Tribunal de Cuentas de la Provincia de La Pampa

ANEXO

POLÍTICA INSTITUCIONAL DE LA SEGURIDAD DE LA INFORMACIÓN DEL TRIBUNAL DE CUENTAS DE LA PAMPA

Índice

13. Glosario

14. Anexos Operativos

- Anexo I: Acta de Confidencialidad.
- Anexo II: Procedimiento de contingencia (uso de soporte papel).
- Anexo III: Políticas de uso a aceptable de correo electrónico institucional e internet
- Anexo IV: Política de alta, modificación y baja de activos informáticos
- Anexo V: Procedimiento de gestión de incidentes.
- Anexo VI: Políticas de Tratamiento y Protección de Datos Personales

1. Introducción

El Tribunal de Cuentas de la Provincia de La Pampa, en el marco de sus competencias establecidas por el Decreto Ley N° 513/69 y la Ley Provincial N° 3428, asume el compromiso de garantizar la protección integral de los datos personales bajo su responsabilidad, en cumplimiento de la Ley Nacional N° 25.326 y a la normativa dictada por la Agencia de Acceso a la Información Pública (AAIP).

Este Manual constituye la política institucional de Seguridad de la Información y será de aplicación a todos los sistemas, aplicaciones, correo electrónico institucional, infraestructura tecnológica y servicios de verificación de identidad provistos por organismos públicos competentes.

A través de este documento, el Tribunal establece un marco que asegura la integridad de los datos y la eficiencia de la gestión administrativa, aún en situaciones de crisis o contingencia.

2. Marco Normativo

El presente Manual se dicta en cumplimiento de:

- Ley N° 25.326 de Protección de Datos Personales.
- Resolución AAIP N° 47/2018: Medidas de seguridad recomendadas para el tratamiento y conservación de datos personales informatizados y no informatizados.
- Decisión Administrativa N° 641/2021 y su Anexo: Requisitos mínimos de seguridad de la información para organismos del Sector Público.
- Ley Orgánica del Tribunal de Cuentas – Decreto Ley N° 513/69.
- Ley Provincial N° 3428, que autoriza al Tribunal a implementar TIC, expedientes electrónicos, notificaciones digitales y domicilios electrónicos.

3. Objetivos de la Política de Seguridad

La Política de Seguridad de la Información del Tribunal de Cuentas tiene como primer objetivo proteger la confidencialidad, la integridad y la disponibilidad de los datos y documentos que administra. La información debe estar disponible únicamente para las personas autorizadas, debe mantenerse completa y exacta, y debe poder ser utilizada en tiempo y forma para el cumplimiento de las funciones institucionales.

En segundo término, la Política asegura el cumplimiento de las normativas nacionales y provinciales en materia de protección de datos personales, estableciendo prácticas claras que impidan accesos indebidos o manipulaciones no autorizadas. También promueve mecanismos que garanticen la trazabilidad de todas las operaciones que se realicen dentro de los sistemas del Tribunal, de modo que sea posible reconstruir las acciones efectuadas ante cualquier eventualidad.

Finalmente, la Política tiene como propósito asegurar la continuidad de los servicios mediante la adopción de planes de contingencia y recuperación, de manera tal que la actividad administrativa y de control no se vea interrumpida frente a fallas técnicas o incidentes de seguridad. Con este Manual se fijan además lineamientos organizativos, técnicos y jurídicos que deberán ser observados por todo el personal, fomentando una cultura institucional de seguridad.

4. Principios Rectores

El tratamiento de la información en el Tribunal de Cuentas se rige por los siguientes principios que aseguran que los datos se utilicen con un objetivo legítimo y explícito.

En conjunto, estos criterios permiten que el Tribunal pueda dar cuenta ante la ciudadanía y los órganos de control de la correcta gestión de la información bajo su custodia.

- Licitud y transparencia: todo tratamiento de datos se realiza conforme a ley, debe basarse en un interés legítimo y con consentimiento informado.

- Finalidad: los datos solo serán usados para validar identidad y verificar vigencia del Documento Nacional de Identidad (D.N.I) en los procesos de control y rendición de cuentas del Tribunal de Cuentas.

- Confidencialidad: todo el personal deberá suscribir actas de confidencialidad

- Minimización y retención limitada: solo se recolectarán los datos estrictamente necesarios y por el tiempo estrictamente requerido.

- Responsabilidad proactiva: el Tribunal garantiza medidas de seguridad continuas, actualizadas y documentadas.

- Responsabilidad demostrada (accountability): el Tribunal adopta medidas técnicas y organizativas apropiadas y puede demostrar su cumplimiento (registros, evidencias, auditorías).

5. Roles y Responsabilidades

La implementación de esta política requiere la participación de diversos actores a fin de dar cumplimiento al presente de acuerdo a las designaciones que realice la alta dirección del organismo. Los diferentes roles y responsabilidades se distinguen en:

- Responsable de Seguridad de la Información: El mismo será designado por el Tribunal, y asistirá técnicamente al organismo a fin de coordinar todas las políticas de seguridad de la información.

- Área de Sistemas: Administra técnicamente los sistemas, implementa y mantiene medidas de seguridad

- Usuarios autorizados: solo las personas individualizadas podrán acceder a los datos de su área y servicios de verificación de identidad en caso de corresponder. deberá firmar compromisos de confidencialidad y participar en capacitaciones periódicas.

