CONTENIDO

1. OBJETIVO

Definir las responsabilidades y las prácticas aceptadas para mantener un ambiente tecnológico seguro, establecer las directrices y lineamientos relacionados con la seguridad de las plataformas tecnológicas en la nube y mantener un manejo seguro de la información en estas.

2. ALCANCE.

Aplica a todos los servicios en la nube (SaaS, PaaS, IaaS) contratados por Proindesa y Sociedades Administradas (en adelante la Organización)[1] así como a todos los funcionarios, administradores de los sitios y terceros (proveedores) que interactúan con la infraestructura tecnológica que soporta los servicios implementados en la nube.

3. DEFINICIONES

Las definiciones relevantes para la interpretación de esta política se encuentran relacionadas en el documento *Glosario de Gestión de Riesgos PNDS-FR-GRC-07*

4. PRINCIPIOS

Estos principios se aplican en todas las fases del ciclo de vida de la información: creación, transmisión, almacenamiento y eliminación.

- **CONFIDENCIALIDAD:** Se refiere a la cualidad de los elementos de información almacenados y procesados en un sistema informático, que busca asegurar que la información sea accedida sólo por quienes tienen una necesidad legítima para la realización de sus funciones, actividades o negocios con el fin de prevenir el uso o divulgación de esta en forma no autorizada.

- **INTEGRIDAD:** Se refiere a la cualidad de mantener la validez y consistencia de los elementos de información almacenados y procesados en un sistema informático, protegiéndolos contra modificaciones no autorizadas ni planeadas, realizadas con o sin intención.

- **DISPONIBILIDAD:** Se refiere a la cualidad de poder tener disponibles cuando sean requeridos, los elementos de información almacenados y procesados en un sistema informático.

[1] En virtud del acuerdo de colaboración empresarial suscrito entre Proindesa S.A.S. y estas sociedades, y cualquier otra operación de estas.

- **PRIVACIDAD o RESERVA**: Hace referencia a que la información personal sólo pueda ser utilizada para los propósitos con que fue obtenida del titular y única y exclusivamente para fines del negocio. Conlleva la obligación de no utilizar, revelar o distribuir la información adquirida para fines diferentes para los cuales fue obtenida del titular y única y exclusivamente para fines del negocio. Análisis de Riesgos *Los riesgos asociados a la implementación del modelo de Cloud Computing deben ser gestionados de acuerdo con su valor, impacto y probabilidad de ocurrencia incluidos los riesgos operativos que se puedan generar*.

5. ORGANIZACIÓN Y RESPONSABILIDADES

La administración de esta Política es responsabilidad del Coordinador de Ciberseguridad y S.I y del Líder de Riesgo y Cumplimiento o quienes hagan sus veces, con apoyo de la Gerencia de T.I y quienes al interior de la Organización desempeñen los roles asociados a la gestión de la Ciberseguridad y Seguridad de la Información (S.I.).

La Organización establece un Modelo de Responsabilidad Compartida entre el proveedor de servicio contratado en la Nube (SaaS, PaaS, IaaS) y la Organización, para lo cual se definen de manera contractual las responsabilidades de administración y configuración de seguridad necesarias que garanticen el correcto funcionamiento de los servicios para las operaciones propias del negocio.

6. POLÍTICAS

6.1. Análisis de Riesgos

6.1.1. Los riesgos asociados a la implementación del modelo de Cloud Computing deben ser gestionados de acuerdo con su valor, impacto y probabilidad de ocurrencia incluidos los riesgos operativos que se puedan generar.

La información que se encuentre en el ambiente de Cloud Computing debe protegerse con base en su valor y en el riesgo en que se pueda ver comprometida.

Previo a la adopción de cualquier modelo de servicios en la nube (SaaS, PaaS, IaaS), la Organización deberá llevar a cabo un proceso estructurado de identificación y evaluación de los riesgos asociados a través de la matriz ITRM suministrada por Corficolombiana, incluyendo aquellos relacionados con la seguridad de la información, la ciberseguridad y la operación del servicio (Arquitectura de Seguridad y Modelo de Controles).

Los proveedores seleccionados deberán contar con una metodología formal y comprobable para la gestión de riesgos, que permita identificar, medir, mitigar, controlar y monitorear los riesgos operacionales del servicio contratado. Esta metodología debe considerar el valor de los activos involucrados, la probabilidad de ocurrencia de los riesgos y su impacto potencial en la continuidad y objetivos del negocio.

El Área líder de contratación para la ejecución de proyectos que utilicen servicios de la nube debe asegurar que se cumplan con los requisitos y controles establecidos en el formato PNDS-FR-GRC-15-*Requerimientos mínimos de Cloud* que aseguren la protección en el ciclo de vida de la información (Origen, Transporte, reposo y eliminación.).

