Procuración del Tesoro
de la Nación
República Argentina

POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

Autoridades

Procurador del Tesoro de la Nación

Dr. Rodolfo Carlos BARRA

Subprocuradores del Tesoro de la Nación

Dr. Marcos Sebastián SERRANO
Dr. Andrés DE LA CRUZ

Director de Coordinación Técnica y Administrativa

Dr. Valentín JALIL

Equipo de trabajo

Coordinación de Gestión Informática
Coordinación de Recursos Humanos
Estas Políticas de Seguridad de la Información han sido elaboradas por la Dra. Claudia Jara, Matias Pereira y la Lic. Maria de los Angeles Armelin.

Gestión de Versiones

Responsable	Fecha de redacción	Documento	Versión	Entrada en vigencia
Titular de la Coordinación de Gestión Informática	Diciembre 2024	Política de Seguridad de la Información	Versión 1.0	A partir de su aprobación por Resolución del Procurador del Tesoro de la Nación

INDICE

INTRODUCCIÓN

La PROCURACION DEL TESORO DE LA NACIÓN (en adelante PTN) reconoce la importancia de la gestión de la seguridad de la información y se compromete a proteger adecuadamente sus activos de información que, como otros bienes y servicios requeridos para el cumplimiento de sus objetivos, resulta esencial para el desarrollo de las actividades de su competencia.

Dicha información puede presentarse en diversos formatos (impresa o escrita en papel, almacenada electrónicamente, transmitida por correo o utilizando medios electrónicos o como contenido multimedia, 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.

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 de la PTN.

Dicho estado de protección adecuada se logra implementando un conjunto de mecanismos de seguridad o controles que incluyen entre otros, procesos, políticas, procedimientos, estructuras organizacionales, software y hardware; teniendo como objetivos la preservación de la confidencialidad, integridad y disponibilidad de la información.

Se declaran inicialmente las políticas generales de seguridad de la información. Posteriormente las políticas particulares, para consolidar la gestión de la seguridad de la información dentro de la PTN.

Objetivos

La presente POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN (en adelante, PSI) tiene como objetivos establecer un marco de referencia para la protección de la información y continuidad de los procesos y/o servicios, a través del resguardo de la confidencialidad, conservación de la integridad y mantenimiento de la disponibilidad de la información y de todos los recursos tecnológicos de la

PTN, utilizados en la transmisión, procesamiento y almacenamiento, frente a posibles amenazas internas o externas, deliberadas o accidentales.

Alcance

Esta PSI se aplica en todo el ámbito de la PTN, a sus recursos y a la totalidad de los procesos.

Debe ser comunicada fehacientemente y cumplida por todos los usuarios.

A fin de dar cumplimiento con la Decisión Administrativa 641/2021 de la JEFATURA DE GABINETE DE MINISTROS, una vez aprobada la PSI se le informará a la Dirección Nacional de Ciberseguridad.

Principios básicos

Los principios de la seguridad de la información, en base a la normativa vigente, son la confidencialidad, la integridad y la disponibilidad de la información a la que le da tratamiento y de los activos de información utilizados para la gestión.

Revisión y actualización

La PTN se compromete a revisar esta PSI anualmente, adaptándola a nuevas exigencias organizativas o del entorno, así como a comunicarla a los usuarios y a los terceros involucrados. También dispondrá las medidas necesarias para que esté a disposición de los alcanzados en todo momento.

Adicionalmente, procederá a su revisión y eventual modificación, cada vez que se produzca un cambio significativo en la plataforma tecnológica o bien una modificación de la normativa vigente aplicable.

La Coordinación de Gestión Informática (en adelante, CGI) es responsable de llevar adelante las revisiones, dejándose constancia de ellas.

Cumplimiento

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

POLÍTICAS GENERALES DE SEGURIDAD DE LA INFORMACIÓN

1. Organización de la Seguridad de la Información:

La PTN apoyará e impulsará las iniciativas de seguridad que se propongan con el objeto de preservar la confidencialidad, integridad y disponibilidad de la información que se gestiona y almacena.

Se establecerán responsables del cumplimiento de los distintos procesos y funciones asociados a la seguridad de los sistemas de información dentro de la PTN, como también la supervisión de los aspectos inherentes a la seguridad tratados en la presente política.

2. Recursos Humanos

La CGI notificará la existencia y el deber de cumplimiento de la PSI y de todas las normas, procedimientos y prácticas que de ella surjan.

Se establece que, ante el incumplimiento de la presente Política y los procedimientos que en consecuencia se aprueben, los usuarios serán pasibles de las sanciones que correspondieren de conformidad con la normativa vigente, y atendiendo las circunstancias del caso particular.

Todas las Unidades Organizativas velarán e impulsarán el cumplimiento de la PSI. Los Superiores Jerárquicos son responsables, ante la baja o cambio de puesto del usuario, que la información que estos posean sea transferida apropiadamente, antes de proceder a la baja o cambio de puesto del usuario, para evitar afectar el normal funcionamiento de las tareas en su ausencia.

Se establece el compromiso de concientizar y capacitar al usuario en temas referidos a las buenas prácticas en seguridad de la información, como también el de promover el entrenamiento especializado y frecuente de quienes desarrollan funciones en áreas de seguridad de la información de la PTN.

Las áreas técnicas responsable de este lineamiento son la CGI y la CRH.

3. Gestión de Activos Informáticos

La gestión y protección efectiva de los activos en función de su clasificación por criticidad es una prioridad para la PTN. Entre los activos se incluyen tanto el hardware como el software y 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 y se exige en caso de baja la devolución de los activos de información en su poder. En el mismo sentido, se procede a una eliminación segura de información en cualquier medio que pueda contenerla, para lo cual, se cuenta con procedimientos adecuados.

Las áreas responsables operativas de este lineamiento son la CGI y la Coordinación de Presupuesto, Contabilidad y Finanzas (en adelante, CPCyF).

4. Autenticación, autorización y control de Acceso

La PTN adopta los mecanismos necesarios para que solo el usuario autorizado acceda a los activos de información, bajo la premisa básica de que “Todo está prohibido a menos que se permita expresamente” para todos los activos. 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 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 los usuarios el uso responsable de los dispositivos y datos de autenticación otorgados por la PTN para el cumplimiento de sus funciones, que no los compartan y que los mantengan siempre seguros, tanto dentro como fuera del Organismo.

El área responsable operativa de este lineamiento es la CGI.

5. Acceso Remoto

Se establecerán conexiones seguras para el trabajo remoto de los usuarios que lo requieran según la necesidad, con sus pertinentes autorizaciones. Para ellos la CGI implementa el uso de VPN y realizará las configuraciones necesarias.

6. Seguridad

Se monitorean los accesos para permitir solo ingresos y egresos debidamente autorizados. Se mantiene un registro actualizado de los activos físicos que procesan información.

Se implementan y hacen cumplir medidas de seguridad para los activos físicos informáticos que deben llevarse fuera de la PTN, manteniéndose el registro correspondiente.

Se implementan y hacen cumplir medidas de seguridad para los activos físicos en soporte papel que deben llevarse fuera de la PTN, manteniéndose el registro correspondiente.

Las áreas responsables operativas de este lineamiento son la CGI, CPCyF y la Mesa de Entradas.

7. Seguridad operativa

Las operaciones de la PTN 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.

Las vulnerabilidades son gestionadas de manera apropiada y se controla la actividad de administradores y operadores.

Se realizarán los debidos backups de la información e infraestructura del Organismo.

Se llevará a cabo el seguimiento de los requerimientos realizados por los usuarios de la PTN mediante un sistema de tickets.

El área responsable operativa de este lineamiento es la CGI.

8. Seguridad de las comunicaciones

La PTN 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.