- Auditoría Interna: controla el cumplimiento de las instrucciones de trabajo y las políticas de seguridad de la información.

6. Medidas Organizativas

Las medidas organizativas constituyen el conjunto de disposiciones internas orientadas a establecer un marco de responsabilidad compartida en materia de seguridad de la información. A través de estas pautas se busca definir las reglas básicas de conducta de los agentes, regular el uso de los recursos tecnológicos, organizar los procesos de capacitación y establecer mecanismos claros para la incorporación, permanencia y desvinculación del personal.

Estas medidas tienen como finalidad crear una cultura de seguridad institucional que complemente los controles técnicos, asegurando que todos los actores conozcan sus obligaciones y actúen en consecuencia para proteger los activos de información del Tribunal.

6.1 Gestión de Software y Licenciamiento

Toda instalación o desinstalación de software requerirá solicitud formal y será realizada exclusivamente por el área técnica competente, previa verificación de licenciamiento. Se prohíbe la instalación de software no autorizado.

6.2 Uso Aceptable, Indebido y Prohibido

- Uso aceptable: el equipamiento y servicios informáticos se utilizan para funciones oficiales. Se permite un uso personal limitado que no interfiera en las tareas ni genere costos adicionales.
- Uso indebido: instalación de software sin autorización, alteración de configuraciones, elusión de controles, acceso a código fuente sin permiso, lectura de archivos ajenos, difusión de información sin autorización.
- Uso prohibido: compartir credenciales, introducir malware, acceder sin autorización, revelar información privada de terceros, usar recursos para fines contrarios a la ley o intereses del Tribunal.

6.3 Seguridad del personal y recursos humanos

- Firma obligatoria de actas de compromisos de confidencialidad.
- Baja inmediata de accesos al cesar la relación laboral.
- Custodiar credenciales, reportar incidentes, usar responsablemente los recursos.
- Registro de incidentes y reporte inmediato al área técnica.

6.4 Concientización y capacitación

- Aprobación y difusión de la presente Política por parte del Tribunal.

- Programas de formación en protección de datos y buenas prácticas digitales

6.5 Relación con proveedores y terceros

- Inclusión en los contratos de cláusulas de confidencialidad y seguridad.

7. Medidas Técnicas de Seguridad

Las medidas técnicas de seguridad comprenden el conjunto de controles, herramientas y procedimientos tecnológicos destinados a garantizar la protección de la información del Tribunal. Su aplicación permite reducir vulnerabilidades, prevenir incidentes y asegurar que los sistemas funcionen de manera confiable y disponible para el cumplimiento de las funciones institucionales.

Estas medidas abarcan desde el control de accesos y la administración de usuarios, hasta la seguridad en redes, la protección de servidores y aplicaciones, la realización de respaldos, el cifrado de la información y el monitoreo de la actividad de los sistemas.

En conjunto, constituyen la base operativa que da soporte a las medidas organizativas, complementándolas y asegurando un nivel de protección integral para los activos informáticos.

7.1 Control de Accesos

- Todos los usuarios deberán contar con credenciales únicas e intransferibles.
- Autenticación mediante contraseña robusta y, cuando corresponda, doble factor de autenticación (2FA).
- Asignación de perfiles de usuario diferenciados.
- Bloqueo automático de sesión tras 10 minutos de inactividad.
- Registro (logs) de todos los accesos, intentos fallidos y operaciones críticas.

7.2 Administración de Usuarios

- Altas, bajas y modificaciones gestionadas el Área de Sistemas.
- Eliminación inmediata de accesos ante bajas de personal.
- Revisión semestral de cuentas activas y privilegios.

7.3 Seguridad en Redes y Comunicaciones

- Segmentación de la red interna (servidores, puestos de trabajo, invitados).
- Uso de firewall institucional y sistemas IDS/IPS.
- Encriptación obligatoria de comunicaciones (HTTPS, VPN, TLS).

Se eliminó el último punto que refería al correo institucional como único canal válido para trámites oficiales

7.4 Protección de Servidores y Software

- Actualización periódica de sistemas operativos, bases de datos y aplicaciones.
- Aplicación inmediata de parches de seguridad críticos.
- Separación de entornos de desarrollo, pruebas y producción.
- Acceso restringido a código fuente.

7.5 Respaldo y Recuperación

- Backups automáticos diarios y semanales en soporte cifrado.
- Copias externas almacenadas en sitio alternativo.
- Pruebas semestrales de restauración de datos.

7.6 Seguridad Física y Ambiental

- Acceso restringido a salas de servidores.
- Cámaras de seguridad y registros de acceso.
- Políticas de escritorios y pantallas limpias.
- Prohibición de uso de dispositivos externos sin autorización (pendrives, discos portátiles).
- Procedimientos documentados y autorizados para el ingreso/egreso de equipamiento
- Copias de resguardo antes de reparaciones.
- Controles frente a incendio, polvo, humedad y variaciones eléctricas.

7.7 Seguridad Criptográfica

- Uso obligatorio de TLS/SSL en todas las comunicaciones.
- Cifrado en reposo de bases de datos y dispositivos críticos.
- Procedimiento formal de gestión de claves (emisión, custodia, rotación, revocación).
- Cifrado de dispositivos y transmisiones de datos.
- Uso obligatorio de certificados digitales en los sitios web institucionales.

