negocio, bajo la guía y supervisión del personal del Área de Seguridad y Continuidad de RACSA.

**Artículo 7.** Para la implementación y puesta en marcha del Sistema de Gestión de Continuidad de Negocio se tomará en cuenta las áreas, departamentos internos, proveedores de servicios, socios comerciales, sistemas, recursos y procedimientos afines para garantizar la continuidad de las operaciones, así como los recursos necesarios.

**Artículo 8.** La Junta Directiva y Gerencia General adoptarán medidas razonables para la continuidad operativa de los procesos y actividades en función de la criticidad de los mismos, según lo defina el Análisis de Impacto de Negocio del Sistema de Gestión de Continuidad de Negocio, dentro de estas medidas están la asignación de recursos humanos, financieros y materiales extraordinarios que ameriten fortalecer y proteger dichos procesos.

**Artículo 9.** Los Directores y los Gestores de Continuidad nombrados en cada Dirección son responsables de elaborar y proporcionar los entregables del Sistema de Gestión de Continuidad de Negocio según corresponda, los cuales deberán ser trasladados al personal del Área de Seguridad y Continuidad en tiempo y forma, a partir de su solicitud en plazos desde los tres días hábiles hasta los quince días hábiles, según la complejidad de lo solicitado, de manera que se posibilite la ejecución por

parte de los responsables y la correcta supervisión por parte del personal del Área de Seguridad y Continuidad de RACSA.

**Artículo 10.** La Dirección Administrativa Financiera velará por la comunicación a todo el personal de sus responsabilidades y de los procedimientos que le competen, en el marco de la continuidad de negocio, lo cual se hará a través de los Gestores de Continuidad de las Direcciones, bajo la guía y supervisión del Área de Seguridad y Continuidad de RACSA, así como campañas de concientización y formación.

**Artículo 11.** La Dirección de Operaciones desarrollará un Sistema de Gestión de Continuidad de Negocio que contemple ciclos anuales de revisión y actualización de todas las fases que lo componen o bien ante cambios significativos a nivel de procesos de negocio u organizacionales, siguiendo los principios de mejora continua y los lineamientos corporativos.

**Artículo 12.** La presente Política de Continuidad de Negocio entra en vigencia a partir de su publicación en el Sitio Web Oficial del Colaborador (Intranet).

## 9. REVISIÓN Y EVALUACIÓN

Esta política debe ser revisada al menos una vez al año, por parte del Área de Seguridad y Continuidad de RACSA para verificar si se deben realizar modificaciones o actualizaciones a la misma.”

2) La implementación de este acuerdo es responsabilidad de la Gerencia General.

### Artículo 4º Política Seguridad de la Información:

La Presidenta, señora Hazel Valverde Richmond, señala que la Gerencia General conforme al planteamiento aprobado en la sesión N°2236 y como parte del esfuerzo de actualización de la normativa empresarial bajo el concepto de Gobierno Corporativo, somete a consideración de la Junta Directiva el documento de referencia GG-995-2019 del 22 de agosto del 2019, la propuesta de una política para la seguridad de la información.

Ingresan a la sala, el Gerente General, señor Francisco Calvo Bonilla, la Directora de Operaciones, la señora Suzeth Rodríguez Solís y por el Área de Seguridad y Continuidad del Negocio, el señor Vladimir Sequeira Cole, quienes explican que el objetivo de este instrumento es regular los principios rectores de la gestión de seguridad de la información de RACSA a partir de la legislación vigente y conforme a las mejores prácticas internacionales. Con el apoyo de una presentación, explican los antecedentes, el alcance, las normas y controles utilizados dentro del sistema de gestión de seguridad de información para definir la política.

La Junta Directiva señala que la propuesta es de alcance a terceros, razón por la cual corresponde la publicación en el Diario Oficial La Gaceta, cuya vigencia queda supeditada a este acto. En términos generales recomiendan realizar pruebas de penetración, que permita analizar la vulnerabilidad y los riesgos involucrados. Concluyen que esta Política es de

relevancia en el proceso de transformación empresarial, razón por la cual deben velar para que la actualización se realice de manera periódica.

Los representantes de la Administración toman nota de las observaciones planteadas y abandonan la sala a partir de este momento.

**La Junta Directiva, basada en el contenido de la información aportada y en los argumentos expuestos, resuelven:**

**Considerando que:**

- a) **La Política de Seguridad de la Información de RACSA vigente, aprobada por la Junta Directiva en la sesión N°2049 del 28 de octubre del 2014, presenta un grado de obsolescencia medio, el cual no permite seguir con las mejores prácticas dictadas en la norma internacional ISO/IEC 27001:2013, además también se incumple con el punto 1.4 “Gestión de la seguridad de la información” de las Normas Técnicas para la Gestión y el Control de las Tecnologías de Información de la Contraloría General de la República.**
- b) **De acuerdo con la norma internacional ISO/IEC 27001:2013, toda política de seguridad de la información debe ser revisada y actualizada anualmente por parte del área de seguridad encargada.**
- c) **La seguridad de la información pertenece a los pilares de arquitectura tecnológica en la transformación del modelo de negocio de RACSA, según lo expuesto en la Estrategia Empresarial 2019-2023.**
- d) **La Asesoría Jurídica, por medio del oficio AJ-544-2019 del 21 de agosto de 2019, otorga el visto bueno a la propuesta de Política de Seguridad de la Información de RACSA.**
- e) **La Gerencia General mediante el oficio de referencia GG-995-2019 del 22 de agosto de 2019, avala y eleva a aprobación de la Junta Directiva la propuesta de Política de Seguridad de la Información de RACSA.**
- f) **Conforme a lo establecido en los artículos 181 del Código de Comercio y 9.4 del Reglamento de Junta Directiva de RACSA, corresponde a la Junta Directiva, aprobar las políticas generales para el manejo seguro de la información.**

**Por tanto, acuerda:**

- 1) **Aprobar la Política de Seguridad de la Información de Radiográfica Costarricense S.A., de acuerdo con el siguiente texto:**

**“Política de Seguridad de la Información  
de Radiográfica Costarricense S.A.**

## **1. GENERALIDADES**

**Proteger la información es una tarea cada vez más difícil y necesaria debido a los riesgos asociados, mismos que se incrementan paralelamente**

con los avances tecnológicos. Elementos como internet, conectividad, Internet de las Cosas (IoT), digitalización, medios de almacenamiento y cómputo en la nube vienen a apoyar la gestión del trabajo y del quehacer de las personas, empresas, instituciones y en general de la sociedad, pero constituyen a su vez espacios físicos o virtuales que pueden ser vulnerados, donde la información que es el activo más importante puede corromperse, extraviarse, volverse inútil o utilizarse en contra de su propietario, accidentalmente o con plena intención de causar cualquiera de las anteriores situaciones.

