



**DIRECCIÓN DE TECNOLOGÍAS DE LA  
INFORMACIÓN Y LAS COMUNICACIONES**

**POLÍTICA DE SEGURIDAD DE LA  
INFORMACIÓN**

<VERSIÓN 1>

## Tabla de contenido

Resumen: .....	3
Términos y Definiciones: .....	3
Políticas y Normativas de Seguridad: .....	4
Introducción: .....	4
Objeto: .....	5
Alcance de la política de Seguridad de la Información: .....	6
Principios básicos: .....	6
Revisión y actualización: .....	8
Lineamientos .....	8
Organización de la Seguridad de la Información: .....	8
Seguridad Informática de los Recursos Humanos: .....	9
Gestión de Activos: .....	10
Autenticación, autorización y control de Acceso: .....	11
Uso de herramientas criptográficas: .....	13
Seguridad física y ambiental: .....	13
Seguridad operativa: .....	14
Seguridad de las comunicaciones: .....	15
Adquisición de sistemas, desarrollo y mantenimiento de sistemas de información: .....	15
Relación con proveedores: .....	16
Gestión de incidentes de seguridad: .....	17
Aspectos de seguridad para la continuidad de la gestión: .....	17
Cumplimiento: .....	17

	<b>DIRECCIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES</b>	VERSIÓN: 1  VIGENCIA: 11/10/2024
<b>POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN</b>		

## Resumen:

EL TRIBUNAL DE TASACIONES DE LA NACIÓN en cumplimiento con la Decisión Administrativa N° 641/2021 de la Jefatura de Gabinete de Ministros, establece la necesidad de contar con una Política de Seguridad de la Información, que defina directivas orientadas a resguardar la confidencialidad, integridad y disponibilidad de la información, protección de los recursos tecnológicos y activos de la información, y la continuidad de las operaciones del organismo, de conformidad con la normativa vigente.

## Términos y Definiciones:

Seguridad de la información:

- 1) Se entiende como seguridad de la información la preservación de las siguientes características:
  - I. **Confidencialidad:** Garantiza que la información sea accesible sólo a aquellas personas autorizadas a tener acceso a ésta.
  - II. **Integridad:** Salvaguarda la exactitud y totalidad de la información y los métodos de procesamiento.
  - III. **Disponibilidad:** Garantiza que las personas usuarias autorizadas tengan acceso a la información y a los recursos relacionados con ésta, toda vez que lo requieran.

Adicionalmente, deben considerarse los conceptos de:

- **Información:** Se refiere a toda comunicación o representación de conocimiento como datos, en cualquier forma, con inclusión de formas textuales, numéricas, gráficas, cartográficas, narrativas o audiovisuales, y en cualquier medio, ya sea magnético, en papel, en pantallas de computadoras, audiovisual u otro.
- **Sistema de Información:** Se refiere a un conjunto independiente de recursos de información organizados para la recopilación, clasificación, procesamiento, mantenimiento, transmisión y difusión de información según determinados procedimientos, tanto automatizados como manuales.
- **Tecnología de la Información:** Se refiere al hardware y software operados por el Organismo, o por un tercero, que procese información en su nombre, para llevar a cabo una función propia del Organismo, independientemente de la tecnología utilizada, ya se trate de computación de datos, telecomunicaciones u otro tipo.

	<b>DIRECCIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES</b>	VERSIÓN: 1  VIGENCIA: 11/10/2024
<b>POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN</b>		

- **No repudio:** Refiere a evitar que una entidad que haya enviado o recibido información alegue ante terceros que no la envió o recibió.
- **Amenaza:** Es toda acción potencial que puede ocasionar daño o pérdida a un sistema o a la organización.
- **Vulnerabilidad:** Una debilidad de un activo o grupo de activos que puede ser aprovechada por una amenaza.
- **Geolocalización:** Localización geográfica de un lugar, o bien de una persona o cosa en un momento determinado.

## Políticas y Normativas de Seguridad:

Se establece la “Política de Seguridad de Información” (PSI), aprobada por la máxima autoridad del TRIBUNAL DE TASACIONES DE LA NACIÓN, publicada y comunicada a todo el personal.

Se establecen, además, políticas, y normas internas complementarias que deberán ser cumplimentadas por todo el personal, de forma obligatoria. Asimismo, se deberá observar, y en su caso, acatar, periódicamente, la revisión de todas las políticas y las normativas que en el futuro se dicten.

En este orden de ideas, en particular se establece como norma interna el “Formulario de Aceptación de Términos de uso de Recursos Informáticos” (F.A.T.U.R.I), el cual establece normas de conducta razonables, que deben observadas y cumplimentadas por el personal del TRIBUNAL DE TASACIONES DE LA NACIÓN, al utilizar los recursos tecnológicos puestos a su disposición para el desempeño de sus tareas.