7.8 Gestión de Vulnerabilidades

- Escaneo de vulnerabilidades trimestral en redes y aplicaciones.
- Actualizaciones periódicas de software y parches de seguridad.
- Auditorías internas y externas de seguridad.
- Monitoreo continuo con Zabbix y Wazuh

7.9 Desarrollo Seguro de Software

- Aplicación de metodologías de seguridad desde el diseño (Secure by Design).
- Pruebas de seguridad en todas las etapas (QA, pentesting).
- Prohibición del uso de bases de datos reales en entornos de prueba.

7.10 Monitorización de uso

El uso de la red y de los equipos institucionales puede ser monitoreado por personal autorizado, con fines de seguridad. La información obtenida se trata confidencialmente y solo se divulga en caso de incumplimiento o incidentes.

8. Activos de Información y Gestión de Incidentes

La gestión de incidentes constituye un componente esencial de la política de seguridad del Tribunal, ya que permite responder de manera ordenada y eficiente frente a cualquier evento que afecte la continuidad de los servicios o la integridad de la información.

Su objetivo es detectar, registrar, clasificar y resolver los incidentes con la mayor rapidez posible, minimizando su impacto y evitando recurrencias a través del análisis de las causas raíz. Este proceso, apoyado en el uso de la herramienta de gestión como mesa de servicios asegura trazabilidad, escalamiento oportuno y la adopción de medidas correctivas y preventivas.

De este modo, se garantiza que la organización cuente con mecanismos claros para enfrentar contingencias tecnológicas o administrativas y preservar la confianza en sus sistemas y procesos.

Los lineamientos generales a enumerar son los siguientes:

- Identificación y clasificación de activos: información, equipos, infraestructura y recursos humanos.
- Elaboración de un inventario de activos críticos.
- Definición de un protocolo de respuesta a incidentes: detección, análisis, contención, erradicación y recuperación.
- Documentación de incidentes con responsables, tiempos de respuesta y medidas adoptadas.

9. Continuidad Operativa

La continuidad operativa se refiere al conjunto de medidas destinadas a garantizar que los procesos críticos del Tribunal de Cuentas puedan mantenerse o restablecerse en un plazo razonable frente a una interrupción no prevista. Estas disposiciones buscan minimizar el impacto de incidentes graves, como fallas técnicas, contingencias en los sistemas electrónicos o eventos externos que afecten la infraestructura.

La continuidad operativa no solo contempla la existencia de planes de contingencia y recuperación, sino también la organización de procedimientos alternativos, como el uso de soporte papel, para asegurar que la gestión administrativa y de control no se detenga.

De este modo, el Tribunal preserva la disponibilidad de la información y la prestación de sus servicios aún en escenarios adversos, manteniendo la confianza y seguridad en su accionar institucional.

- El Tribunal implementará planes de contingencia para asegurar la continuidad de la gestión en caso de fallas técnicas o incidentes.

- Procedimientos para uso de papel y firma ológrafa en casos de contingencia, conforme normativa vigente del Tribunal.
- Identificación de procesos críticos y tiempos máximos de recuperación (RTO/RPO).
- Backups diarios (30 días), semanales (12 semanas), mensuales (12 meses).
- Pruebas de restauración documentadas (qué, quién, cuándo, resultado).

10. Indicadores y Mejora Continua

Estos indicadores se revisarán periódicamente para mejorar la seguridad.

- Número de incidentes detectados.
- Tiempo promedio de respuesta.
- Cumplimiento de backups.
- Porcentaje de agentes capacitados.

11. Cumplimiento y Auditoría

El cumplimiento y la auditoría constituyen los mecanismos mediante los cuales el Tribunal de Cuentas asegura que las políticas y procedimientos establecidos en este Manual se apliquen de manera efectiva y sostenida en el tiempo.

A través de controles periódicos, revisiones internas y auditorías externas, se verifica que las áreas y los agentes cumplan con las normas de seguridad de la información, identificando posibles desvíos y promoviendo acciones correctivas.

Este enfoque permite no solo garantizar la observancia de las disposiciones legales y reglamentarias, sino también fortalecer la transparencia institucional y consolidar una cultura de mejora continua en la protección de los activos de información del organismo.

- La presente Política será revisada y actualizada anualmente.

- Se realizarán auditorías internas y externas anuales según los lineamientos de la normativa vigente.
- Régimen sancionatorio por incumplimiento, conforme normativa laboral y disciplinaria vigente.

12. Disposiciones Finales

El presente Manual rige desde su aprobación por resolución del Tribunal de Cuentas y será de cumplimiento obligatorio para todas las áreas y agentes del organismo.
El incumplimiento será pasible de sanciones graduadas según la gravedad, sin perjuicio de responsabilidades civiles o penales.”

Asimismo, todos los procedimientos específicos que deban desarrollarse en función de los lineamientos establecidos en este Manual serán elaborados por las áreas competentes mediante Instrucciones de Trabajo (IT). Dichas IT definirán con precisión los procesos, responsables, recursos y controles bajo los cuales se ejecutan las diferentes actividades, en concordancia con los estándares de calidad vigentes en el Tribunal de Cuentas.