La información por lo tanto debe ser protegida porque constituye un activo estratégico para RACSA y debe ser identificada en sus distintos soportes para clasificarla de acuerdo con su confidencialidad, integridad y disponibilidad con el fin de implementar controles de acuerdo con su criticidad.

## **2. OBJETIVO**

Regular los principios rectores de la gestión de seguridad de información de RACSA a partir de la legislación vigente y conforme a mejores prácticas internacionales tales como: los estándares ISO 27001 “Sistemas de Gestión de Seguridad de Información” y 27002 “Código para los Controles de Seguridad de información”.

## **3. ALCANCE**

La Política de Seguridad de la Información de RACSA (en adelante la Política) es de acatamiento obligatorio para todo el personal, practicantes y contratistas con quienes RACSA desarrolle actividades conjuntas para la prestación de servicios los cuales tengan acceso a información empresarial a través de los documentos, equipos de cómputo, infraestructura tecnológica y canales de comunicación de la Empresa. También aquellas personas tanto físicas como jurídicas con quienes se firmen acuerdos de confidencialidad específicos con RACSA podrán ser sujetos de cumplimiento de los principios de la presente política y del cuerpo normativo que la instrumentalice.

## **4. APROBACIÓN**

Es responsabilidad de la Junta Directiva de RACSA, de acuerdo con el Reglamento vigente de ese Órgano Colegiado aprobado el 9 de abril de 2019 en la sesión ordinaria N°2217, el dictar las políticas generales para el manejo seguro y confidencial de la información, según se indica en el artículo 9.4 del Reglamento en marras. El Gerente General de RACSA, es responsable de garantizar la existencia del proceso de seguridad empresarial encargado de la implementación y supervisión del cumplimiento transversal del Sistema de Gestión de Seguridad de Información y por ende de la Política de Seguridad de la Información.

## 5. ABREVIATURAS

- **RACSA:** Radiográfica Costarricense S.A.
- **ISO:** International Organization for Standardization (Organización Internacional para la Estandarización).
- **COBIT:** Control Objectives for Information and related Technology (Objetivos de Control para la Información y Tecnologías Relacionadas).
- **DTIC:** Departamento de Tecnologías de Información y Comunicación.

## 6. DEFINICIONES

**Activo de información:** es todo aquel elemento digital o físico que tiene o transfiere información para la Empresa.

**Administración de usuarios:** son labores de creación, modificación, consulta, bloqueo, desbloqueo y eliminación de la cuenta de un usuario.

**Análisis de riesgos:** proceso en el que se estudia, a partir de una probabilidad de ocurrencia y un impacto estimado, el nivel de criticidad de una determinada amenaza que pueda afectar el logro de un objetivo de proceso o estratégico.

**Confidencialidad:** carácter que tiene la información industrial, comercial y económica que por motivos estratégicos de competencia debe procurarse su confidencialidad, de modo que no procede su divulgación, adquisición o utilización por parte de terceros así como la información de tipo personal de los clientes.

**Control:** acción que tiene como objetivo mitigar el impacto o reducir el nivel de riesgo que pueda presentar una determinada amenaza, en caso de que se materialice.

**Disponibilidad:** propiedad de la información de estar accesible y utilizable cuando sea requerido por una parte autorizada.

**Encriptación:** mecanismo de seguridad que permite almacenar datos utilizando algoritmos matemáticos de codificación o cifrado, con el fin de ocultar y proteger los datos contra accesos no autorizados. Este mecanismo requiere del uso de un software de encriptación para proteger los datos y una contraseña para tener acceso a la misma.

**Evento de seguridad de la información:** es cualquier situación identificada, que indique una posible brecha en las Políticas de Seguridad o falla en los controles y protecciones establecidas.

**Incidente de seguridad de la información:** evento que haya vulnerado la Política de Seguridad de la Información o cualquier lineamiento o normativa que la instrumentalice. También se cataloga como incidente

**cualquier intento de vulnerar la Política y su cuerpo normativo sin importar la información afectada, la plataforma tecnológica, la frecuencia, las consecuencias, el número de veces ocurrido o si el origen es interno o externo.**

**Información:** conjunto organizado de datos procesados, que tienen un significado y valor en un momento y lugar determinados para los negocios de la Empresa, independiente de su soporte (físico, digital, conocimiento, entre otros).

**Integridad:** cualidad de salvaguardar la exactitud y completitud de los datos que hacen parte de la información, tal que solamente puedan modificarse por partes autorizadas.

**Propietario de la información:** titular subordinado responsable del activo de información que va a ser protegido, y quien genera y mantiene los datos que utiliza la compañía a través de un conjunto determinado de sistemas y que son utilizados por un proceso determinado.

**Recursos tecnológicos:** elementos de tecnología que pueden ser hardware y software, tales como: equipos de cómputo, servidores, impresoras, teléfonos, faxes, programas y aplicativos de software, dispositivos de almacenamiento Flash, entre otros.

**Seguridad de la información:** preservación de la confidencialidad, integridad y disponibilidad de la información. Tiene como característica la autenticidad, el no repudio y la confiabilidad.

**Sistema de Gestión de Seguridad de la Información (SGSI):** es el conjunto de elementos, relacionados entre sí, que se implementan para lograr el objetivo de proteger la seguridad de la información en la Empresa, compuesto por: políticas, estándares, procedimientos, estructura organizacional de gestión, recursos, planes y demás elementos que permitan lograr ese objetivo en un ciclo de mejora continua.

**Sistema de información:** conjunto de datos, aplicaciones, equipos, y recursos humanos que, en forma interrelacionada, proveen a la Empresa la información necesaria para la ejecución de las tareas y la toma de decisiones del nivel estratégico, táctico y operativo.

**Terceros:** toda persona, jurídica o física, como proveedores, contratistas, socios comerciales o consultores, que provean o intercambien servicios o productos con la Empresa.

**Usuario:** será aquella persona, jurídica o física, que, para ejercer sus funciones normales en el desempeño de sus actividades necesita acceder a la información de la Empresa y a sus recursos informáticos.

