LINEAMIENTOS DE SEGURIDAD PARA SERVICIOS EN LA NUBE			
PROCESO:	GESTIÓN TICs		
PROCEDIMIENTO:	ADMINISTRACIÓN DE PLATAFORMA TECNOLOGICA		
FECHA DE APROBACIÓN:	**CÓDIGO:**	**VERSIÓN:**	**PÁGINA:**
29/07/2026	GTI02-GUI04	*01*	1 de 20

1. OBJETIVO

Definir las políticas, y criterios de seguridad para la adquisición, uso, gestión, monitoreo, continuidad y salida de los servicios en la nube utilizados por la Contaduría General de la Nación, independientemente del proveedor de servicios en la nube (CSP, por sus siglas en inglés) y el modelo de servicios adoptado (IaaS, PaaS o SaaS) o de despliegue (nube pública, privada, comunitaria o híbrida), el modelo de responsabilidad compartida, asegurando la adecuada protección, administración, monitoreo, continuidad y salida de los servicios, recursos y datos alojados en la nube, bajo los principios de confidencialidad, integridad, disponibilidad, trazabilidad y cumplimiento normativo.

Esta guía se estructura con base en los dominios de control del Anexo A de la norma ISO/IEC 27001:2022. Su aplicación debe ser proporcional al riesgo, a la criticidad del servicio, al tipo de información tratada y a las responsabilidades que correspondan a la CGN y al proveedor.

2. ALCANCE

La presente guía aplica a todos los servicios, recursos, usuarios, roles, aplicaciones, datos y configuraciones alojados o administrados en cualquier servicio en la nube contratado o utilizado por la Contaduría General de la Nación (CGN). Incluye los lineamientos de seguridad para la adquisición, uso, gestión, monitoreo y salida de servicios en la nube, así como para la gestión de identidades y accesos, la protección de la información, la administración de recursos, el registro y monitoreo, el respaldo, la continuidad del servicio y la atención de incidentes de seguridad y ciberseguridad asociados al entorno del servicio en la nube contratado.

Su cumplimiento es obligatorio para servidores públicos, contratistas, administradores, proveedores y terceros autorizados que usen, gestionen o soporten los recursos en la nube de la entidad.

3. DEFINICIONES

- **Autenticación multifactor - MFA:** mecanismo de seguridad que requiere dos o más métodos de verificación para confirmar la identidad de un usuario.
- **Cifrado:** técnica de protección que convierte la información en un formato

no legible para evitar accesos no autorizados.

- **Identidad:** cuenta o entidad digital utilizada para autenticar a usuarios, aplicaciones o servicios dentro del entorno de nube.
- **Modelo de responsabilidad compartida:** distribución de las obligaciones de seguridad entre el proveedor de nube y la entidad, según el modelo de servicio adoptado.
- **Monitoreo:** actividad que permite supervisar el estado, comportamiento, eventos y alertas de los recursos alojados en la nube.
- **Nube:** modelo de prestación de servicios tecnológicos a través de internet, que permite acceder a infraestructura, plataformas y software sin necesidad de contar con todos los recursos físicamente en la entidad.
- **Principio de mínimo privilegio:** buena práctica de seguridad que consiste en otorgar únicamente los permisos necesarios para cumplir una función específica.
- **Recurso en la nube:** elemento creado y administrado dentro del entorno de nube, como máquinas virtuales, bases de datos, cuentas de almacenamiento, redes, aplicaciones o servicios de seguridad.
- **Registro de eventos:** información generada por sistemas, aplicaciones o usuarios sobre actividades realizadas en la plataforma, útil para auditoría y trazabilidad.
- **Requisitos Legales:** observancia de leyes, normas, políticas, requisitos contractuales y lineamientos internos aplicables a la seguridad de la información y gestión tecnológica.
- **Respaldo:** copia de seguridad de la información o de los recursos tecnológicos, utilizada para su recuperación ante pérdida, daño o incidente.
- **RTO / RPO:** objetivo de Tiempo de Recuperación (RTO) y Objetivo de Punto de Recuperación (RPO); parámetros que definen, respectivamente, el tiempo máximo tolerable de interrupción de un servicio y la máxima pérdida de datos admisible ante un incidente.

4. MARCO NORMATIVO Y DE REFERENCIA

La presente guía se fundamenta y articula con los siguientes, normas y modelos de referencia, los cuales orientan la definición, verificación y mejora de los controles aquí establecidos:

- **ISO/IEC 27032**: Directrices para la ciberseguridad; orienta la protección del ciberespacio, la colaboración entre partes interesadas y la gestión de ciberincidentes.

LINEAMIENTOS DE SEGURIDAD PARA SERVICIOS EN LA NUBE			
PROCESO:	GESTIÓN TICs		
PROCEDIMIENTO:	ADMINISTRACIÓN DE PLATAFORMA TECNOLOGICA		
FECHA DE APROBACIÓN:	**CÓDIGO:**	**VERSIÓN:**	**PÁGINA:**
29/07/2026	GTI02-GUI04	*01*	3 de 20

- **ISO/IEC 27017:** Código de prácticas para los controles de seguridad de la información aplicables a los servicios en la nube.
- **ISO/IEC 27018:** Código de prácticas para la protección de datos personales (PII) en nubes públicas que actúan como encargadas del tratamiento.
- **MSPI**: Modelo de Seguridad y Privacidad de la Información de MinTIC, de obligatoria adopción por las entidades del Estado colombiano, basado en el ciclo PHVA (Planificar, Hacer, Verificar, Actuar).
- **GTI10-FOR10** Matriz de requisitos legales y normativos de seguridad de la información y seguridad digital.
- **Acuerdo Marco de Precios de Nube Pública - Colombia Compra Eficiente:** Instrumento de agregación de demanda aplicable a la adquisición de servicios en la nube por parte de las entidades estatales.