13. Glosario:

- **Activo de información:** cualquier recurso que contenga o procese datos (documentos, bases de datos, equipos, servidores).
- **Amenaza:** todo evento que pueda dañar la información (ejemplo: un virus, un incendio).
- **Confidencialidad:** acceso solo para personas autorizadas.
- **Disponibilidad:** acceso a la información cuando sea requerido por usuarios autorizados.
- **Incidente:** un hecho que afecta la seguridad de la información.
- **Información:** datos en cualquier formato (papel, digital, imagen, audio, video).
- **Integridad:** garantía de exactitud y completitud de la información.
- **Respaldo (backup):** copia de seguridad de la información.
- **Sistema de información:** conjunto de recursos para recopilar, procesar y difundir información.
- **Vulnerabilidad:** una debilidad que puede ser aprovechada por una amenaza.

14. Anexos Operativos

Los anexos forman parte integrante de este Manual y tienen por finalidad desarrollar, en forma práctica y operativa, los procedimientos y modelos que complementan las políticas generales de seguridad de la información aquí establecidas.

Cada anexo constituye una guía concreta para la aplicación de los lineamientos, ofreciendo instrucciones claras que permiten a las áreas y a los agentes del Tribunal cumplir con sus responsabilidades de manera uniforme y documentada.

Su incorporación garantiza que los criterios definidos en este Manual se traduzcan en acciones específicas y controlables, contribuyendo a la estandarización de procesos y al fortalecimiento de la cultura de seguridad institucional.

ANEXO I – Acta de Confidencialidad

Entre el Tribunal de Cuentas de la Provincia de La Pampa, representado en este acto por el Sr/Sra …… DNI ……, en su de carácter de ……, con domicilio legal en la calle ……. el "TRIBUNAL DE CUENTAS" por una parte; y por la otra el/la Sr./Sra. ……..DNI …… en su carácter de (**agente / contratista / proveedor / funcionario)** ……., con domicilio en ……..……, en adelante el "RESPONSABLE" , acuerdan celebrar el presente Acuerdo de Confidencialidad , sujeto a las siguientes cláusulas y condiciones:

Primera: EL/LA RESPONSABLE se obliga a guardar estricta confidencialidad y reserva sobre toda la información y documentación a la que tenga acceso en virtud de sus funciones, incluyendo datos personales, datos sensibles, información contable, administrativa, financiera, técnica, operativa, sistemas informáticos y cualquier otra que, por su naturaleza, deba mantenerse en reserva.----------

Segunda: La obligación de confidencialidad comprende la información en soporte papel, digital, electrónico, audiovisual, oral o cualquier otro medio. Incluye los datos provenientes de plataformas tecnológicas administradas por el Tribunal, del Sistema de Gestión Documental Electrónica (GDE) y de servicios provistos por organismos externos -

Tercera: La obligación asumida en este Acta subsistirá durante la vigencia de la relación con el Tribunal y aún después de su finalización, sin limitación temporal de la que solo podrá ser relevado mediante resolución judicial y/o por mediar razones fundadas de acuerdo a la normativa vigente.----------

Cuarta: EL/LA RESPONSABLE se compromete a no divulgar, transmitir, ceder, transferir o utilizar para fines ajenos a su función la información a la que acceda. No reproducir o copiar información confidencial sin autorización expresa. No almacenar información en dispositivos externos no autorizados. No revelar claves de acceso, contraseñas o credenciales otorgadas para su desempeño.----------

Quinta: El incumplimiento de la presente obligación dará lugar a las sanciones administrativas, civiles y penales que correspondan según la normativa vigente.----------

Sexta: Al finalizar su relación con el TRIBUNAL DE CUENTAS, EL/LA RESPONSABLE deberá devolver todo soporte que contenga información institucional y abstenerse de conservar copias de la misma en cualquier formato.----------

Séptima: En prueba de conformidad se firma la presente en dos ejemplares de un mismo tenor y a un solo efecto.

Firma del Comprometido/a

Nombre y Apellido: _____

DNI: _____

Cargo/Función: _____

Por el Tribunal de Cuentas de la Provincia de La Pampa

Nombre y Apellido: _____

Cargo: _____

Anexo II: Procedimiento de contingencia para uso en soporte papel de documentos electrónicos

1. Objeto

Establecer el procedimiento de excepción que deberá aplicarse frente a contingencias que impidan el normal funcionamiento de los sistemas electrónicos del Tribunal de Cuentas, a fin de garantizar la continuidad de la gestión administrativa mediante el uso de soporte papel con firma ológrafa.

2. Habilitación del procedimiento de contingencia

El procedimiento se considerará habilitado cuando:

- El sistema se encuentre indisponible por un lapso superior a una (1) hora, corroborado por el área de TI.
- La falla no sea local (del puesto de trabajo), sino generalizada.
- El Responsable del área de Tecnologías del Tribunal confirme la activación de la contingencia.

3. Emisión de documentos en contingencia

- Los actos administrativos y documentos institucionales se emitirán en formato papel con firma ológrafa.
- Se utilizarán Actas de Contingencia, rubricado por el área legal/técnica, donde se registrarán los actos emitidos durante la contingencia.
- El registro deberá incluir como mínimo: fecha, área emisora, nombre del firmante, tipo de acto/documento, numeración especial asignada y observaciones.
- En caso de duplicidad de documentos, tendrá validez el que haya sido notificado formalmente.

6. Incorporación posterior al sistema electrónico

- Una vez reanudado el sistema, cada documento emitido en contingencia deberá ser digitalizado, registrado y cargado en el sistema electrónico correspondiente manteniendo la correlación cronológica.
- La carga deberá efectuarse en un plazo máximo de 5 días hábiles desde el restablecimiento del servicio.