## **7. RESPONSABILIDADES**

### **Junta Directiva**

- **Aprobar la Política de Seguridad de la Información y sus futuras modificaciones.**

### **Gerencia General**

- **Elevar a la Junta Directiva la presente política para su respectiva aprobación.**
- **Aprobar la normativa interna que instrumentalice la Política de Seguridad de la Información.**
- **Apoyar la gestión transversal empresarial del proceso Continuidad de Negocio y Seguridad de la Información.**
- **Aprobar los recursos humanos y financieros necesarios para implementar la presente Política.**

### **Área de Seguridad y Continuidad**

- **Promover e implementar una cultura de seguridad de la información en RACSA.**
- **Elevar a la Gerencia General para su aprobación la normativa interna que instrumentalice la Política de Seguridad de la Información.**
- **Definir las directrices estratégicas, la normativa y cualquier otra medida necesaria para la gobernabilidad y gestión de seguridad de la información, fundamentadas en el principio de eficiencia y en consideración del logro de los objetivos empresariales.**
- **Presentar a la Gerencia General el requerimiento de recursos necesarios (presupuesto, capacitación empresarial, recurso humano, normativa) para la gestión de la seguridad de la información de RACSA.**
- **Guiar transversalmente a la Empresa en el proceso de incorporación e implementación del Sistema de Gestión de Seguridad de la Información, conforme la norma ISO 27001.**
- **Identificar y aplicar modificaciones a la presente Política.**
- **Supervisar el cumplimiento de la normativa interna en las distintas Direcciones.**
- **Presentar el Plan de Seguridad Empresarial de forma anual a la Gerencia General y al Comité de Tecnologías de Información.**
- **Evaluar el cumplimiento del Plan de Seguridad Empresarial en RACSA en las distintas dependencias.**
- **Atender la gestión de incidentes de seguridad de la información de acuerdo con el Lineamiento de Operación que lo rige.**

### **Directores**

- **Proveer en tiempo y forma los requerimientos de información y recursos que solicite el Área de Seguridad y Continuidad para la**

instrumentalización de esta política y la gestión de incidentes de seguridad de información.

- Aprobar las declaratorias de confidencialidad de cada una de las áreas respectivas.
- Apoyar la gestión de seguridad de información en todos los procesos a cargo.
- Administrar los riesgos de seguridad de información de todos los procesos a cargo bajo la supervisión y acompañamiento del proceso de Continuidad de Negocio y Seguridad de la Información y del personal especialista.

#### **Jefaturas**

- Velar por el cumplimiento de esta Política en las áreas de su competencia.
- Identificar acciones de mejora de seguridad de la información concretas en su área.
- Realizar la gestión de riesgos de seguridad de información en su proceso a cargo.
- Identificar de acuerdo con la clasificación de la información la cual deberá ser catalogada como pública, confidencial y privada.
- Identificar y designar los roles asociados a la seguridad de la información de su área.
- Reportar oportunamente, a través de los canales establecidos de la Empresa, los riesgos, eventos o sospechas de vulnerabilidades o amenazas de seguridad de la información.

#### **Área de Comunicación**

- Brindar el soporte necesario para las campañas de divulgación de la presente política.
- Fungir como el canal oficial de comunicación de RACSA para la gestión de incidentes de seguridad de información o comunicaciones relacionadas a seguridad de la información.

#### **Funcionarios de RACSA**

- Acatar en todos sus extremos la presente Política de Seguridad de la Información.

#### **Departamento de Gestión Estratégica y Desempeño Empresarial:**

- Realizar la inclusión, modificación, control de cambios y aprobaciones que se le realice a la política.
- Velar para que la presente política se ajuste al formato y estructura propia de las guías, de acuerdo con la Guía para la Estructura y Contenido de los Documentos aprobada.



- Custodiar la última versión oficial aprobada del documento, una vez publicada en el Diario Oficial La Gaceta se debe incluir en el sitio web oficial Intranet Empresarial.

## 8. DOCUMENTOS DE REFERENCIA

- ISO 27001 Sistema de Gestión de Seguridad de la Información.
- COBIT DS5 Garantizar la Seguridad de los Sistemas.
- COBIT DS12 Administrar el Ambiente Físico.
- COBIT DS13 Administración de las Operaciones.
- COBIT PO9 Evaluar y Administrar los Riesgos de TI.
- GG-LN-001 Lineamiento de Uso de Recursos Informáticos de RACSA.

## 9. CONTENIDO

**Artículo 1.** La Gerencia General reconoce la información como un activo vital y estratégico para la Empresa, por lo tanto, se compromete a establecer las acciones que conlleven a la Gestión de la Seguridad de la Información con el fin salvaguardar la confidencialidad, integridad y disponibilidad de la información, mediante estrategias orientadas a la continuidad del negocio, la administración de riesgos informáticos y de información y la consolidación de una cultura de seguridad.

**Artículo 2.** El Área de Seguridad y Continuidad será provisto de los recursos tanto financieros como humanos necesarios para la Gestión de la Seguridad de la Información de manera transversal en RACSA.

**Artículo 3.** La Gerencia General aplicará la legislación vigente en materia de seguridad de la información y la norma internacional ISO 27001 “Sistemas de Gestión de Seguridad de Información” que fungirá como marco de referencia y de mejores prácticas para aplicación interna.

**Artículo 4.** La Gerencia General creará los lineamientos técnicos, administrativos y jurídicos que instrumentalicen esta política, mismos que son de acatamiento obligatorio para funcionarios y terceros que posean información de RACSA.

**Artículo 5.** La Dirección de Operaciones promoverá y mantendrá una cultura orientada a las mejores prácticas de seguridad de la información mediante la capacitación y concientización de los funcionarios de RACSA, para minimizar la ocurrencia de incidentes de seguridad de la información.

**Artículo 6.** La Gerencia General garantizará a los funcionarios el acceso a la información necesaria y suficiente para el cumplimiento de sus actividades y definirá el nivel de acceso a la información de acuerdo con las funciones o roles de cada colaborador.

**Artículo 7.** La Dirección de Operaciones establecerá los mecanismos para proteger la información catalogada como confidencial ante terceros

mediante declaratorias de confidencialidad, controles de seguridad y suscripción de convenios de confidencialidad en las relaciones comerciales o de otra índole con terceros. Para ello contarán con el acompañamiento de la Asesoría Jurídica.

