

La Uruca, San José, Costa Rica, jueves 26 de setiembre del 2019

AÑO CXLI

Nº 182

84 páginas



Imprenta Nacional
Costa Rica

COMUNICADO OFICIAL

Se informa que la oficina de la Imprenta Nacional ubicada en el Registro Nacional, en Curridabat, permanecerá cerrada el viernes 27 de setiembre de 2019, debido al cierre de esa institución por la conmemoración del 154 aniversario de la función registral en Costa Rica.

Nuestros servicios continuarán habilitados en las oficinas centrales en la Uruca y a través del sitio web www.imprentanacional.go.cr.



Imprenta Nacional
Costa Rica

CAPÍTULO V

Reincorporación a la modalidad presencial

Artículo 18.—**Causas para la reincorporación a la modalidad presencial.** La persona teletrabajadora tendrá que reincorporarse a la modalidad presencial cuando se dé alguna de las siguientes circunstancias:

- a) Cambio en las condiciones de la persona teletrabajadora: cuando la jefatura superior o la URH conozca del incumplimiento o cambio de alguna de las condiciones o requisitos solicitados en este Reglamento.
- b) Por conveniencia institucional: Cuando se determine por las Autoridades Superiores o jefatura inmediata, que existe un interés institucional para que la persona teletrabajadora continúe sus labores presencialmente.
- c) Por interés de la persona teletrabajadora: Cuando la persona teletrabajadora solicite la reincorporación a la modalidad presencial debe comunicarlo oportunamente a su superior inmediato y a la URH, para proceder con su reincorporación a la mayor brevedad posible.

Artículo 19.—Cuando la persona teletrabajadora no logre los objetivos y metas planteados en el plan de trabajo, el superior inmediato hará un análisis de las causas que obstaculizaron el alcance de los objetivos y metas, en caso necesario gestionará las acciones que corresponda, en el marco de lo establecido en el artículo 18 de este reglamento.

CAPÍTULO VI

Recursos Informáticos

Artículo 20.—**Recursos informáticos.** La modalidad de teletrabajo está sujeta a que el INA suministre la computadora con los dispositivos y accesorios requeridos a la persona funcionaria que presta servicios bajo la modalidad de teletrabajo.

CAPÍTULO VII

Disposiciones finales

Artículo 21.—Lo no contemplado en este reglamento. En caso de omisiones en materia laboral, técnica y administrativa en el presente reglamento, se aplicará la normativa establecida por ley o vía administrativa.

Artículo 22.—**Vigencia.** El presente reglamento rige a partir del primero de noviembre de dos mil diecinueve.

Disposiciones transitorias

Transitorio I.—Dentro de los tres meses siguientes de la entrada en vigencia de este reglamento, la URH debe actualizar los instructivos, los procedimientos y formularios necesarios para aplicarlo a las personas funcionarias que se encuentran laborando en esta modalidad. Así como la incorporación de instructivo, procedimiento y formularios requeridos para aplicar a la modalidad de teletrabajo.

Lic. Allan Altamirano Díaz, Jefe.—1 vez.—O. C. N° 26976.—Solicitud N° 163447.—(IN2019385162).

INSTITUTO NACIONAL DE LAS MUJERES

PROVEEDURÍA

REFORMA PARCIAL AL REGLAMENTO DE ATENCIÓN LEGAL DEL INSTITUTO NACIONAL DE LAS MUJERES (INAMU)**Considerando:**

I.—Que el inciso d) del artículo 8 de la Ley de Creación del INAMU, número 7801, faculta a la Junta Directiva a dictar los reglamentos internos de la Institución.

II.—Que resulta necesario modificar el artículo 18 relacionado con el procedimiento que el INAMU debe dictar sobre el Reglamento de Servicios de Atención Legal vigente en el Instituto Nacional de las Mujeres. **Por tanto,**

Mediante acuerdo número cuatro de la Sesión Ordinaria N°20-2019 del 22 de agosto de 2019, la Junta Directiva del Instituto Nacional de las Mujeres, acuerda una reforma parcial Reglamento de Atención Legal del Instituto Nacional de las Mujeres, de conformidad con lo siguiente:

Artículo 1°—Se modifica la redacción del artículo 18°, de la siguiente forma:

Artículo 18°—**Del procedimiento.** El Instituto Nacional de las Mujeres procederá a dictar un procedimiento sobre lo regulado en el presente Reglamento, el cual será elaborado por el Área de Violencia de Género, revisado por la Dirección Técnica y aprobado por la Presidencia Ejecutiva. De previo a entrar en vigencia dicho procedimiento, el mismo será de conocimiento de la Junta Directiva.

Artículo 8°—Rige a partir de su publicación en el Diario Oficial *La Gaceta*.

Encargado de la publicación:

Carlos Barquero Trigueros, Coordinador.—1 vez.—O.C. N° 2123.—Solicitud N° 163327.—(IN2019384988).

AVISOS**RADIOGRÁFICA COSTARRICENSE S. A.**

Con fundamento en el acuerdo tomado por la Junta Directiva, en el artículo 4° de la sesión ordinaria N° 2238, celebrada el 3 de setiembre del 2019, se aprueba el la Política de Seguridad de la Información de Radiográfica Costarricense S.A., de la siguiente manera:

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.