Se asignan cuentas institucionales a todos los usuarios, quienes están obligados a utilizarlas para toda comunicación vinculada a sus funciones.

El área responsable operativa de este lineamiento es la CGI.

9. Adquisición y gestión de hardware y software

La PTN llevará a cabo las tareas necesarias para la adquisición de equipamiento y software para que la infraestructura del Organismo esté actualizada y en óptimas condiciones para el correcto funcionamiento del mismo.

10. Relación con proveedores

La PTN incluye en los pliegos de bases y condiciones particulares cláusulas vinculadas a la seguridad de la información, de cumplimiento efectivo y obligatorio por parte de los proveedores y cocontratantes. Estas disposiciones consideran los aspectos pertinentes a la protección de la información y los servicios que se brinden, desde el inicio de la relación contractual y a perpetuidad. 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.

El área responsable operativa de este lineamiento es la Coordinación de Compras y Contrataciones (en adelante, CCyC).

11. Gestión de incidentes de seguridad

La PTN adopta las medidas necesarias para prevenir, detectar, gestionar, resolver y reportar los incidentes de seguridad que puedan afectar sus activos de información. Las debilidades en los procesos son debidamente comunicadas, identificadas y minimizadas de forma tal que se apliquen las acciones correctivas en el menor tiempo posible.

De detectarse un evento que podría constituir un incidente de seguridad, el mismo deberá ser comunicado a la CGI. De producirse el incidente, y que éste hubiera afectado información o datos personales de terceros, la PTN informará públicamente tal ocurrencia, de acuerdo a lo dispuesto por la normativa vigente.

El área responsable operativa de este lineamiento es la CGI.

POLÍTICAS PARTICULARES DE SEGURIDAD DE LA INFORMACIÓN

1. Organización de la Seguridad de la Información

La PTN asegura la implementación de la presente PSI.

Las responsabilidades operativas relativas a la seguridad de la información son asignadas a la CGI, que tendrá a su cargo la coordinación de todas las actividades tendientes a la implementación de la PSI.

Dicha Coordinación velará por una adecuada segregación de funciones, por un abordaje de la seguridad de la información en todos los proyectos y programas de la PTN y por la confección de adecuados procedimientos de seguridad.

La PTN se compromete a impulsar las iniciativas que el área competente proponga con el objetivo de preservar la confidencialidad, integridad y disponibilidad de la información que gestiona.

2. Recursos Humanos

2.1. Compromiso de confidencialidad

2.1.1. Alta de usuario.

La CGI pondrá a disposición de los usuarios el COMPROMISO DE CONFIDENCIALIDAD, el cual deberán suscribir, declarando conocer la existencia de la PSI, conforme el Anexo I.

Una vez producida el alta, la CRH enviará a la CGI una COMUNICACIÓN OFICIAL (en adelante, CCO) notificando el alta de acuerdo a los datos solicitados en los formularios respectivos de Alta, Baja o Modificación según corresponda, adjuntando la documentación respaldatoria (Formularios Anexo V; VI y VII).

El Área de soporte validará que la información de los formularios esté completa. En caso de no cumplir se solicitará a la CRH la documentación complementaria. Luego se continuará con el proceso de ingreso conforme la cláusula 4.7.1.

2.1.2. Permisos de Acceso

El Superior Jerárquico establecerá para todos los usuarios de su Unidad Organizativa, los permisos de acceso a la información y sistemas utilizados diariamente, de conformidad a lo establecido en la cláusula 4.5.2.

Si hubiese algún tipo de excepción el Superior Jerárquico lo solicitará vía CCO dirigido a la CGI.

2.1.3 Baja o Cambio de puesto de usuario

La CRH deberá informar a la CGI -con copia a CCyC y CPCyF- mediante una CCO la baja o cambio de puesto de los usuarios a los fines de garantizar el resguardo de los activos.

Ante la baja la CRH consultará a la CGI si el usuario tiene en su poder algún bien activo propiedad de la PTN.

La CGI deshabilitará los permisos de acceso a todos los sistemas y servicios de información utilizados por el usuario.

Ante un cambio de puesto de usuario se canalizará la gestión a través de la CRH. Asimismo, la CRH comunicara mediante una CCO a la CGI el cambio de puesto del usuario a fin de realizar las modificaciones de permisos de acceso que correspondieren, comprendiendo todos los permisos de accesos lógicos y físicos.

3- Gestión de Activos Informáticos

3.1. Inventario de activos

La CPCyF realiza el inventariado y el alta patrimonial de bienes tangibles e intangibles registrables.

Para ello, la CGI deberá informar a la CPCyF todos los activos adquiridos que resulten registrables.

3.2. Administración de activos

Cumplido el inventario, la CGI llevará un registro propio de los Activos a efectos de identificar la descripción de los mismos, su asignación, ubicación, traslado y estado de conservación.

3.3. Responsable de la gestión de los activos

El responsable de los activos será la CGI, quien deberá asegurar la clasificación y asignación de los mismos.

3.4. Asignación de activos

A partir de la aprobación de la presente, la CGI le hará firmar un ACTA DE ENTREGA según el ANEXO II con los datos de los activos asignados en la actualidad a todos los usuarios de la PTN.

Asimismo, al inicio del alta de un usuario y de acuerdo a las necesidades de las unidades organizativas de la PTN, la CGI asignará los activos al usuario que ingresa. A tal fin, realizará su instalación y puesta en marcha. Se le hará firmar un ACTA DE ENTREGA según el ANEXO II con los datos de los activos asignados.

El usuario será responsable del buen uso de los activos.

En caso de ser necesario que algún usuario retire un equipo de la PTN deberá ser requerido por su Superior Jerárquico mediante CCO dirigida a la CGI. La misma al entregar el activo le hará firmar un ACTA DE EGRESO DE EQUIPOS DE ESCRITORIO O NOTEBOOK según ANEXO IV.

3.5. Devolución de activos

La devolución de activos puede darse en dos supuestos:

En caso de baja, el usuario hará devolución de los activos que se le hubieran asignado para el cumplimiento de sus tareas conforme el ACTA DE DEVOLUCIÓN según ANEXO III.

En el caso de la devolución de un activo que había sido retirado de las instalaciones de la PTN se firmará el ACTA DE DEVOLUCIÓN según ANEXO III.

3.6. Cesión y/o Baja de activos

La CGI informará a la CPCyF sobre aquellos activos que se encuentren en estado de desuso o rezago a fin de llevar a cabo el procedimiento previsto en la normativa vigente.

4- Autenticación, autorización y control de Acceso

4.1. Usos Aceptables

4.1.1. Uso General

Los recursos tecnológicos de la PTN solo deben ser utilizados de modo que guarden relación con las tareas asignadas.

Los usuarios de los sistemas informáticos toman conocimiento que una cuenta de usuario representa una identidad digital. Por lo tanto, cada vez que se utilicen o se intentaren utilizar los recursos informáticos de los diferentes sistemas, se registrarán los accesos y/o actividades que se realizan con dicha cuenta de usuario. La contraseña utilizada para autenticar una cuenta de usuario, es de uso estrictamente personal y confidencial.

4.1.2. Uso del Equipamiento

La PTN proveerá a los usuarios las herramientas de hardware y software necesarias, siendo los mismos responsables de su uso y debiendo ser utilizados exclusivamente para propósitos relacionados con sus actividades diarias.

El usuario está obligado a dar el debido tratamiento para el cuidado de dichas herramientas, de forma tal de evitar cualquier daño, conexión, desconexión o traslado sin la debida autorización.

En el caso de la instalación de una Notebook en su puesto de trabajo la CGI colocará una Linga que se enlazará al escritorio asignado al usuario. Cada una tendrá un código de seguridad diferente que solo la CGI sabrá y se llevará un registro de las mismas.