**Artículo 8.** El Área de Seguridad y Continuidad definirá los roles y responsabilidades de la Gerencia General, directores, jefaturas, procesos y funcionarios involucrados en relación con la seguridad de la información.

**Artículo 9.** Los responsables de los procesos empresariales -directores y jefaturas- deberán clasificar toda la información que se genera en su proceso de acuerdo con su nivel confidencialidad, integridad y disponibilidad, siguiendo los procedimientos aprobados.

**Artículo 10.** La Asesoría Jurídica brindará el acompañamiento necesario a la Dirección de Operaciones a fin de definir los mecanismos jurídicos necesarios para salvaguardar el uso de la información en la gestión con terceros y para resguardar la información confidencial.

**Artículo 11.** Los sistemas de información y plataformas tecnológicas, deberán contar con controles de acceso, que garanticen que únicamente los usuarios autorizados puedan accederlos. Lo anterior de conformidad con los privilegios definidos de acuerdo con las funciones que le hayan sido asignadas.

**Artículo 12.** Los funcionarios son responsables conforme a la legislación vigente de sus claves de acceso y la información que acceden y procesan mediante cualquier activo de soporte (físico, correo electrónico, internet, entre otros similares) y darán un uso adecuado a la misma con el fin de evitar el robo, fuga de información a terceros no autorizados.

**Artículo 13.** La utilización de la información para beneficio propio o de un tercero se catalogará como un incidente de seguridad y de comprobarse acarreará para los responsables de estos actos, responsabilidad administrativa, disciplinaria, civil y penal de acuerdo con la gravedad del impacto y de los hechos suscitados, conforme a lo establecido en el Estatuto de Personal de RACSA.

**Artículo 14.** El Área de Seguridad y Continuidad previa comunicación a los funcionarios podrá monitorear todas las actividades realizadas por los usuarios en los sistemas de información y plataformas tecnológicas, contemplando siempre el respeto al derecho constitucional de intimidad de las comunicaciones.

**Artículo 15.** Toda la información empresarial deberá clasificarse por parte de los titulares subordinados de acuerdo con el nivel de integridad, confidencialidad y disponibilidad que requiera, y deberá quedar ubicada de acuerdo con los anteriores pilares en alguno de los siguientes estados de clasificación.

- **Información Pública:** datos que conforme a la transparencia administrativa y a su naturaleza son de dominio público y puede ser accedido por todas las personas.
- **Privada:** información de interés exclusivo para un área o Dirección específica.
- **Confidencial:** es aquella información industrial, comercial y económica que por motivos estratégicos de competencia tiene carácter confidencial, de modo que no procede su divulgación, adquisición o utilización por parte de terceros, así como la información de tipo personal de los clientes. Dicha información únicamente podrá ser divulgada a personas, entidades y procesos que cuenten con un interés legítimo de obtenerla en el momento indicado y previa autorización.

La información empresarial susceptible de ser declarada confidencial y/o no ser divulgada a terceros es de dos tipos:

- a) La que pueda obtener RACSA en sus relaciones comerciales, de sus clientes, la que, por definición es información confidencial en tanto atañe a éstos quienes la brindan para obtener un servicio.
- b) La relacionada con la actividad de RACSA que haya sido calificada como cubierta por el secreto industrial, comercial o económico, cuando razones calificadas de estrategia comercial o de mercadeo y, en general, por razones comerciales o de libre competencia no resulte conveniente divulgarla a terceros, por cuanto, puede otorgarles una ventaja a sus competidores en un mercado abierto y acarrearle perjuicios a RACSA.

Toda dependencia que administre documentos que contienen información que la Empresa ha declarado confidencial, los identificará de la siguiente manera:

- En el caso de archivos digitales, se consignará en las páginas que conforman el documento una marca de agua con la leyenda “CONFIDENCIAL”, de forma diagonal, semitransparente, con el tipo de letra “calibri”, tamaño 80 y en mayúscula, así como utilizarse el mecanismo de encriptación.
- En el caso que toda la información contenida en un documento haya sido declarada confidencial, se consignará en las páginas que conforman el documento una marca de agua con la leyenda “CONFIDENCIAL”, de forma diagonal, semitransparente, con el tipo de letra “calibri”, tamaño 80 y en mayúscula.
- Se debe indicar al pie de cada una de las páginas (en letra “Arial”, tamaño 10) la siguiente leyenda: “©Documento confidencial

**Propiedad de RACSA, queda prohibida su utilización, reproducción, modificación, distribución, transmisión, manipulación y eliminación, así como cualquier otro uso sin la debida autorización del titular subordinado correspondiente”.**

**Artículo 16. El acceso no autorizado a información privada o confidencial por parte de funcionarios constituye una falta grave que puede desencadenar procesos disciplinarios cuyo resultado dependerá del impacto del incidente presentado.**

**Artículo 17. El personal que posea información clasificada como privada o confidencial, deberá asegurar los medios de protección físicos o digitales brindados por DTIC para que la misma no pueda ser accedida de forma no autorizada por terceros.**

**Artículo 18. Todos los cambios o actualizaciones de los activos de información, deberán estar debidamente documentados y autorizados por quién compete antes de su aplicación e implantación.**

**Artículo 19. El Área de Seguridad y Continuidad desarrollará los lineamientos que instrumentalicen la presente política tomando como base lo consignado en las normas ISO 27001 “Sistemas de Gestión de Seguridad de Información” e ISO 27002 “Controles para la Seguridad de Información” y otras que a futuro sean de interés empresarial.**

## **10. DISPOSICIONES FINALES**

**Con el objetivo de establecer mecanismos más eficientes y dinámicos en la actualización de lineamientos y disposiciones sobre la materia de seguridad de información, en homologación con el formato de las políticas que en esta materia se tienen vigentes en el Grupo ICE, deróguese la “Política de Seguridad de Información de RACSA” aprobada en Junta Directiva en la sesión N°2049 del 28 de octubre del 2014.**

## **11. VIGENCIA**

**La presente política rige a partir de su publicación en el Diario Oficial La Gaceta y su posterior inclusión en la Intranet Empresarial.**

## **12. REVISIÓN Y EVALUACIÓN**

**La presente Política de Seguridad de la Información implica la estandarización y aplicación de la seguridad de la información en la empresa y deberá ser revisada por el Área de Seguridad y Continuidad, al menos una vez al año con el fin de contemplar algún cambio que se deba implementar.”**

**2) La implementación de este acuerdo es responsabilidad de la Gerencia General.**

**Artículo 5º      Reglamento para el reconocimiento económico de los servicios móviles a los colaboradores de RACSA:**

La Presidenta, señora Hazel Valverde Richmond, somete a conocimiento de la Junta Directiva el documento de la Gerencia General de referencia GG-1000-2019 de fecha 22 de agosto mediante el cual presenta una propuesta para regular el reconocimiento económico de los servicios móviles a los colaboradores.