## Introducción:

La información es un activo que, como otros bienes y servicios requeridos para el cumplimiento de los objetivos del TRIBUNAL DE TASACIONES DE LA NACIÓN, resulta esencial para el desarrollo de las actividades de competencia. En consecuencia, necesita ser protegida adecuadamente, frente a riesgos internos o externos que pudieran afectarla.

Dicha información puede presentarse en diversos formatos (impresa o escrita en papel, almacenada electrónicamente, transmitida por correo o utilizando medios electrónicos o como contenido multimedial, entre otros). Por lo tanto, y sin perjuicio del formato en que se encuentre y del soporte que se utilice, debe estar apropiadamente protegida desde su creación, durante todo su ciclo de vida y hasta su eventual destrucción, desuso o archivo definitivo.

	<b>DIRECCIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES</b>	VERSIÓN: 1  VIGENCIA: 11/10/2024
<b>POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN</b>		

La seguridad de la información es la protección de la información de un rango amplio de amenazas, con el objeto de minimizar los riesgos a los que se encuentra expuesta y asegurar la continuidad de la operación normal del TRIBUNAL DE TASACIONES DE LA NACIÓN. Tiene por objetivo la preservación de la confidencialidad, integridad y disponibilidad de la información.

Dicho estado de protección adecuada se logra implementando un conjunto de mecanismos de seguridad y controles que incluyen entre otros, procesos, políticas, procedimientos, estructuras organizacionales, software y hardware. Se necesita establecer, implementar, monitorear, revisar y mejorar estos mecanismos para fortalecer el cumplimiento de los objetivos de seguridad específicos. Esto se debe realizar en forma coordinada con otros procesos de gestión del organismo.

Del mismo modo, los procesos, sistemas y redes de apoyo son también activos importantes. Definir, lograr, mantener y mejorar la seguridad de la información es esencial para preservarlos, mantener la eficacia en la operación, cumplir con el marco legal y las normas internas, y preservar la imagen institucional del TRIBUNAL DE TASACIONES DE LA NACIÓN y del Estado Nacional en su conjunto.

Los organismos, como cualquier organización, enfrentan amenazas de seguridad en sus sistemas y redes de información, cada vez más frecuentes y sofisticadas. La seguridad de la información es importante para el desarrollo de actividades del sector público y para proteger las infraestructuras críticas de información que proveen servicios esenciales a la sociedad. En este aspecto, el Estado puede proveer los servicios en forma directa o ejercer un rol regulatorio, que lo obliga a velar por la seguridad de los datos y servicios tratados.

## **Objeto:**

La presente Política de Seguridad de la Información (en adelante, PSI) establece las directrices y líneas de actuación en materia de seguridad de la información, que establecen el modo en que el TRIBUNAL DE TASACIONES DE LA NACIÓN debe gestionar y proteger los datos a los que da tratamiento, los recursos tecnológicos que utiliza y los servicios que brinda. Detalla también lineamientos respecto a la comunicación de esta Política a todo el personal del TRIBUNAL DE TASACIONES DE LA NACIÓN, bajo cualquier modalidad de contratación, y demás personas involucradas internas y externas, así como respecto a su implementación en todas las dependencias de la jurisdicción.

El objetivo principal de esta PSI es definir el propósito, la dirección, los principios, las reglas básicas y los mecanismos de comunicación para la protección de la información del TRIBUNAL DE TASACIONES DE LA NACIÓN, así como de los recursos utilizados en su tratamiento.

	<b>DIRECCIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES</b>	VERSIÓN: 1  VIGENCIA: 11/10/2024
<b>POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN</b>		

El presente documento se dicta en cumplimiento con las disposiciones legales vigentes, leyes, decretos, resoluciones y disposiciones que sean aplicables a los datos, los sistemas informáticos y el ambiente tecnológico que utiliza, así como también con las normas internas de la propia entidad, sus políticas, procedimientos, cláusulas contractuales y acuerdos con agentes de la jurisdicción y terceros, etc.

Una adecuada gestión de la seguridad de la información permite proteger los recursos de información y la tecnología utilizada para su procesamiento, frente a amenazas internas o externas, deliberadas o accidentales, con el fin de asegurar la confidencialidad, integridad, disponibilidad de la información, así como también cumplimentar/dar cumplimiento con las normas aplicables.

### **Alcance de la política de Seguridad de la Información:**

Esta PSI se aplica en todo el ámbito del TRIBUNAL DE TASACIONES DE LA NACIÓN, a sus recursos y a la totalidad de los procesos, ya sean internos o externos, vinculados a la entidad a través de contratos o acuerdos con terceros.

Debe ser comunicada fehacientemente y cumplida por todo el personal del TRIBUNAL DE TASACIONES DE LA NACIÓN, independientemente de la modalidad de contratación, vinculación con el organismo, y las fuentes de financiamiento correspondientes.

Su alcance se circunscribe a todo el personal que desempeñe funciones directivas, administrativas o técnicas, cualquiera sea su vínculo/relación contractual, su nivel jerárquico, su situación de revista y las tareas que desempeñe.