En caso de requerir el traslado de una Notebook, de forma excepcional, por cuestiones operativas el superior Jerárquico del usuario deberá enviar un email a soporte@ptn.gob.ar para que quede registro en el sistema de Tickets y la CGI acuda a colocar el código de la Linga para el traslado de la misma. En ningún caso se le dará el código de la Linga al usuario.

4.1.3. Uso de los Sistemas de Software

Solo los usuarios que fueran autorizados podrán acceder a los sistemas y a la información de la PTN para el desarrollo de sus actividades. Cualquier acceso no autorizado o intento de acceso no autorizado será considerado como una posible violación a la PSI.

Los usuarios que por alguna razón consideren que necesitan accesos adicionales, deberán canalizar el pedido a través de su superior jerárquico, quien podrá solicitar por una CCO a la CGI el acceso correspondiente.

La CGI es responsable de la instalación, configuración, puesta en funcionamiento y mantenimiento de todo el equipamiento y software existente en la PTN.

Cuando las Unidades Organizativas requieran para el desempeño de sus tareas un software específico, deberán remitir la solicitud de adquisición y/o instalación mediante una CCO a la CGI. Todo aquel software que se encuentre instalado sin la debida autorización o almacenado en carpetas locales o compartidas que no guarde correspondencia con el software autorizado por la PTN será desinstalado y/o eliminado.

4.1.4. Uso de la Información

La información perteneciente a la PTN será utilizada únicamente dentro del marco de las actividades propias del organismo, quedando prohibida la utilización de la misma en beneficio propio y todo tipo de divulgación a terceros, sin previa autorización de las autoridades superiores.

La CGI se reserva el derecho de auditar los archivos en las carpetas de los usuarios, ya sea en los servidores compartidos como en los dispositivos de almacenamientos internos (discos locales de almacenamiento en las estaciones de trabajo) pertenecientes a la PTN, y podrá ser considerada información no deseada y ser pasible a ser borrada sin aviso previo.

Los usuarios en caso de baja o cambio de puesto, están obligados a entregar a su Superior Jerárquico, toda la información y documentos electrónicos que hubieran elaborado en el cumplimiento de sus tareas hasta el momento que la desempeñaban, de forma tal que dicha situación no genere problema alguno en la continuidad de las tareas que se venía desarrollando.

Todos aquellos archivos de documentos que se encuentren en carpetas locales o compartidas que no guarden relación con las tareas desempeñadas, podrán ser eliminados.

Queda prohibido realizar cualquier actividad contraria a los intereses de la PTN, así como también, difundir y/o publicar información reservada, confidencial o secreta, acceder sin autorización a recursos compartidos o archivos, e impedir el acceso a otros usuarios mediante el mal uso deliberado de recursos comunes.

Al que altere, destruya o inutilice datos, documentos, programas o sistemas informáticos; o venda, distribuya, haga circular o introduzca en el sistema informático, cualquier programa destinado a causar daños, serán pasibles de las sanciones que correspondieren de conformidad con la normativa vigente y atendiendo en cada caso la situación de revista y forma de contratación de cada usuario.

4.1.5. Uso de las Contraseñas

Los usuarios se comprometen a mantener las contraseñas en secreto. Cuando existiera indicio de que la confidencialidad de la contraseña hubiera sido comprometida, se informará y solicitará a la CGI el cambio de la misma, inmediatamente.

El usuario no podrá almacenar contraseñas en papel, archivos de texto, planillas de cálculo o cualquier aplicación cuya función no sea expresamente el almacenamiento seguro de contraseñas.

4.1.6. Uso del correo electrónico institucional

La cuenta de correo electrónico institucional de todos los usuarios del organismo se utilizará exclusivamente para toda comunicación vinculada con sus funciones.

4.2. Usos Inadecuados de los Recursos

Los recursos informáticos de la PTN se suministran con el propósito de asistir al usuario en la ejecución de sus tareas y en el correcto procesamiento de la información. Toda utilización de estos recursos con propósitos no autorizados o ajenos al destino para el cual fueron provistos será considerada como uso indebido.

4.3. Uso del Almacenamiento de Información por el Usuario

4.3.1. Almacenamiento Local

Los discos locales de los equipos informáticos no se utilizarán para uso personal. Cada usuario es responsable de administrar el espacio y resguardo seguro de la información que el equipo informático contenga. Por ello se indica que para el mantenimiento de una copia de resguardo es necesario almacenar los datos en el servidor de archivos que ofrece la CGI, para asegurar la existencia de una copia de resguardo en el caso que se lo requiera.

4.3.2. Almacenamiento en Repositorios de la PTN

Los archivos electrónicos relacionados con las tareas deberán almacenarse en servidor de archivos de la PTN, este servidor cuenta con una estructura de datos en la cual cada Unidad Organizativa cuenta con su respectiva carpeta compartida y solo los integrantes de la misma podrán acceder a sus datos. Asimismo, la estructura interna de las carpetas y sus respectivos permisos serán conformados por los Superiores Jerárquicos de acuerdo a la forma de trabajar de cada Unidad Organizativa.

La información almacenada en dicho servidor será asegurada a través de procesos de copias de resguardo establecidos por la CGI.

En caso de requerir la restauración de una copia de resguardo, el Superior Jerárquico del que depende el usuario deberá enviar una CCO a la CGI para iniciar el proceso de restauración de copias de resguardo.

4.3.3. Almacenamiento en Servicios Externos a la PTN

Está prohibido almacenar archivos laborales o documentos electrónicos de la PTN en los servicios de almacenamiento de Internet, ya que se expone al riesgo de pérdida de la confidencialidad de los mismos.

Cuando se requiera utilizar de forma excepcional un servicio de almacenamiento accesible desde Internet para compartir o almacenar archivos, el Superior Jerárquico de la Unidad Organizativa a la que pertenece el usuario deberá enviar una CCO a través del SISTEMA DE GESTIÓN DOCUMENTAL ELECTRÓNICA (en adelante, GDE), de uso obligatorio, a la CGI justificando la necesidad de dicho acceso.

4.4. Política de Control de Accesos

Se controlará el acceso a la información y a los recursos tecnológicos de la PTN, por lo cual se declara la:

a) Revocación o modificación de los derechos de acceso ante cambios de puesto o baja.
b) Revisión periódica de los permisos de acceso concedidos.

4.5. Gestión de Acceso de Usuario

4.5.1. Cuentas

Se utilizará una cuenta de usuario asociada a un usuario con una identificación unívoca para su uso personal exclusivo, de manera que las actividades puedan rastrearse con posterioridad a los fines de garantizar la trazabilidad de sus acciones.

Las cuentas de servicio se crean y utilizan para fines específicos de software y sistemas. Podrán estar asociadas y configuradas en más de un sistema y su alta, baja y modificación será responsabilidad de la CGI.

Se establecerá una revisión con el objeto de:

- Deshabilitar cuentas de usuarios de los sistemas principales de gestión de usuarios (controladores de dominio) inactivas.

- Deshabilitar las cuentas de usuarios redundantes o no identificables previo análisis de sus actividades.
- Las excepciones para evitar deshabilitar cuentas de usuario, deberán ser formalmente comunicadas por el solicitante a la CGI a través de una CCO.

4.5.2. Gestión de Permisos de Accesos

Se controlarán los permisos de acceso a los activos de información.

Se identificarán niveles de acceso de lectura, escritura o una combinación de ambos para los sistemas, bases de datos y aplicaciones.

Se priorizará el principio de asignación de mínimos privilegios, suficientes para realizar las tareas solicitadas.

