Política de Uso de Servicios en la Nube

Fecha: 10/10/2025

Versión: 1.0

Control de versiones

Fecha	Versión	Descripción	Autor
10/10/2025	0.1	Creación del Documento	PM SGSI
17/10/2023	1.0	Revisión del Documento	Comité de Seguridad de la Información

Contenido

1 Objetivo

Establecer los lineamientos que aseguren el uso seguro, controlado y conforme a la normativa de los servicios en la nube utilizados por Interfase ISA, garantizando la protección de los activos de información, la confidencialidad de los datos y la continuidad de las operaciones corporativas.

Esta política tiene por finalidad definir criterios para la evaluación, aprobación, monitoreo y gobernanza de los servicios en la nuble (IaaS, PaaS, SaaS), asegurando que su adopción y operación se realicen bajo un enfoque basado en riesgo y en concordancia con los controles del Sistema de Gestión de Seguridad de la Información (SGSI).

Forma parte del ciclo de mejora continua (PDCA) del SGSI y complementa las políticas de Gestión de Activos de Información, Seguridad en Redes y Comunicaciones y Relaciones con Proveedores.

Esta política aplica los principios de gobernanza de la información en entornos en la nuble establecidos en los controles A.5.23 y A.5.19 de la norma ISO/IEC 27001:2022. Se basa en un enfoque de gestión de riesgos, de modo que toda adopción, operación o terminación de servicios en la nube se realice previa evaluación técnica, legal y de seguridad, documentada en el SGSI.

2 Alcance

Aplica a todas las sedes de Interfase ISA y a todas las áreas, colaboradores, contratistas y proveedores que adquieran, administren o utilicen servicios en la nube, sean de tipo IaaS, PaaS o SaaS, en el marco de las operaciones corporativas.

Incluye servicios utilizados para almacenamiento, procesamiento, desarrollo, comunicación o cualquier otra función que implique el tratamiento de información corporativa o de clientes en entornos en la nuble.

3 Roles y responsabilidades

La gestión segura de los servicios en la nube es una responsabilidad compartida entre el Directorio, el Comité de Seguridad, el Área de Tecnología de la Información (TI), Administración y las áreas usuarias que utilicen o soliciten estos servicios.

- Directorio: aprueba esta política, asigna los recursos necesarios y supervisa su cumplimiento durante la Revisión por la Dirección. Valida la incorporación de nuevos servicios en la nuble estratégicos dentro del marco del SGSI.

- Comité de Seguridad: supervisa la aplicación de esta política y autoriza el uso de nuevos servicios en la nube previa evaluación técnica, legal y de riesgo. Define los criterios de seguridad, cumplimiento y monitoreo aplicables a proveedores de la nube. Revisa los informes de desempeño y cumplimiento elaborados por el Área de TI y asesora sobre acciones correctivas.

- PM del SGSI: coordina la integración de esta política con las demás del SGSI y asegura la trazabilidad documental de las aprobaciones de servicios de la nube. Mantiene actualizado el Registro de Servicios En la nuble Autorizados e impulsa la mejora continua de los controles asociados.

- Área de Tecnología de la Información (TI): evalúa los riesgos técnicos y operativos de los servicios en la nuble, implementa controles de acceso, cifrado, respaldo y monitoreo. Gestiona las credenciales y cuentas corporativas de los entornos de la nube. Supervisa el cumplimiento de los acuerdos de nivel de servicio (SLA) y mantiene evidencia de revisiones y auditorías.

- Área de Administración: gestiona los procesos de contratación o renovación de servicios en la nuble, asegurando que los acuerdos incluyan cláusulas de seguridad, confidencialidad, disponibilidad y cumplimiento normativo. Coordina con Asesoría Legal la revisión de términos y condiciones antes de la firma o extensión de contratos. Mantiene actualizado el archivo contractual de proveedores en la nuble y colabora en la evaluación de desempeño.