Asimismo, debe ser conocida y cumplida por todas aquellas personas, internas o externas, vinculadas a la entidad a través de contratos, convenios, acuerdos o algún otro instrumento válido para establecer la relación con terceros, en la medida en que les sea aplicable y en las secciones que le corresponden.

### **Principios básicos:**

Los principios básicos de la seguridad de la información son la confidencialidad, la integridad y la disponibilidad de la información que el TRIBUNAL DE TASACIONES DE LA NACIÓN utilice y/o tenga acceso, así como también los activos de información utilizados para su gestión.

	<b>DIRECCIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES</b>	VERSIÓN: 1  VIGENCIA: 11/10/2024
<b>POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN</b>		

Los contenidos de este documento están alineados y se complementan con el resto de las políticas y normativas internas del TRIBUNAL DE TASACIONES DE LA NACIÓN, que entiende la importancia de gestionar eficazmente la seguridad de la información. En consecuencia, declara su compromiso y total apoyo a la gestión de la seguridad de la información como parte integrante de la gestión del resto de los procesos establecidos en su ámbito. Por otra parte, promueve el uso responsable de la información y de los recursos utilizados.

Asimismo, las autoridades del TRIBUNAL DE TASACIONES DE LA NACIÓN se comprometen a liderar la mejora continua de los procesos de gestión de seguridad de la información, asegurando su eficacia y eficiencia.

Las personas alcanzadas por esta PSI reciben una concientización periódica y pertinente a su función, respecto del compromiso que asumen para cumplir con esta PSI. Para ello, se asignan los recursos necesarios. En el mismo sentido, el TRIBUNAL DE TASACIONES DE LA NACIÓN se compromete a cumplir con la normativa legal y reglamentaria aplicable a todos los niveles, así como incorporar y cumplir futuras normas que se dicten y requisitos del contexto interno o externo y a aquellos que emanan de la vinculación con terceros involucrados. En idéntico sentido, el TRIBUNAL DE TASACIONES DE LA NACIÓN se compromete a notificar a la Dirección Nacional de Ciberseguridad la ocurrencia de incidentes de seguridad dentro de las CUARENTA Y OCHO (48) horas de su detección.

El incumplimiento de esta política tendrá como resultado la aplicación de sanciones disciplinarias, conforme a la magnitud y característica del aspecto no cumplido, de acuerdo con la normativa aplicable al organismo. Al respecto y de acuerdo a la mencionada normativa, se establece como falta el incumplimiento de los lineamientos y disposiciones de esta PSI, por parte del personal del TRIBUNAL DE TASACIONES DE LA NACIÓN, en función de lo dispuesto por el régimen sancionatorio establecido en la Ley Marco de Regulación de Empleo Público Nacional N° 25.164, su Decreto Reglamentario N° 1.421/02 y sus normas modificatorias y complementarias. Para ello, se establece una graduación en las responsabilidades y sanciones administrativas que se aplicarán de acuerdo con la gravedad de la infracción cometida, sin perjuicio de las acciones legales que pudieran corresponder. El TRIBUNAL DE TASACIONES DE LA NACIÓN establece sus requisitos de seguridad de la información en base a la evaluación y posterior gestión de riesgos de seguridad sobre sus activos de la información.

	<b>DIRECCIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES</b>	VERSIÓN: 1  VIGENCIA: 11/10/2024
<b>POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN</b>		

## Revisión y actualización:

EL TRIBUNAL DE TASACIONES DE LA NACIÓN se compromete a revisar esta PSI anualmente, adaptándola a nuevas exigencias organizativas o del entorno, así como a comunicarla a su planta de personal y a las terceras partes involucradas. También dispondrá las medidas necesarias para que esté a disposición de las personas alcanzadas en todo momento.

Adicionalmente, procederá a su revisión y eventual modificación, cada vez que se produzca un cambio significativo en la plataforma tecnológica, una modificación de la normativa vigente aplicable, un cambio en los objetivos estratégicos del TRIBUNAL DE TASACIONES DE LA NACIÓN o cualquier otro evento que lo amerite.

La persona responsable de las tareas relativas a la seguridad de los sistemas de información llevará adelante las revisiones sean periódicas o ad-hoc, dejándose constancia de ellas en el presente documento. Dicha persona será responsable también de la aprobación de las nuevas versiones, que serán comunicadas en tiempo y forma a todos los alcanzados para su cumplimiento.

## Lineamientos

### **Organización de la Seguridad de la Información:**

EL TRIBUNAL DE TASACIONES DE LA NACIÓN asigna a la persona responsable de las tareas relativas a la seguridad de los sistemas de información la coordinación de todas las actividades tendientes a la implementación de la presente PSI. Dicha unidad organizativa velará por una adecuada segregación de funciones, por un abordaje de la seguridad de la información en todos los proyectos y programas del TRIBUNAL DE TASACIONES DE LA NACIÓN y por el establecimiento de adecuados procedimientos de seguridad, en base a un plan de tratamiento de riesgos.

