República Argentina

Poder Ejecutivo de la Provincia de La Pampa

ANEXO

Política de Seguridad de la Información

I. **Introducción**

La información es un activo que resulta esencial para el desarrollo de las actividades de su competencia. En consecuencia, necesita ser protegida adecuadamente.

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

La seguridad de la información es la protección de la misma frente a 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 cada organismo. La misma resulta fundamental para el desarrollo de actividades de la Administración Pública Provincial y, en consecuencia, demanda indiscutiblemente la protección de las infraestructuras críticas de información que proveen servicios esenciales a la sociedad.

II. **Objetivo**

La presente Política de Seguridad de la Información (en adelante, PSI) establece las directrices y líneas de actuación en materia de seguridad, con el fin de proteger los recursos de información y la plataforma tecnológica del Gobierno de La Pampa utilizada para su procesamiento, frente a amenazas, internas o externas, deliberadas o accidentales, con el fin de preservar la confidencialidad, integridad, disponibilidad, legalidad y confiabilidad de la información.

Garantizar la implementación de las medidas de seguridad comprendidas en esta PSI, identificando los recursos de información y la tecnología involucrados, posibilita diseñar, desplegar, mantener y mejorar la gestión de la seguridad de la información.

La PSI es una herramienta necesaria para gestionar la confidencialidad, integridad y disponibilidad de la información. Mediante el dictado del Decreto N° 2431/20 que aprueba el Plan Estratégico de Modernización e Innovación de la Administración Pública (PEMIAP), se determinó como uno de sus lineamientos, el de:"*...profundizar políticas de ciberseguridad en el ámbito de la gestión pública provincial y fortalecer la seguridad de las infraestructuras de información digital críticas...*".También constituye uno de sus objetivos específicos el de:"*...definir, implementar y auditar la aplicación de normas, procedimientos y controles destinados a proteger los activos de información propios y/o administrados por el Estado Provincial...*".

Por otra parte, el plan estratégico incluye entre sus principios rectores el de "Confidencialidad de la Información", a fin de respaldar que la información almacenada y/o transmitida por cualquier medio de comunicación, deba ser accedida sólo por el recurso humano o tecnológico que posea su autorización correspondiente.

III. **Principios básicos**

La **confidencialidad, integridad, disponibilidad, autenticación, autorización, no repudio y evaluación de riesgos** son pilares fundamentales para proteger la información a la que se da tratamiento, y de los activos de información utilizados para su gestión, como así también, la protección de los derechos de los titulares de los datos personales procesados.

///.-

Cada principio básico adoptados por esta PSI, con el fin de orientar las acciones de preservación de la seguridad de la información, se ponderan de la siguiente manera:
Confidencialidad de modo que únicamente quienes estén autorizadas accedan a la información.
Integridad de modo que la exactitud de los datos transportados o almacenados sea protegida de la modificación, pérdida o destrucción, garantizándose la no alteración de los mismos.
Disponibilidad de modo que los datos e información estén accesibles por los usuarios o procesos autorizados cuando así lo requieran.
Autenticación de modo que se asegure la identidad del emisor de la información que se envíe, a través de una validación que evite la suplantación de identidades.
Autorización de modo tal que se otorguen privilegios a un usuario para acceder a ciertas áreas de una red o sistema, evitando la intrusión de usuarios no autorizados.
No Repudio de modo de dar garantía de que una parte involucrada en una transacción o comunicación no puede negar la autenticidad de su firma o el envío de un mensaje en un momento posterior.
Evaluación de Riesgos de modo de identificar, analizar, priorizar y categorizar las amenazas a los sistemas de información de una organización.

IV **Alcance**

La presente política se dicta con el objeto de gestionar adecuadamente la seguridad de la información, los sistemas informáticos y el ambiente tecnológico del Gobierno de La Pampa, sus recursos y la totalidad de los procesos, ya sean internos o externos vinculados a través de contratos o acuerdos con terceros.
La PSI se aplica indefectiblemente sobre todos los activos de información producidos dentro del ámbito de la Administración Pública Provincial, cualquiera sea el soporte en que se encuentren, y particularmente, en todos los ambientes tecnológicos de procesamiento, transmisión y almacenamiento de datos perteneciente a la misma. Asimismo, se hace extensible a todo Recurso Humano, propio o externo que manipule activos digitales propiedad del Gobierno de La Pampa.
Los activos de información deben ser clasificados de acuerdo con la sensibilidad y criticidad de la información que contienen, o bien, según la relevancia de la funcionalidad que cumplen, y rotularlos en base a ello con el objeto de señalar cómo ha de ser tratada y protegida dicha información.

V. **Lineamientos**

1. **Organización y clasificación de la información**

OBJETIVO
Definir los diferentes niveles de seguridad requeridos para la información digital de acuerdo a la criticidad de la misma.
PROCEDIMIENTO
Los aspectos, a tener presente, al organizar la clasificación de la información son:

I. Evaluar el perjuicio que ocasionara la ausencia de protección de datos, al impacto en cualquiera de los siguientes contextos:
   - Falta de transparencia de Actos Administrativos.
   - Denegación de Servicios.
   - Interrupción o Desvíos en la ejecución de procedimientos administrativos establecidos.
   - Reputación y buen nombre de la Administración Pública Provincial.