- Asesoría Legal: verifica que los servicios en la nuble contratados cumplan con las normativas de protección de datos, jurisdicción y privacidad aplicables. Evalúa los riesgos legales asociados a la transferencia internacional de información o uso de subproveedores.

- Responsables de Área: garantizan que los servicios en la nube utilizados por su área estén autorizados, sean necesarios para el negocio y cumplan con esta política. Monitorean el uso adecuado de las cuentas asignadas y notifican de inmediato cualquier incidente o acceso no autorizado.

- Colaboradores y terceros: deben utilizar únicamente los servicios en la nube autorizados por el Comité de Seguridad y el Área de TI. Tienen la obligación de proteger las credenciales corporativas, aplicar buenas prácticas de seguridad y reportar incidentes relacionados con el uso de servicios en la nuble.

Las funciones y responsabilidades específicas se encuentran documentadas en la Matriz RACI del SGSI, que constituye evidencia formal de auditoría y soporte para la trazabilidad de los controle.

4 Principios para el uso de servicios en la nube

Interfase ISA adopta los siguientes principios para garantizar un uso seguro de los servicios de la nube:

- Aprobación previa: todo servicio en la nube deberá ser evaluado y aprobado por el Comité de Seguridad antes de su uso.
- Clasificación de información: la información tratada en la nube deberá clasificarse y protegerse conforme a su nivel de sensibilidad.
- Cumplimiento legal y contractual: los servicios deberán ajustarse a la normativa vigente sobre protección de datos y seguridad de la información.
- Ubicación y jurisdicción: las ubicaciones de los centros de datos deberán identificarse y cumplir las leyes aplicables del país de origen y destino.
- Gestión de accesos: el acceso a servicios de la nube deberá autenticarse mediante MFA y controlarse según el principio de mínimo privilegio.
- Cifrado y seguridad técnica: toda información sensible deberá cifrarse en tránsito y reposo utilizando algoritmos aprobados.
- Continuidad y respaldo: los servicios críticos deberán contar con planes de recuperación y copias de respaldo verificadas.
- Monitoreo permanente: el desempeño y la seguridad de los servicios de la nube deberán ser revisados periódicamente.
- Evaluación basada en riesgo: todo servicio de la nube deberá contar con un análisis de riesgos documentado, considerando la confidencialidad, integridad, disponibilidad, residencia de datos y dependencia del proveedor.
- Clasificación y autorización: los servicios se clasificarán según su nivel de criticidad (alto, medio, bajo) y solo podrán utilizarse los que figuren en el Registro de Servicios En la nuble Autorizados del SGSI, aprobado por el Comité de Seguridad.
- Revisión de seguridad: los servicios autorizados deberán ser revisados al menos una vez al año o cuando ocurran cambios tecnológicos o contractuales relevantes.

5 Evaluación y contratación de servicios en la nube

- Antes de la adopción de un servicio en la nube, se deberá realizar una evaluación de riesgo y cumplimiento, considerando aspectos técnicos, legales, contractuales y de privacidad.
- Los contratos deberán incluir cláusulas de confidencialidad, seguridad, disponibilidad, portabilidad de datos y notificación de incidentes.
- El Área de TI y el Comité de Seguridad deberán mantener un registro actualizado de servicios en la nube aprobados y su nivel de criticidad.
- El Comité de Seguridad deberá validar que los servicios contratados cumplan con los requisitos mínimos de seguridad definidos por Interfase ISA, incluyendo:
    - Autenticación multifactor (MFA) para accesos administrativos.
    - Cifrado de datos en tránsito y en reposo con algoritmos aprobados.
    - Registro y trazabilidad de actividades administrativas.
    - Definición clara de ubicación de datos y jurisdicción aplicable.
- La contratación de servicios en la nube deberá realizarse únicamente con proveedores que demuestren cumplimiento de estándares reconocidos.
- Los resultados de las evaluaciones deberán conservarse como evidencia en el Registro de Evaluación y Selección de Proveedores en la nube.