Estos controles deben ser revisados y actualizados de forma continua por las áreas de Ciberseguridad y S.I y la Gerencia T.I, en función de la evolución de las amenazas, los cambios tecnológicos y las necesidades del negocio.

Se debe implementar estrategias de concientización y formación al menos 1 vez al año, lideradas por el área de Riesgo y Cumplimiento, (capacitaciones, piezas de comunicación, entre otros) dirigidas a funcionarios y otras partes interesadas reforzando los roles y responsabilidades, brindando actualización sobre amenazas emergentes y buenas prácticas para proteger los activos de información en materia de Ciberseguridad y S.I de la Organización, de acuerdo con lo establecido el en documento *PNDS-PR-TAH-02 Procedimiento Inducción y reinducción a funcionarios*

Cada funcionario que accede o gestiona información dentro de la Organización debe estar plenamente informado y comprometido con el cumplimiento de los procedimientos establecidos para el reporte de incidentes y eventos que puedan afectar la ciberseguridad y la seguridad de la información (S.I.), (*Ver formato PNDS-FR-GRC-06 Bitácora de Eventos e Incidentes de Seguridad la Información*) con el fin de mantener la confidencialidad, integridad y disponibilidad de la información, mediante el aseguramiento e identificación de ciberamenazas. La divulgación de los procedimientos relacionados es realizada por el área de Calidad.

Toda sospecha, anomalía, eventos o incidente relacionado con la Seguridad de la Información debe ser reportado de manera inmediata al área de Ciberseguridad y S.I., a través del buzón oficial: seguridad.informacion@proindesa.com.co

6.2. Cumplimiento de regulaciones

6.2.1. El modelo de servicios en nube debe cumplir con la normatividad aplicable a la Organización.

El modelo de servicios en la nube debe estar acorde al cumplimiento de la normatividad aplicable a la Organización, por lo que, siempre se debe verificar que se está alineado y se está cumpliendo con las leyes y regulaciones que sean pertinentes por decisiones de negocio.

El uso de la información por terceros, que se encuentre alojada en cualquier plataforma de la nube, debe ser formalizado por medio de acuerdos y/o cláusulas de servicios en nube en los contratos.

Para el cumplimiento de este numeral se deben identificar, registrar y actualizar anualmente los requerimientos regulatorios en los normogramas de la Organización y para cada implementación o proyecto orientado a nube de acuerdo con lo registrado en el documento PNDS-PR-GRC-10 Procedimiento de Actualización Normograma.

6.3. Portabilidad e Interoperatividad

6.3.1. La infraestructura tecnológica debe preservar los controles de seguridad cuando se realicen cambios en su infraestructura o servicios

En el ambiente de servicios en la nube que ameriten cambios de entornos de desarrollo e infraestructura por el proveedor se deben mantener los controles de Ciberseguridad y S.I. y los requisitos mínimos definidos en el formato PNDS-FR-GRC-15-*Requrimientos mínimos de Cloud*.

En caso de migración entre proveedores, se debe garantizar la portabilidad segura de datos mediante cifrado y validación de integridad, conforme a ISO/IEC 27017.

6.4. Protección de Acceso físico

6.4.1. Todas las áreas físicas del ambiente tecnológico donde opere el modelo de servicios en la nube deben tener un nivel de seguridad acorde con el valor de la información de la Organización.

La Infraestructura física que soporte el servicio de la nube de la Organización, debe cumplir con los requisitos mínimos establecidos en el formato PNDS-FR-GRC-15-*Requerimientos mínimos de Cloud*

6.5. Continuidad del negocio

6.5.1. Todos los activos de información y procesos críticos que corren en el ambiente de servicios en la nube deben contar con un plan de Continuidad del Negocio y un Plan de Recuperación de Desastres.

La información debe estar disponible para la Organización en el momento en que se requiera, garantizando su integridad, confidencialidad y disponibilidad, incluso ante eventos disruptivos. Para ello, el ambiente de servicios en la nube que dependan de procesos críticos de la organización debe contar con la infraestructura necesaria para dar continuidad de la operación y estar cubiertos por el *PNDS-MN-TEC-01 Plan de Continuidad de Negocio y el PNDS-DG-TEC-06 Manual de recuperación de Desastres*, con pruebas anuales documentadas.

6.6. Manejo de incidentes

6.6.1. Los activos informáticos de la Organización en el ambiente de servicios en la nube deben contar con un programa de respuestas a Incidentes.

