Hagamos el futuro juntos

# POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN DE RACSA

| Gerencia General<br>Dirección de Operaciones | | |
|---|---|---|
| **Elaborado por:** | **Revisado por:** | **Aprobado por:** |
| Paula Porras Aguilar/Carolina Morales Camacho/Vladimir Sequeira Cole | Yandell Salazar Soto/Illiana Maria Rodriguez Quiros | Junta Directiva<br>Sesión N°2506 |
| Código: DO-PT-001 | Versión: 01 | Fecha: 19/09/2024 |

## CONTENIDO

## 1. 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 sus normas complementarias.

## 2. ALCANCE

La Política de Seguridad de la Información de RACSA (en adelante la política) es de acatamiento obligatorio para la Junta Directiva y todos los niveles jerárquicos de la organización, incluyendo unidades de apoyo, así como practicantes y terceros con quienes RACSA interactúe y con los cuales se tenga acceso a información empresarial, comercial o de carácter sensible a través de documentos, equipos de cómputo, infraestructura tecnológica y canales de comunicación.

También aquellas personas tanto físicas como jurídicas con quienes se firmen acuerdos de confidencialidad específicos con RACSA deberán cumplir los principios de confidencialidad de la presente política y del cuerpo normativo que la instrumentalice.

## 3. ABREVIATURAS

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

## 4. DEFINICIONES

**Activo de Información:** se entiende por activo de Información todo aquel elemento digital o físico que tiene o transfiere información de la Empresa que debe ser protegida según su importancia.
**Ataque:** intento de destruir, exponer, alterar, inhabilitar, robar u obtener acceso no autorizado o hacer uso no autorizado de un activo.
**Confidencialidad:** es la propiedad de la información, por la que se garantiza que está accesible únicamente a individuos, entidades o procesos autorizados a acceder a dicha información.
**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 requerida por una parte autorizada.

**Evento de Seguridad de la Información:** ocurrencia identificada del estado de un sistema, servicio o red que indica una posible infracción a la política de seguridad de la información, falla de los controles o una situación previamente desconocida que puede ser relevante para la seguridad.
**Incidente de Seguridad de la Información:** uno o una serie de eventos de seguridad de la información no deseados o inesperados que tienen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.
**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.
**Parte Interesada:** persona u organización que puede afectar, ser afectada, o percibirse a sí misma afectada por una decisión o actividad de la empresa (toda persona, jurídica o física, como proveedores, contratistas, socios comerciales, consultores, entidades regulatorias, casa matriz, entidades de gobierno, clientes, entre otros).
**Seguridad de la Información:** capacidad de preservar la confidencialidad, integridad y disponibilidad de la información.
**Sistema de Gestión de Seguridad de la Información (SGSI):** un SGSI se compone de las políticas, procedimientos, directrices, recursos y actividades asociadas, administradas colectivamente por la Empresa, en la búsqueda de la protección de sus activos de información.

## 5. RESPONSABILIDAD

*Junta Directiva:*

- Aprobar la Política de Seguridad de la Información, así como sus modificaciones.

*Gerencia General:*

- Elevar a la Junta Directiva la política para su respectiva aprobación.
- Apoyar la gestión transversal empresarial del Proceso de Seguridad de la Información.
- Aprobar los recursos humanos y financieros necesarios para implementar la presente política y el Sistema de Gestión de Seguridad de la Información.

*Dirección de Operaciones:*

- Elevar a la Gerencia General para su aprobación la normativa interna que instrumentalice la Política de Seguridad de la Información de RACSA.

*Área de Gestión Operativa (Dirección de Operaciones):*

- Promover e implementar una cultura de Seguridad de la Información en RACSA.
- Definir las directrices empresariales, la normativa y cualquier otra medida necesaria para la gobernabilidad y gestión de Seguridad de la Información.

- Gestionar el aprovisionamiento de los recursos necesarios (presupuesto, capacitación empresarial, recurso humano, normativa) para la gestión transversal 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.
- Supervisar el cumplimiento de la normativa de Seguridad de la Información en los procesos empresariales.

