8/02/23 8:16hs

CORTE SUPREMA DE JUSTICIA
Secretaría General

Compromiso con la gente

N.S. N°.121.....

Asunción, 7 de febrero de 2023.

Señora
Lic. Rosa Liz Chamorro, Directora General Interina
Dirección General de Tecnología de la Información y las Comunicaciones

El Secretario General Interino de la Corte Suprema de Justicia, Abg. Alex Almada Cáceres, se dirige a Usted, con el objeto de comunicarle que por Resolución N° 9906, de fecha 3 de febrero de 2023, la Corte Suprema de Justicia resolvió:

"…**POR LA QUE SE APRUEBA EL REGLAMENTO DE POLÍTICAS DE SEGURIDAD INFORMÁTICA DEL PODER JUDICIAL.**

VISTA: La Nota presentada por la Directora General Interina de Tecnología de la Información y las Comunicaciones, Lic. Rosa Liz Chamorro Ibarrola; y

C O N SI D E R A N D O:

Que, por la mencionada nota la Directora General Interina de Tecnología de la Información y las Comunicaciones, Lic. Rosa Liz Chamorro Ibarrola, elevó para análisis y aprobación el "Reglamento de Políticas de Seguridad Informática del Poder Judicial – PJ".

El objetivo del presente reglamento es establecer las directrices y pautas acerca del uso de los sistemas informáticos y de comunicaciones del Poder Judicial (PJ), por parte de los usuarios, funcionarios o terceros, protegiendo los activos de información de la institución, así como toda tecnología utilizada para su gestión y procesamiento, contra amenazas internas o externas internacionales o accidentales, de tal manera a preservar sus atributos de confidencialidad integridad y disponibilidad.

El presente reglamento complementa y actualiza los aprobados por Resolución Nº 183 del 14 de marzo de 2005 y Nº 96 del 25 de febrero de 2008, posibilitando a la Dirección General de Tecnologías de la Información y Comunicaciones (DGTIC) proveer un marco normativo general más completo y moderno, a través del cual impulsar la formalización de procedimientos, disposiciones, normativas, mecanismos e instructivos más específicos, que recojan todas las medidas técnicas y organizativas definidas por las propias áreas involucradas en que este resguardo y custodia ocurra efectivamente.

El Art.3º de la Ley 609/95 que organiza la Corte Suprema de Justicia, en su inc. b), le confiere a la Corte Suprema de Justicia la facultad de **"Dictar su propio Reglamento Interno, las Acordadas, y todos los actos que fueren necesarios para mejor organización y eficiencia de la administración de justicia"**. En sesión plenaria del 3 de febrero de 2023, se resolvió aprobar el "Reglamento de Políticas de Seguridad Informática del Poder Judicial – PJ".

LA CORTE SUPREMA DE JUSTICIA
R E S U E L V E:

ART. 1º: **APROBAR** "Reglamento de Políticas de Seguridad Informática del Poder Judicial – PJ", conforme al Anexo de la presente Resolución, con 25 (veinticinco) fojas.

ART. 2º: **ANOTAR**, registrar y notificar…".

Muy atentamente.

PODER JUDICIAL * CORTE SUPREMA DE JUSTICIA * SECRETARIA GENERAL

Abg. Alex Almada Cáceres
Secretario Interino

CORTE SUPREMA DE JUSTICIA

Compromiso con la gente

ANEXO DE LA RESOLUCIÓN Nº...9906.....

Asunción, 3 de febrero de 2023.

REGLAMENTO DE POLÍTICAS DE SEGURIDAD INFORMÁTICA

El objetivo de este documento es establecer las pautas acerca del uso de los sistemas informáticos y de comunicaciones del Poder Judicial – PJ, por parte de usuarios, funcionarios o terceros, protegiendo los activos de información de la institución así como toda tecnología utilizada para su gestión y procesamiento, contra amenazas internas o externas, intencionales o accidentales, de tal manera a preservar sus atributos primarios de confidencialidad, integridad y disponibilidad

Dirección de Ciberseguridad & Protección de la Información DCPI | Dirección General de Tecnologías de la Información y Comunicaciones DGTIC – Poder Judicial PJ – República del Paraguay

ES COPIA

Abg. Alex Almada Cáceres
Secretario Interino

PODER JUDICIAL
CORTE SUPREMA DE JUSTICIA
SECRETARIA GENERAL

ANEXO DE LA RESOLUCIÓN Nº 9906

Asunción, 3 de febrero de 2023.

Contenido

ES COPIA

PODER JUDICIAL – CORTE SUPREMA DE JUSTICIA – SECRETARIA GENERAL

Abg. Alex Almada Cáceres
Secretario Interino

ANEXO DE LA RESOLUCIÓN Nº 9906

Asunción, 3 de febrero de 2023.

Introducción

La información se ha convertido en un activo de alto valor para todas las organizaciones y el Poder Judicial (PJ) de la República del Paraguay no es la excepción. A medida que sus procesos se hacen más dependientes de la información y de la tecnología que la aloja, se hace ineludible contar con reglas de alto nivel que posibiliten un control integral de los sistemas informáticos y una gestión segura de los datos alojados en ellos.

Una política de seguridad define *qué* se debe proteger y plantea una propuesta del *cómo*, es decir, el conjunto de controles que enmarcan su cumplimiento. Cada una de estas políticas, sin perjuicio de los controles mencionados en este propio reglamento, debe ser instrumentalizada, especializada y formalizada en una serie de procedimientos, disposiciones, normativas, mecanismos e instructivos que recojan todas las medidas técnicas y organizativas que se establezcan y sean necesarias para asegurar su cumplimiento, por parte de las áreas encargadas de que ello ocurra efectivamente.

Como las políticas de seguridad informática buscan brindar el mejor uso posible a los activos informáticos de la institución y, al mismo tiempo, evitar al máximo los riesgos sobre ellos, dichos procedimientos, disposiciones, normativas, mecanismos e instructivos generados por las áreas responsables, basados en ellas, deberán ir actualizándose de acuerdo a las necesidades emergentes y de actualidad que comprometan y certifiquen el correcto cumplimiento de las mismas.

Cabe destacar que estas políticas no solo van destinadas a los equipos técnicos e informáticos de la institución, sino a todos los funcionarios de la misma que puedan provocar algún error o descuido de seguridad, ya que la mayoría de los problemas de seguridad en las instituciones tienen su origen en los propios colaboradores, cuando éstos no tienen en cuenta la vulnerabilidad de los datos y la información de la que son responsables.

Por esta razón, la Dirección General de Tecnologías de la Información y Comunicaciones del PJ (DGTIC), a través de su Dirección de Ciberseguridad y Protección de la Información (DCPI), elaboró el presente reglamento que contiene las principales directrices y lineamientos que reglan el proceder de los servidores públicos y los proveedores del PJ, en observancia a las disposiciones legales vigentes, con el objeto de resguardar y proteger los activos informáticos de la institución.

ES COPIA

PODER JUDICIAL – CORTE SUPREMA DE JUSTICIA – SECRETARIA GENERAL

Abg. Alex Almada Cáceres
Secretario Interino

ANEXO DE LA RESOLUCIÓN Nº...9906.....

Asunción, 3 de febrero de 2023.

Objetivo

Este reglamento, a través de las políticas de seguridad informática que establece, tiene como meta primordial definir las reglas sobre el uso de los sistemas informáticos y de comunicaciones del Poder Judicial (PJ), por parte de funcionarios, usuarios, administradores o terceros, buscando la protección de los recursos de información de la institución y la tecnología utilizada para su procesamiento y almacenamiento, frente a amenazas o vulnerabilidades internas o externas, intencionales o accidentales, con el fin de preservar los atributos primarios y críticos de *confidencialidad*, *integridad* y *disponibilidad* asociados a la información.