Nota aclaratoria: cuando una obligación legal exija residencia o soberanía de los datos en el territorio nacional, la selección del proveedor y de las regiones de nube deberá considerar dicho requisito.

5. RESPONSABLES DE CUMPLIMIENTO

El cumplimiento de la presente guía será responsabilidad de todos los servidores públicos, contratistas, administradores, proveedores y terceros de la Contaduría General de la Nación (CGN), autorizados que tengan acceso, gestionen, operen, administren o soporten los recursos y servicios alojados en cualquier servicio en la nube de la entidad. Cada usuario deberá hacer uso adecuado de los recursos asignados, proteger sus credenciales de acceso, cumplir con las políticas de seguridad establecidas y reportar oportunamente cualquier evento, anomalía, vulnerabilidad o incidente que pueda afectar la seguridad de la información.

Para garantizar la correcta aplicación de la presente guía de seguridad para servicios en la nube, se establecen los siguientes roles y responsabilidades:

Roles	Responsabilidades
Alta Dirección	Aprobar y respaldar la implementación de los lineamientos de seguridad definidos para los servicios en la nube, garantizando los recursos necesarios para su cumplimiento y promover el cumplimiento de las políticas de seguridad de la información y requisitos legales aplicables.

LINEAMIENTOS DE SEGURIDAD PARA SERVICIOS EN LA NUBE			
PROCESO:	GESTIÓN TICs		
PROCEDIMIENTO:	ADMINISTRACIÓN DE PLATAFORMA TECNOLOGICA		
FECHA DE APROBACIÓN:	**CÓDIGO:**	**VERSIÓN:**	**PÁGINA:**
29/07/2026	GTI02-GUI04	*01*	4 de 20

Roles	Responsabilidades
Oficial de Seguridad de la Información- Equipo de Seguridad de la Información	Definir, revisar y actualizar los lineamientos de seguridad aplicables al entorno de nube; verificar el cumplimiento de los controles establecidos, apoyar la gestión de riesgos, realizar seguimiento a eventos de seguridad, coordinar el análisis de vulnerabilidades y acompañar la atención de incidentes que puedan afectar la confidencialidad, integridad o disponibilidad de la información.
El GIT de Apoyo Informático	Administrar técnicamente la plataforma de nube, asegurando la correcta configuración, operación, disponibilidad y mantenimiento de los recursos tecnológicos. Es responsable de gestionar los servicios, aplicar actualizaciones, realizar respaldos, monitorear la infraestructura, administrar redes, almacenamiento, máquinas virtuales o cómputo, aplicaciones y demás componentes desplegados en la nube.
Administradores de la plataforma de nube	Gestionar los recursos, permisos, roles, configuraciones y servicios dentro de la plataforma, aplicando el principio de mínimo privilegio y las buenas prácticas de seguridad. Garantizar que las cuentas administrativas estén protegidas, que los accesos sean autorizados y que las actividades realizadas en la plataforma sean trazables y verificables.
Líderes de proceso o dueños de la información	Definir las necesidades de acceso a la información y a los servicios en la nube, de acuerdo con las funciones de los usuarios y los objetivos del proceso. Validar periódicamente los permisos otorgados; apoyar la clasificación de la información y reportar cualquier uso indebido, riesgo o necesidad de ajuste en los controles aplicados.
Usuarios autorizados	Usar los servicios y recursos únicamente para fines institucionales y de acuerdo con los permisos asignados; proteger sus credenciales, no compartir usuarios ni contraseñas, cumplir las políticas de seguridad, reportar incidentes o comportamientos sospechosos y hacer uso adecuado de la información a la que tengan acceso.
Proveedores y terceros	Cumplir las políticas de seguridad de la entidad, los acuerdos de confidencialidad, los requisitos contractuales y los lineamientos definidos para la administración, soporte u operación de recursos en la nube; y reportar oportunamente cualquier incidente, vulnerabilidad, falla o situación que

LINEAMIENTOS DE SEGURIDAD PARA SERVICIOS EN LA NUBE			
PROCESO:	GESTIÓN TICs		
PROCEDIMIENTO:	ADMINISTRACIÓN DE PLATAFORMA TECNOLOGICA		
FECHA DE APROBACIÓN:	**CÓDIGO:**	**VERSIÓN:**	**PÁGINA:**
29/07/2026	GTI02-GUI04	*01*	5 de 20

Roles	Responsabilidades
	pueda comprometer la seguridad de la plataforma o de la información.

6. PROCEDIMIENTOS Y CONTROLES DE SEGURIDAD PARA SERVICIOS EN LA NUBE

Los controles se presentan agrupados según los cuatro dominios del Anexo A de la norma ISO/IEC 27001:2022, con el fin de facilitar su verificación en auditorias. Cada bloque incluye la referencia a los controles aplicables y su correspondencia con la ISO/IEC 27001:2022 y MSPI.