*Departamento de Gestión de Infraestructura de Tecnologías de Información:*

- Diseñar el Plan de Inversiones en Seguridad informática para RACSA.
- Implementar el Plan aprobado en Seguridad informática para RACSA.
- Presentar informes semestrales de la ejecución del Plan de Seguridad Informática.
- Atender la Gestión de Incidentes de Seguridad de la Información de acuerdo con lo indicado en el Proceso SOP10 – Gestión Integral de la Seguridad.

*Unidad de Prensa y Comunicación:*

- Brindar el soporte necesario para las campañas de divulgación de la presente política.
- Ejercer como el canal oficial de comunicación de RACSA para la gestión de Incidentes de Seguridad de la Información o comunicaciones relacionadas a Seguridad de la Información.

*Direcciones:*

- Proveer en tiempo y forma los requerimientos de información y recursos que solicite el Proceso SOP10 - Gestión Integral de Seguridad de la Información para la instrumentalización de esta política y la gestión de incidentes de Seguridad de la Información.
- Impulsar proactivamente la gestión de Seguridad de la Información en todos los departamentos a cargo.
- Acatar y promover recomendaciones en materia de Seguridad de la Información.
- Elevar las declaratorias de confidencialidad en las áreas respectivas.

*Jefaturas:*

- Alertar riesgos detectados de ciberseguridad de todos los procesos a cargo al Departamento de Gestión de Infraestructura de Tecnologías de Información.
- Velar por el cumplimiento de esta política en las áreas de su competencia.
- Identificar e implementar acciones de mejora de Seguridad de la Información concretas en su área.
- Realizar la identificación y tratamiento de riesgos de Seguridad de la Información en los procesos a cargo.

- Identificar, de acuerdo con la Guía para la Creación de Inventario y Clasificación de Activos de Información, aquella información que deba ser catalogada como pública o de uso restringido.
- Identificar y designar los roles asociados a la Seguridad de la Información de su área.
- Reportar oportunamente, al Departamento de Gestión de Infraestructura de Tecnologías de Información, los riesgos, eventos o sospechas de vulnerabilidades o amenazas de Seguridad de la Información.

*Funcionarios:*

- Acatar en todos sus extremos la presente Política de Seguridad de la Información y el cuerpo normativo que la complementa.

*Departamento de Estrategia e Innovación:*

- Identificar y aplicar, en conjunto con el Área de Gestión Operativa, modificaciones a la presente política.
- Custodiar la última versión oficial aprobada del documento e incluirla en el repositorio del Sistema de Gestión Integral de RACSA.

## 6. DOCUMENTOS DE REFERENCIA

- Estatuto de Personal de RACSA.
- Guía para la Creación de Inventario y Clasificación de Activos de Información.
- INTE/ISO/IEC 27000:2018 Tecnologías de la información. Técnicas de Seguridad. Sistemas de gestión de la seguridad de la información. Visión general y vocabulario.
- INTE/ISO/IEC 27001:2023 Seguridad de la información, ciberseguridad y protección de la privacidad. Sistemas de gestión de la seguridad de la información. Requisitos.
- INTE/ISO/IEC 27002:2023 Seguridad de la información, ciberseguridad y protección de la privacidad. Controles de seguridad de la información.
- Ley N°8660, Ley de Fortalecimiento y Modernización de las Entidades Públicas del Sector Telecomunicaciones. Artículo 35.
- Marco de Referencia COBIT 2019 – Proceso APO12 Gestionar el Riesgo.
- Marco de Referencia COBIT 2019 – Proceso APO13 Gestionar la Seguridad.
- Marco de Referencia COBIT 2019 – Proceso DSS01 Gestionar las Operaciones.
- Marco de Referencia COBIT 2019 – Proceso DSS05 Gestionar los Servicios de Seguridad.
- Política Corporativa de Ciberseguridad.
- Política Corporativa de Confidencialidad de la Información.
- Procedimiento para Declarar Confidencial la Información.
- Proceso SOP10 – Gestión Integral de la Seguridad.
- Reglamento de Uso de Recursos Informáticos de RACSA.