Alcance

Este Reglamento aplica a todo el ámbito del Poder Judicial (PJ) y sus Circunscripciones componentes, a sus activos de información digitales almacenados, procesados y transmitidos por medios electrónicos, tales como (aunque no ceñidos únicamente a) las unidades de almacenamiento magnético y óptico (fijas y removibles), estaciones de trabajo, terminales y demás dispositivos tecnológicos (teléfonos inteligentes, pendrives, discos externos, etc.), así como a la totalidad de los procesos relacionados a éstos, ya sean estos internos o externos.

Las políticas de seguridad informática están orientadas a toda la información almacenada, procesada y transmitida en medios electrónicos, estas políticas deben ser conocidas y cumplidas tanto por funcionarios de planta como por los proveedores externos de servicios que apoyan la gestión y por los terceros o grupos de interés que utilicen la información generada y custodiada por el PJ, y por quienes hagan uso de los servicios tecnológicos de la institución.

Acrónimos

CPD	Centro de Procesamiento de Datos
CSJ	Corte Suprema de Justicia
DCPI	Dirección de Ciberseguridad y Protección a la Información
DGTIC	Dirección General de Tecnologías de la Información y Comunicaciones
PJ	Poder Judicial
UPS	Uninterruptible Power Supply (Sistema de alimentación ininterrumpida)

ES COPIA

PODER JUDICIAL * CORTE SUPREMA DE JUSTICIA * SECRETARIA GENERAL

Abg. Alex Almada Cáceres
Secretario Interino

ANEXO DE LA RESOLUCIÓN Nº.....9906.....

Asunción, 3 de febrero de 2023.

Definiciones

Para los efectos de este reglamento, las siguientes definiciones aplican:

Acceso físico: La posibilidad de acceder físicamente a una estación de trabajo, periféricos o cualquier otro dispositivo tecnológico institucional y manipularlo, tanto de manera interna como externa.

Acceso lógico: Ingresar al sistema operativo o aplicaciones instaladas en los equipos tecnológicos institucionales y operarlos, ya sea directamente, o a través de la red de datos interna (intranet o dominio corporativo), o de Internet.

Activos de Información: Toda aquella información o elemento relacionado con el tratamiento de ésta, que la Institución considera importante o fundamental para sus procesos y que, por lo tanto, debe ser protegido; pueden ser ficheros y bases de datos, contratos y acuerdos, resoluciones y acordadas, documentación del sistema, manuales de usuario y de administración, aplicaciones, software del sistema, recursos humanos, hardware, servidores, middleware, vídeos, imágenes, dispositivos de comunicación, etc.

Aplicaciones o aplicativos: Son herramientas informáticas que permiten a los usuarios comunicarse, realizar trámites, cumplir etapas de un proceso, entretenerse, orientarse, aprender, trabajar, informarse y realizar una serie de tareas de manera práctica y desde distintos tipos de terminales, como estaciones de trabajo, tabletas o teléfonos inteligentes.

Cableado estructurado: Cableado de un edificio o una serie de edificios, que permite interconectar equipos activos, de diferentes o igual tecnología, permitiendo la integración de los diferentes servicios que dependen del tendido de cables como datos, telefonía, control, etc.

Cifrado de datos: Proceso por el que una información legible se transforma mediante un algoritmo (llamado cifra) en información ilegible, llamada criptograma o secreto. Esta información ilegible se puede enviar a un destinatario con muchos menos riesgos de ser leída indebidamente por terceras partes.

Configuración Lógica: conjunto de datos que determina el valor de algunas variables de un programa o de un sistema operativo, elegir entre distintas opciones con el fin de obtener un programa o sistema informático personalizado en cuanto a sus funcionalidades y privilegios o para poder ejecutar dicho programa correctamente.

ES COPIA

PODER JUDICIAL * CORTE SUPREMA DE JUSTICIA * SECRETARIA GENERAL

Abg. Alex Almada Cáceres
Secretario Interino

ANEXO DE LA RESOLUCIÓN Nº...9906.....

Asunción, 3 de febrero de 2023.

Respaldo o copia de seguridad (backup): Operación que consiste en duplicar y preservar datos e información contenida en un sistema informático, servidor o base de datos institucionales.

Contenido: Todos los tipos de información o datos que se divulguen a través de los diferentes servicios informáticos, entre los que se encuentran: textos, imágenes, vídeo, diseños, software, animaciones, etc.

Contraseñas: Clave criptográfica utilizada para la autenticación de usuario y que se utiliza para acceder a los diferentes recursos informáticos corporativos.

Cuenta de acceso: Colección de información que permite a un usuario identificarse en un sistema informático o servicio, mediante un usuario y una contraseña, para que pueda obtener seguridad, acceso al sistema y sus datos, perfil, privilegios y funcionalidades, administración de recursos, etc.

Dispositivos/Periféricos: Aparatos auxiliares e independientes conectados directamente a la estación de trabajo o a la red corporativa, que brindan una potencialidad adicional específica.

Dominio: Es un conjunto de computadores, conectados en una red interna corporativa o intranet, que confían a uno de los equipos de dicha red (servidor de dominio) la administración de los usuarios y los privilegios que cada uno de los usuarios tiene en la red.

Información confidencial: Se trata de una propiedad fundamental de la información que pretende garantizar el acceso sólo a personas autorizadas.

Información/Documento electrónico: Es la información generada, enviada, recibida, almacenada o comunicada por medios electrónicos, ópticos o similares. Se pueden clasificar por su forma y formato en documentos ofimáticos, cartográficos, correos electrónicos, imágenes, videos, audio, mensajes de datos de redes sociales, formularios electrónicos, bases de datos, entre otros.

Integridad: propiedad de salvaguardar la exactitud y estado completo de los activos de información.

Mantenimiento lógico preventivo: Es el trabajo realizado en la configuración y/u optimización de la estación de trabajo y/o servidor, con la finalidad de mejorar el rendimiento general del equipo.

ES COPIA

PODER JUDICIAL
CORTE SUPREMA DE JUSTICIA
SECRETARIA GENERAL

Abg. Alex Almada Cáceres
Secretario Interino

ANEXO DE LA RESOLUCIÓN Nº....9906.....

Asunción, 3 de febrero de 2023.

Mantenimiento físico preventivo: Actividad de limpieza de elementos como polvo, residuos de alimentos y otro tipo de partículas que debe realizarse sobre la estación de trabajo y/o servidor, con el propósito de posibilitar su correcto funcionamiento y prolongar su vida útil.

Medios de almacenamiento extraíble: Son aquellos soportes de almacenamiento diseñados para ser extraídos del computador sin tener que apagarlo. Por ejemplo, memorias USB, discos duros externos, discos ópticos (CD, DVD), tarjetas de memoria (SD, CompactFlash, Memory Stick, etc.).

Plataforma web: Sistema que permite la ejecución de diversas aplicaciones bajo un mismo entorno, dando a los usuarios la posibilidad de acceder a ellas a través de Internet.

Recurso informático: Todos aquellos componentes o dispositivos (Hardware) y programas o controladores (Software) que son necesarios para el buen funcionamiento de un computador o un sistema de gestión de la información. Los recursos informáticos incluyen medios para entrada, procesamiento, producción, comunicación y almacenamiento.

Red de datos: Es un conjunto de ordenadores que están conectados entre sí, y comparten recursos, información, y servicios.

Riesgo: Posibilidad de que se produzca un contratiempo o una desgracia, por causa de las vulnerabilidades y amenazas a las que se encuentran expuestos los activos de información.