6 Seguridad, protección de datos y continuidad

- Toda información almacenada o procesada en la nube deberá protegerse mediante cifrado, control de accesos, registro de actividad y auditoría.
- Los proveedores deberán asegurar la disponibilidad y recuperación de los datos, conforme a los acuerdos de nivel de servicio (SLA) aprobados.
- En caso de terminación del contrato, el proveedor deberá garantizar la eliminación o devolución segura de la información corporativa.
- El Comité de Seguridad y el Área de TI deberán realizar revisiones anuales de desempeño y cumplimiento de los servicios en la nube contratados.

- Los servicios en la nube críticos deberán contar con planes documentados de respaldo y restauración, incluyendo pruebas anuales de recuperación.
- En caso de incidentes o fallos del proveedor, el Comité de Seguridad deberá coordinar la activación del Plan de Contingencia En la nuble, que defina los pasos para migrar o restaurar la información en entornos alternos.
- Toda transferencia internacional de datos en entornos en la nube deberá cumplir con la Ley 18.331 (Uruguay) o la normativa local equivalente, y registrarse en el Registro de Transferencias de Datos Internacionales mantenido por Asesoría Legal.

7 Auditoría, monitoreo y revisión

El Comité de Seguridad y el Área de TI deberán realizar revisiones periódicas sobre los servicios en la nube contratados, incluyendo:

- Validación de controles técnicos y de cumplimiento.
- Verificación del cumplimiento de los SLA y cláusulas de seguridad.
- Auditorías documentadas del uso, almacenamiento y eliminación de datos.

Los resultados deberán documentarse en el Informe de Revisión de Servicios En la nuble, conservado como evidencia dentro del SGSI. En caso de detectar desviaciones, se deberán implementar acciones correctivas dentro de los plazos definidos por el Comité de Seguridad.

8 Indicadores de eficacia

El Comité de Seguridad y el PM del SGSI medirán la eficacia de esta política mediante los siguientes indicadores:

- Porcentaje de servicios en la nube evaluados y aprobados.
- Número de revisiones de proveedores en la nube realizadas en el año.
- Incidentes o brechas relacionados con entornos en la nube.
- Porcentaje de servicios que cumplen los niveles mínimos de seguridad establecidos.

Los resultados se presentarán durante la Revisión por la Dirección y servirán de base para las decisiones de mejora continua del SGSI.

9 Cumplimiento y mejora continua

El cumplimiento de esta política es obligatorio para todas las áreas y personas que utilicen o administren servicios en la nube.

El Comité de Seguridad, junto con el Área de TI y el PM del SGSI, supervisará su aplicación y consolidará los resultados en un informe anual de cumplimiento presentado al Directorio durante la Revisión por la Dirección.

Las desviaciones o hallazgos deberán gestionarse mediante acciones correctivas o preventivas, asegurando la mejora continua del SGSI y del modelo de gobernanza en la nube.

10 Vigencia y Publicación

Esta política es de aplicación obligatoria a partir de su aprobación por el Directorio de Interfase ISA.

La versión vigente será comunicada mediante los canales institucionales y publicada en la intranet corporativa, dentro del repositorio del SGSI.

El Comité de Seguridad garantizará su difusión, revisión anual y control de versiones, o antes si se producen cambios tecnológicos, regulatorios o contractuales significativos.

Esta política deberá revisarse al menos una vez al año o cuando se incorporen nuevos servicios en la nube, se modifiquen las condiciones contractuales o se detecten cambios regulatorios que impacten en el tratamiento de información.

Toda modificación deberá contar con la aprobación formal del Directorio antes de su aplicación, asegurando su adecuada comunicación y registro bajo control documental.

Versión	Fecha de aprobación	Próxima revisión	Aprobado por:
1.0	DD/MM/AAAA	DD/MM/AAAA	Directorio – Interfase ISA

tuid
FIRMA DIGITAL
Leonardo Adrian Noach Meierovich