Ingresan a la sala el Gerente General, señor Francisco Calvo Bonilla y la Directora Administrativa Financiera, la señora Patricia Chavarría Lizano, quienes explican que el objetivo de esta gestión es que la Empresa disponga de un instrumento que defina los lineamientos para regular el reconocimiento económico por el uso de servicios móviles y sus respectivos dispositivos propiedad de los colaboradores, para que sean utilizados como herramientas de trabajo. Con el apoyo de una presentación hacen referencia a los elementos estratégicos que sustentan la propuesta, de manera general al contenido del reglamento, con énfasis en la tabla que establece las categorías y el tope máximo a autorizar. Concluyen que por el alcance de la propuesta y según establece la normativa vigente corresponde a la Junta Directiva la aprobación.

La Junta Directiva recomienda valorar la posibilidad de establecer un mecanismo que permita resguardar la información sensible de cara al negocio, ante un escenario de finalización de la relación laboral, específicamente en los casos donde se visualice mayor riesgo. Respecto al monto a reconocer por parte de RACSA, expresan que es conveniente precisar que los topes aprobados no dependerán de los planes del operador, sino a aspectos de sostenibilidad financiera de la Empresa. Agradecen la participación de los representantes de la Administración, quienes toman nota de las observaciones y abandonan la sala a partir de este momento.

**La Junta Directiva, una vez conocida la propuesta, basados en la documentación aportada y en los argumentos expuestos, resuelven:**

**Considerando que:**

- a) **RACSA está inmersa en un mercado de telecomunicaciones en competencia, que demanda mayor agilidad para brindar soluciones integrales de manera oportuna a los clientes.**
- b) **La Estrategia Empresarial 2019-2023, requiere que la Empresa y los colaboradores cuenten con herramientas de gestión que impulsen la consecución de los objetivos empresariales.**
- c) **El uso de servicios móviles como instrumento de trabajo es considerado una necesidad empresarial, para poder facilitar el mejor desempeño de las labores del funcionario y brindar una continuidad del negocio.**
- d) **El Reglamento de Reconocimiento Económico de Servicios Móviles para Colaboradores de RACSA es un instrumento orientado a regular los lineamientos que deben observar los colaboradores de la Empresa que requieran el reconocimiento económico por el uso de servicios móviles en**

labores propias de las funciones que desempeñan, obteniendo mayor agilidad y ajustando las condiciones empresariales a un mercado dinámico e innovador.

- e) Es necesario que RACSA emita formalmente la normativa interna de control que regule la utilización del reconocimiento económico de servicios móviles a los colaboradores de la Empresa con el fin de obtener un instrumento que coadyuve en la consecución de los objetivos empresariales.
- f) De acuerdo con lo establecido en los artículos 188 del Código de Comercio y 6 del Reglamento de la Junta Directiva de RACSA, la aprobación de este tipo de normativa corresponde a la Junta Directiva.
- g) La Asesoría Jurídica, por medio del oficio AJ-458-2019 del 12 de julio del 2019 emite criterio jurídico positivo en relación con dicho Reglamento.
- h) La Dirección Administrativa Financiera por medio del oficio DAF.445.2019 del 13 de agosto del 2019, remite a la Gerencia General la propuesta de Reglamento para el Reconocimiento Económico de Servicios Móviles para Colaboradores de RACSA.
- i) La Gerencia General mediante el oficio de referencia GG.1000.2019 del 22 de agosto del 2019, avala y eleva a aprobación de la Junta Directiva la propuesta de Reglamento para el Reconocimiento Económico de Servicios Móviles a los Colaboradores de RACSA.

Por tanto, se acuerda:

- 1) Aprobar el Reglamento para el Reconocimiento Económico de Servicios Móviles para Colaboradores de RACSA de acuerdo con el siguiente texto:

**“REGLAMENTO PARA EL RECONOCIMIENTO ECONÓMICO  
DE SERVICIOS MÓVILES A LOS COLABORADORES DE RACSA**

**1. OBJETIVO**

Definir los lineamientos que regulan el reconocimiento por el uso de servicios móviles y sus respectivos dispositivos propiedad de los colaboradores de RACSA que sean utilizados como herramienta de trabajo, así como las condiciones, restricciones y requisitos para optar por los mismos.

**2. ALCANCE**

Es aplicable a todos los colaboradores de RACSA que, de acuerdo con su nivel jerárquico, funciones y responsabilidades justifique se haga un reconocimiento económico en razón de hacer uso de los servicios móviles como herramientas de trabajo.

### 3. ABREVIATURAS

**ICE:** Instituto Costarricense de Electricidad.

**LCI:** Ley de Control Interno.

**RACSA:** Radiográfica Costarricense, S.A.

### 4. DEFINICIONES

**Puesto:** posición dentro de la Estructura Organizacional a la cual se le asigna funciones y responsabilidades.

**Reconocimiento económico:** monto que la Empresa reconoce al colaborador por el uso de servicios móviles para el adecuado desempeño de las funciones asignadas.

**Servicios móviles:** servicios de telecomunicaciones que son utilizados como herramienta de trabajo incluye voz, mensajería y datos, no incluye dispositivos móviles (terminales).

### 5. RESPONSABILIDAD

#### Junta Directiva

- Aprobar el Reglamento para el Reconocimiento Económico de Servicios Móviles a los Colaboradores de RACSA así como sus modificaciones y actualizaciones.

#### Gerencia General

- Elevar a Junta Directiva para su aprobación el Reglamento para el Reconocimiento Económico de Servicios Móviles a los Colaboradores de RACSA.
- Velar por la correcta aplicación del Reglamento para el Reconocimiento Económico de Servicios Móviles a los Colaboradores de RACSA.
- Aprobar o rechazar las solicitudes de los colaboradores para el uso de servicios móviles mediante nota formal.