Servicio informático: Conjunto de actividades asociadas al manejo y procesamiento automatizado de la información, que satisfacen las necesidades de los usuarios.

Servidor: Es aquel software que dispone un equipo informático (usualmente con mayores prestaciones) para facilitar el acceso a la red y sus recursos, así como albergar sistemas informáticos para usuarios finales. También puede ofrecer a los clientes la posibilidad de compartir datos, información y recursos de hardware y software.

Sistema de información: Es un conjunto de elementos orientados al tratamiento y administración de datos e información, organizados y listos para su uso posterior, generados para cubrir una necesidad o un objetivo específico para un usuario final o grupo de ellos.

Software antivirus: Son programas que buscan prevenir, detectar y eliminar virus informáticos. En los últimos años, y debido a la expansión de Internet, los nuevos navegadores y el uso de ingeniería social, los antivirus han evolucionado para detectar varios tipos de software fraudulento o malicioso, también conocidos como malware.

ES COPIA

PODER JUDICIAL ★ CORTE SUPREMA DE JUSTICIA ★ SECRETARIA GENERAL

Abg. Alex Almada Cáceres
Secretario Interino

ANEXO DE LA RESOLUCIÓN Nº...9906.....

Asunción, 3 de febrero de 2023.

Software de gestión: Son todos aquellos programas utilizados a nivel institucional, que por su definición genera acción de emprender algo y por su aplicación persigue fines lucrativos o laborales, tanto misionales como de administración. También es un software que permite gestionar todos los procesos de un negocio o de una empresa en forma integrada.

Software malicioso (malware): Es aquel que se ha diseñado específicamente para dañar un computador o los datos que éste alberga. Este tipo de software realiza acciones maliciosas o fraudulentas, como instalar software sin el consentimiento del usuario que busca comprometer alguna de las características principales de todo activo de información: su confidencialidad, su integridad o su disponibilidad.

Tráfico de red: Es la cantidad de datos enviados y recibidos por los usuarios de la red.

UPS: Sistema de alimentación ininterrumpida (SAI), en inglés Uninterruptible Power Supply (UPS), es un dispositivo que, gracias a sus baterías u otros elementos almacenadores de energía, puede proporcionar energía eléctrica por un tiempo limitado y durante un apagón eléctrico a todos los dispositivos que tenga conectados.

Políticas de seguridad informática del Poder Judicial

El Poder Judicial y sus ministros, los directores de área, los jefes de oficina, la DGTIC con su personal técnico, funcionarios judiciales en general y todo el personal interno y/o externo que se relacione de algún modo con la institución, son responsables de conocer y asegurar la implementación de las políticas de seguridad informática presentadas en este apartado, dentro de sus áreas de responsabilidad, así como del cumplimiento de las mismas por parte de su equipo de trabajo.

La edición, agregado y/o ajuste a este Reglamento y sus políticas de seguridad informática serán de competencia de la Dirección de Ciberseguridad y Protección de la Información, bajo la aprobación del Pleno de la Corte Suprema de Justicia, y podrán ser sugeridas a través de los canales definidos por la DGTIC para tal efecto.

Las oficinas a cargo de los Ministros de la Corte Suprema de Justicia (Despacho, Gabinete, Sala de Relatores y/o Sala de Auxiliares) y los dispositivos tecnológicos ubicados en las mismas, solo podrán ser verificados con la autorización expresa del Ministro respectivo.

La inobservancia e incumplimiento de estas políticas y las disposiciones establecidas en este reglamento, acarreará las sanciones disciplinarias y/o de otra índole para los responsables implicados en las mismas, vía denuncia correspondiente a la Superintendencia de Justicia.

ES COPIA

PODER JUDICIAL – CORTE SUPREMA DE JUSTICIA – SECRETARIA GENERAL

Abg. Alex Almeda Cáceres
Secretario Interino

ANEXO DE LA RESOLUCIÓN Nº...9906.....

Asunción, 3 de febrero de 2023.

1. ***Políticas orientadas a los dispositivos tecnológicos (Hardware) y aplicaciones informáticas (Software)***

1.1. No se permite el uso de la plataforma y servicios informáticos del Poder Judicial (estaciones de trabajo, periféricos, impresoras, dispositivos en general, internet, red de datos, correo electrónico institucional y similares), para actividades que no estén relacionadas con las labores propias de la institución.

1.2. La instalación y desinstalación de aplicaciones informáticas, la conexión a la red corporativa, la configuración lógica y de acceso al dominio institucional, la instalación y desinstalación de dispositivos tecnológicos, la manipulación interna y la reubicación de las estaciones de trabajo y periféricos, será realizada únicamente por personal idóneo de la DGTIC, sin excepciones.

1.3. No está permitido instalar y/o utilizar software pirata, crackeado o adquirido de forma fraudulenta, ni activadores de licencias de aplicaciones propietarias. La DGTIC, a través de su área competente, realizará revisiones y auditorías periódicas en las estaciones de trabajo del PJ, tendientes a asegurar el cumplimiento de esta directiva.

1.4. No está permitido conectar periféricos que no sean del PJ a las estaciones de trabajo institucionales, sin el consentimiento explícito y por escrito del jefe del área, la justificación correspondiente y la aprobación de la DGTIC.

1.5. El espacio en el disco duro de las estaciones de trabajo pertenecientes al PJ será ocupado únicamente con información institucional, no se hará uso de ellos para almacenar información de tipo personal (documentos, instaladores de aplicativos, fotos, imágenes, músicas, videos y otros) que no competan a lo estrictamente laboral.

1.6. La información derivada del trabajo y de las tareas cumplidas por funcionarios y/o personal de proveedores externos de servicios en el ejercicio de sus funciones para la institución deberá ser guardada únicamente en la carpeta (directorio) correspondiente a su usuario de dominio en la/s estación/es de trabajo utilizadas, dentro de la jerarquía correspondiente: ***[Usuario de Dominio]/[SubCarpetas o SubDirectorios]/[Archivos de trabajo]***. Todo archivo guardado por el usuario en otra locación de la estación de trabajo no estará contemplado en los procesos de respaldo realizados por el ámbito competente, en las situaciones previstas para tal efecto.

ES COPIA

PODER JUDICIAL * CORTE SUPREMA DE JUSTICIA * SECRETARIA GENERAL

Abg. Alex Almada Cáceres
Secretario Interino

ANEXO DE LA RESOLUCIÓN Nº...9906.....

Asunción, 3 de febrero de 2023.

1.7. Ningún funcionario o proveedor externo de servicios podrá acceder a los dispositivos tecnológicos o aplicaciones informáticas del PJ con otro usuario diferente al suyo. En caso de ser necesario hacer disponible y accesible el trabajo o documentos de un usuario que ya no forma parte de la dependencia en cuestión, el jefe de área deberá solicitar ese servicio con su consentimiento explícito y por escrito, la justificación correspondiente y la aprobación de la DGTIC.

1.8. Ningún funcionario o proveedor externo podrá interceptar datos informáticos en su origen, destino, tránsito de red o en el interior de un sistema informático, protegido éste o no con medidas de seguridad, sin la autorización correspondiente por parte de la DGTIC.

1.9. Ningún funcionario o personal de un proveedor externo de servicios podrá impedir u obstaculizar el funcionamiento o el acceso normal a un sistema informático, a los datos digitales contenidos en él, o a la red de telecomunicaciones, salvo el personal autorizado de la DGTIC en aplicación de las políticas o medidas de seguridad que correspondan.

1.10. Los funcionarios y/o proveedores externos contratados serán responsables de contar con conocimientos actualizados y certificados por un órgano competente, en las habilidades necesarias para desarrollar sus actividades profesionales en el ámbito respectivo, así como en informática básica y en el uso de herramientas ofimáticas.