Asimismo, se contempla la necesidad de disponer de fuentes con conocimiento experimentadas para el asesoramiento, cooperación y colaboración en materia de seguridad de la información, con lo cual se apoya el contacto con otros organismos públicos y entidades privadas para el intercambio de experiencias en materias de seguridad, con el objeto de actualizar e intercambiar conocimientos relativos a seguridad y promover la capacitación continua.

Las autoridades del TRIBUNAL DE TASACIONES DE LA NACIÓN se comprometen a impulsar las iniciativas que el área competente proponga con el objetivo de preservar la confidencialidad, integridad y disponibilidad de la información que gestiona. Asimismo, requerirá a

 <b>Tribunal de Tasaciones de la Nación</b>	<b>DIRECCIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES</b>	<b>VERSIÓN: 1</b>  <b>VIGENCIA: 11/10/2024</b>
<b>POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN</b>		

las áreas competentes la inclusión en contratos, Términos de Referencia o instrumentos similares, cláusulas que contemplen el cumplimiento de la presente PSI.

### **Seguridad Informática de los Recursos Humanos:**

El personal es considerado un recurso central para la protección de la información, motivo por lo cual es adecuadamente entrenado en caso del personal técnico y concientizado periódicamente a través de programas específicos, para quienes no realizan actividades de ese tenor.

Todo el personal del TRIBUNAL DE TASACIONES DE LA NACIÓN y, cuando sea pertinente, las personas usuarias externas y terceros que desempeñen funciones en el Organismo, deben recibir una adecuada capacitación y actualización periódica en materia de la política, normas y procedimientos del TRIBUNAL DE TASACIONES DE LA NACIÓN. Ello comprende los requerimientos de seguridad y las responsabilidades legales, así como la capacitación referida al uso correcto de las instalaciones de procesamiento de información y el uso correcto de los recursos en general, como por ejemplo un puesto de trabajo despejado para el cumplimiento de los estándares mínimos de seguridad TI o el manejo de información cualquiera sea el soporte y formato en el que se encuentren

A tal fin, se establecen las medidas necesarias en los procesos de selección de personal, durante la vinculación laboral y al momento de la desvinculación, pudiendo inclusive excederlo.

Durante el proceso de selección de personal se deberá informar al postulante acerca de las responsabilidades de los puestos de trabajo las funciones y responsabilidades en materia de seguridad de la información.

Asimismo, se deberán revisar los antecedentes referidos en el currículum, referencias, títulos académicos, etc., de los postulantes al empleo, en concordancia con el puesto y activos a los cuales tendrá acceso.

Las direcciones en todos los niveles impulsarán que se aplique la política de seguridad de la información en concordancia con las pautas y procedimientos establecidos, por lo que deberán también informar de su existencia y las expectativas de cumplimiento en el desempeño de sus funciones.

En el momento del cese del empleo o cambio de puesto de trabajo se deberán definir procedimientos y asignar responsabilidades para controlar que los procesos de cambio de función y desvinculación laboral de los empleados, contratistas o terceras personas no afecte el normal desempeño de las actividades del Organismo.

	<b>DIRECCIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES</b>	VERSIÓN: 1  VIGENCIA: 11/10/2024
<b>POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN</b>		

Todas las personal o terceras personas que tengan conocimiento relevante de ciertas operaciones y dicho conocimiento sea desconocido por el personal restante del área donde prestan servicios, deberán documentar dicha información y transferirla al Organismo antes de proceder a su desvinculación.

En todo momento se protegen los derechos individuales de las personas que trabajan en el TRIBUNAL DE TASACIONES DE LA NACIÓN, especialmente aquellos relacionados con la privacidad.

Se establece la obligatoriedad de la suscripción de compromisos de confidencialidad para todo el personal del TRIBUNAL DE TASACIONES DE LA NACIÓN mediante la firma del Formulario de Aceptación de Términos de Uso de Recursos Informáticos (F.A.T.U.R.I.) en función de las responsabilidades que correspondan y a las funciones que se desarrollen.

La obligación de confidencialidad asumida seguirá vigente luego de rescindirse o resolverse la relación de empleo o de servicio que se vincula con el TRIBUNAL DE TASACIONES DE LA NACIÓN, haciéndose responsable civil y/o penalmente por la difusión, transmisión y/o transferencia no autorizada de datos o informes no publicados.

Los responsables del área correspondiente deberán informar a todo su personal la existencia de la Política de Seguridad de la Información, y velarán por el cumplimiento de las normativas vigentes e informarán que el incumplimiento podrá ser pasible de un proceso administrativo disciplinario y/o judicial.

Los permisos de acceso son otorgados en función de cada perfil de trabajo y se mantienen actualizados.