6.1. CONTROLES ORGANIZACIONALES (ISO/IEC 27001:2022 – A.5)

6.1.1. Políticas de gobierno de seguridad para servicios en la nube

La CGN deberá establecer, aprobar, comunicar y mantener actualizadas las políticas y procedimientos de seguridad aplicables a los servicios en la nube, alineados con el SGSI y con el MSPI de la entidad.

Controles:

- Aprobar la presente guía por la instancia competente y comunicarla a todas las partes interesadas.
- Asignar formalmente roles y responsabilidades de seguridad para el entorno de nube.
- Revisar y actualizar la guía al menos una vez al año, o ante cambios significativos de la plataforma, de la normatividad o del contexto de riesgo.
- Mantener procedimientos operativos documentados para las actividades críticas de administración de la nube

6.1.2. Seguridad de la información en el uso de servicios en la nube

La adquisición, uso, gestión y salida de servicios en la nube deberán realizarse bajo criterios de seguridad definidos, documentando para cada servicio el modelo de responsabilidad compartida.

Este control es transversal y constituye el eje de la presente guía; complementa los demás controles con los requisitos propios del entorno de nube.

LINEAMIENTOS DE SEGURIDAD PARA SERVICIOS EN LA NUBE			
PROCESO:	GESTIÓN TICs		
PROCEDIMIENTO:	ADMINISTRACIÓN DE PLATAFORMA TECNOLOGICA		
FECHA DE APROBACIÓN:	**CÓDIGO:**	**VERSIÓN:**	**PÁGINA:**
29/07/2026	GTI02-GUI04	*01*	6 de 20

Controles:

- Definir criterios de seguridad para la selección y contratación de proveedores de nube (certificaciones, ubicación de datos, cumplimiento normativo, niveles de servicio).
- Documentar el reparto de responsabilidades de seguridad (entidad / proveedor) para cada servicio IaaS, PaaS o SaaS.
- Verificar la residencia y soberanía de los datos conforme a los requisitos legales aplicables.
- Establecer requisitos de seguridad en los acuerdos y contratos (confidencialidad, cifrado, respaldo, notificación de incidentes, derecho de auditoría, portabilidad y devolución de datos).
- Definir desde la contratación una estrategia de salida que evite la dependencia tecnológica (vendor lock-in) y garantice la recuperación de la información.
- Realizar y documentar una evaluación de riesgos de seguridad de la información y, cuando se traten datos personales, una evaluación de impacto en la privacidad, de manera previa a la adopción de cualquier servicio en la nube.
- Establecer un proceso de aprobación formal para la adopción de nuevos servicios en la nube, y detectar y controlar el uso de servicios no autorizados por la entidad (shadow IT).

6.1.3. Gestión de relaciones y seguimiento de proveedores

Los proveedores y terceros que administren soporten u operen recursos en la nube deberán cumplir los requisitos de seguridad de la entidad, y su desempeño deberá ser monitoreado durante toda la relación contractual.

Controles:

- Incluir cláusulas de seguridad, confidencialidad y protección de datos en todos los acuerdos.
- Evaluar periódicamente el cumplimiento de los proveedores y solicitar evidencias (informes SOC 2, certificaciones ISO/IEC 27001, reportes de auditoría).
- Gestionar los cambios en los servicios prestados por proveedores que puedan afectar la seguridad.
- Controlar la seguridad en la cadena de suministro TIC (subcontratistas, componentes y servicios de terceros).

LINEAMIENTOS DE SEGURIDAD PARA SERVICIOS EN LA NUBE			
PROCESO:	GESTIÓN TICs		
PROCEDIMIENTO:	ADMINISTRACIÓN DE PLATAFORMA TECNOLOGICA		
FECHA DE APROBACIÓN:	**CÓDIGO:**	**VERSIÓN:**	**PÁGINA:**
29/07/2026	GTI02-GUI04	*01*	7 de 20

6.1.4. Inteligencia de amenazas

La entidad deberá recopilar y analizar información sobre amenazas relevantes para el entorno de nube, con el fin de anticipar, prevenir y responder de forma informada.

Controles:

- Suscribirse y atender los boletines y alertas de organismos como el CSIRT de Gobierno / ColCERT y del propio proveedor de nube.
- Analizar las amenazas aplicables a los servicios en la nube utilizados y ajustar los controles en consecuencia.
- Compartir información de amenazas con las áreas pertinentes y usarla para la gestión de vulnerabilidades y la detección.

6.1.5. Clasificación y etiquetado de la información

La información alojada o procesada en la nube deberá clasificarse según su nivel de sensibilidad y criticidad, y etiquetarse de forma coherente para determinar los controles de protección aplicables.

Controles:

- Clasificar la información conforme a los niveles definidos por la entidad (por ejemplo, pública, reservada o clasificada).
- Etiquetar la información y los recursos para orientar los controles de cifrado, acceso y retención.
- Aplicar controles diferenciados según la clasificación (especialmente para datos personales y reservados).

6.1.6. Política de control de acceso

La CGN deberá establecer y mantener una política de control de acceso que garantice que el acceso a los servicios y recursos en la nube sea único, personal, autorizado, trazable y acorde con las funciones asignadas, bajo el principio de mínimo privilegio.

Controles:

- Definir reglas de acceso basadas en roles y en la necesidad de conocer.
- Gestionar el ciclo de vida de las identidades (alta, modificación y baja).
- Proteger la información de autenticación (contraseñas, tokens, secretos).