#### Directores

- Velar por la correcta aplicación del Reglamento en la dirección a su cargo.
- Revisar que las solicitudes presentadas por los diferentes Jefes de Departamento para el reconocimiento por uso de servicios móviles de alguno de sus colaboradores a cargo, esté acorde a lo dispuesto en el presente Reglamento.
- Autorizar las solicitudes que cumplan con lo dispuesto en el presente reglamento.
- Remitir periódicamente al Departamento de Tesorería la lista consolidada de los colaboradores que cuentan con dicho beneficio.

#### Jefes de Departamento

- Velar por la correcta aplicación del Reglamento para el Reconocimiento Económico de Servicios Móviles a los Colaboradores de RACSA.

- Realizar el proceso de inclusión de un colaborador al pago por reconocimientos de servicios móviles.
- Verificar que las solicitudes que se presenten contengan la debida justificación, contenido presupuestario y que obedezca a una necesidad empresarial manifiesta y razonable.
- Gestionar ante el Director respectivo las solicitudes para el reconocimiento por uso de servicios móviles de sus colaboradores, para su revisión y aprobación.
- Revisar y actualizar las declaraciones de conocimiento para el reconocimiento de servicios móviles.
- Llevar el registro y control de los colaboradores que cuentan con el beneficio del reconocimiento económico de servicios móviles así como los pagos que se realicen.
- Suscribir todas las declaraciones de conocimiento y finalizarlas por escrito.
- Informar en forma oportuna al Departamento de Tesorería para la suscripción o finalización de las declaraciones de conocimiento.

#### **Departamento de Tesorería**

- Verificar que el comprobante o factura permita hacer el reintegro del dinero en forma oportuna.
- Realizar la liquidación de caja chica correspondiente.
- Enviar un reporte del consumo mensual a la jefatura de cada Departamento que tenga colaboradores que cuenten con el beneficio del reconocimiento económico, para llevar el control y fiscalización del gasto presupuestario.

#### **Departamento de Logística**

- Custodiar la declaración de conocimiento original firmada y expediente de cada colaborador.
- Gestionar a solicitud de la Dirección, Gerencia General o Junta Directiva el proceso de eliminación o suspensión del beneficio.

#### **Colaborador usuario del servicio móvil**

- Cumplir con las disposiciones que establece este Reglamento y firmar la declaración de conocimiento respectiva.

#### **Área Gestión Estratégica y Desempeño Empresarial**

- Realizar la inclusión, modificación, control de cambios y aprobaciones que se le realice al reglamento, así como de custodiar la última versión oficial aprobada del documento.
- Velar para que la presente normativa se ajuste al formato y estructura propia de los Reglamentos, de acuerdo con la Guía para la Estructura y Contenido de los Documentos aprobada.

## **6. DOCUMENTOS DE REFERENCIA**

- Reglamento para la Operación de Fondos de Trabajo de RACSA.
- Ley de Control Interno N°8292.



## REGLAMENTO PARA EL RECONOCIMIENTO ECONÓMICO DE SERVICIOS MÓVILES A LOS COLABORADORES DE RACSA

### Capítulo I. Disposiciones Generales

**Artículo 1.** El presente Reglamento tiene como objetivo establecer los lineamientos que deben observar los colaboradores de RACSA que requieran el reconocimiento económico por el uso de servicios móviles en labores propias de las funciones que desempeñan.

**Artículo 2.** Este Reglamento será de acatamiento obligatorio para todos los colaboradores de la Empresa que gocen del reconocimiento económico.

**Artículo 3.** El monto a reconocer por parte de RACSA se refiere únicamente a los topes aprobados en las categorías según la siguiente tabla.

Tipo	Categoría	Tope máximo autorizado
1	• Gerente General	Total de la factura
2	• Directores	¢26,000
3	• Jefaturas de Departamento que por su índole en las funciones de trabajo justifique el reconocimiento. • Secretaría de Junta Directiva. • Asesores Comerciales Portafolio de servicios de RACSA.	¢18,000
4	• Puestos Técnicos responsables de la operación y mantenimiento de los sistemas que por su índole en las funciones de trabajo justifique el reconocimiento.	¢12,000
5	• Otros que por su índole en las funciones de trabajo justifique el reconocimiento.	¢8,000

**Tabla 1 Reconocimiento Económico por Servicios Móviles**

### Capítulo II. Condiciones para el Reconocimiento del Pago de Servicios Móviles

**Artículo 4.** El reconocimiento económico por el uso del servicio móvil se establece bajo las siguientes condiciones:

- a) El colaborador debe estar dentro de los rangos establecidos en la tabla N°1 y contar con la solicitud aprobada por parte del Director correspondiente.

- b) El servicio de telefonía móvil, voz, mensajería y datos, lo contratará directamente el colaborador.
- c) El colaborador adquiere a su nombre y por su cuenta el plan de consumo, el aparato telefónico, la línea telefónica así como cualquier otro dispositivo u accesorio adicional.
- d) RACSA únicamente reconoce un monto mensual por consumo de hasta el máximo establecido en los topes especificados en la Tabla N°1 del presente Reglamento. El consumo cubre: voz (nacional o internacional), mensajería y datos.
- e) Si el consumo es superior al monto reconocido según la Tabla N°1, el colaborador deberá cubrir dicha diferencia de su propio peculio.
- f) El servicio móvil será post pago brindado por el operador ICE y su marca kölbi.

### **Capítulo III. Procedimiento de solicitud y cancelación del reconocimiento**

**Artículo 5.** El Director del área interesada formaliza la solicitud para el uso de servicios móviles mediante nota formal dirigido al Departamento de Logística, en la cual deberá constar la justificación, el respectivo contenido presupuestario y que obedezca a una necesidad empresarial manifiesta y razonable asociada con la contribución del rol que ejerce el colaborador a la generación de ingresos o la continuidad de los negocios de la Empresa así como el contrato de servicios suscrito con el operador del servicio.

**Artículo 6.** El Departamento de Logística será el responsable de custodiar toda la documentación y elaborar la declaración de conocimiento para firma del colaborador.

**Artículo 7.** Todo colaborador a quien se le autorice el reconocimiento por el uso de servicios móviles, debe firmar una declaración de conocimiento en la cual se fijarán las normas de uso, los derechos y obligaciones de las partes, de acuerdo con lo establecido en el presente Reglamento. La procedencia de dicho derecho se revisará una vez al año por parte del Jefe inmediato.