El proveedor en su ambiente de servicios en la nube debe contar con un programa de manejo de incidentes que dé prioridad y respuesta a las alertas de seguridad que afecten a la Organización.

El proveedor debe garantizar un SLA para respuesta a incidentes alineado con la criticidad definida en el contrato.

6.7. Aseguramiento de la infraestructura tecnológica

6.7.1. Implementación de controles de ciberseguridad y seguridad de la información (S.I.) en cada uno de los componentes de la infraestructura utilizada en el modelo de servicios en la nube, a nivel de hardware, software, y comunicaciones.

La Organización, establece que todo componente de infraestructura tecnológica implementado en el modelo de servicios en la nube ya sea hardware, software, comunicaciones, repositorios de certificados o llaves criptográficas debe contar con controles definidos en Ciberseguridad y S.I. alineados a los marcos normativos aplicables (ISO/IEC 27001, ISO/IEC 27017, NIST, CSA, especialmente al ser desplegado en ambientes productivos y de acuerdo con lo descrito en el documento *PNDS-MN-GRC-03 Normas de Ciberseguridad y S.I*

6.8. Gestión de acceso e identidad

6.8.1. El uso de los recursos informáticos de la Organización en el ambiente de servicios en la nube debe tener una gestión de acceso e identidad

La identidad de los funcionarios o proveedores que acceden a los recursos informáticos en el ambiente de nube debe ser establecida y autenticada de una manera única y no podrá ser compartida. El proveedor deberá definir una estrategia de autenticación, de acuerdo con el valor de la información y nivel de riesgo con base en los lineamientos establecidos por Grupo AVAL.

La Organización debe propender por implementar autenticación multifactor (2FA) a todos los accesos con roles privilegiados, como medida esencial para fortalecer la seguridad de los entornos en la nube.

El acceso a la información confidencial por parte de terceros se dará según lo establecido en la *PNDS-PO-GRC-11 Política Tratamiento de Información (PTI)*

La Organización en conjunto con el proveedor de servicio en la nube propenderán a determinar el sitio adecuado de almacenamiento de la información, evaluando factores políticos, geográficos, energía y eficiencia energética, conectividad, infraestructura de red y panorama regulatorio local.

6.9. Control de Activos de información.

6.9.1. La Organización debe mantener un inventario preciso y actualizado de todos los activos de información que se tienen en servicios en la nube.

La Organización deben contar con un inventario de activos de servicios en la nube. de acuerdo con su valor y riesgo de pérdida de confidencialidad, integridad y privacidad.

En el proceso de clasificación de activos de T.I se deberá registrar según lo definido en *el PNDS-PR-GRC-07 Procd de Gest de Activos de Info.*

6.10. Gestión del cambio.

6.10.1. En todos los nuevos procesos, actividades, productos y sistemas críticos que se lleven y/o se implementen en la nube, se debe pasar a través del proceso de aprobación definido por la Organización en donde se evalúan los riesgos en Ciberseguridad y S.I.

Las áreas responsables de los proyectos o de los cambios, deben asegurar que haya un proceso de aprobación que evalúe plenamente los riesgos de Ciberseguridad y S.I., en todos los nuevos procesos, productos o sistemas que se lleven a la nube.

La gestión del cambio en servicios en la nube se realiza y aprueba conforme al *PNDS-PR-TEC-05 Proced_Gest_de_Camb_TI,* aplicable únicamente a los procesos implementados en la Organización.

7. DOCUMENTOS DE REFERENCIA

- PNDS-MN-GRC-03 Norma de Ciberseguridad y S.I.
- PNDS-FR-GRC-15 Requisitos mínimos de Cloud.
  PNDS-PR-TEC-05 0806 Proced_Gest_de_Camb_TI
- PNDS-PR-GRC-07 Procd de Gest de Activos de Info

8. CONTROL DE CAMBIOS

VERSIÓN	FECHA	DESCRIPCIÓN DEL CAMBIO
1	18/12/2025	Creación del documento

9. FIRMAS APROBACIÓN

Elaborado por:	Revisado por:	Revisado por:	Aprobado por:
FIRMADO EN ORIGINAL	FIRMADO EN ORIGINAL	FIRMADO EN ORIGINAL	FIRMADO EN ORIGINAL
PROFESIONAL DE CALIDAD	LIDER DE RIESGO Y CUMPLIMIENTO	GERENTE T.I.	VICEPRESIDENTE EJECUTIVA Y DE SOSTENIBILIDAD
Diego Alejandro Pinzón	Jusseth Guzman Castrillon	Sandra Milena Sepúlveda	Vanessa Garay Guzman

Documento aprobado en la sesión de Junta Directiva No. 173 del 18 de diciembre de 2025