LINEAMIENTOS DE SEGURIDAD PARA SERVICIOS EN LA NUBE			
PROCESO:	GESTIÓN TICs		
PROCEDIMIENTO:	ADMINISTRACIÓN DE PLATAFORMA TECNOLOGICA		
FECHA DE APROBACIÓN:	**CÓDIGO:**	**VERSIÓN:**	**PÁGINA:**
29/07/2026	GTI02-GUI04	*01*	8 de 20

- Revisar y recertificar periódicamente los derechos de acceso otorgados.

6.1.7. Inventario y uso aceptable de los activos

Los recursos y servicios en la nube deberán mantenerse inventariados y asociados a un responsable, y su uso deberá ajustarse a las reglas de uso aceptable definidas por la entidad.

Controles:

- Mantener un inventario actualizado de recursos, servicios, suscripciones y responsables.
- Etiquetar los recursos para identificar responsable, ambiente, criticidad y finalidad.
- Definir y comunicar las reglas de uso aceptable de los servicios en la nube.
- Revisar periódicamente recursos activos, obsoletos o sin uso, y controlar costos y consumo.

6.1.8. Gestión de incidentes de seguridad y ciberincidentes

La entidad deberá contar con un procedimiento para planificar, identificar, reportar, evaluar, contener, erradicar, recuperar y aprender de los incidentes de seguridad y ciberincidentes que afecten los servicios en la nube.

Controles:

- Definir canales formales y roles para el reporte y la atención de incidentes.
- Clasificar los incidentes según impacto y criticidad, y decidir sobre eventos de seguridad.
- Registrar fecha, hora, recurso afectado, usuario involucrado y descripción del evento.
- Contener oportunamente accesos no autorizados o recursos comprometidos y preservar evidencias (cadena de custodia).
- Coordinar la respuesta entre Tecnología, Seguridad de la Información y los dueños del proceso, y notificar a las autoridades cuando corresponda.
- Notificar a la Superintendencia de Industria y Comercio (SIC) los incidentes que afecten datos personales, conforme a la Ley 1581 de 2012, y actualizar el Registro Nacional de Bases de Datos cuando aplique.
- Ejecutar acciones correctivas y preventivas y documentar las lecciones aprendidas para actualizar los controles.

LINEAMIENTOS DE SEGURIDAD PARA SERVICIOS EN LA NUBE			
PROCESO:	GESTIÓN TICs		
PROCEDIMIENTO:	ADMINISTRACIÓN DE PLATAFORMA TECNOLOGICA		
FECHA DE APROBACIÓN:	**CÓDIGO:**	**VERSIÓN:**	**PÁGINA:**
29/07/2026	GTI02-GUI04	*01*	9 de 20

6.1.9. Continuidad y disponibilidad ante interrupciones

La entidad deberá preparar las TIC para la continuidad del negocio, garantizando la disponibilidad de los servicios y la recuperación ante interrupciones que afecten el entorno de nube.

Controles:

- Definir requisitos de disponibilidad y objetivos de recuperación (RTO/RPO) para los servicios críticos.
- Diseñar mecanismos de redundancia y alta disponibilidad acordes con la criticidad.
- Probar periódicamente los planes de continuidad y recuperación asociados a la nube.
- Gestionar la capacidad de los servicios en la nube (cuotas, límites y consumo de recursos), monitoreando su uso para asegurar la disponibilidad requerida y controlar los costos.

6.1.10. Cumplimiento legal, protección de datos y revisión independiente

La entidad deberá identificar y cumplir los requisitos legales, reglamentarios y contractuales aplicables al uso de servicios en la nube, con especial atención a la protección de datos personales, y verificar el cumplimiento mediante revisiones independientes.

Controles:

- Identificar y mantener actualizado el marco legal aplicable (protección de datos, transparencia, retención documental).
- Aplicar controles de privacidad y protección de datos personales (PII) conforme a la Ley 1581 de 2012.
- Proteger los registros conforme a los requisitos de retención y las tablas de retención documental.
- Verificar periódicamente el cumplimiento de políticas y normas, y realizar revisiones independientes de la seguridad.

LINEAMIENTOS DE SEGURIDAD PARA SERVICIOS EN LA NUBE			
PROCESO:	GESTIÓN TICs		
PROCEDIMIENTO:	ADMINISTRACIÓN DE PLATAFORMA TECNOLOGICA		
FECHA DE APROBACIÓN:	**CÓDIGO:**	**VERSIÓN:**	**PÁGINA:**
29/07/2026	GTI02-GUI04	*01*	10 de 20

6.2. CONTROLES DE PERSONAS (ISO/IEC 27001:2022 - A.6)

6.2.1. Concientización, educación y formación

El personal con acceso a los servicios en la nube deberá recibir formación y concientización periódica en seguridad de la información y ciberseguridad, acorde con sus funciones.

Controles:

- Realizar campañas periódicas de concientización (phishing, manejo de credenciales, uso seguro de la nube).
- Capacitar a administradores y usuarios privilegiados en configuración y operación segura de los servicios.
- Registrar la asistencia y evaluar la efectividad de las actividades de formación.

6.2.2. Gestión de vinculación, cambio y desvinculación

Los accesos a los servicios en la nube deberán otorgarse, ajustarse y revocarse de forma oportuna ante la vinculación, el cambio de funciones o la desvinculación de funcionarios, contratistas o terceros.