7. Firma y validez

- Los documentos en papel firmados durante la contingencia tendrán la misma validez jurídica que los documentos electrónicos, conforme la normativa nacional y provincial.
- Una vez incorporados al sistema, los documentos digitales derivados de la contingencia deberán adjuntar el escaneo del documento en papel original firmado.

8. Responsabilidades

- **Área de TI:** verificar indisponibilidad, comunicar activación de la contingencia y asistir en la posterior digitalización.
- **Áreas firmantes:** confeccionar y firmar documentos en papel, registrar en las Actas de Contingencia.
- **Secretaría Administrativa:** resguardar las Actas y garantizar su archivo seguro.

Procedimiento específico para GDE

En lo referente al Sistema de Gestión Documental Electrónica (GDE), cedido por la Subsecretaría de Innovación, Ciencia y Tecnología dependiente de la Jefatura de Gabinete de Ministros del Gobierno Nacional en su modalidad CLOUD, el Tribunal aplicará el Procedimiento de Contingencia establecido en la Resolución N° 301/2024 del Tribunal de Cuentas, que regula las condiciones, plazos y mecanismos de registración de documentos confeccionados en soporte papel durante la contingencia, así como su posterior incorporación al sistema.

En el supuesto que la contingencia no se encuentre relacionada a un inconveniente local, el Administrador Central del Sistema, asistido por el Área Técnica en caso de corresponder, deberá realizar el incidente a la Subsecretaría de Innovación a través del sistema de seguimientos Jira.

9. Auditoría y control

- Todos los documentos emitidos bajo contingencia serán objeto de auditoría interna y externa.
- El RSI deberá elaborar un informe posterior a cada contingencia, consignando fecha, duración, causas, actos emitidos y medidas adoptadas.

ANEXO III – Políticas de uso aceptable de correo electrónico institucional e internet.

1. Alcance

Las presentes políticas son de aplicación obligatoria para todo el personal del Tribunal de Cuentas de la Provincia de La Pampa, cualquiera sea su situación de revista, así como para contratistas o terceros que accedan a cuentas de correo electrónico institucional o a los servicios de internet provistos por el organismo.

2. Uso obligatorio del correo institucional

- Las cuentas institucionales podrán ser de carácter personal (asignadas a cada agente) o genéricas institucional (asignadas a áreas, sistemas o programas).
- El correo electrónico institucional es de dominio del organismo y deberá usarse únicamente con fines laborales vinculados a las funciones del Tribunal de Cuentas.

3. Credenciales y contraseñas

- Cada usuario será responsable de la custodia de su cuenta y clave de acceso.
- Las contraseñas deberán ser robustas: mínimo 12 caracteres, combinando mayúsculas, minúsculas, números y símbolos.
- Queda prohibido compartir claves o delegar su uso.
- No debe seleccionarse la opción “recordar contraseña” en navegadores o webmail.

4. Buenas prácticas en el uso del correo electrónico

- No abrir mensajes de remitentes desconocidos ni archivos adjuntos sospechosos (especialmente con extensiones .exe, .bat, .zip, etc.).
- Verificar que las direcciones de correo y enlaces recibidos sean coherentes y seguros (preferentemente HTTPS).
- No responder solicitudes de datos personales, contraseñas o información sensible. El Tribunal nunca solicitará dichos datos por correo.
- No reenviar cadenas de mensajes, SPAM o publicidad.
- Limitar el uso de la cuenta institucional a fines laborales; evitar su uso para registros en redes sociales, foros o sitios comerciales.
- Evitar adjuntar archivos de gran tamaño (>5MB); en su lugar, utilizar compresión o herramientas autorizadas.
- Cerrar sesión siempre al finalizar la jornada o al dejar de usar el correo.

5. Buenas prácticas en internet

- Utilizar internet únicamente para fines vinculados a la función laboral.

- Queda prohibido navegar en sitios de apuestas, descargas ilegales o que puedan comprometer la seguridad institucional.
- No instalar software ni extensiones de navegador sin autorización del área técnica.
- Evitar la divulgación de información institucional en redes sociales o foros sin autorización expresa.
- Se deberá utilizar siempre un equipo con antivirus actualizado y medidas de seguridad vigentes.

6. Protección de la información sensible

- No enviar por correo electrónico información personal, financiera o sensible sin utilizar los mecanismos de cifrado provistos por el área técnica.
- Consultar al Responsable de Seguridad de la Información ante la necesidad de enviar información crítica.

7. Responsabilidades y sanciones

- El incumplimiento de estas políticas será considerado falta grave y podrá derivar en sanciones administrativas, civiles y/o penales, sin perjuicio de las responsabilidades que correspondan conforme la Ley N° 25.326 y normativa complementaria.
- Las cuentas de correo institucional que no se utilicen por más de 6 meses serán dadas de baja de manera definitiva.

Anexo IV – Política de alta, modificación y baja de activos informáticos

1. Objeto

La presente política tiene como finalidad establecer los lineamientos y procedimientos para la gestión del ciclo de vida de los activos informáticos del Tribunal de Cuentas de la Provincia de La Pampa, incluyendo altas, modificaciones y bajas de usuarios, cuentas de correo electrónico, equipos, software, dispositivos móviles y medios de almacenamiento y cualquier otro recurso tecnológico.