# 7. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN DE RACSA

## 7.1 CAPÍTULO I – DISPOSICIONES GENERALES

**Artículo 1. Compromiso.** RACSA reconoce la información como un activo vital y estratégico para la Empresa, por tanto, se compromete a establecer las acciones que apoyen 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. Recursos.** Los procesos responsables de la Gestión de la Seguridad en sus distintos enfoques serán provistos de los recursos tanto financieros como humanos necesarios para su correcto funcionamiento.

**Artículo 3. Cumplimiento Normativo.** RACSA aplicará la legislación vigente en materia de Seguridad de la Información y la norma internacional ISO 27001 “Sistemas de gestión de la seguridad de la información” como marco de referencia y de mejores prácticas para aplicación interna.

**Artículo 4. Normativa Interna.** RACSA creará y dará mantenimiento al cuerpo normativo que instrumentalice esta política. Dicho cuerpo normativo será de acatamiento obligatorio para funcionarios y terceros que posean información de RACSA.

**Artículo 5. Cultura.** RACSA 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 el impacto y probabilidad de la materialización de incidentes de Seguridad de la Información.

**Artículo 6. Acceso.** RACSA 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. Protección.** RACSA establecerá los mecanismos para proteger la información catalogada como confidencial mediante declaratorias de confidencialidad, controles de seguridad y convenios de confidencialidad en las relaciones comerciales o de otra índole.

**Artículo 8. Acompañamiento.** El Área de Gestión Operativa acompañará a la Gerencia General, Directores, Jefaturas, procesos y funcionarios involucrados en la definición de roles y responsabilidades en relación con la Seguridad de la Información.

**Artículo 9. Clasificación de Información.** 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 de confidencialidad, integridad y disponibilidad, siguiendo los procedimientos aprobados.

**Artículo 10. Mecanismos Jurídicos.** RACSA establecerá los mecanismos jurídicos necesarios para salvaguardar el uso de la información en la gestión con terceros y para resguardar la información confidencial.

**Artículo 11. Controles de Acceso.** 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. Responsabilidad de Credenciales**. Los funcionarios son responsables de la confidencialidad y el manejo de sus credenciales de acceso y la información que acceden y procesan mediante cualquier activo de soporte (físico, correo electrónico, internet, entre otros similares). La información que sea accedida deberá atenderse de tal manera que se evite el robo y fuga de información a terceros no autorizados.

**Artículo 13. Uso No Autorizado.** El uso no autorizado de la información empresarial 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. Monitoreo y Privacidad.** Con el objetivo de resguardar los intereses empresariales de seguridad de la información y ciberseguridad, además de la confidencialidad, integridad y disponibilidad de la información empresarial, RACSA se reserva el derecho de monitorear actividades de conectividad, cambios en la configuración local, u otras actividades realizadas por los usuarios en los sistemas de información, equipos de usuario final y plataformas tecnológicas, asegurando siempre el respeto al derecho constitucional de intimidad de las comunicaciones y la información personal.

**Artículo 15. Confidencialidad.** La información que se identifique como confidencial deberá cumplir lo establecido en la Política Corporativa de Confidencialidad de la Información y en el Procedimiento para Declarar Confidencial la Información vigentes.

**Artículo 16. Faltas Graves.** 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, conforme a lo establecido en el Estatuto de Personal de RACSA.

**Artículo 17. Protección Física y Digital.** El personal que posea información clasificada como privada o confidencial, deberá asegurarse que cuenta con los medios de protección físicos o digitales, brindados por el Departamento de Gestión de Infraestructura de Tecnologías de Información para que la misma no pueda ser accedida de forma no autorizada por terceros.

**Artículo 18. Lineamientos.** El Área de Gestión Operativa desarrollará los lineamientos que instrumentalicen la presente política tomando como base lo consignado en las normas ISO 27001 “Sistemas de gestión de la seguridad de la información” e ISO 27002 “Controles de seguridad de la información” y otras que a futuro sean de interés empresarial.

## 7.2 CAPÍTULO II – DISPOSICIONES FINALES

**Artículo 19. Vigencia.** Esta política deja sin efecto la Política de Seguridad de la Información de RACSA aprobada por Junta Directiva en la sesión N°2296 del 4 de noviembre del 2020 y publicada en El Diario Oficial La Gaceta del 3 de diciembre de 2020 y rige a partir del día de su publicación en El Diario Oficial La Gaceta.