4.5.3. Permisos de Acceso de Administrador

La asignación de permisos de acceso de administrador se concederá solo a los usuarios de la CGI. Los usuarios con permisos de acceso administrador podrán poseer dos cuentas de usuario, una para sus tareas habituales y otra para realizar estrictamente actividades que requieren estos permisos de acceso administrador.

No se deberá utilizar la cuenta de usuario con permisos de administrador para realizar actividades habituales como ser navegación en Internet o lectura del correo electrónico, sino que estas, sólo se utilizarán ante la necesidad de realizar tareas específicas que lo requieran, como ser de instalación, reconfiguración, contingencia y/o recupero.

4.5.4. Gestión Central de Contraseñas

Se establecerán mecanismos automáticos que permitan a los usuarios cambiar las contraseñas asignadas inicialmente, la primera vez que ingresan al sistema.

Se establecen como mínimo las siguientes características básicas de complejidad: longitud mínima de OCHO (8) caracteres, compuesta por mayúsculas, minúsculas, caracteres numéricos y caracteres especiales en su conformación.

Se configurarán los sistemas principales de gestión de usuarios (controladores de dominio) de forma tal que soliciten el recambio de la contraseña cada

CUARENTA Y CINCO (45) días, impidiendo la reutilización de la última contraseña.

4.6. Control de Acceso a Sistemas y Aplicaciones

4.6.1. Política de Restricción del Ingreso a los Sistemas e Información

Al igual que la política de control de accesos a las redes y servicios asociados se restringirá el acceso a la red interna, a los sistemas, base de datos y otros activos de información en base a la premisa “Todo acceso a la información y recursos tecnológicos está prohibido, a menos que se permita explícitamente”.

Los usuarios tendrán acceso solo a los sistemas y activos de información que hubieran sido específicamente autorizados.

La CGI autorizará el acceso a los sistemas, bases de datos y activos de información, mediante el pedido formal del Superior Jerárquico de la información a la cual se pretende acceder.

Esta autorización describirá detallada y explícitamente los permisos concedidos a los usuarios para acceder a los sistemas y activos de información.

4.6.2. Directivas para Asegurar los Inicios de Sesión

El acceso a los servicios de información se realizará a través de inicios seguros de sesión.

El mismo contempla:

a) Evitar mostrar mensajes de ayuda que pudieran asistir al usuario durante el procedimiento de conexión, que diera indicio del dato erróneo (usuario o contraseña) ante una autenticación incorrecta. Es decir, no divulgar ningún indicio que provea asistencia a usuarios aún no autenticados.
b) Validar la información de la conexión sólo al completarse la totalidad de los datos de entrada. Si surgiere una condición de error, el sistema no indicará que parte de los datos fue correcta o incorrecta.
c) Suscribir el compromiso de confidencialidad antes de acceder a los recursos tecnológicos de la PTN, consintiendo mediante esta firma su conocimiento y aceptación.
d) Registrar todas las conexiones exitosas y los intentos de conexión fallidas.
e) Evitar implementaciones que transmitan las contraseñas en texto plano sobre

la red de datos.

f) Implementar medidas para la protección ante ataques de fuerza bruta, como ser:
   - Bloqueo de la cuenta del usuario luego de TRES (3) reintentos fallidos.
   - Desbloqueo de la cuenta: en caso de tratarse de un usuario que está en las instalaciones de la PTN podrá solicitar el desbloqueo llamando al interno de soporte; en el caso de los usuarios que se encuentren en el interior del País podrán enviar un email desde su casilla personal, la cual será chequeada con el email registrado por la CRH en la Base de Datos, a la cuenta de soporte@ptn.gob.ar.

4.6.3. Uso de programas utilitarios privilegiados

Se prohíbe el uso de programas con capacidades de evasión de los sistemas de control y seguridad, como así también la búsqueda y evaluación de vulnerabilidades de seguridad sin el debido control y la autorización de la CGI.

4.7. Gestión de cuentas de Usuario

4.7.1. Alta

El alta consiste en la creación del usuario y sus respectivos permisos para poder acceder a los sistemas correspondientes que le permita desempeñar las tareas en la PTN.

La CGI procederá a crear la cuenta de usuario de acceso a la red de la PTN, la cuenta de email institucional, el usuario del GDE y permisos a las carpetas compartidas.

A continuación, la CGI confeccionará una CCO, que enviará a la firma al Superior Jerárquico de la Dirección de Coordinación Técnica y Administrativa, a fin de ser remitida a la Dirección General de Tecnologías de la Información y las Telecomunicaciones del Ministerio de Justicia o la que en un futuro la reemplace, solicitando la creación de las cuentas de usuario de los sistemas de administración por parte del citado Ministerio. Se pedirá la creación de usuario del Sistema Borges y en caso que el usuario ingresante sea SINEP se pedirá la creación de usuario del Sarha Online.

Cabe señalar que si el usuario va a realizar tareas en la CRH se solicitará también usuario del Sarha Unidad Registro, Sarha Unidad central, Sarha Unidad Intermedia y Sarha Unidad Central Consultas, Borges con permisos de carga de incidencias, Tramix y Admage. En el supuesto que el usuario realice tareas en la CPCyF se le pedirá el usuario del Sarha Unidad Haberes. En el caso de los sistemas de la administración financiera del Servicio Administrativo Financiero (SAF) de la PTN el Titular de la CPCyF es el administrador local de los mismos, siendo responsable de crear usuarios y otorgar los permisos pertinentes para el uso del e-Sidif, BNA (Banco de la Nación Argentina), del BI (Business Intelligence) y el SIRHU.

Para el caso del Sistema Compr.ar el Titular de la CCyC mediante una CCO dirigida a la Oficina Nacional de Contrataciones (ONC), realiza el pedido de alta de un usuario al sistema.

Los permisos de acceso asignados se limitan al sector de la PTN definido en el formulario.

Una vez creada la cuenta de usuario se procederá a configurar la misma en el EQUIPO DE ESCRITORIO O NOTEBOOK que le haya sido asignada al usuario. Se le configurará: el email institucional, el acceso a las carpetas compartidas, la instalación de las impresoras, etc.

4.7.3. Baja

Se eliminarán los permisos de acceso de los usuarios una vez cumplido el procedimiento indicado en la cláusula 2.1.3.

Así, el área de soporte o el área de Infraestructura realizará la deshabilitación de la cuenta de usuario en los sistemas de la PTN (Correo Electrónico, Carpeta Compartida, EQUIPOS DE ESCRITORIO O NOTEBOOK, Acceso Remoto).

La CGI dará de baja la cuenta de usuario del sistema GDE.

La CGI confeccionará una CCO, que enviará a la firma al Superior Jerárquico de la Dirección de Coordinación Técnica y Administrativa, a fin de ser remitida a la Dirección General de Tecnologías de la Información y las Telecomunicaciones del Ministerio de Justicia o la que en un futuro la reemplace, solicitando la baja de las cuentas de usuario de los sistemas de administración por parte del citado Ministerio.

La CPCyF deberá dar de baja, de corresponder los usuarios en el Sistema e-Sidif, BNA, del BI (Business Intelligence) y el SIRHU.

Para el caso del Sistema COMPR.AR el Titular de la CCYC mediante una CCO dirigida a la Oficina Nacional de Contrataciones (en adelante, ONC), realiza el pedido de baja del usuario al sistema.

El área de Soporte retirará el EQUIPO DE ESCRITORIO O NOTEBOOK para reconfigurarlo será fin de poder ser reutilizado.

4.7.4. Modificación

La modificación consiste en un cambio en la cuenta de usuario.

El área de soporte o el área de Infraestructura modificarán la cuenta de usuario en los sistemas de la PTN, como ser la cuenta de Correo Electrónico, los Grupos de Distribución, las Carpeta Compartida, el usuario de GDE y EQUIPOS DE ESCRITORIO O NOTEBOOK de ser necesario.