**Artículo 8:** El colaborador a quien se le autorice el reconocimiento económico deberá indicar el número de teléfono que aportará para ser utilizado en las labores que desempeña y deberá notificar al Departamento de Logística de forma inmediata cualquier cambio en el número de teléfono.

**Artículo 9:** El Jefe respectivo del área interesada debe informar mediante nota formal al Departamento de Logística, cuando un colaborador cambie de puesto o deje de laborar para la Empresa, para que el beneficio sea revocado. Con base en dicha nota el Departamento de Logística preparará una nota formal con el colaborador y coordinará con las áreas internas (Tesorería) la suspensión del pago.

**Artículo 10: Cancelación del monto reconocido:**

- a) El colaborador deberá cancelar el importe atribuible del recibo de consumo de telefonía móvil, voz, mensajería, datos por su cuenta.
- b) De forma mensual en un plazo máximo de 15 días naturales después de la fecha de cancelación de la factura por el servicio, el colaborador deberá presentar el recibo y comprobante de liquidación de caja chica debidamente autorizado al Departamento de Tesorería.
- c) Superado ese plazo, RACSA no reconocerá ni realizará el reembolso al colaborador.
- d) El Departamento de Tesorería procede con la verificación de la información contenida en el comprobante y verifica que el recibo esté dentro del tiempo establecido y realiza el pago al colaborador.

**Capítulo IV. Contratación de Servicio y Adquisición de Equipo por parte del colaborador**

**Artículo 11.** El colaborador contratará directamente y por su propia cuenta el servicio de telefonía móvil, voz, mensajería y datos el cual debe estar a su nombre y en la modalidad post pago.

**Artículo 12.** El colaborador adquiere bajo su cuenta y riesgo el equipo terminal y accesorios requerido de acuerdo con las características de la red del proveedor del servicio.

**Artículo 13.** El colaborador debe garantizar que el servicio de telefonía móvil y el dispositivo se encuentren disponibles durante el tiempo que se mantenga el reconocimiento para el desempeño de las funciones de su puesto; de lo contrario el Director o Jefe respectivo deberá valorar si mantiene las condiciones o si por el contrario se elimina el reconocimiento.

**Artículo 14.** El colaborador es responsable de cancelar al operador de servicio kôlbi los cargos que correspondan por uso de servicios móviles post pago, liberándose RACSA de responsabilidad alguna por este concepto.

**Artículo 15.** El colaborador es el único responsable de realizar ante el operador del servicio kôlbi los trámites requeridos para habilitar y mantener operando el servicio, así como realizar los reclamos que procedan de acuerdo con los términos del contrato firmado entre las partes.

**Artículo 16.** El colaborador es el único responsable por el equipo terminal adquirido para el uso del servicio móvil, por lo tanto, en caso de daños, pérdida, extravío o robo, RACSA no tiene responsabilidad alguna con respecto al equipo adquirido. Es responsabilidad del colaborador reponer de forma inmediata el terminal para tener disponibilidad del servicio.

**Artículo 17.** El reconocimiento económico a un colaborador(a) en razón de su cargo no genera derecho alguno, ni se considera parte de su salario, ni salario en especie. En consecuencia, RACSA lo puede retirar en cualquier

momento, por incumplimiento a las disposiciones de este Reglamento, por limitaciones presupuestarias o por cualquier otra causa a juicio de RACSA.

**Artículo 18.** Cuando un colaborador se encuentre en periodo de vacaciones, incapacitado, con permiso con goce y sin goce de salario por un periodo de 5 días hábiles o más, el reconocimiento económico se cancelará proporcionalmente según la siguiente escala para tal efecto se seguirá el procedimiento descrito en el artículo 19:

Días	Porcentaje a cancelar
5	75%
5 a 10	50%
10 a 15	24%
15 o más	0%

**Artículo 19.** Procedimiento de cancelación proporcional del beneficio económico:

- a) El Director o Jefe correspondiente deberá enviar al Departamento de Tesorería una lista al final de cada mes con los nombres de los colaboradores a su cargo que estuvieron ausentes de sus labores por los motivos indicados en el artículo 18.
- b) El Departamento de Tesorería revisa la lista y realiza el procedimiento según el artículo 10 y siguiendo lo establecido en la escala del artículo 18.

**Artículo 20:** El incumplimiento de las disposiciones contenidas en este Reglamento hará acreedor(a) al (la) colaborador(a) responsable, de las medidas disciplinarias, civiles y penales, contenidas en el Estatuto de Personal, la Ley General de Control Interno y el Código de Trabajo cuando resulten procedentes.

**Artículo 21. Restricción de asignación:** El beneficio económico será asignado a una única línea telefónica por colaborador, sin excepción alguna.

**Artículo 22.** La jefatura podrá solicitar un desglose de las llamadas del colaborador, que cuente con el reconocimiento económico de servicios móviles, como mecanismo operativo necesario para controlar el uso de los recursos (beneficio económico) asignados a los colaboradores. Conforme a lo establecido en artículo 14, inciso d) de la Ley General Control Interno.

## Capítulo V. Obligaciones

**Artículo 23:** Son obligaciones del colaborador las siguientes:

- a) Conocer y cumplir con lo que establece y dispone el presente reglamento.

- b) Presentar recibo telefónico y comprobante de liquidación de caja chica después de cancelado el recibo telefónico, o no será válido el reintegro del dinero.
- c) Asumir el gasto de la factura del servicio kölbi si el consumo excede el monto reconocido por RACSA.
- d) Hacer uso adecuado del beneficio brindado por la Empresa, que sea seguro, que se utilice exclusivamente en el desempeño de las funciones designadas por la Empresa.
- e) Suscribir la Declaratoria de Conocimiento.
- f) Indicar el número de teléfono que aportará para ser utilizado en las labores que desempeña.
- g) Contratar directamente y por su propia cuenta el servicio de telefonía móvil, voz, mensajería y datos en la modalidad post pago.
- h) Mantener operando el servicio de telefonía móvil.

## Capítulo VI. Disposiciones finales

### Artículo 24: Eliminación del Reconocimiento

- a) RACSA se reserva la potestad de eliminar este reconocimiento en cualquier momento, sin responsabilidad, al cambiar las condiciones que dieron origen al beneficio o a discreción de la Empresa.
- b) El trámite de retiro del reconocimiento económico de un colaborador será realizado por el jefe inmediato respectivo, mediante una nota formal en donde indica el motivo por el cual se elimina el reconocimiento, la nota debe enviarla al Departamento de Logística con copia al colaborador.