1.11. Deberá preverse la actualización periódica de las aplicaciones, software, middleware y hardware a las últimas versiones estables sugeridas por los desarrolladores, fabricantes o integradores de estos activos de información. Las mismas se realizarán siempre con el acompañamiento del proveedor y/o fabricante del activo de información y este servicio deberá ser previsto en los procesos de adquisición, arriendo o usufructo de los mismos.

2. Políticas para los usuarios de dominio y las cuentas de acceso institucionales

2.1. Todos los usuarios del dominio corporativo, las cuentas de acceso a los sistemas y recursos de las tecnologías de información, son personales e intransferibles; cada funcionario y/o proveedor externo es responsable por las cuentas de acceso asignadas y las transacciones que con ellas se realicen. Se permite su uso única y exclusivamente durante el tiempo que tenga vínculo laboral o contractual con el Poder Judicial, bajo las directrices expresadas en este reglamento.

ES COPIA

PODER JUDICIAL * CORTE SUPREMA DE JUSTICIA * SECRETARIA GENERAL

Abg. Alex Almada Cáceres
Secretario Interino

ANEXO DE LA RESOLUCIÓN Nº...9906.....

Asunción, 3 de febrero de 2023.

2.2. La contraseña inicial de acceso al dominio corporativo que sea asignada a cada usuario debe ser cambiada la primera vez que éste acceda al sistema; además, debe ser cambiada periódicamente mínimo cada 45 días, o cuando se considere necesario, debido a alguna vulnerabilidad en los criterios de seguridad o algún factor que pueda haberla comprometido en su confidencialidad.

2.3. Las contraseñas de acceso deben poseer un mínimo de ocho (8) caracteres y deben cumplir con al menos tres de los siguientes requerimientos: una letra mayúscula, una letra minúscula, un número y un carácter especial (+-*/@#$%&).

2.4. Las cuentas de usuario no pueden tener el rol de administrador local de las estaciones de trabajo, y la cuenta de administrador predeterminada será deshabilitada para la entrega de los equipos a los usuarios, de tal manera a salvaguardar la integridad de los sistemas ante cualquier riesgo por el uso indebido de privilegios elevados. Serán realizadas revisiones periódicas y campañas de verificación y cumplimiento de esta directiva, por parte de la dependencia responsable de la entrega de equipos y soporte a usuarios.

2.5. Solamente puede solicitar cambio o restablecimiento de contraseña el funcionario o proveedor externo al cual pertenece dicho usuario, o su jefe inmediato, mediante solicitud formal al Departamento de Asistencia Técnica & Soporte Informático de la DGTIC, el cual establecerá los mecanismos de verificación de la titularidad de la cuenta.

2.6. Todo funcionario o proveedor externo que se retire de la institución de forma definitiva o temporal (superior a 1 semana) deberá hacer entrega formal, a quien lo reemplace en sus funciones o a su superior inmediato, de la información y documentos de trabajo asociados a las cuentas asignadas y utilizadas por él, con el fin de garantizar la continuidad de las operaciones a su cargo cuando dicho personal ya no se encuentre disponible. En caso que esto no ocurriera, el jefe de área podrá solicitar a la DGTIC el acceso a la cuenta de ese usuario o proveedor externo, siguiendo los mismos pasos mencionados en el literal 1.7.

3. Políticas relacionadas al correo electrónico institucional

3.1. Todo uso del correo electrónico debe ser coherente con las políticas y procedimientos del PJ en materia de conducta ética, seguridad, cumplimiento de las leyes aplicables y prácticas institucionales adecuadas.

ES COPIA

PODER JUDICIAL ★ CORTE SUPREMA DE JUSTICIA ★ SECRETARIA GENERAL

Abg. Alex Almada Cáceres
Secretario Interino

ANEXO DE LA RESOLUCIÓN Nº...9906.....

Asunción, 3 de febrero de 2023.

3.2. El correo electrónico institucional es de uso exclusivo para el envío y la recepción de mensajes relacionados con las actividades del Poder Judicial y, por lo tanto, no se hará uso de él para fines personales como, por ejemplo: registros en redes sociales, registros en sitios web con actividades particulares o comerciales, reenvío de cadenas de mensajes o chistes, o en general para entablar comunicaciones en asuntos no relacionados con las funciones y actividades que el funcionario desempeña en la institución.

3.3. Está prohibido utilizar el correo electrónico institucional para divulgar información confidencial, reenviar mensajes que falten al respeto o atenten contra la dignidad e intimidad de las personas, difundir propaganda de índole comercial, religiosa, política, racista, sexista o similares, así como reenviar contenido y anexos que atenten contra la propiedad intelectual. Adicionalmente, los funcionarios que reciban cualquier correo electrónico con este tipo de contenido, de cualquier otro funcionario del PJ, deben reportarlo a su superior jerárquico directo de manera inmediata.

3.4. La información transmitida a través de las cuentas de correo electrónico institucional no se considera correspondencia privada, ya que éstas tienen como fin principal posibilitar el envío y recepción de la información relacionada con las actividades ordinarias y laborales del Poder Judicial y sus funcionarios. Por lo tanto, los funcionarios no tendrán ninguna expectativa de privacidad en nada de lo que almacenen, envíen o reciban en el sistema de correo electrónico de la institución, salvaguardando la transparencia pública.

3.5. Los funcionarios tienen prohibido reenviar automáticamente el contenido de los correos electrónicos institucionales a un sistema de correo electrónico de terceros (nombrados en el 3.6, a continuación). Los mensajes individuales que son reenviados por los funcionarios no deben contener información institucional de índole confidencial o restringida.

3.6. Los funcionarios no deben utilizar sistemas de correo electrónico y/o servidores de almacenamiento de terceros, tales como Google, Yahoo y MSN Hotmail, etc. (listado de proveedores solo enunciativo, no exhaustivo) para almacenar correos electrónicos en nombre del PJ o para realizar sus labores y responsabilidades oficiales, o para crear o formalizar cualquier transacción vinculante, pudiendo sí hacerlo cuando sea para alojar borradores, documentos preliminares o información informal en proceso de elaboración. En el caso de comunicaciones laborales formales, servicios y/o

ES COPIA

PODER JUDICIAL * CORTE SUPREMA DE JUSTICIA * SECRETARIA GENERAL

Abg. Alex Almada Cáceres
Secretario Interino

transacciones con cariz institucional, los mismos deben llevarse a cabo a través de los canales designados, autorizados y formalizados por la normativa correspondiente aprobada por el PJ.

3.7. Es responsabilidad del funcionario o proveedor externo depurar su cuenta de correo electrónico institucional periódicamente, así como realizar la correspondiente copia de seguridad completa de sus correos, tanto los recibidos como los enviados. De ser necesario, el funcionario podrá requerir al personal idóneo especializado de la DGTIC, la asistencia técnica específica y la capacitación inicial pertinente para el cumplimiento de tales fines.

4. Políticas referidas al servicio de internet

4.1. El Servicio de internet del Poder Judicial no podrá ser usado para fines diferentes a los pertinentes en el desarrollo de las actividades propias de la institución. Esta restricción incluye el acceso a páginas o sitios web con contenido pornográfico, terrorismo, juegos en línea, redes sociales y demás, cuyo contenido no sea requerido para desarrollar las labores vinculadas al cargo, establecidas por la institución.

4.2. No está permitido el uso de Internet para actividades ilegales o que atenten contra la ética y el buen nombre del Poder Judicial o de las personas.

4.3. No se harán descargas de archivos por internet que no provengan de páginas certificadas, conocidas o relacionadas con las funciones y actividades en la institución.