5. Acceso Remoto

En el caso que un usuario tenga la necesidad de contar con un acceso remoto deberá ser previamente autorizado por su Superior Jerárquico mediante CCO.

Todo acceso remoto será implementado mediante una conexión cifrada, la cual será monitoreada y controlada por los dispositivos de seguridad de la CGI, implementando restricciones de acceso a determinados activos de información dependiendo de la criticidad de la misma y perfil del usuario.

Se establecerán factores de autenticación para asegurar la identidad de las conexiones remotas a las redes privadas virtuales (VPN) de la PTN.

6- Seguridad

6.1. Seguridad de Oficinas e Instalaciones

Se controlará el ingreso y egreso a las sedes del Organismo mediante personal de seguridad correspondiente.

6.1.1. Protección contra amenazas de origen ambiental, internas y externas

Existirá control de acceso en las entradas de la sala del centro de procesamiento de datos con el objeto de contrarrestar cualquier amenaza interna o externa que pusiera en peligro los activos y operaciones de la PTN.

6.2. Seguridad de los equipos

6.2.1. Ubicación y Protección de Equipos

El centro de cómputos será de acceso restringido y deberá permitir la supervisión constante a los fines de minimizar el riesgo de amenazas potenciales por robo, hurto, incendio, polvo, calor y radiaciones electromagnéticas.

Se establece que está prohibido comer, beber y fumar dentro del centro de cómputos, la sala de comunicaciones, como también está prohibido tomar fotografías o realizar grabaciones sin la debida autorización.

6.2.2. Seguridad en el Suministro Eléctrico

Los centros de procesamientos de datos y las salas de comunicaciones estarán protegidos ante posibles fallas en el suministro de energía u otras anomalías eléctricas. La continuidad del suministro de energía se realizará por medio de la existencia de equipamiento de Suministro de Energía Ininterrumpible (UPS) y el uso de Generador de Energía Eléctrica de respaldo.

Se deberá contar con la iluminación de emergencia en caso de falla en el suministro principal de energía.

6.3. Mantenimiento del Equipamiento Informático

6.3.1. Ingreso y Egreso de Equipos de Escritorio o Notebook

Se registrará el ingreso y egreso de Equipos de Escritorio o Notebook.

En el caso de necesitar retirar un equipo de escritorio de las instalaciones de la PTN y a fin de proceder a su egreso, el Superior Jerárquico de la Unidad Organizativa requirente deberá comunicar el mismo mediante CCO a la CGI, correspondiendo suscribir un ACTA DE EGRESO DE EQUIPOS DE ESCRITORIO O NOTEBOOK (Anexo IV). Asimismo, la CGI registrará dicho egreso.

6.3.2. Seguridad de los Equipos fuera de las Instalaciones

Los usuarios deberán respetar el cuidado de los activos siguiendo las pautas de la cláusula 4.1.

En caso de robo o hurto, el usuario al cual se le hubiera asignado el bien deberá efectuar una denuncia policial en donde se proporcionen los datos del bien sustraído.

Asimismo, deberá enviar un memorándum, comunicando los hechos a la CGI, con copia a su Superior Jerárquico, remitiendo como archivo embebido la denuncia policial. A su vez, el usuario comunicará a los grupos de trabajo a los cuales potencialmente podría comprometer la información almacenada en el dispositivo.
Recibido el Memorándum, la CGI procederá al blanqueo de la contraseña de la cuenta de usuario asociada; y solicitará la apertura de un Expediente Electrónico al cual vinculará la documentación remitida por el usuario, y el ACTA DE ENTREGA suscripta oportunamente.
Mediante una PV remitirá las actuaciones a la CPCyF, a efectos de solicitar la baja definitiva del bien en cuestión conforme la normativa vigente.

6.3.3. Reutilización o Baja de Equipamiento Informático

Se deberán aplicar operaciones de borrado seguro a todo equipamiento informático, antes de que el mismo sea normalizado para su reutilización o fuera dado de baja, previo resguardo de la información útil o licencias alojadas en dicho equipamiento.

6.3.4. Equipos Desatendidos y Pantallas Limpias

Los usuarios deberán cerrar las sesiones de las aplicaciones, sistemas y servicios de red, cuando no estén siendo utilizados y son desatendidos.
Los usuarios al ausentarse momentáneamente de su puesto de trabajo deberán cerrar las sesiones activas o en su defecto, bloquear el equipo informático para evitar el acceso indebido al mismo en su ausencia. Este cierre o bloqueo deberá realizarse aun cuando se establece el bloqueo automático de las pantallas de las estaciones de trabajo y servidores en todo equipo que se encuentre desatendido.

6.3.5. Escritorios Limpios

Los usuarios deben proteger la información no pública que utilizan en sus tareas diarias, no exponiendo documentación en papel sobre su puesto de trabajo de manera desatendida.
Toda documentación en papel información reservada, confidencial o crítica deberá mantenerse resguardada.

7- Seguridad operativa

7.1. Política de Dispositivos Personales

No podrán ser conectados a la red física del Organismo, solo pudiendo conectarse a la red Wifi disponible provista por la PTN, no pudiendo ingresar a los servidores y archivos compartidos.

7.2. Protección contra Código Malicioso

Se protegerán los sistemas tecnológicos mediante la implementación de controles para prevenir, detectar, eliminar y recuperar los sistemas afectados por código malicioso. Los sistemas de detección de código malicioso deberán estar instalados y actualizados en todas las estaciones de trabajo y servidores que conforman la infraestructura tecnológica de la PTN.

Se controlará todo tráfico de carga y descarga de archivos y el control en los correos electrónicos con archivos adjuntos o accesos sitios de Internet, con el objeto de evitar la ejecución de código que pudiera dañar o alterar el normal funcionamiento de la infraestructura tecnológica del PTN.

Se ejecutarán periódicamente análisis preventivos para la detección y eliminación de código malicioso en los servidores y estaciones de trabajo.

7.3. Copias de Seguridad, Resguardo y Restauración

Se establecerán procedimientos para las actividades de Copia de Resguardo y Restauración, debiendo ser los mismos revisados y actualizados cuando se requiera. Se definirá un esquema de rotulado de las copias de resguardo, que permita contar con toda la información necesaria para identificar y administrar cada una de ellas debidamente.

Se almacenará en una ubicación remota del origen, las copias de resguardo junto con registros exactos y completos de las mismas a una distancia suficiente como para evitar daños provenientes de un desastre en el sitio origen de la copia.

Se verificarán la efectividad de los procedimientos de copias y restauración, asegurándose que cumplan con los requerimientos de los planes de continuidad de las actividades, a los efectos de minimizar las posibles interrupciones de las mismas (sean éstas resultado de desastres naturales, accidentes, fallas en el equipamiento, acciones deliberadas u otros hechos).

Se establecerá el cifrado de las Copias de Resguardo.

Se establece la siguiente periodicidad para la realización de copias de resguardo:

a) Una copia diaria incremental de la infraestructura critica almacenada en los servidores desde la última copia completa a un Servidor de Almacenamiento (NAS) para tal fin.

b) Una copia semanal completa resguardada en el Servidor de Almacenamiento (NAS).

c) Una copia completa mensual bajada a medio extraíble, es decir a cinta magnética.

Se establecerá el siguiente alcance, como mínimo, para realizar copias de seguridad de los activos de información de los entornos en Producción de:

a) Las máquinas virtuales completas en ejecución dentro de los servidores físicos.

b) Los servidores de base de datos.

c) Los servidores de repositorios y recursos compartidos que almacenan archivos de los usuarios.

d) Los servidores de correo electrónico.