### **Gestión de Activos:**

La gestión y protección efectiva de los activos en función de su clasificación por criticidad es una prioridad para el TRIBUNAL DE TASACIONES DE LA NACIÓN. Entre los activos se incluyen tanto el hardware como el software, los dispositivos de comunicación, los elementos de apoyo, la información y los datos en sí mismos, cualquiera sea el soporte y formato en el que se encuentren. Para la clasificación se tienen en cuenta la confidencialidad, integridad y disponibilidad de los datos, así como las funciones que soporta el activo y la normativa aplicable.

Se llevan inventarios actualizados designándose responsables de los mismos a los propietarios de los activos, estos son asignados en forma temporaria con el único objetivo de cumplimentar los proyectos y tareas asignadas con fines laborales, conforme criterios de razonabilidad, responsabilidad, integridad y confidencialidad y que, por lo tanto, se monitorearán las actividades a tales fines.

	<b>DIRECCIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES</b>	VERSIÓN: 1  VIGENCIA: 11/10/2024
<b>POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN</b>		

Se establece que el personal no debe realizar copias de los datos e información confidencial en su poder sin previa autorización escrita por parte del TRIBUNAL DE TASACIONES DE LA NACIÓN. Por otro lado, se exige a todo el personal que se desvincule del TRIBUNAL DE TASACIONES DE LA NACIÓN la devolución de los activos de información en su poder, los cuales deberán ser conservados en buen estado, restituidos en tiempo y forma al concluir la relación de empleo o de servicio (cualquiera fuera el modo y forma de contratación) y/o cuando lo solicite la DIRECCIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES y/o la autoridad competente.

En el mismo sentido, al momento de desecharlos, se procederá a una destrucción segura de cualquier medio que pueda contener información crítica o datos personales, para lo cual, se cuenta con procedimientos adecuados.

El TRIBUNAL DE TASACIONES DE LA NACIÓN, como titular de los derechos o licencias sobre el software y hardware empleado, se obliga a controlar y auditar su uso conforme a criterios de razonabilidad y responsabilidad, atendiendo a los principios de integridad, disponibilidad y confidencialidad de la información, pero a la vez resguardando la seguridad de la información y el BUEN USO de las herramientas provistas por esta cartera gubernamental.

En caso de pérdida, robo o hurto del equipamiento informático-tecnológico se deberá informar inmediatamente tal circunstancia a la DIRECCIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES para tomar las medidas tendientes a la protección de la información involucrada.

En materia de Almacenamiento de Información Crítica, resulta obligatoria la utilización del servicio de nube privada del TRIBUNAL DE TASACIONES DE LA NACIÓN como único sistema de resguardo de información, con fines meramente laborales, y por tanto se debe utilizar conforme a criterios de razonabilidad, privacidad, confidencialidad de la información allí contenida y BUEN USO de la herramienta. En caso de utilizar la modalidad de acceso remoto, se encuentra prohibida la utilización de esta funcionalidad desde un sitio público con equipos de uso compartido, como ser un “cibercafé” o “locutorio”.

### **Autenticación, autorización y control de Acceso:**

El TRIBUNAL DE TASACIONES DE LA NACIÓN adopta los mecanismos necesarios para que solo el personal autorizado acceda a los activos de información, bajo la premisa básica de que “Todo está prohibido a menos que se permita expresamente” para aquellos activos considerados críticos. El acceso a la información se establecerá en base a la “necesidad de saber”, es decir que quienes accedan deben tener un motivo válido para hacerlo en razón de su rol y/o funciones y

 <b>Tribunal de Tasaciones de la Nación</b>	<b>DIRECCIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES</b>	<b>VERSIÓN: 1</b>  <b>VIGENCIA: 11/10/2024</b>
<b>POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN</b>		

usando una política de “Mínimo Privilegio”. Estos privilegios se otorgan en forma expresa, son autorizados por los niveles competentes y se gestionan adecuadamente las altas y bajas de las cuentas y permisos de acceso, con revisiones periódicas. Se requiere a todas las personas usuarias el uso responsable de los dispositivos y datos de autenticación otorgados por el TRIBUNAL DE TASACIONES DE LA NACIÓN para el cumplimiento de sus funciones, que no los compartan y que los mantengan siempre seguros, tanto dentro como fuera del TRIBUNAL DE TASACIONES DE LA NACIÓN.

Las contraseñas de las cuentas de acceso a los diferentes sistemas informáticos que son asignadas por la Dirección General de Tecnologías de la Información y las Comunicaciones son personales, secretas, intransferibles y modificables sólo por la PERSONA USUARIA TITULAR. Ergo, toda actividad registrada con dichas cuentas se entenderá como efectuada por la misma persona, salvo prueba en contrario. Por lo tanto, el uso del sistema, dominio o recurso informático-tecnológico que se encuentre protegido mediante una contraseña, está restringido a quien se le haya otorgado tal permiso, junto con la clave para acceder a dicho servicio y/o recurso.