Controles:

- Desactivar oportunamente las cuentas de usuarios retirados, contratistas o terceros sin vínculo vigente.
- Ajustar los permisos ante cambios de rol o funciones.
- Definir las responsabilidades de seguridad que permanecen tras la finalización del vínculo (confidencialidad, devolución de activos).

6.2.3. Acuerdos de confidencialidad

El personal y los terceros con acceso a información alojada en la nube deberán suscribir acuerdos de confidencialidad o no divulgación.

Controles:

- Suscribir acuerdos de confidencialidad con funcionarios, contratistas y terceros.
- Revisar y actualizar los acuerdos conforme a los requisitos de la entidad.

LINEAMIENTOS DE SEGURIDAD PARA SERVICIOS EN LA NUBE			
PROCESO:	GESTIÓN TICs		
PROCEDIMIENTO:	ADMINISTRACIÓN DE PLATAFORMA TECNOLOGICA		
FECHA DE APROBACIÓN:	**CÓDIGO:**	**VERSIÓN:**	**PÁGINA:**
29/07/2026	GTI02-GUI04	*01*	11 de 20

6.2.4. Trabajo remoto y acceso desde ubicaciones externas

El acceso a los servicios en la nube desde ubicaciones remotas o en modalidad de teletrabajo deberá realizarse bajo condiciones de seguridad controladas.

Controles:
- Aplicar políticas de acceso condicional según ubicación, dispositivo y riesgo.
- Exigir MFA y conexiones seguras para el acceso remoto.
- Restringir el acceso administrativo desde equipos públicos o no confiables.

6.2.5. Reporte de eventos de seguridad

Todos los usuarios deberán reportar oportunamente los eventos, anomalías, vulnerabilidades o comportamientos sospechosos que puedan afectar la seguridad de los servicios en la nube.
Controles:
- Disponer de canales claros y accesibles para el reporte de eventos.
- Promover una cultura de reporte oportuno y sin represalias.
- Articular el reporte con el procedimiento de gestión de incidentes (6.1.8).

6.3. CONTROLES FÍSICOS (ISO/IEC 27001:2022 - A.7)

En un entorno de nube, la mayoría de los controles físicos sobre los centros de datos (perímetros, entrada física, monitoreo físico, servicios de soporte y seguridad ambiental) son responsabilidad del proveedor de nube. La entidad los verifica de forma indirecta a través de las certificaciones e informes de auditoría del proveedor, y conserva bajo su responsabilidad la seguridad física de los dispositivos y puestos de trabajo desde los cuales se accede a la nube.

6.3.1. Verificación de la seguridad física del proveedor de nube

La entidad deberá verificar que el proveedor de nube mantenga controles físicos y ambientales adecuados en sus centros de datos, mediante la revisión de certificaciones e informes independientes.

Controles:
- Solicitar y revisar certificaciones (ISO/IEC 27001, ISO/IEC 27017/27018) e informes SOC 2 del proveedor.
- Verificar que las regiones de nube utilizadas cumplan los requisitos de disponibilidad y protección física.

LINEAMIENTOS DE SEGURIDAD PARA SERVICIOS EN LA NUBE			
PROCESO:	GESTIÓN TICs		
PROCEDIMIENTO:	ADMINISTRACIÓN DE PLATAFORMA TECNOLOGICA		
FECHA DE APROBACIÓN:	**CÓDIGO:**	**VERSIÓN:**	**PÁGINA:**
29/07/2026	GTI02-GUI04	*01*	12 de 20

- Documentar la delegación de responsabilidades físicas dentro del modelo de responsabilidad compartida.

6.3.2. Seguridad física de dispositivos y puestos de acceso

Los dispositivos y puestos de trabajo desde los cuales se accede a los servicios en la nube deberán contar con controles físicos que reduzcan el riesgo de acceso indebido o pérdida de información.

Controles:
- Aplicar políticas de escritorio y pantalla despejados y bloqueo automático de sesión.
- Proteger los equipos fuera de las instalaciones (portátiles, dispositivos móviles).
- Reportar la pérdida, robo o compromiso de dispositivos con acceso a la nube.

6.3.3. Eliminación segura de medios y equipos

Los medios de almacenamiento y equipos que hayan contenido información de la entidad deberán ser objeto de eliminación o reutilización segura, coordinada con la eliminación lógica de información en la nube.

Controles:
- Aplicar procedimientos de borrado seguro o destrucción de medios físicos.
- Coordinar con el proveedor la eliminación segura de datos cuando el servicio finalice (ver 6.4.8 y sección 9).

6.4. CONTROLES TECNOLÓGICOS (ISO/IEC 27001:2022 — A.8)

6.4.1. Gestión de identidades y autenticación segura

La CGN deberá gestionar de forma segura las identidades de usuarios, administradores, aplicaciones y servicios, garantizando accesos únicos, personales, autorizados y trazables, con mecanismos de autenticación robustos.

Controles:
- Crear cuentas individuales para cada usuario autorizado y evitar cuentas genéricas o compartidas.
- Habilitar autenticación multifactor (MFA) para usuarios y administradores.