**Artículo 25:** Todo colaborador al que se le justifique el beneficio de reconocimiento económico de servicios Móviles, deberá suscribir una declaración de conocimiento del Reglamento para el Reconocimiento Económico de Servicios Móviles a los Colaboradores de RACSA, según el siguiente formato:

**“DECLARACIÓN DE CONOCIMIENTO DEL  
REGLAMENTO PARA EL RECONOCIMIENTO  
ECONÓMICO DE SERVICIOS MÓVILES  
A LOS COLABORADORES DE RACSA**

*El suscrito \_\_\_\_\_ en mi condición de colaborador de RADIOGRÁFICA COSTARRICENSE, S.A., declaro que conozco el Reglamento para el Reconocimiento Económico de Servicios Móviles y asumo el compromiso personal de cumplimiento con la Empresa, haciendo todo a mi alcance para cumplir dicho cuerpo normativo.*

*Soy consciente que el incumplimiento comprobado de las disposiciones contenidas en este Reglamento hará acreedor(a) al (la) colaborador(a) responsable, de las medidas disciplinarias, civiles y penales, contenidas en el Estatuto de Personal, la Ley*

**General de Control Interno y el Código de Trabajo cuando resulten procedentes.**

**En fe de lo anterior, firmo en la ciudad de, \_\_\_\_\_ el día \_\_\_\_\_ de \_\_\_\_\_ del año \_\_\_\_\_.**

**Firma:** \_\_\_\_\_

**Identificación:** \_\_\_\_\_

**c.c. Expediente Departamento de Logística”.**

#### **Artículo 26: Vigencia**

- a) El presente Reglamento deroga la norma emitida el 1° de mayo del 2005 según comunicación en nota 20.SGR.430.2005 y cualquier otra reglamentación o disposición relacionada al reconocimiento de servicios móviles en RACSA.
- b) Este Reglamento rige a partir de su publicación en el sitio web oficial de RACSA.

#### **7. REVISIÓN Y EVALUACIÓN**

Se debe realizar una revisión anual del Reglamento por parte del Departamento de Logística en conjunto con Área de Gestión Estratégica y Desempeño Empresarial, esto para verificar si el Reglamento requiere de modificaciones.”

- 2) La implementación de este acuerdo es responsabilidad de la Gerencia General.

#### **Artículo 6°      Operador Móvil Virtual “fullmóvil”. Informe mensual. Confidencial:**

Confidencialidad otorgada por el Consejo Directivo del ICE en la sesión N°6073 del 14 de enero del 2014.

### **CAPÍTULO III    ASUNTOS DE JUNTA DIRECTIVA**

#### **Artículo 7°      Oportunidades de negocio con el ICE. Oficio del Comité de Vigilancia:**

La Junta Directiva señala que el Comité de Vigilancia de la Empresa, mediante la nota de referencia CV.41.2019 de fecha 23 de agosto, somete a conocimiento un informe preparado por la Administración sobre las oportunidades de negocio que se han desarrollado con el ICE como cliente que no se han concretado y el impacto que produce en el plan financiero, tema que también fue abordado en el Informe de Gestión correspondiente al I Semestre del 2019, conocido en la sesión N°2235 del pasado 13 de agosto, en donde la recomendación fue aceptada y se encomienda a la Gerencia para que presente un procedimiento orientado al

cumplimiento de las obligaciones y compromisos de los clientes durante el proceso de formalización de las oportunidades de negocio.

En virtud de lo anterior, agradecen la información suministrada por el Comité de Vigilancia y la dan por recibida.

## **CAPÍTULO IV COMENTARIOS Y PROPOSICIONES**

### **Artículo 8º      Gobernanza Empresarial:**

La Junta Directiva, conforme a lo dispuesto en la sesión anterior, solicitan al Gerente General ingresar a la sala para analizar de manera integral temas de gobernanza empresarial, estratégicos y de carácter empresarial.

A partir de este momento se incorpora el Gerente General, señor Francisco Calvo Bonilla a la sesión.

La Junta Directiva expresa que el motivo de este acercamiento es sostener un espacio para manifestar a la Gerencia General la preocupación sobre la calidad y consistencia de la información que se somete a discusión y resolución de este órgano colegiado, así como comentar las inquietudes que han surgido sobre la metodología que sustenta el Modelo de Clasificación y Valoración de Puestos de la Empresa y la Escala Salarial, con el propósito de gestionar los riesgos de manera oportuna.

Comentan que las propuestas que se someten a conocimiento y resolución deben estar debidamente respaldadas, con los diferentes criterios, como una acción propia que garantice la seguridad jurídica de las decisiones que adopta este órgano colegiado.

Expresan que tanto la Gerencia General como el equipo que lo acompaña tomen conciencia sobre la responsabilidad de sus cargos y la obligación de sustentar debidamente las propuestas, así como aplicar mayor rigurosidad y criterio, con posiciones firmes y contundentes que transmitan seguridad y certeza, bajo el principio de salvaguardar el interés empresarial.

Indican lo que en lo respecta al Modelo de Compensación y Valoración de Puestos de la Empresa, la Gerencia General deberá definir un plan remedial que permita mantener la equidad empresarial, los valores respecto al mercado y la sostenibilidad financiera.

El Gerente General, señor Francisco Calvo Bonilla, comenta que realiza un proceso de control permanente y se apoya en las competencias funcionales de cada área; no obstante, reconoce que, por diferentes limitaciones, en las últimas ocasiones se han identificado debilidades en el proceso, por lo que toma nota de las observaciones con el propósito de capitalizar la experiencia. En ese sentido, procederá a trasladar las inquietudes al siguiente nivel de dirección, como un llamado a mejorar los procesos y definir el plan correctivo en lo que corresponde al Modelo de Clasificación y Valoración de Puestos, para presentar la propuesta respectiva en los próximos días.



Finalmente agradecen la participación del señor Calvo Bonilla, quien abandona la sala a partir de este momento.

*La Presidenta, señora Hazel Valverde Richmond, levanta la sesión al ser las veintiún horas y treinta minutos. Agradece a los Directivos y a los representantes de la Administración su asistencia y participación.*

*Secretaría Junta Directiva  
6/9/2019 08:08 hrs*