7.4. Gestión de Vulnerabilidades

7.4.1. Vulnerabilidades Técnicas y Remediación

Se instalarán las actualizaciones de seguridad de forma automática de los sistemas operativos y se implementarán directrices de configuraciones seguras.

Se establecerán escaneos periódicos en busca de vulnerabilidades de seguridad sobre la infraestructura de la PTN.

7.4.2. Restricciones en la Instalación de Software

Se prohíbe la instalación de software en las estaciones de trabajo que no sea autorizada por la CGI, ya que la instalación no controlada de estos en sistemas informáticos puede dar inicio a la introducción de vulnerabilidades, fuga de información, falta de integridad u otros incidentes de seguridad.

7.5. Almacenamiento en servidores

A través del Área de Infraestructura se gestionará el resguardo de la información en los servidores de la PTN.

7.5.1. Análisis de capacidad de almacenamiento

La CGI revisará regularmente la capacidad de almacenamiento de los servidores para determinar la necesidad de su incremento. Esto puede incluir el monitoreo de los niveles de ocupación de disco y la identificación de archivos o aplicaciones que estén utilizando una gran cantidad de espacio.

7.5.2. Planificación de expansión de almacenamiento

Frente a la necesidad de contar con mayor almacenamiento, será la CGI la encargada de proyectar el modo de expansión de almacenamiento y seleccionará el modo más conveniente.

7.5.3. Redundancia

La CGI configurará los discos duros en un sistema RAID (Redundant Array of Independent Disks) a fines de proporcionar una mayor seguridad y disponibilidad del almacenamiento o bien otra tecnología superadora.

7.5.4. Configuración de respaldo

La CGI elaborará los procedimientos de respaldo para garantizar la seguridad de la información almacenada en los servidores. Esto incluirá la configuración de copias de seguridad automatizadas a disco y cinta.

7.5.5. Monitoreo y mantenimiento

La CGI deberá monitorear regularmente el almacenamiento en los servidores y realizar el mantenimiento necesario para garantizar que los servidores estén funcionando correctamente. Esto deberá incluir la verificación de errores en los discos duros y la optimización de los sistemas de almacenamiento.

7.5.6. Análisis y mejora continua

La CGI analizará regularmente el almacenamiento en los servidores para identificar tendencias y áreas de mejora conforme el análisis realizado, implementará cambios para alcanzar un mayor índice de eficacia y eficiencia del almacenamiento en los servidores.

7.6. Soporte a usuarios.

7.6.1. Creación del ticket

El ingreso al Sistema de Tickets de la Coordinación de Gestión Informática, se realiza ingresando a http://tickets.ptn.gob.ar. El ingreso se realiza con el mismo usuario y contraseña con la que se ingresa al equipo de la PTN.

El usuario envía un email a soporte@ptn.gob.ar solicitando asistencia técnica y automáticamente se genera un nuevo ticket en el sistema.
También se puede crear un nuevo ticket desde el mismo sistema ingresando desde la WEB arriba mencionada.
Al momento de la creación de un nuevo ticket el sistema manda un correo electrónico al usuario solicitante informándole de la creación del mismo.

7.6.2. Asignación del ticket

Una vez creado el ticket será asignado a un usuario de la CGI con conocimiento en el tema a ser tratado.

7.6.3. Análisis y resolución

El usuario de la CGI que tenga asignado el ticket realizará un análisis del ticket y se procederá a la solución del mismo.

7.6.4. Cierre del ticket y documentación de la solución

Una vez resuelto el requerimiento la CGI dará cierre al ticket, dejando constancia de la solución adoptada, a los fines de identificar tendencias y áreas de mejora en el proceso de soporte.

8- Seguridad de las comunicaciones

8.1. Uso de Internet

La PTN otorga acceso a Internet para mejorar y facilitar la actividad de sus usuarios, a efectos de acceder a información técnica, comunicación con otros organismos oficiales, instituciones académicas y/o accesos relativos a temas inherentes con las tareas que realizan.

El servicio de acceso a Internet es restringido y controlado, ya que se bloquean sitios clasificados con determinadas categorías. Por ello, con el objeto de minimizar el riesgo de violación a la seguridad a través del uso incorrecto del servicio de Internet, se encuentran prohibidas las siguientes acciones:

a) Evadir los controles de navegación por medio de software especializado o por medio de sitios de terceros que actúan como servidores intermediarios (proxies externos).
b) El uso de streaming para entretenimiento.
c) La descarga de archivos de software sin la debida autorización.

d) El incumplimiento de lo dispuesto por la Ley N° 11.723 de Propiedad Intelectual.
e) Distribuir software malicioso (malware).
f) Acceder a material pornográfico, actividades lúdicas o de entretenimiento, diversión o pasatiempos de similar tenor, páginas que promuevan el odio, el racismo, inciten a la violencia o con contenido contrario a las normas de orden público y buenas costumbres.
g) Emitir comentarios o brindar información en redes sociales sobre incidentes de seguridad acaecidos dentro de la PTN.
h) Atentar contra la infraestructura tecnológica de terceros y/o de la PTN.

8.2. Monitoreo y Auditoría

El uso del equipamiento, los sistemas y la información que componen la infraestructura tecnológica será monitoreado y/o auditado mediante herramientas de seguridad, comprendiendo dicha actividad el uso de los equipos informáticos, tráfico de la red de datos, accesos a sistemas y bases de datos, uso de Internet y del correo electrónico, con las limitaciones que las disposiciones legales imponen en cuanto al respeto de la privacidad.

8.3. Uso del Correo Electrónico

8.3.1. Correo Electrónico

El usuario se compromete a cumplir con la normativa aplicable y es el único responsable de todos los actos u omisiones que sucedan en relación con su cuenta de correo electrónico y/o contraseña.

El servicio de correo electrónico es para uso laboral, debiendo ser usado únicamente para el desempeño de sus funciones.

Los correos electrónicos enviados y recibidos por los usuarios serán controlados por los sistemas de seguridad antimalware y antispam, para minimizar el riesgo de recibir y enviar por este medio, correos y/o adjuntos maliciosos que pudieran vulnerar la seguridad de la infraestructura tecnológica del PTN.

El espacio de almacenamiento de mensajes en el servicio de correo electrónico es limitado, esto significa que el servicio cumple la función de recepción y envío mientras tenga espacio suficiente para tal operación, por lo que el usuario debe gestionar los mismos de manera adecuada.

Con el objeto de mejorar la gestión y seguridad del correo electrónico se requiere el cumplimiento de las siguientes directivas:

a) No adjuntar en los correos electrónicos archivos que puedan presentar un riesgo a la seguridad de la información. A saber: programas ejecutables, librerías, scripts, macros, y archivos multimedia, o los que en un futuro la CGI pueda considerar un riesgo.
b) No adjuntar archivos de más de 15 Mb.
c) Periódicamente mover los mensajes enviados y recibidos a Carpeta Locales del usuario del correo electrónico, a fin de mantener la casilla de correo con el espacio usado por debajo de su límite para evitar inconvenientes de denegación del servicio por falta de espacio.
d) Evitar escribir el texto del “Asunto” en mayúsculas, debido a la posibilidad de que los sistemas antispam de los destinos cataloguen el correo como spam.
e) Comunicar al área de Soporte aquellos correos que consideren como “maliciosos” o catalogados como “spam” para contribuir a mejorar los sistemas antimalware y antispam.
f) No abrir ni guardar localmente correos de origen desconocido que contengan archivos adjuntos.
g) Evitar acceder a los enlaces embebidos en los cuerpos de los correos recibidos, para no caer en correos maliciosos de ataques de phishing. En caso de duda consultar a los usuarios de la CGI.