LINEAMIENTOS DE SEGURIDAD PARA SERVICIOS EN LA NUBE			
PROCESO:	GESTIÓN TICs		
PROCEDIMIENTO:	ADMINISTRACIÓN DE PLATAFORMA TECNOLOGICA		
FECHA DE APROBACIÓN:	**CÓDIGO:**	**VERSIÓN:**	**PÁGINA:**
29/07/2026	GTI02-GUI04	*01*	13 de 20

- Implementar políticas de acceso condicional según riesgo, ubicación, dispositivo o rol.
- Revisar periódicamente usuarios activos, inactivos y cuentas con privilegios.
- Registrar y monitorear los inicios de sesión exitosos y fallidos.
- Gestionar de forma segura las identidades (cuentas de servicio, identidades administradas y aplicaciones), incluyendo su inventario, la rotación de sus credenciales y la revisión periódica de sus permisos.

6.4.2. Derechos de acceso privilegiado

Los accesos privilegiados deberán asignarse únicamente a usuarios autorizados bajo el principio de mínimo privilegio, evitando permisos excesivos o permanentes.

Controles:

- Asignar permisos administrativos solo cuando exista justificación funcional.
- Utilizar control de acceso basado en roles (RBAC) y evitar el uso permanente de cuentas con altos privilegios (acceso just-in-time / elevación temporal).
- Implementar aprobación previa para accesos críticos o cambios sensibles.
- Monitorear las acciones de usuarios privilegiados y documentar la asignación, modificación y retiro de permisos administrativos.
- Controlar el uso de programas utilitarios privilegiados.

6.4.3. Restricción de acceso a la información

El acceso a bases de datos, almacenamiento y servicios críticos deberá restringirse a nivel de recurso conforme a la clasificación de la información y a los roles autorizados.

Controles:

- Restringir el acceso a bases de datos, almacenamiento y servicios críticos.
- Implementar controles de acceso a nivel de recurso, carpeta, contenedor o servicio.
- Evitar la exposición pública de cuentas de almacenamiento, bases de datos o recursos sensibles.
- Monitorear accesos no autorizados o actividades inusuales sobre la información.

LINEAMIENTOS DE SEGURIDAD PARA SERVICIOS EN LA NUBE			
PROCESO:	GESTIÓN TICs		
PROCEDIMIENTO:	ADMINISTRACIÓN DE PLATAFORMA TECNOLOGICA		
FECHA DE APROBACIÓN:	**CÓDIGO:**	**VERSIÓN:**	**PÁGINA:**
29/07/2026	GTI02-GUI04	*01*	14 de 20

6.4.4. Seguridad de los dispositivos de usuario final

Los dispositivos desde los cuales se accede a los servicios en la nube deberán contar con controles mínimos de seguridad que reduzcan riesgos de acceso indebido, *malware* o fuga de información.

Controles:

- Permitir el acceso únicamente desde dispositivos autorizados o confiables.
- Mantener sistemas operativos y aplicaciones actualizados.
- Implementar acceso condicional según el estado y cumplimiento del dispositivo.
- Restringir descargas de información sensible en equipos no autorizados.

6.4.5. Protección contra software malicioso

Los recursos y dispositivos asociados al entorno de nube deberán contar con protección contra software malicioso.

Controles:

- Contar con protección antimalware o solución EDR en los puntos de acceso.
- Habilitar las capacidades de protección contra amenazas del proveedor de nube.
- Mantener actualizadas las firmas y motores de detección.

6.4.6. Gestión de vulnerabilidades técnicas y postura de seguridad

La entidad deberá identificar, evaluar y tratar oportunamente las vulnerabilidades técnicas y las recomendaciones de seguridad emitidas por las herramientas del proveedor de nube, y hacer seguimiento a su postura de seguridad.

Controles:

- Revisar periódicamente las recomendaciones de seguridad de las herramientas del proveedor y priorizar las de alto impacto.
- Asignar responsables y plazos para el tratamiento de vulnerabilidades y recomendaciones.
- Corregir configuraciones inseguras detectadas y validar el cierre efectivo.

LINEAMIENTOS DE SEGURIDAD PARA SERVICIOS EN LA NUBE			
PROCESO:	GESTIÓN TICs		
PROCEDIMIENTO:	ADMINISTRACIÓN DE PLATAFORMA TECNOLOGICA		
FECHA DE APROBACIÓN:	**CÓDIGO:**	**VERSIÓN:**	**PÁGINA:**
29/07/2026	GTI02-GUI04	*01*	15 de 20

- Hacer seguimiento a un indicador o puntaje de postura de seguridad y reportar desviaciones, integrándolo a los informes de seguridad y a los planes de mejora.

6.4.7. Gestión de la configuración

Los recursos en la nube deberán configurarse de forma segura desde su despliegue y mantenerse conforme a líneas base (baselines) definidas, gestionando los cambios de configuración de manera controlada.

Controles:

- Aplicar configuraciones seguras (hardening) desde el despliegue inicial.
- Definir y aplicar líneas base de configuración y políticas de cumplimiento automatizadas.
- Organizar los recursos mediante agrupaciones lógicas y etiquetas, y separar ambientes de producción, pruebas y desarrollo.
- Documentar la creación, modificación y eliminación de recursos y restringir la creación de recursos no autorizados.

6.4.8. Eliminación de información y enmascaramiento de datos

La información deberá eliminarse de forma segura cuando ya no sea necesaria, y los datos sensibles deberán protegerse mediante enmascaramiento cuando corresponda.

Controles:

- Definir y aplicar procedimientos de eliminación segura de información en la nube.
- Aplicar enmascaramiento o seudonimización de datos sensibles en ambientes de prueba y desarrollo.
- Verificar la eliminación efectiva de datos al finalizar servicios o retirar recursos.