4.4. El Poder Judicial se reserva el derecho a registrar los accesos y monitorear el contenido al que el usuario puede acceder a través de la red, y desde los recursos y servicios tecnológicos que provee la institución.

5. Políticas acerca de la gestión de la Información

5.1. Todo funcionario institucional o proveedor externo de servicios que inicie labores en el Poder Judicial, relacionadas con el uso de estaciones de trabajo, software de gestión, aplicativos, plataformas web y servicios informáticos, debe aceptar las condiciones de confidencialidad y de uso adecuado de los recursos informáticos, así como cumplir y respetar las directrices impartidas en este reglamento.

ES COPIA

PODER JUDICIAL * CORTE SUPREMA DE JUSTICIA * SECRETARIA GENERAL

Abg. Alex Almada Cáceres
Secretario Interino

ANEXO DE LA RESOLUCIÓN Nº...9906.....

Asunción, 3 de febrero de 2023.

5.2. Todo contrato o convenio relacionado con servicios de tecnología y/o acceso a información, debe contener una obligación o cláusula donde el proveedor externo de servicios o tercero acepte el conocimiento de las políticas de seguridad establecidas en este reglamento y convenga mantener la confidencialidad de la información con la suscripción de un acuerdo o compromiso de confidencialidad de la información, el cual se hará extensivo a todos sus colaboradores.

5.3. Toda la información recibida y producida en el ejercicio de las funciones y cumplimiento de las obligaciones contractuales, que se encuentre almacenada en las estaciones de trabajo, pertenece al Poder Judicial y, por lo tanto, no se hará divulgación ni extracción de la misma sin previa autorización de las máximas autoridades (ministros) de la institución.

5.4. No se realizará por parte de los funcionarios o proveedores externos de servicios copia no autorizada de información electrónica confidencial y software de propiedad del Poder Judicial. El retiro de información electrónica perteneciente al Poder Judicial y clasificada como confidencial, se hará única y exclusivamente con la autorización de la máxima autoridad competente (ministros).

5.5. Ningún funcionario o proveedor externo de servicios podrá visualizar, copiar, enviar, alterar y/o destruir información que no se encuentre bajo su custodia.

5.6. Los funcionarios que se desvinculen y los proveedores externos que culminen su vínculo contractual con el Poder Judicial, deberán hacer entrega formal de los equipos asignados, en las condiciones que fueron recibidos, así como de la totalidad de la información electrónica que se produjo y se recibió con motivo de sus funciones y actividades, como requisito para la expedición de liquidación de contrato.

6. Políticas sobre la seguridad física del equipamiento institucional

6.1. Los recursos tecnológicos (computadores, periféricos, impresoras, etc.) son propiedad del PJ y como tales, pueden ser redistribuidos y/o asignados a los funcionarios como mejor corresponda, de acuerdo al criterio del jefe de cada área correspondiente y eventualmente, de la propia DGTIC, teniendo presente criterios de optimización, buen uso, seguridad y racionalidad en la utilización de los recursos públicos.

6.2. Es responsabilidad de los funcionarios y proveedores externos de servicios velar por la conservación física de los equipos a ellos asignados, haciendo uso adecuado de los

ES COPIA

PODER JUDICIAL ★ CORTE SUPREMA DE JUSTICIA ★ SECRETARIA GENERAL

Abg. Alex Almada Cáceres
Secretario Interino

ANEXO DE LA RESOLUCIÓN Nº....9906.....

Asunción, 3 de febrero de 2023.

mismos. En caso de daño, pérdida o robo, se establecerá su responsabilidad a través de los procedimientos definidos por la normativa vigente en el Poder Judicial para tal fin.

6.3. En cuanto a los equipos portátiles o notebooks, estos podrán ser retirados de las oficinas de la institución única y exclusivamente por el usuario a cargo y estrictamente para ejercer labores que estén relacionadas con las actividades del Poder Judicial. Para ello, se deberá contar con la solicitud por escrito del jefe de área, su autorización y justificación correspondiente, las configuraciones técnicas de rigor al dispositivo por parte del personal técnico autorizado de la DGTIC y la autorización pertinente por parte del Departamento de Patrimonio, en su rol de custodio de los bienes institucionales.

6.4. Los funcionarios y proveedores externos de servicios deberán reportar de forma inmediata al personal de la DGTIC la detección de riesgos reales o potenciales sobre las estaciones de trabajo o equipos de comunicaciones, tales como caídas de agua, choques eléctricos, caídas o golpes, peligro de incendio, peligro de robo, entre otros; así como reportar de cualquier problema o violación de la seguridad de la información, del cual ellos fueren testigos.

6.5. Se debe evitar colocar objetos encima de las estaciones de trabajo, que obstruyan las salidas de ventilación de sus componentes y/o periféricos, o cuyo peso pueda comprometer la integridad estructural de los mismos.

6.6. Mientras las estaciones de trabajo son utilizadas, no se deberá consumir alimentos ni ingerir bebidas que puedan poner en riesgo el equipamiento patrimonial institucional.

7. *Políticas vinculantes al personal de la DGTIC*

7.1. El acceso a los sistemas de información y red de datos será controlado por medio de nombres de usuario personales y su contraseña correspondiente. La DGTIC será la encargada de crear y asignar las cuentas de acceso y sus permisos al dominio de red corporativo, sistemas de información y correo electrónico institucional, previo cumplimiento del procedimiento establecido para tal fin.

7.2. Siempre que sea factible técnicamente, se deben asignar usuarios unificados para todos y cada uno de los sistemas, servicios y aplicaciones, utilizando el servidor de dominio corporativo para las debidas autenticaciones y garantizando así la estandarización en el acceso; es decir, que cada usuario debe tener el mismo nombre de usuario para todos los sistemas y aplicaciones de la Institución. Para dichos escenarios y para los nuevos

ES COPIA

PODER JUDICIAL * CORTE SUPREMA DE JUSTICIA * SECRETARIA GENERAL

Abg. Alex Almada Cáceres
Secretario Interino

ANEXO DE LA RESOLUCIÓN Nº...9906.....

Asunción, 3 de febrero de 2023.

sistemas informáticos a ser desarrollados, la estandarización de los nombres de usuario estará compuesta de la siguiente forma: Primera letra del primer nombre + guion bajo (_) + primer apellido; en caso de existir duplicidad: primeras dos letras del primer nombre + guion bajo (_) + primer apellido; o de lo contrario, el documento de identidad de la persona. En el caso de sistemas legados o muy antiguos, aún en vigencia, esta política se implementará cuando se dé la renovación tecnológica de los mismos y sean reemplazados por nuevas versiones.

7.3. El control lógico de los equipos tecnológicos estará bajo la responsabilidad del Departamento de Asistencia Técnica & Soporte Informático y la asignación de usuarios, a cargo del Departamento de Relevamiento e Implementación de Proyectos Tecnológicos, ambas dependencias de la DGTIC. En cuanto a la ubicación física de dichos equipos tecnológicos, dicho control será ejercido por el Departamento de Patrimonio del PJ.

7.4. El Departamento de Patrimonio llevará un control total y sistematizado (inventario) de los recursos tecnológicos, tanto de hardware como de software. La DGTIC, a través de su Departamento de Infraestructura Tecnológica y Comunicaciones, brindará apoyo poniendo a disposición toda la información que disponga para el cumplimiento de esta tarea.

7.5. La DGTIC será la encargada de velar porque se cumpla la normativa y reglamentación vigente, sobre la propiedad intelectual de soporte lógico (software).