No deberán utilizarse cuentas de personas usuarias con derechos de acceso privilegiados para realizar actividades regulares, sino que sólo serán utilizadas ante la necesidad de realizar tareas específicas que lo requieran. Solo deberán ser utilizadas ante necesidades específicas para realizar tareas de contingencia, recupero o reconfiguración que lo requieran.

Las contraseñas no pueden ser distribuidas a otras personas y la PERSONA USUARIA TITULAR es responsable de todos los daños que sufran los sistemas como resultado de la distribución de las mismas.

En caso de que más de una persona necesite la contraseña única, perteneciente a la PERSONA USUARIA TITULAR, ésta última deberá solicitar permiso por escrito fundamentándolo, entendiendo que la Dirección General de Tecnologías de la Información y las Comunicaciones no tendrá obligación alguna de aprobar dicha solicitud.

Las contraseñas otorgadas inicialmente deben ser de carácter temporal. Los sistemas deberán pedirán que la PERSONA USUARIA TITULAR las cambie en el primer inicio de sesión.

Las contraseñas deberán caducar periódicamente y los sistemas avisarán con CINCO (5) días de anticipación solicitando el cambio.

Las cuentas se bloquearán al QUINTO (5°) intento fallido y, para su reactivación, será necesario comunicarse con la DIRECCIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES.

	<b>DIRECCIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES</b>	VERSIÓN: 1  VIGENCIA: 11/10/2024
<b>POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN</b>		

Se deberá evitar almacenar contraseñas en papel, archivos de texto, planillas de cálculo, medio extraíble o cualquier aplicación cuya función no sea expresamente el almacenamiento seguro de contraseñas.

Las contraseñas deberán cumplir con los siguientes criterios:

- No debe coincidir con las últimas TRES (3) contraseñas utilizadas.
- Debe contener al menos OCHO (8) caracteres.
- No debe contener su nombre de cuenta o nombre completo.
- Debe contener al menos una letra mayúscula (A - Z).
- Debe contener al menos un número (0 a 9).
- Debe contener al menos un carácter especial (#,%,?, etc.).

De no recordar las contraseñas, se deberá seguir el proceso de blanqueo de las mismas, informando a la DIRECCIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES.

### **Uso de herramientas criptográficas:**

Se utilizan sistemas y técnicas criptográficas para la protección de la información del TRIBUNAL DE TASACIONES DE LA NACIÓN, con el fin de preservar su confidencialidad, integridad, autenticidad y no repudio, tanto para su almacenamiento como para su transmisión. Para ello, se requiere el cifrado de toda la información crítica, especialmente cuando ésta sea transmita fuera del TRIBUNAL DE TASACIONES DE LA NACIÓN, contenga datos personales, o se encuentre contenida en medios de almacenamiento que se trasladen fuera de la institución. Asimismo, se protegen las claves criptográficas durante todo su ciclo de vida y se utilizan certificados digitales válidos en los sitios web institucionales.

En materia de Firma Digital existe una normativa aplicable, dada por la Ley N° 25.506, sus complementarias, modificatorias y concordantes.

### **Seguridad física y ambiental:**

El TRIBUNAL DE TASACIONES DE LA NACIÓN protege sus instalaciones y activos físicos, incluyendo sus puestos de trabajo, en función de la criticidad de la información que éstos gestionan, mediante el establecimiento de perímetros de seguridad, áreas protegidas y controles ambientales, en la medida en que se considere necesario.

Además, se monitorean los accesos físicos para permitir solo ingresos y egresos debidamente autorizados y se mantiene un registro actualizado de los activos físicos que procesan información. Se implementan y hacen cumplir medidas de seguridad para los activos físicos que

	<b>DIRECCIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES</b>	VERSIÓN: 1  VIGENCIA: 11/10/2024
<b>POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN</b>		

deben llevarse fuera del TRIBUNAL DE TASACIONES DE LA NACIÓN, manteniéndose el registro correspondiente.

El uso de equipamiento destinado al procesamiento de información, fuera del ámbito del TRIBUNAL DE TASACIONES DE LA NACIÓN debe ser autorizado. El mismo podrá contener sistemas que permitan la geolocalización del equipamiento. La seguridad provista debe ser equivalente a la suministrada dentro del ámbito del TRIBUNAL DE TASACIONES DE LA NACIÓN para un propósito similar, teniendo en cuenta los riesgos de trabajar fuera de éste.

Se debe realizar el mantenimiento del equipamiento para asegurar su disponibilidad e integridad permanentes, sólo el personal de mantenimiento autorizado puede brindar mantenimiento y llevar a cabo reparaciones en el equipamiento.

Las personas usuarias, al ausentarse momentáneamente de su puesto de trabajo, deberán cerrar la sesión activa o en su defecto, bloquear el equipo informático, para evitar el acceso indebido al mismo en su ausencia.