6.4.9. Prevención de fuga de datos

La entidad deberá aplicar medidas para prevenir la fuga o extracción no autorizada de información sensible desde los servicios en la nube.

LINEAMIENTOS DE SEGURIDAD PARA SERVICIOS EN LA NUBE			
PROCESO:	GESTIÓN TICs		
PROCEDIMIENTO:	ADMINISTRACIÓN DE PLATAFORMA TECNOLOGICA		
FECHA DE APROBACIÓN:	**CÓDIGO:**	**VERSIÓN:**	**PÁGINA:**
29/07/2026	GTI02-GUI04	*01*	16 de 20

Controles:

- Aplicar controles de prevención de fuga de datos (DLP) sobre la información sensible.
- Restringir la salida de información hacia destinos no autorizados.
- Monitorear transferencias y descargas inusuales de información.

6.4.10. Copias de seguridad y redundancia

Los recursos críticos deberán contar con copias de seguridad y mecanismos de redundancia que permitan recuperar la información y los servicios ante pérdida, daño, error humano o incidente.

Controles:

- Definir la periodicidad de las copias según la criticidad del recurso.
- Habilitar respaldos para cómputo, bases de datos, almacenamiento y servicios críticos.
- Proteger las copias contra modificación o eliminación no autorizada (inmutabilidad) y restringir su acceso.
- Validar periódicamente la restauración de respaldos y documentar las pruebas de recuperación.
- Implementar redundancia para los servicios de alta disponibilidad y monitorear las fallas en la ejecución de copias.

6.4.11. Registro de eventos (logging).

La entidad deberá habilitar y conservar los registros de actividad, autenticación y auditoría de los servicios en la nube, garantizando su integridad y disponibilidad para trazabilidad y análisis.

Controles:

- Habilitar registros de actividad, inicio de sesión y auditoría de la plataforma.
- Sincronizar los relojes de los sistemas para asegurar la coherencia temporal de los registros.
- Proteger los registros contra alteración o eliminación no autorizada.
- Conservar los registros por el tiempo definido en la política institucional.

LINEAMIENTOS DE SEGURIDAD PARA SERVICIOS EN LA NUBE			
PROCESO:	GESTIÓN TICs		
PROCEDIMIENTO:	ADMINISTRACIÓN DE PLATAFORMA TECNOLOGICA		
FECHA DE APROBACIÓN:	**CÓDIGO:**	**VERSIÓN:**	**PÁGINA:**
29/07/2026	GTI02-GUI04	*01*	17 de 20

6.4.12. Actividades de monitoreo, detección y gestión de alertas

La CGN deberá monitorear de forma continua los servicios en la nube para detectar oportunamente eventos sospechosos, accesos no autorizados, cambios críticos o comportamientos anómalos, y gestionar las alertas resultantes.

Controles:

- Integrar los eventos relevantes en una solución de monitoreo y correlación (SIEM) o equivalente del proveedor.
- Configurar alertas ante cambios críticos en recursos, permisos o configuraciones, y clasificarlas por severidad.
- Definir responsables para la revisión y atención de las alertas, y escalar las críticas al equipo de Seguridad de la Información.
- Analizar alertas de identidad, red, recursos, datos y amenazas; registrar las acciones tomadas y cerrar las alertas solo cuando hayan sido tratadas.
- Generar reportes de seguimiento y análisis, y conservar evidencia de la gestión realizada.

6.4.13. Seguridad de redes

Las redes y los servicios de red del entorno de nube deberán protegerse, segmentarse y controlarse para reducir la superficie de exposición y prevenir accesos no autorizados.

Controles:

- Segmentar las redes y separar los ambientes mediante controles de red (grupos de seguridad, subredes, cortafuegos).
- Utilizar conexiones y puntos de acceso privados para servicios críticos y evitar la exposición pública innecesaria.
- Aplicar controles de filtrado web y de tráfico saliente cuando corresponda.
- Asegurar los servicios de red y monitorear el tráfico en busca de anomalías.

6.4.14. Uso de criptografía

La información alojada, procesada o transmitida en la nube deberá protegerse mediante cifrado, con una gestión segura de las claves criptográficas.

Controles:

- Aplicar cifrado de datos en reposo y en tránsito.

LINEAMIENTOS DE SEGURIDAD PARA SERVICIOS EN LA NUBE			
PROCESO:	GESTIÓN TICs		
PROCEDIMIENTO:	ADMINISTRACIÓN DE PLATAFORMA TECNOLOGICA		
FECHA DE APROBACIÓN:	**CÓDIGO:**	**VERSIÓN:**	**PÁGINA:**
29/07/2026	GTI02-GUI04	*01*	18 de 20

- Gestionar de forma segura las claves de cifrado (almacenes de claves/secretos, rotación, control de acceso).
- Configurar políticas de retención y protección de la información conforme a su clasificación.

6.4.15. Seguridad en el ciclo de vida de desarrollo (DevSecOps)

Los procesos de desarrollo, integración y despliegue en la nube deberán incorporar controles de seguridad que reduzcan vulnerabilidades, protejan las credenciales y garanticen la integridad del código y de los ambientes.