7.6. A partir de la entrada en vigencia de estas políticas, todas las nuevas licencias de uso de software adquiridas por el PJ estarán bajo custodia del Departamento de Infraestructura Tecnológica y Comunicaciones de la DGTIC, así como también los manuales y los medios de almacenamiento (CD, cintas magnéticas u otros medios) que acompañen a las versiones originales del software.

7.7. La DGTIC es la única dependencia autorizada para realizar copia de seguridad del software original, aplicando los respectivos controles. Cualquier otra copia del programa original será considerada como una copia no autorizada y su utilización conllevará las sanciones administrativas y legales pertinentes.

7.8. Todas las publicaciones que se realicen en el sitio web de la institución, deberán atender el cumplimiento de las normas en materia de propiedad intelectual.

ES COPIA

PODER JUDICIAL * CORTE SUPREMA DE JUSTICIA * SECRETARIA GENERAL

Abg. Alex Almada Cáceres
Secretario Interino

ANEXO DE LA RESOLUCIÓN Nº....9906.....

Asunción, 3 de febrero de 2023.

7.9. Las cuentas de acceso a sistemas, servicios y aplicaciones serán inactivadas al retiro de los funcionarios o proveedores externos y se procederá a su eliminación transcurridos **5 años** de inactividad de las mismas. Esta operación será requerida por la Dirección General de Recursos Humanos cuando se trate de desvinculaciones de personal, dando aviso de esta situación a la DGTIC para que la misma proceda a la inactivación de todas las cuentas de usuario correspondientes.

7.10. Se realizará respaldo (backup) a la información institucional y bases de datos, conforme a lo establecido en la sección de las políticas de respaldos y recuperaciones, así como en los casos extraordinarios: desvinculación de funcionario o proveedor externo de servicios, envío de equipo para garantía, mantenimiento correctivo de equipo, etc.

7.11. Las contraseñas de los usuarios administradores de las plataformas tecnológicas y sistemas de información de la institución, deberán ser salvaguardadas por la DGTIC en un archivo protegido a través de técnicas de cifrado de datos u otro mecanismo seguro. Estas contraseñas deben reunir las medidas de seguridad necesarias como: complejidad, uso de letras y números, no repetición y mínimo 12 (doce) caracteres de longitud.

7.12. Las contraseñas de acceso a las bases datos y permisos serán responsabilidad del área de Base de Datos de la DGTIC y deben reunir las medidas de seguridad necesaria como: complejidad, uso de letras y números, no repetición y mínimo 12 (doce) caracteres de longitud.

7.13. La red interna del Poder Judicial deberá estar protegida de amenazas externas, a través de sistemas que permitan implementar reglas de control de tráfico desde y hacia la red.

7.14. Todos los equipos de la institución deben tener instalado el antivirus corporativo, en funcionamiento, actualizado y debidamente licenciado.

7.15. Se realizará mantenimiento lógico preventivo a las estaciones de trabajo mínimo cada 6 meses y mantenimiento físico preventivo mínimo una vez por año, que incluya el cableado estructurado. El Departamento de Asistencia Técnica y Soporte Informático (estaciones de trabajo) y la División de Redes y Conectividad (cableado y dispositivos de red) de la DGTIC elaborarán sus planes y cronogramas de mantenimientos, con eventual contratación de terceros en base a la envergadura de los trabajos requeridos, los cuales serán debidamente notificados a los usuarios; adicionalmente, deberá informarse el nombre e identificación del personal autorizado (interno o externo) para realizar las actividades de mantenimiento, con el fin de evitar el riesgo de hurto y/o pérdida de equipos, periféricos y/o información.

ES COPIA

PODER JUDICIAL * CORTE SUPREMA DE JUSTICIA * SECRETARIA GENERAL

Abg. Alex Almada Cáceres
Secretario Interino

ANEXO DE LA RESOLUCIÓN Nº 9906

Asunción, 3 de febrero de 2023.

8. Políticas vinculadas a los usuarios externos y su equipamiento

8.1. El acceso de terceras personas a la institución debe ser controlado, y su ingreso a las diferentes dependencias debe ser autorizado por los funcionarios a cargo.

8.2. Proveedores, terceros o externos a la institución deberán contar con la autorización formal y por escrito de la DGTIC, que les otorga el permiso para la manipulación y/o utilización del equipamiento tecnológico o servicios que pertenezcan al Poder Judicial.

8.3. El acceso de equipos informáticos no pertenecientes al Poder Judicial, así como su conexión a la red institucional o Intranet, será relevado y controlado por el Departamento de Asistencia Técnica y Soporte Informático de la DGTIC, para luego ser configurado y habilitado por el Departamento de Infraestructura Tecnológica y Comunicaciones de la DGTIC, de tal manera a no permitir el acceso y/o uso indebido de información interna de la institución y/o la introducción de malware a la red corporativa.

8.4. Todos los equipos foráneos deben tener instalado un antivirus en funcionamiento, actualizado y debidamente licenciado. Esto será configurado y corroborado por el Departamento de Asistencia Técnica y Soporte Informático de la DGTIC y, posteriormente el Departamento de Infraestructura Tecnológica y Comunicaciones de la DGTIC le otorgará el permiso (o no) para su inclusión en la intranet corporativa y bajo qué perfil de seguridad se conectará a la misma.

9. Políticas orientadas al centro de procesamiento de datos

9.1. Se destinará un espacio en la institución que servirá como centro de procesamiento de datos (CPD), red y telecomunicaciones, en el cual se ubicarán los servidores de los diferentes sistemas informáticos, así como los sistemas de redes y telecomunicaciones, debidamente protegidos con la infraestructura, de manera que se restrinja el acceso directo a usuarios no autorizados.

9.2. El CPD deberá contar con piso flotante, sistema de protección contra incendios, control de temperatura (aire acondicionado) permanente a una temperatura no superior a 21 grados centígrados, sistema eléctrico de respaldo (UPS), así como todo lo recomendado por las buenas prácticas en la industria para este tipo de instalaciones.

9.3. Cumplir con los estándares de protección eléctrica vigentes para minimizar el riesgo de daños físicos de los servidores, equipos de red y de telecomunicaciones.

ES COPIA

PODER JUDICIAL * CORTE SUPREMA DE JUSTICIA * SECRETARIA GENERAL

Abg. Alex Almada Cáceres
Secretario Interino

ANEXO DE LA RESOLUCIÓN Nº...9906.....

Asunción, 3 de febrero de 2023.

9.4. Las instalaciones eléctricas y de comunicaciones, estarán preferiblemente fijas o en su defecto, resguardadas del paso de personas o materiales, y libres de cualquier interferencia eléctrica o magnética.

9.5. Contar por lo menos con dos extintores de incendio adecuados y cercanos al CPD.

9.6. Los equipos que hacen parte de la infraestructura tecnológica del Poder Judicial, tales como servidores, estaciones de trabajo, centro de cableado, UPS, dispositivos de almacenamiento, entre otros, deben estar protegidos y ubicados en sitios libres de amenazas como humedad, inundaciones, calor excesivo, robo, incendio, explosiones, vandalismo, agentes biológicos, y terrorismo.

10. Políticas de gestión de respaldos y recuperaciones

10.1. En cuanto al contenido, la información y los datos en cada estación de trabajo, tanto de documentos como de otros tipos de archivos, cada funcionario y/o consultor externo deberá realizar los respaldos que entienda oportunos en su propio ambiente o entorno de trabajo en la institución. Para esta tarea, podrá solicitar apoyo del personal competente de la DGTIC, de tal manera a evacuar cualquier duda o consulta relacionada a su correcta realización.