2. Alcance

Será de aplicación obligatoria para todas las áreas del Tribunal de Cuentas y para todo el personal, cualquiera sea su situación de revista, así como para contratistas, pasantes o terceros que utilicen activos informáticos provistos por el organismo.

3. Definición de activos informáticos

Se consideran activos informáticos:

- **Usuarios y credenciales de acceso** a sistemas, redes, aplicaciones y correo electrónico institucional.
- **Equipos de cómputo** (PC, notebooks, servidores, terminales).
- **Dispositivos móviles y removibles** (celulares, tablets, discos externos, pen drives).
- **Software y licencias** adquiridas o desarrolladas.
- **Medios de almacenamiento** físicos o virtuales.
- **Cuentas institucionales** en sistemas, aplicaciones o servicios externos.

4. Principios rectores

- **Seguridad:** todo proceso de alta, modificación o baja debe preservar la confidencialidad, integridad y disponibilidad de la información.
- **Trazabilidad:** cada acción debe estar documentada.
- **Plazos:** las altas y bajas deberán procesarse en plazos breves, priorizando la seguridad.
- **Responsabilidad compartida:** Recursos Humanos, el área solicitante y el área de Tecnologías de la Información (TI) son responsables en conjunto.

5. Procedimientos

5.1 Altas, modificaciones y bajas de usuarios

- El área designada por el Tribunal de Cuentas deberá solicitar al área de **Sistemas** toda alta, baja, suspensión o cambio de puesto de agentes o contratistas que implique modificación de accesos. La notificación se realizará mediante el sistema de gestión designado, con firma del responsable del área.
- Una vez recibida la notificación, la solicitud deberá gestionarse en un plazo máximo de 24 horas en el cual se deberá en caso de corresponder a
    - Bloquear el acceso a la cuenta de correo electrónico institucional.
    - Revocar permisos asociados a sistemas y aplicaciones vinculadas a esa cuenta.
    - Iniciar el procedimiento de resguardo y/o transferencia de la información contenida en la casilla al responsable designado por el área del agente saliente.
- Los activos informáticos que no sean dadas de baja formalmente, pero que permanezcan inactivos por más de 6 meses, serán eliminadas de manera definitiva.
- El área de Sistemas mantendrá un registro de altas, bajas y modificaciones de usuarios, el cual podrá ser auditado por la Auditoría Interna del Tribunal.

5.2 Altas, modificaciones y bajas de activo informático

- Toda alta, modificación o baja de activo informático deberá solicitarse formalmente mediante el sistema de gestión autorizado.
- El área de TI generará las credenciales iniciales, aplicando políticas de contraseñas seguras (mínimo 12 caracteres, con mayúsculas, minúsculas, números y símbolos).
- Los equipos asignados deberán incorporarse al inventario institucional, con número de serie, características técnicas y responsable asignado.
- El alta de software incluirá la verificación de licencias y condiciones de uso, incorporándose al registro de activos.
- Las modificaciones deberán quedar asentadas en el registro de activos informáticos.

- El área de TI actualizará los privilegios en un plazo máximo de **24 horas** desde la notificación.
- La baja de equipos requerirá:
    - Copia de resguardo de la información institucional.
    - Borrado seguro de datos (wipe o destrucción física).
    - Actualización del inventario institucional.
- La baja de software implicará desinstalación, revocación de accesos y actualización del registro de licencias.
- La baja de medios de almacenamiento incluirá borrado seguro o destrucción física con registro documentado.

6. Registro y auditoría

El área de Sistemas mantendrá un registro actualizado de altas, modificaciones y bajas de activos informáticos, incluyendo usuarios, equipos, software y medios de almacenamiento. Dicho registro podrá ser auditado por la Auditoría Interna del Tribunal.

7. Sanciones

El incumplimiento de esta política será considerado falta grave y podrá derivar en sanciones administrativas, civiles y/o penales, conforme normativa vigente.

Anexo V: Procedimiento de Gestión de Incidentes

1. Objeto

Establecer una política general para la gestión de incidentes en el Tribunal de Cuentas, garantizando una respuesta organizada, ágil y trazable ante cualquier interrupción o falla en los servicios informáticos o administrativos, utilizando como soporte tecnológico el sistema Gestor Libre de Parque Informático - GLPI

2. Definición de incidente

Se considera incidente a cualquier evento que provoque o pueda provocar una interrupción, degradación o malfuncionamiento de un servicio, sistema, equipo o proceso del Tribunal de Cuentas, incluyendo:

- Falla de hardware o software.
- Problemas de conectividad.
- Errores en aplicaciones (ej.: GDE, correo institucional).
- Incidentes de seguridad de la información (virus, accesos no autorizados, fuga de datos).
- Incumplimientos de niveles de servicio acordados.

3. Principios rectores

- Registro obligatorio**:** todo incidente debe ser registrado en GLPI, sin importar su gravedad.
- Priorización: los incidentes serán clasificados por impacto y urgencia (crítico, alto, medio, bajo).
- Transparencia y trazabilidad: cada incidente contará con un historial en GLPI que documente acciones, responsables y tiempos de resolución.
- Escalamiento: los incidentes que no puedan resolverse en primera instancia deberán ser escalados al nivel superior en forma inmediata.
- Mejora continua: los incidentes serán analizados para identificar causas raíz y evitar recurrencias.