### **Seguridad operativa:**

Las operaciones del TRIBUNAL DE TASACIONES DE LA NACIÓN se desarrollan en forma segura, en todas las instalaciones de procesamiento de información, asignándose las debidas responsabilidades y desarrollando procedimientos acordes. Se adoptan medidas para minimizar los riesgos de acceso y cambios no autorizados o pérdida de información y para proteger las instalaciones y plataformas tecnológicas contra infecciones de código malicioso. Se monitorea continuamente la seguridad de los sistemas e infraestructuras que soportan las operaciones críticas del organismo, así como también los requerimientos de capacidad desde la perspectiva de la seguridad de la información. Las vulnerabilidades son gestionadas de manera apropiada y se controla la actividad de administradores y operadores.

Deben separarse los ambientes de desarrollo, prueba y operaciones de los sistemas del TRIBUNAL DE TASACIONES DE LA NACIÓN, estableciendo procedimientos que aseguren la calidad de los procesos que se implementen en el ámbito operativo, a fin de minimizar los riesgos de incidentes producidos por la manipulación de información operativa.

Se establecen procedimientos de rutina para implementar la política de respaldo acordada y la estrategia para tomar copias de respaldo de los datos y practicar su restauración oportuna.

Se mantiene un control estricto sobre el software y su integridad en entornos productivos. En idéntico sentido, se llevan registros de los eventos de seguridad y se revisan periódicamente con el fin de detectar posibles incidentes, al igual que se gestionan de manera apropiada los reportes de vulnerabilidades y recomendaciones de actualización.

	<b>DIRECCIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES</b>	VERSIÓN: 1  VIGENCIA: 11/10/2024
<b>POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN</b>		

Se declara la prohibición de toda instalación de software, salvo que sea autorizada por la Dirección General de Tecnologías de la Información y las Comunicaciones, ya que la instalación no controlada de software en sistemas informáticos puede dar pie a la introducción de vulnerabilidades y a la fuga de información, a la falta de integridad u otros incidentes de seguridad de la información o bien a la transgresión de derechos de propiedad intelectual.

### **Seguridad de las comunicaciones:**

EL TRIBUNAL DE TASACIONES DE LA NACIÓN adopta las medidas necesarias para proteger adecuadamente la información que se comunica por sus redes informáticas y para minimizar los riesgos que pudieran afectar la infraestructura de soporte. Toda información que se transfiere fuera del TRIBUNAL DE TASACIONES DE LA NACIÓN, incluyendo la que se transmite a través de los servicios de correo electrónico es protegida de acuerdo a su nivel de criticidad.

Se asignan cuentas de correo institucionales a todo el personal del TRIBUNAL DE TASACIONES DE LA NACIÓN, quienes están obligados a utilizarlas para toda comunicación vinculada a sus funciones. El personal es informado por sus respectivas autoridades sobre los riesgos de incumplir este requerimiento, y se les exige la firma de acuerdos de confidencialidad y no divulgación, en los casos en los que el TRIBUNAL DE TASACIONES DE LA NACIÓN lo considere necesario, haciéndose responsables de la información allí contenida, por lo tanto, se entenderá, salvo prueba en contrario, que los correos electrónicos emitidos desde la casilla de correo electrónico institucional fueron enviados por la persona a la cual le fue asignada la casilla de correo.

Cuando se realicen acuerdos entre organizaciones para el intercambio de información y software, se debe especificar el grado de sensibilidad de la información del TRIBUNAL DE TASACIONES DE LA NACIÓN involucrada y las consideraciones de seguridad sobre ésta.

### **Adquisición de sistemas, desarrollo y mantenimiento de sistemas de información:**

El software es una creación u obra intelectual y como tal se encuentra tutelada por la Ley N° 11.723, sus complementarias, modificatorias y concordantes. Por lo tanto, las modificaciones, variaciones, nuevas aplicaciones o desarrollos de software realizados en el marco de las tareas encomendadas y en cuanto a los mismos pudieran ser conceptuados como invenciones, descubrimientos, o procedimientos registrables, son derivados de los procedimientos y actividades del TRIBUNAL DE TASACIONES DE LA NACIÓN y en consecuencia le pertenecen en exclusividad. De este modo, toda reproducción de software que no cuente con la expresa

	<b>DIRECCIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES</b>	VERSIÓN: 1  VIGENCIA: 11/10/2024
<b>POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN</b>		

autorización de su autor, significa una infracción a sus derechos y constituye un delito severamente sancionado.

El TRIBUNAL DE TASACIONES DE LA NACIÓN rechaza todo tipo de uso no autorizado de software.

El TRIBUNAL DE TASACIONES DE LA NACIÓN adopta las medidas de seguridad necesarias para proteger por defecto y desde el diseño todas las aplicaciones que se desarrollen internamente, utilizando una metodología de desarrollo seguro, capacitando a sus desarrolladores, e incorporando requerimientos y evaluaciones de seguridad en el proceso de contratación de aplicaciones a terceros. Esto se aplica especialmente a aquellas que se utilicen para brindar servicios o realizar trámites por parte de la ciudadanía e involucren el tratamiento de datos personales. En tal sentido, mediante protocolos, se evita la divulgación, adulteración o duplicación no autorizada de transacciones, evitando así la actividad fraudulenta.