10.2. En relación a los servidores (virtuales o físicos), los sistemas informáticos del PJ, así como a sus datos y las bases de datos subyacentes a los mismos, la realización y ejecución de procedimientos de respaldos o copias de seguridad (backups) periódicas serán responsabilidad de la DGTIC a través de sus áreas competentes. La realización de respaldos y/o restauraciones específicas a estaciones de trabajo individuales serán ejecutadas por la DGTIC solo bajo pedido fundamentado de autoridad competente.

10.3. La ejecución de las tareas de respaldo, su configuración, periodicidad, modalidad, almacenamiento, rotación y reescritura, tiempo máximo de preservación y demás aspectos asociados serán definidos por la DGTIC a través de sus áreas competentes: el Departamento de Infraestructura Tecnológica y Comunicaciones (servidores y sistemas informáticos) y el Departamento de Control e Integridad de la Información (bases de datos).

10.4. Los respaldos podrán ser realizados en dos modalidades:

10.4.1. Respaldo incremental: se realiza una copia de todos los archivos que han sido modificados desde que fue ejecutado el último respaldo completo.

10.4.2. Respaldo completo: se realiza una copia de seguridad completa de todos archivos involucrados, abarcando la totalidad de los datos.

ES COPIA

PODER JUDICIAL ★ CORTE SUPREMA DE JUSTICIA ★ SECRETARIA GENERAL

Abg. Alex Almada Cáceres
Secretario Interino

ANEXO DE LA RESOLUCIÓN Nº...9906.....

Asunción, 3 de febrero de 2023.

Referencias

Adsero Security. (29 de agosto de 2019). *So what exactly is a Security Risk Assessment?* Recuperado el 5 de abril de 2022, de Adsero Security (sitio web oficial): https://www.adserosecurity.com/2019/08/29/so-what-exactly-is-a-security-risk-assessment/

Adsero Security. (s.f.). *IT Security Policies - Ten IT Security Policies Organization Should Have.* Recuperado el 7 de abril de 2022, de Adsero Security | Security 101 (sitio web oficial): https://www.adserosecurity.com/security-learning-center/ten-it-security-policies-every-organization-should-have/

Carisio, E. (s.f.). *Políticas de seguridad informática y su aplicación en la empresa.* Recuperado el 14 de marzo de 2022, de MediaCloud | Inicio | Blog de Seguridad (sitio web oficial): https://blog.mdcloud.es/politicas-de-seguridad-informatica-y-su-aplicacion-en-la-empresa/

Cassetto, O. (1 de marzo de 2022). *The 12 Elements of an Information Security Policy.* Recuperado el 4 de abril de 2022, de Exabeam | Information Security (sitio web oficial): https://www.exabeam.com/information-security/information-security-policy/

Dirección de Informática. (26 de agosto de 2021). *Políticas y Lineamientos de Seguridad Informática de la Universidad Tecnológica de Tabasco.* Recuperado el 16 de marzo de 2022, de Universidad Tecnológica de Tabasco - UTTAB | Inicio | Normatividad (sitio web oficial): https://www.uttab.edu.mx/resources/normatividad/Politicas_y_lineamientos_de_seguridad_para_los_sistemas_informaticos.pdf

Dirección de Tecnologías de la Información y de la Comunicación (Proyecto SOFÍA). (15 de julio de 2020). *Políticas de Seguridad Informática de la Dirección Nacional de Aduanas.* Recuperado el 17 de marzo de 2022, de Dirección Nacional de Aduanas, Paraguay (sitio web oficial): https://www.aduana.gov.py/uploads/archivos/ANEXO%20POLITICA%20DE%20SEGURIDAD%20DE%20LA%20INFORMACION%20V4%203%202_1.pdf

Disete Comunicaciones. (16 de septiembre de 2020). *Qué son las políticas de seguidad informática y por qué tu empresa debe tener una.* Recuperado el 16 de marzo de 2022, de Disete Comunicaciones | Home (sitio web oficial): https://disete.com/que-son-las-politicas-de-seguridad-informatica-y-por-que-tu-empresa-debe-tener-una/

Escudero, J. M. (s.f.). *Políticas de Seguridad Informática.* Recuperado el 16 de marzo de 2022, de IEDGE Business School | Blog (sitio web oficial): https://www.iedge.eu/juan-manuel-escudero-politicas-de-seguridad-informatica

ES COPIA

PODER JUDICIAL CORTE SUPREMA DE JUSTICIA SECRETARIA GENERAL

Abg. Alex Almeda Cáceres
Secretario Interino

ANEXO DE LA RESOLUCIÓN Nº...9906.....

Asunción, 3 de febrero de 2023.

FiberTelco Internet + Tv hogares. (septiembre de 2021). *Manual de Políticas de Seguridad Informática.* Recuperado el 14 de marzo de 2022, de FiberTelco Internet + Tv hogares (sitio web oficial): https://fibertelco.com/normatividad/

Instituto de Cultura y Patrimonio de Antioquia. (31 de mayo de 2020). *Manual de Políticas de Seguridad.* Recuperado el 14 de marzo de 2022, de Instituto de Cultura y Patrimonio de Antioquia (sitio web oficial): https://www.culturantioquia.gov.co/index.php/transparencia-acceso-informacion-publica/politicas-de-seguridad-de-la-informacion-y-proteccion-de-datos

Juliá, S. (s.f.). *Informática para empresas | Backup online | ¿Qué son las políticas de seguridad informática?* Recuperado el 15 de marzo de 2022, de Gadae Netweb | Blog | Amenazas de seguridad informática (sitio web oficial): https://www.gadae.com/blog/politicas-de-seguridad-informatica/

PaloAlto Networks. (s.f.). *What is an IT Security Policy?* Recuperado el 7 de abril de 2022, de PaloAlto Networks | Cyberpedia | Search | Network Security (sitio web oficial): https://www.paloaltonetworks.com/cyberpedia/what-is-an-it-security-policy

Superintendencia de Industria y Comercio - SIC. (2018). *Inicio | Transparencia y acceso a la información pública*. Recuperado el 14 de noviembre de 2022, de Superintendencia de Industria y Comercio - SIC sitio web oficial: https://www.sic.gov.co/sites/default/files/files/Nuestra_Entidad/Transparencia_y_acceso_a_la_informacion_publica/SC05-I03%20ACTIVOS%20DE%20INFORMACION%20(1)%20(1).doc

UNIR. (5 de mayo de 2020). *Claves de las políticas de seguridad informática*. Recuperado el 10 de marzo de 2022, de Universidad Internacional de la Rioja, España - UNIR | Ingeniería y Tecnología (sitio web oficial): https://www.unir.net/ingenieria/revista/politicas-seguridad-informatica/

UNIR. (30 de abril de 2020). *Principios de la seguridad informática: consejos para la mejcra de la ciberseguridad*. Recuperado el 12 de marzo de 2022, de Universidad Internacional de la Rioja, España - UNIR | Ingeniería y Tecnología (sitio web oficial): https://www.unir.net/ingenieria/revista/principios-seguridad-informatica/

ES COPIA

PODER JUDICIAL
CORTE SUPREMA DE JUSTICIA
SECRETARIA GENERAL

Abg. Alex Almada Cáceres
Secretario Interino

ANEXO DE LA RESOLUCIÓN Nº…9906…..

Asunción, 3 de febrero de 2023.