4. Roles y responsabilidades

- **Usuarios:** reportar incidentes a través de GLPI, aportando información clara y completa.
- **Área de Sistemas:** recibir, registrar, clasificar y priorizar los incidentes. Resolver los de bajo impacto y escalar los que requieran atención especializada.
- **Responsable de Seguridad de la Información (RSI):**

- Evaluar incidentes de seguridad, garantizar reporte a AAIP/Dirección Nacional de Ciberseguridad en plazos legales.

- Intervenir en incidentes críticos de seguridad o infraestructura; tomar decisiones sobre continuidad y escalamiento externo.

- Evaluar incidentes recurrentes o críticos para implementar acciones preventivas.

5. Flujo de gestión de incidentes

1. **Registro:** todo incidente debe ingresarse en GLPI (por el usuario o la mesa de ayuda).
2. **Clasificación:** identificar tipo de incidente y servicio afectado.
3. **Priorización:** determinar impacto y urgencia (matriz de criticidad).
4. **Asignación:** derivar al equipo correspondiente (Nivel 1, 2 o 3).
5. **Diagnóstico inicial:** análisis preliminar y, en caso posible, resolución inmediata.
6. **Escalamiento:** si no se resuelve, derivación a niveles superiores o proveedores externos.
7. **Resolución:** implementación de la solución definitiva.
8. **Cierre:** el incidente se cierra en GLPI solo cuando el usuario confirma o el responsable valida la solución.
9. **Revisión post-incidente:** para incidentes críticos, se realizará un análisis de causa raíz y se definirán medidas preventivas.

6. Reportes y auditoría

- GLPI generará reportes periódicos sobre incidentes abiertos, tiempos de resolución, categorías más frecuentes y responsables.
- Estos reportes serán revisados por el RSI y el Comité de Seguridad para detectar áreas de mejora.
- Se elaborará un **informe anual de incidentes** para la Presidencia del Tribunal.

7. Sanciones

El incumplimiento de este procedimiento (ej. no registrar incidentes, cerrar tickets sin resolución) será considerado falta y podrá dar lugar a sanciones administrativas, sin perjuicio de responsabilidades civiles o penales en caso de negligencia grave.

Anexo VI – Políticas de Tratamiento y Protección de Datos Personales

Introducción.

El Tribunal de Cuentas de la Provincia de La Pampa, en su carácter de órgano de control externo de la hacienda pública provincial y municipal, accede y administra datos

personales en el marco de sus funciones constitucionales y legales. Dichos datos provienen de la fiscalización de cuentas, la revisión de actos administrativos, la gestión de proveedores, contratistas, beneficiarios y agentes públicos.

En virtud de ello, y considerando la normativa vigente en materia de protección de datos personales, resulta esencial establecer un conjunto de principios y buenas prácticas específicas que orienten la labor de las distintas áreas del Tribunal, garantizando el pleno respeto a la intimidad, la dignidad y los derechos de las personas.

El presente documento se fundamenta en la Ley Nacional N.º 25.326 de Protección de Datos Personales, las disposiciones de la Agencia de Acceso a la Información Pública como autoridad de aplicación, y en los estándares internacionales en la materia.

1. Marco normativo aplicable.

La Ley N.º 25.326 tiene como finalidad la protección integral de los datos personales contenidos en archivos, registros, bancos de datos o cualquier otro medio técnico de tratamiento, tanto públicos como privados, con el objeto de resguardar el derecho al honor, la intimidad y el acceso a la información de las personas.

En el ámbito del Tribunal de Cuentas, la aplicación de esta ley cobra especial relevancia, dado que el organismo:

- Recibe y procesa información personal en expedientes administrativos sujetos a control.
- Administra registros de proveedores, contratistas y beneficiarios de fondos públicos.
- Accede a nóminas de personal, declaraciones juradas y otros documentos de carácter sensible.

En este contexto, el cumplimiento de la normativa vigente no solo constituye una obligación legal, sino que también fortalece la confianza ciudadana en el accionar del organismo de control.

2. Principios rectores.

El tratamiento de datos personales en el Tribunal de Cuentas debe regirse por los siguientes principios:

- **Licitud y Finalidad:** los datos deberán recolectarse de manera legal y con conocimiento del titular. Solo pueden ser utilizados para fines propios de las funciones de control, fiscalización y auditoría, evitando todo uso ajeno a dichos propósitos.
- **Pertinencia y Proporcionalidad:** únicamente se recabarán los datos estrictamente necesarios, adecuados y no excesivos en relación con el objeto del procedimiento de control.

- **Seguridad y confidencialidad:** se garantizará la protección contra adulteración, pérdida, acceso no autorizado o tratamiento indebido. El personal del Tribunal tiene la obligación de custodiar la información a la que accede, incluso después de finalizada su relación de empleo.
- **Transparencia**: los titulares de los datos tienen derecho a ser informados de la existencia de bases de datos en el Tribunal, así como de las finalidades de su tratamiento.
- **No discriminación**: está prohibido el tratamiento de datos sensibles que pueda implicar distinciones arbitrarias o discriminatorias.
- **Exactitud y actualización:** deberán mantenerse completos y actualizados.