Se deben tomar recaudos para la protección de la integridad de la información publicada electrónicamente, a fin de prevenir la modificación no autorizada que podría dañar la reputación del TRIBUNAL DE TASACIONES DE LA NACIÓN que emite la publicación.

Se deberán realizar evaluaciones de seguridad en búsqueda de vulnerabilidades sobre los nuevos sistemas a implementar, sistemas de información utilizados, incluyendo desarrollos propios y de terceros, como también a las plataformas del sistema operativo sobre los cuales están implementados los mismos, con el objeto de detectar canales encubiertos de transmisión de datos no autorizados o cualquier otra vulnerabilidad que atente contra la seguridad.

### **Relación con proveedores:**

El TRIBUNAL DE TASACIONES DE LA NACIÓN incluye en los pliegos de bases y condiciones particulares cláusulas vinculadas a la seguridad de la información, de cumplimiento efectivo y obligatorio por parte los cocontratantes. Estas disposiciones consideran los aspectos pertinentes a la protección de la información y los servicios que se brinden, desde el inicio del proceso contractual hasta su finalización. Los requisitos a incluir son acordes a la criticidad de la información y los servicios, la evaluación de riesgos y el cumplimiento de todas las normas legales y contractuales aplicables.

La violación de las obligaciones de confidencialidad impuestas en los pliegos de bases y condiciones y/o en cualquier otro instrumento relativo a la confidencialidad que se celebre podrá acarrear responsabilidad civil por daños y perjuicios y/o responsabilidad penal, conforme a lo dispuesto en la Ley N° 25.326, sus complementarias, modificatorias y concordantes.

	<b>DIRECCIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES</b>	VERSIÓN: 1  VIGENCIA: 11/10/2024
<b>POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN</b>		

Se debe llevar a cabo el seguimiento, control y revisión de los servicios de las terceras partes asegurando que se encuentran adheridos a los términos de seguridad de la información y las condiciones definidas en los acuerdos, y que los incidentes de seguridad de la información y los problemas son manejados en forma apropiada.

### **Gestión de incidentes de seguridad:**

EL TRIBUNAL DE TASACIONES DE LA NACIÓN adopta las medidas necesarias para prevenir, detectar, gestionar, resolver y reportar los incidentes de seguridad que puedan afectar sus activos de información. El organismo cuenta con procedimientos de gestión de incidentes de seguridad documentados, aprobados y comunicados, de acuerdo a las áreas funcionales necesarias. Los eventos que podrían constituir un incidente de seguridad y las debilidades en los procesos detectados por el personal son debidamente, identificados, minimizados y comunicados a la DIRECCIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES y/o la autoridad competente, de forma tal que se apliquen las acciones correctivas en el menor tiempo posible.

EL TRIBUNAL DE TASACIONES DE LA NACIÓN recopilará la evidencia necesaria para adoptar medidas administrativas o judiciales posteriores, resguardando la debida cadena de custodia.

### **Aspectos de seguridad para la continuidad de la gestión:**

La administración de la continuidad de las actividades es un proceso crítico que debe involucrar a todos los niveles del TRIBUNAL DE TASACIONES DE LA NACIÓN.

El desarrollo e implementación de planes de contingencia es una herramienta básica para garantizar que las actividades del TRIBUNAL DE TASACIONES DE LA NACIÓN puedan restablecerse dentro de los plazos requeridos.

Se contemplan todos los aspectos de seguridad requeridos en los procedimientos de continuidad de la gestión del TRIBUNAL DE TASACIONES DE LA NACIÓN que se desarrollan, especialmente cuando se trate de información, servicios o sistemas críticos. Se realizan análisis de impacto y se identifican las ventanas de recuperación requeridas en los procesos críticos.

### **Cumplimiento:**

EL TRIBUNAL DE TASACIONES DE LA NACIÓN cumple la normativa legal aplicable y promueve el acatamiento de las políticas y normas de seguridad que se aprueban en su ámbito. En el mismo sentido, atiende y da cumplimiento a las recomendaciones correspondientes a los

 <b>Tribunal de Tasaciones de la Nación</b>	<b>DIRECCIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES</b>	VERSIÓN: 1
<b>POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN</b>		VIGENCIA: 11/10/2024

hallazgos de las auditorías internas y externas que se realicen, adoptando las medidas correctivas que correspondan.



República Argentina - Poder Ejecutivo Nacional  
1983/2023 - 40 AÑOS DE DEMOCRACIA

**Hoja Adicional de Firmas**  
**Informe gráfico**

**Número:**

**Referencia:** Política de Seguridad de la Información del TTN v1

---

El documento fue importado por el sistema GEDO con un total de 18 pagina/s.