Control de cambios

Versión	Fecha	Editor	Descripción de la actualización
18	03/02/2022	Marcelo Demestri	Modificaciones sugeridas por el Gabinete del Ministro Luis María Benítez Riera.
17	18/11/2022	Marcelo Demestri	Por pedido de la directora general Rosa Liz Chamorro, se ajusta el punto 3.6 ya que los juzgados utilizan servicios en la nube de terceros para almacenar su información y el punto 6.3 colocando al departamento de Patrimonio como el autorizante, ya que es responsable de la salvaguarda de los equipos informáticos y bienes institucionales.
16	14/11/2022	Marcelo Demestri	Modificaciones y ajustes en base a las sugerencias del Lic. Rubén Portillo en fecha 14/11/2022. Sección "Introducción", alcance de las políticas y su formalización en disposiciones, procedimientos, normativas, mecanismos e instructivos que las áreas responsables deberán crear para asegurar su oportuno cumplimiento. Edición en la redacción del punto 1.10, donde se amplían los requisitos de conocimientos y habilidades. Agregado del punto 1.11, estableciendo actualizaciones periódicas para los activos de información, con el acompañamiento del proveedor y/o fabricante. Edición en la redacción del punto 2.4, donde se agrega deshabilitar la cuenta de administrador local de los equipos y las revisiones periódicas del cumplimiento de esto. Edición en la redacción del punto 2.5, mecanismos de verificación.
15	27/09/2022	Marcelo Demestri	Modificaciones y ajustes en base a los comentarios remitidos por Francisco Zacarías en fecha 06/09/2022.
14	19/08/2022	Marcelo Demestri	Agregado de la responsabilidad de la Dirección de Ciberseguridad & Protección de la Información (DCPI) en el contenido de este reglamento y las necesidades de ajustes al mismo que puedan surgir, en el apartado "Políticas de seguridad informática del Poder Judicial". En base a la reunión mantenida con Francisco Zacarías el martes 16/08/2022, se establece como responsable de la

ES COPIA

PODER JUDICIAL * CORTE SUPREMA DE JUSTICIA * SECRETARIA GENERAL

Abg. Alex Almada Cáceres
Secretario Interino

ANEXO DE LA RESOLUCIÓN Nº...9906.....

Asunción, 3 de febrero de 2023.

			ejecución de la política 2.5 al Departamento de Asistencia Técnica & Soporte Informático.
13	11/08/2022	Marcelo Demestri	Arreglo de la sangría de los ítems numerados en las viñetas usadas en las secciones de políticas (las de 2 dígitos producían una sangría más grande). Marcación (resaltado del texto en amarillo) de los puntos más importantes a ser discutidos con Francisco Zacarías en la reunión pactada para el martes 16/08/2022. Correcciones menores y agregado del segundo párrafo en la sección "Políticas de seguridad informática del Poder Judicial".
12	08/08/2022	Marcelo Demestri	En base a la reunión con Casildo Miranda: se ajustó la redacción y se invirtió el orden de aparición de los puntos 10.1 y 10.2, haciendo hincapié en que la DGTIC solo será responsable de backups periódicos a servidores, sistemas y BD del PJ ; se agregó un párrafo en la sección inicial "Políticas de seguridad informática del PJ", que menciona sanciones en caso de incumplimiento del reglamento (queda pendiente el aporte de los abogados de DGTIC). De acuerdo a la retroalimentación de Zulma Villalba, edición en la redacción del punto 7.3 (Dpto. de Relevamiento e Implementación de Proyectos Tecnológicos)
11	21/07/2022	Marcelo Demestri	Edición en la redacción del punto 3.7, donde se aclara que la responsabilidad en la salvaguarda del espacio y el respaldo de los correos electrónicos entrantes y salientes de la cuenta institucional es responsabilidad del propio funcionario dueño de dicho correo institucional. Disgregación del punto 6.1, dejando lo relativo a las notebooks en un nuevo punto 6.2 y renumerando todos los ítems siguientes de esa sección, llegando ahora hasta el literal 6.5. La aplicación de lo requerido en el punto 7.2 se condiciona a factibilidad técnica y a los nuevos sistemas a ser desarrollados. Pequeñas ediciones al 8.3 y el 8.4, con agregado de área responsable de la DGTIC. Ajustes al texto del punto 10.2, para aclarar que los respaldos periódicos son solo para servidores y sistemas, no para equipos individuales.
10	15/07/2022	Marcelo Demestri	Ajustes en relación a los comentarios reportados en el documento de reunión de fecha 13/07/2022.
9	14/07/2022	Marcelo Demestri	Cambio de imagen de cabecera: ahora reza "Poder Judicial" y DGTIC.

ES COPIA

PODER JUDICIAL * CORTE SUPREMA DE JUSTICIA * SECRETARIA GENERAL

Abg. Alex Almada Cáceres
Secretario Interino

ANEXO DE LA RESOLUCIÓN Nº...9906.....

Asunción, 3 de febrero de 2023.

			Reemplazo (todo el documento) de las menciones a la "Corte Suprema de Justicia" (CSJ) por "Poder Judicial" (PJ). Se agregó "externo de servicios" al término "proveedor" para dar mayor claridad.
8	13/07/2022	Marcelo Demestri	Ajustes en sección "Alcance" (agregado ámbito de las Circunscripciones), "Acrónimos" (nuevos) y "Definiciones" (ajustes y correcciones varias a muchos de los ítems de esa sección). Se borra la redacción anterior del punto 2.6 y queda la nueva propuesta en la versión 6 de este documento (página 8/18).
7	08/07/2022	Marcelo Demestri	Nueva redacción para el punto 1.7 del tópico "1. Políticas orientadas a los dispositivos tecnológicos (Hardware) y aplicaciones informáticas (Software)", teniendo presente los comentarios de Francisco Zacarías en relación a una explicación más detallada de la casuística que lleva a necesitar de establecer este punto.
6	23/06/2022	Marcelo Demestri	Redacción de una alternativa más adecuada en redacción para reemplazar lo establecido en el numeral 2.6, página 7/16.
5	08/04/2022	Marcelo Demestri	Agregado de más reglamentación para el uso correcto del Correo Electrónico y las estaciones de trabajo. Agregado de la sección de Referencias del documento.
4	01/04/2022	Marcelo Demestri	Agregado de Políticas Generales de Seguridad Física.
3	28/03/2022	Marcelo Demestri	Reestructuración y agregado de políticas en las secciones respectivas.
2	15/02/2020	Marcelo Demestri	Correcciones y sugerencias.
1	06/01/2022	Francisco Zacarías	Versión inicial.

ES COPIA

PODER JUDICIAL
CORTE SUPREMA DE JUSTICIA
SECRETARIA GENERAL

Abg. Alex Almada Cáceres
Secretario Interino

ANEXO DE LA RESOLUCIÓN Nº 9906

Asunción, 3 de febrero de 2023.

Formalización

Actividad	Nombre	Cargo	Firma
Elaboró	Marcelo Demestri	Director – Dirección de Ciberseguridad & Protección de la Información (DCPI)	
	Francisco Zacarías	Jefe – Departamento de Infraestructura Tecnológica y Comunicaciones (DITC)	
Revisó	Marcelo Demestri	Director – Dirección de Ciberseguridad & Protección de la Información (DCPI)	
	Rubén Portillo	Jefe División – Dirección de Ciberseguridad & Protección de la Información (DCPI)	
	Rosa Liz Chamorro	Directora – Dirección General de Tecnologías de la Información y Comunicaciones (DGTIC)	
	Diego López	Director – Dirección de Soluciones Informáticas (DSI)	
	Zulma Villalba	Directora – Dirección de Administración de la Información (DAI)	
	Casildo Miranda	Asesor – Coordinación Técnica y Administrativa (CTA)	
Aprobó	Rosa Liz Chamorro	Directora – Dirección General de Tecnologías de la Información y Comunicaciones (DGTIC)	

ES COPIA

PODER JUDICIAL – CORTE SUPREMA DE JUSTICIA – SECRETARIA GENERAL

Abg. Alex Almada Cáceres
Secretario Interino