8.3.2. Firma de Correo Electrónico

Los correos electrónicos que sean enviados mediante el correo institucional deberán contener al pie del mismo, la firma respectiva del usuario indicando nombre, función, correo electrónico, domicilio, teléfono y Unidad Organizativa -en caso de corresponder Coordinación- a la cual pertenece.

8.3.3. Envío de Correos Electrónicos Masivos

8.3.3.1. Externo

Se define como el envío de correo electrónico masivo externo a todo mensaje que es enviado simultáneamente a más de CIEN (100) casillas. Superado dicho umbral los correos serán bloqueados, salvo expresa autorización.

8.3.3.2. Interno.

Las áreas que por razones inherentes a sus funciones necesitaren realizar una comunicación masiva a todos los usuarios de la PTN mediante el envío de un correo electrónico, deberán solicitarlo a través de un pedido formal mediante el envío de un email a soporte@ptn.gob.ar.

8.4. Gestión en la Seguridad en las Redes de Datos

8.4.1. Seguridad en las Redes

Se documentará la información referida a topologías de redes internas, externas, redes de interconexión con otros organismos y enlaces de proveedores de servicios de Internet.

Se establecen las reglas de acceso sobre la premisa “Todo acceso a la información y recursos tecnológicos está prohibido, a menos que se permita explícitamente”.

Los usuarios deberán tener acceso solo a las redes respecto a las cuales hubieran sido específicamente autorizados.

Se deberán monitorear y registrar las actividades en la red de manera preventiva, para lo cual se definirán controles que inspeccionen los paquetes de datos que circulan en la red con el objeto de detectar tráfico indebido que pueda vulnerar la seguridad de los sistemas informáticos.

Se limitará la navegación de Internet para evitar comprometer el rendimiento y/o estabilidad del acceso a la misma.

Se controlará el tráfico de datos interno y externo de la red informática mediante dispositivos de seguridad que controlen activamente las comunicaciones con origen y destino autorizados.

Se implementarán controles para mantener la alta disponibilidad de los servicios de red y equipamiento informático interconectado.

Las conexiones externas hacia equipos internos estarán restringidas y sujetas al cumplimiento de procesos de aprobación del responsable.

Se implementarán mecanismos de autenticación cifrada a las conexiones que accedan mediante redes privadas virtuales (VPN) a la infraestructura interna de a PTN.

Se promoverá el uso de certificados digitales para validar los extremos de la conexión. Las conexiones externas estarán cifradas por medio de algoritmos actualizados.

8.4.2. Nivel de Acuerdo de Servicios en Redes y Telecomunicaciones

Se establecerá el acuerdo de Nivel de Servicio para las redes internas con las siguientes características: disponibilidad del 99%, velocidad 100 Mbps como mínimo, segregación de redes y seguridad de puertos, existencia de procedimiento para verificar conectividad y escalamiento hasta nivel 3 (especialista en redes y comunicaciones) para resolución de problemas.

9. Adquisición y gestión de hardware y software

Será la DCTA quien tome intervención en aquellos supuestos de adquisición y mantenimiento de los sistemas y programas informáticos necesarios para el funcionamiento de la PTN.

En ese sentido, la CGI deberá encargarse del asesoramiento para identificar las tecnologías disponibles en el mercado, métodos de adquisición, especificaciones técnicas, informes técnicos, al tiempo que operarán como interlocutores entre el organismo y la Oficina Nacional de Tecnologías de Información en aquellos procesos en que por normativa requiera su intervención.

10- Relación con proveedores

El Organismo incluye en los pliegos de bases y condiciones particulares cláusulas vinculadas a la Seguridad de la Información, de cumplimiento efectivo y obligatorio por parte de los proveedores o cocontratantes.

Estas disposiciones consideran los aspectos pertinentes a la protección de la Información y los servicios que se brinden.

11- Gestión de incidentes de seguridad

11.1. Procedimientos y Responsabilidades

Se establece que la CGI tiene la facultad para acceder a todo sistema, dispositivo o equipamiento tecnológico involucrado en alertas de seguridad que considere apropiado, para analizar un incidente, evitar que escale y afecte la disponibilidad, confidencialidad e integridad de la información o de los sistemas

de la PTN como también para realizar actividades forenses luego que hubiera ocurrido un incidente.

11.2. Comunicación de Alertas o Incidentes de Seguridad

Se establece la obligatoriedad de comunicar cualquier alerta o incidente de seguridad, tan pronto como estos sean detectados, enviando un email a soporte@ptn.gob.ar.

11.3. Comunicación de Debilidades de Seguridad de la Información

Todos los usuarios de la PTN deberán informar cualquier debilidad de seguridad sospechada o detectada en los sistemas o servicios del Organismo.

Se prohíbe que los usuarios intenten buscar o probar dichas debilidades de seguridad detectadas o sospechadas, por medio de cualquier software de evaluación de vulnerabilidades o pruebas de penetración. Tal actitud se podrá interpretar como un intento de violación a la seguridad de los sistemas de la PTN.

La CGI reportará a la Dirección Nacional de Ciberseguridad de la Secretaria de Innovación Publica, mediante el CERT.ar (https://www.argentina.gob.ar/jefatura/innovacion-publica/ssetic/direccion-nacional-ciberseguridad/cert-ar/reportar-un-incidente), los eventuales incidentes de seguridad que se produzcan dentro de la PTN, dentro de las 48 horas de tomado conocimiento de su ocurrencia o de su potencial ocurrencia.

11.4. Evaluación de los Eventos y Análisis de los Incidentes de Seguridad de la Información

Se deberá proceder a la evaluación inicial de los eventos de seguridad catalogados como incidentes y analizar su impacto y urgencia de resolución. Por ello se establecerán criterios de priorización de incidentes dependiendo del sistema, servicio, información o usuario afectado.

11.5. Respuesta a los Incidentes de Seguridad

Ante incidentes de seguridad se llevará a cabo la recopilación, el registro de evidencias para su evaluación inicial, el análisis de incidente, acciones de remediación, aprendizaje del incidente y análisis forense para profundizar su estudio y confirmar la causa. Posteriormente, se comunicará el estado de situación de la resolución a todos los usuarios con incumbencia.

11.6. Aprendizaje de los Incidentes de la Seguridad

Se documentará la resolución del incidente, con el objeto de identificar y evaluar aquellos que sean recurrentes o de alto impacto, a efectos de mejorar y agregar controles para limitar la frecuencia, daño y costo de futuros similares.

Se documentarán todas las fallas encontradas en los procedimientos descriptos u operaciones desarrolladas y los inconvenientes detectados para su resolución.

GLOSARIO

ACTIVO: A los efectos de esta PSI, los activos refieren a cualquier dato, aplicación equipos informáticos, personal, soportes de información, redes, equipamiento auxiliar o instalaciones, entre otros.

ÁREA DE INFRAESTRUCTURA: Responsables de la CGI de la gestión del hardware de servidores, software de base de servidores, redes y comunicaciones, y la seguridad de la PTN.

ÁREA DE SOPORTE: Responsables de la CGI de la gestión del equipamiento informático de usuarios y gestión de software de usuarios de la PTN.

CÓDIGO MALICIOSO: Es un tipo de software que tiene como objetivo dañar o infiltrarse sin el consentimiento de su propietario en un sistema de información. Palabra que nace de la unión de los términos en inglés de software malintencionado: malicious software.
Algunos ejemplos comunes de malware incluyen Virus, Gusanos (worms), Troyanos (Trojan horse), Ransomware, Spyware, Adware, etc.

CONFIDENCIALIDAD: Garantiza que la información sea accesible sólo a aquellas personas autorizadas a tener acceso a ésta.