3. Datos personales y categorías especiales.

Los datos personales son toda información que permite identificar directa o indirectamente a una persona. En el ámbito del Tribunal de Cuentas, estos datos pueden comprender entre otros:

- Nombre, apellido y documento de identidad.
- Domicilio, correo electrónico y datos de contacto.
- Información patrimonial, ingresos y declaraciones juradas.
- Registros laborales de agentes públicos.
- Imágenes captadas por sistemas de videovigilancia.

Asimismo, se consideran **categorías especiales de datos**, con un nivel superior de protección:

- Origen racial o étnico.
- Opiniones políticas, convicciones religiosas o filosóficas.
- Orientación sexual.
- Afiliación sindical.
- Datos biométricos, genéticos o de salud.

El Tribunal solo podrá tratar este tipo de datos en los supuestos legalmente habilitados, asegurando la protección contra usos indebidos o discriminatorios.

4. Responsables y encargados del tratamiento.

- **Responsable del tratamiento**: el Tribunal de Cuentas y en el marco de sus atribuciones legales, determina los fines y medios del tratamiento de los datos.
- **Encargados del tratamiento**: las diferentes áreas que, bajo instrucciones del Tribunal, acceden y procesan los datos personales.

Cada área deberá adoptar medidas organizativas y técnicas para evitar la adulteración, pérdida, acceso no autorizado o uso indebido de los datos bajo su gestión.

5. Condiciones de tratamiento.

El Tribunal de Cuentas podrá tratar datos personales sin consentimiento del titular cuando:

- Sea necesario para el cumplimiento de sus competencias legales de fiscalización.
- Se trate de datos obtenidos en el marco de expedientes administrativos sujetos a control.
- Exista una obligación legal de conservación o utilización.
- Se actúe en el marco de un interés público esencial vinculado a la rendición de cuentas.

No obstante, en todos los casos el tratamiento deberá ser razonable, limitado y compatible con los fines institucionales.

6. Derechos de los titulares de datos

Toda persona cuyos datos se encuentren en registros del Tribunal de Cuentas posee los siguientes derechos:

- **Acceso**: conocer qué información obra en el organismo y con qué finalidad.
- **Rectificación y actualización**: corregir datos inexactos o incompletos.
- **Supresión**: solicitar la eliminación de sus datos cuando no exista obligación legal de conservación.
- **Portabilidad**: requerir copia en formato accesible cuando corresponda.
- **Revocación del consentimiento**: en los casos en que el tratamiento se funde en la voluntad del titular.

El ejercicio de estos derechos deberá canalizarse mediante los procedimientos que disponga el Tribunal, garantizando celeridad, transparencia y debido proceso.

7. Casos específicos de tratamiento

- **Menores de edad**: se respetará el principio de autonomía progresiva, recabando el consentimiento de los representantes legales cuando corresponda.
- **Videovigilancia**: las imágenes recolectadas en sistemas de seguridad del Tribunal constituyen datos personales y deberán estar registradas como base de datos ante la autoridad de control.
- **Procesos automatizados**: el Tribunal no podrá adoptar decisiones que se funden exclusivamente en el tratamiento automatizado de datos personales, salvo supuestos legalmente autorizados.

8. Gestión de incidentes y violaciones de seguridad

Si se produjera una violación de datos personales bajo responsabilidad del Tribunal, se deberá:

1. Notificar inmediatamente a la autoridad de aplicación (AAIP).
2. Informar a los titulares afectados cuando el incidente implique un riesgo significativo para sus derechos.
3. Implementar medidas correctivas para reducir el impacto y evitar su reiteración.

9. Evaluación de impacto

Previo a implementar sistemas de auditoría digital, gestión documental electrónica u otros proyectos tecnológicos que impliquen tratamiento intensivo de datos personales, el Tribunal deberá realizar una Evaluación de Impacto en la Protección de Datos (EIPD).

Esta herramienta permitirá identificar riesgos, establecer medidas de mitigación y garantizar la incorporación del principio de "privacidad por diseño y por defecto" desde etapas tempranas.

10. Registro de bases de datos

Los archivos y bases de datos que gestione el Tribunal deberán inscribirse en el Registro Nacional de Bases de Datos Personales de la AAIP.

Cada base deberá contar con con los siguientes datos como mínimo: finalidad, responsables, categoría de datos, medidas de seguridad, cesiones previstas, tiempo de conservación y procedimiento para el ejercicio de derechos.

11. Confidencialidad

Todo agente, funcionario o contratista que acceda a datos personales deberá firmar el Acta de Confidencialidad (Anexo I). La obligación de confidencialidad se mantiene aún después de finalizada la relación laboral o contractual.

12. Infracciones y sanciones

El incumplimiento de las normas de protección de datos personales puede generar sanciones administrativas, civiles y/o penales previstas por la Ley N° 25.326, sin perjuicio de las responsabilidades disciplinarias que correspondan en el ámbito del Tribunal de Cuentas.

El principio de responsabilidad proactiva obliga al Tribunal a adoptar medidas preventivas y demostrar su cumplimiento en todo momento.

Conclusión

La adopción de buenas prácticas en materia de protección de datos personales en el Tribunal de Cuentas de La Pampa no solo responde a una exigencia normativa, sino que constituye una condición indispensable para fortalecer la confianza ciudadana, la transparencia institucional y la legitimidad del control público.

El respeto por los derechos de las personas y la protección adecuada de su información refuerzan el compromiso del Tribunal con una gestión responsable, moderna y ajustada a los más altos estándares de integridad y legalidad.