Controles:

- Separar los ambientes de desarrollo, pruebas y producción, y controlar el acceso a repositorios, pipelines y artefactos.
- Evitar almacenar contraseñas, claves o secretos en el código fuente; utilizar almacenes seguros de secretos y certificados.
- Aplicar prácticas de codificación segura y realizar revisiones de código antes del despliegue.
- Ejecutar análisis de vulnerabilidades en código, dependencias e imágenes, y realizar pruebas de seguridad en desarrollo y aceptación.
- Proteger las APIs e interfaces expuestas mediante mecanismos robustos de autenticación y autorización, pasarelas (API gateway), limitación de tasa y monitoreo de su uso.
- Registrar y aprobar los cambios antes de llevarlos a producción, manteniendo trazabilidad de despliegues, responsables y versiones.

6.4.16. Gestión de cambios

Los cambios sobre los recursos, configuraciones y servicios en la nube deberán planificarse, aprobarse, documentarse y verificarse de forma controlada.

Controles:

- Registrar y aprobar los cambios antes de su implementación.
- Evaluar el impacto en seguridad de los cambios relevantes.
- Mantener trazabilidad de los cambios y prever mecanismos de reversión.

LINEAMIENTOS DE SEGURIDAD PARA SERVICIOS EN LA NUBE			
PROCESO:	GESTIÓN TICs		
PROCEDIMIENTO:	ADMINISTRACIÓN DE PLATAFORMA TECNOLOGICA		
FECHA DE APROBACIÓN:	**CÓDIGO:**	**VERSIÓN:**	**PÁGINA:**
29/07/2026	GTI02-GUI04	*01*	19 de 20

7. SEGUIMIENTO, REVISIÓN Y MEJORA CONTINUA

La presente guía deberá ser revisada y actualizada periódicamente por el GIT de Apoyo Informático y Seguridad de la Información, con el fin de garantizar que los lineamientos, procedimientos y controles se mantengan vigentes, efectivos y alineados con las necesidades institucionales, los cambios en las plataformas de nube utilizadas, las buenas prácticas y la normatividad aplicable.

El seguimiento y la mejora continua se enmarcan en el ciclo PHVA (Planificar, Hacer, Verificar, Actuar) del MSPI y en las cláusulas 9 (evaluación del desempeño) y 10 (mejora) de la norma ISO/IEC 27001:2022:

- **Planificar:** Definir objetivos, controles y criterios de seguridad para los servicios en la nube.
- **Hacer:** Implementar y operar los controles descritos en esta guía.
- **Verificar:** Analizar resultados de monitoreo, alertas, incidentes, auditorías, revisiones internas y recomendaciones de las herramientas del proveedor.
- **Actuar:** Definir y ejecutar acciones correctivas, preventivas y de mejora que fortalezcan la postura de seguridad.

Los controles definidos deberán revisarse para verificar su correcta implementación, cumplimiento y efectividad, realizando los ajustes necesarios en las configuraciones y controles para atender los riesgos identificados, corregir desviaciones y fortalecer de manera continua la postura de seguridad del entorno de nube de la entidad.

8. DESVINCULACIÓN, MIGRACIÓN O SALIDA DE SERVICIOS EN LA NUBE

En caso de que la entidad decida suspender, migrar, reemplazar o finalizar el uso de un servicio o proveedor de nube, se deberá realizar un proceso controlado de desvinculación que garantice la protección, integridad, disponibilidad y recuperación de la información alojada.

Antes de retirar los servicios, el GIT de Apoyo Informático, en coordinación con Seguridad de la Información y los dueños de la información, deberá identificar los recursos activos, servicios críticos, bases de datos, cuentas de almacenamiento, respaldos, configuraciones, usuarios, roles, dependencias, integraciones y contratos asociados.

LINEAMIENTOS DE SEGURIDAD PARA SERVICIOS EN LA NUBE			
PROCESO:	GESTIÓN TICs		
PROCEDIMIENTO:	ADMINISTRACIÓN DE PLATAFORMA TECNOLOGICA		
FECHA DE APROBACIÓN:	**CÓDIGO:**	**VERSIÓN:**	**PÁGINA:**
29/07/2026	GTI02-GUI04	*01*	20 de 20

Se deberá elaborar un plan de migración o retiro que contemple la copia, exportación, validación y transferencia segura de la información hacia la nueva plataforma, infraestructura o repositorio definido, garantizando que la información sea recuperable, íntegra, legible y disponible para la continuidad operativa. La estrategia de salida definida en el control 6.1.2 debe orientar este proceso y mitigar la dependencia tecnológica (vendor lock-in).

Una vez finalizada la migración o retiro, se deberán eliminar o deshabilitar los recursos que ya no sean requeridos, revocar accesos, cerrar cuentas administrativas, cancelar servicios activos y verificar la eliminación segura de datos cuando aplique, conservando las evidencias del proceso. Todo el proceso deberá quedar documentado mediante acta, inventario de recursos retirados, evidencias de respaldo, validación de restauración o transferencia, aprobación de los responsables y constancia de cierre del servicio.

9. DOCUMENTOS DE REFERENCIA

GTI02-MAN01 - Anexo términos y definiciones de seguridad de la información y ciberseguridad

CONTROL DE CAMBIOS

Versión	Fecha	Descripción del cambio	Responsable
1	29/07/2026	Generalización a servicios en la nube (cloud-agnóstica); reorganización de controles conforme a los dominios del Anexo A de ISO/IEC 27001:2022; incorporación del marco normativo (ISO/IEC 27032, MSPI); matriz de trazabilidad; y traslado de la implementación específica de Azure al Anexo A.	Equipo de Seguridad de la Información