DATOS: Elementos básicos de información que pueden ser representados en forma numérica, textual, gráfica, visual o cualquier otro formato legible por una computadora u otro sistema.

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.

INVENTARIO: Refiere al registro y control de los activos físicos e intangibles.

MEDIDAS DE SEGURIDAD: Conjunto de acciones tendientes a proteger a la información de una amplia gama de amenazas, a fin de garantizar la continuidad de los sistemas de información y de la operación de la PTN, minimizar los riesgos de daño y asegurar el eficiente cumplimiento de los objetivos del Organismo.

RECURSOS INFORMÁTICOS: Se refieren a los activos, herramientas y tecnologías utilizadas para respaldar y facilitar las operaciones y servicios mediante el uso de sistemas informáticos y tecnología de la información.

SUPERIOR JERARQUICO: Directores Nacionales, Subdirectores Nacionales y Directores Simples.

UNIDAD ORGANIZATIVA: Direcciones Nacionales y Direcciones Simples de la PTN.

USUARIO: Persona que hace uso de los servicios informáticos de la PTN.

ANEXO I: COMPROMISO DE CONFIDENCIALIDAD

ALCANCE: La POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN (PSI) es de aplicación obligatoria para todos los usuarios de la PROCURACIÓN DEL TESORO DE LA NACIÓN.

El / La que suscribe , DNI N.° ……., declaro conocer y aceptar medidas de seguridad y confidencialidad de la información amparadas en la PSI aprobada por Resolución N.° xxxxxxxxxx y sus respectivos Anexos.

Mediante la suscripción del presente instrumento, me comprometo a guardar la máxima reserva y secreto sobre los datos e información a que acceda en virtud de las tareas encomendadas, a utilizar dicha información solamente para el fin específico al que se la ha destinado, a no comunicar o hacer pública la información no clasificada como "pública" o de carácter confidencial, y a observar y adoptar cuantas medidas de seguridad sean necesarias para asegurar la confidencialidad, integridad, disponibilidad y legalidad de la información, salvo autorización previa y escrita del Superior Jerárquico.

De acuerdo a lo establecido en la "Clausula 3 - Gestión de Activos Informáticos" de la PSI, me comprometo a seguir las reglas para el uso aceptable de la información y los activos asociados con las instalaciones de su procesamiento, incluyendo:

Correo electrónico e internet

Equipos de Escritorio o Notebook

Software

A fin de mejorar el funcionamiento y la seguridad de los recursos de este Organismo, presto conformidad ante el requerimiento de que las actividades y funciones desarrolladas puedan ser objeto de control y monitoreo por parte de la CGI.

Esta obligación de reserva y confidencialidad seguirá en vigencia aún después de operada la baja asumiendo la responsabilidad penal, administrativa o civil de los daños y perjuicios que por dolo o negligencia pudiera ocasionar la difusión de datos o información no publicados.

Lugar y fecha

Firma Aclaración **Tipo y N° de doc.**

ANEXO II: ACTA DE ENTREGA N°

En el día de la fecha, en mi carácter de representante de la COORDINACIÓN DE GESTIÓN INFORMÁTICA (CGI) de la PROCURACIÓN DEL TESORO DE LA NACIÓN (PTN), se hace entrega del equipo detallado al pie de la presente, a……, DNI ……, perteneciente a ……. (indicar Unidad Organizativa de la PTN).

En caso de baja o bien si las autoridades superiores de la PTN lo dispusieran, deberá hacer entrega de el/los equipo/s en la CGI, donde deberá suscribir un acta de devolución de los mismos.

1) El usuario no podrá bajo ningún concepto:

Abrir el/los equipo/s para proceder a ninguna clase de reparación por su propia cuenta.

Utilizar accesorios o componentes que no sean del equipo o accesorios que no sean originales.
Proceder a la carga de ninguna clase de Software, que no estuviera aprobado por la CGI.

Ceder en calidad de préstamo ningún equipo o componente del mismo a otro usuario del Organismo, sin previo consentimiento de la CGI.
Pedir reparaciones por su propia cuenta.

2) En caso de hurto y/o robo deberá cumplir con el procedimiento establecido en la POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN de la PTN.

3) Al momento de la devolución de bienes, los mismos deberán encontrarse en condiciones operativas normales conjuntamente con todos los componentes y/o accesorios entregados.

CANTIDAD	DESCRIPCIÓN	MODELO	N° SERIE	N° INVENTARIO	OBSERVACIONES

La entrega se efectúa de entera conformidad por parte del usuario aceptando la totalidad de los términos expresados en la presente y en pleno conocimiento de la PSI.

En virtud de lo expuesto, se firma la presente Acta entre las distintas partes involucradas.

Lugar y fecha:

Firma del CGI **Aclaración** **N° de DNI**

Firma del usuario **Aclaración** **N° de DNI**

ANEXO III: ACTA DE DEVOLUCIÓN

En el día de la fecha, ……/……/……..., ……, quien suscribe, en su carácter de …… deja constancia que se recepcionó el equipo y accesorios detallados al pie de la presente que fuere entregado mediante ACTA DE ENTREGA N° ……de fecha ……

CANTIDAD	DESCRIPCIÓN	MODELO	N° SERIE	N° INVENTARIO	OBSERVACIONES

Lugar y fecha:

Firma del CGI **Aclaración** **N° de DNI**

ANEXO IV: ACTA DE EGRESO DE EQUIPOS DE ESCRITORIO O NOTEBOOK

En el día de la fecha, ……/……/……..., ……, quien suscribe, en su carácter de …… autoriza la salida del equipamiento tecnológico que se detalla a continuación:

CANTIDAD	DESCRIPCIÓN	MODELO	N° SERIE	N° INVENTARIO	OBSERVACIONES

El retiro de equipamiento obedece a los siguientes motivos:

Rol	Apellido y nombre	Firma
Autorizado por		
Retirado/Transportado por		

ANEXO V: SOLICITUD DE ALTA

FECHA:	
LEGAJO:	
NOMBRES:	
APELLIDOS:	

DNI:	
CUIL:	
FECHA DE NACIMIENTO:	
CORREO ELECTRÓNICO:	

DIRECCIÓN/COORDINACIÓN:	
MODALIDAD DE CONTRATACION:	
UBICACIÓN FISICA:	

TIENE GDE PREVIO:	
USUARIO GDE:	
REPARTICIÓN:	

REQUERIMIENTOS ESPECIALES:

ANEXO VI: SOLICITUD DE MODIFICACIÓN

FECHA:	
LEGAJO:	
NOMBRES:	
APELLIDOS:	
DIRECCION/COORDINACIÓN ORIGINAL:	
DIRECCION/COORDINACIÓN DESTINO:	
UBICACIÓN FISICA DE DESTINO:	

REQUERIMIENTOS ESPECIALES:

ANEXO VII: SOLICITUD DE BAJA

FECHA:	
LEGAJO:	
NOMBRES:	
APELLIDOS:	

República Argentina - Poder Ejecutivo Nacional
AÑO DE LA DEFENSA DE LA VIDA, LA LIBERTAD Y LA PROPIEDAD

Hoja Adicional de Firmas
Informe gráfico

Número: IF-2024-130118738-APN-CGI#PTN

CIUDAD DE BUENOS AIRES
Miércoles 27 de Noviembre de 2024

Referencia: POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

El documento fue importado por el sistema GEDO con un total de 46 pagina/s.

Digitally signed by GESTION DOCUMENTAL ELECTRONICA - GDE
Date: 2024.11.27 14:22:06 -03:00

Ángeles Armelin
Coordinadora
Coordinación de Gestión Informática
Procuración del Tesoro de la Nación

Digitally signed by GESTION DOCUMENTAL ELECTRONICA - GDE
Date: 2024.11.27 14:22:07 -03:00