II. Realizar la clasificación por niveles según el grado de sensibilidad de la información, la cual resulta determinante para garantizar la protección de datos. El ordenamiento lo determinará quién produzca la información, o quién sea

designado normativamente, responsable de su gestión.

III. Se definirán los niveles de sensibilidad en los cuales se clasificará la información digital:
   - **Restringida**: Se considera como Confidencial-Nivel 1 a toda información digital que requiere de estrictos controles de acceso y que también minimice la cantidad de usuarios que pueden acceder a los datos.
   - **Sensible**: Se considera como Sensible-Nivel 2 a toda información digital de carácter táctico, cuya pérdida, alteración o exposición pueda generar perjuicios a la Administración Pública Provincial, en su operatoria diaria o vulnerar la protección de los derechos de los titulares de los datos personales contenidos. Esta información requiere de la autorización previa de su propietario para su acceso.
   - **Reservada**: Se considera como Reservada-Nivel 3 a toda información digital que hace referencia a circuitos internos de la Administración Pública Provincial. Requieren de controles de acceso, al igual que los datos confidenciales, pero una gama más amplia de usuarios puede acceder a ella.
   - **Pública**: Se considera como Pública-Nivel 4 a toda información pública que no requiere de mucha seguridad para protegerla de una filtración de datos.

2. **Evaluación y tratamiento de riesgos de seguridad.**

Todo organismo se encuentra expuesto a riesgos en materia de seguridad de la información. No existe la seguridad absoluta, por lo que es necesario conocer cuál es el mapa de riesgos a los cuales se enfrenta la Administración Pública Provincial y tomar acciones tendientes a minimizar los posibles efectos negativos de la materialización de los mismos.

Es por ello que resulta imprescindible gestionar los riesgos, como pilar fundamental para la gestión de seguridad.

OBJETIVO

I. Relevar y Evaluar los riesgos a los que se expone el GLP en materia de seguridad de la información.
II. Generar información de utilidad para la toma de decisiones en materia de controles de seguridad.

2.1 Responsabilidad

El Gobierno de La Pampa es responsable de que se gestionen los riesgos de seguridad de la información, brindando su apoyo para el desarrollo de dicho proceso y su mantenimiento en el tiempo.

La Autoridad de Aplicación de la presente PSI, junto con los responsables de las restantes reparticiones de tecnologías del Gobierno de La Pampa, tienen la responsabilidad del desarrollo del proceso tecnológico de gestión de riesgos de seguridad de la información. Cumplen la función de cubrir los requerimientos de seguridad informática establecidos para la operación, administración y comunicación de los sistemas y recursos de tecnología de la organización. Por otra parte, tienen la función de efectuar las tareas de toma de conocimiento y supervisión de la investigación y monitoreo de los incidentes relativos a la seguridad, en el entorno de ejecución de los sistemas de su repartición.

2.2 Evaluación

El Gobierno de La Pampa, en cada una de sus áreas organizacionales, evaluará sus riesgos identificándolos, cuantificándolos y priorizándolos en función de los criterios de aceptación de riesgos y de sus objetivos de control relevantes. Los resultados determinarán la acción apropiada y las prioridades para gestionar los riesgos de seguridad de la información y para la implementación de controles seleccionados para protegerse contra estos.

Se debe efectuar la evaluación de riesgos periódicamente, para tratar con los cambios en los requerimientos de seguridad y en las situaciones de riesgo. Asimismo, se debe efectuar la

evaluación cada vez que ocurran cambios significativos. Es conveniente que estas evaluaciones de riesgos se lleven a cabo de una manera metódica capaz de producir resultados comparables y reproducibles.
El alcance de dicha evaluación puede incluir a toda la organización, una parte, un sistema de información particular, componentes específicos de un sistema, o servicios.

2.3 Tratamiento

Antes de considerar el tratamiento de un riesgo, cada organismo susceptible de ser afectado por el posible impacto de una amenaza expuesta debe decidir los criterios para determinar si los riesgos pueden, o no, ser aceptados. Luego de su evaluación, se determinan las acciones a seguir debidamente documentadas.
Para cada uno de los riesgos identificados durante la evaluación de riesgos, se necesita tomar una decisión para su tratamiento. Las posibles opciones para el tratamiento de riesgos incluyen:

a. **Mitigar** los riesgos, mediante la aplicación de controles apropiados para reducirlos a un nivel aceptable.
   Las posibles opciones para el tratamiento de riesgos incluyen:
   1. Requerimientos y restricciones de legislaciones y regulaciones nacionales e internacionales;
   2. Objetivos organizacionales;
   3. Requerimientos y restricciones operativos;
   4. Costo de implementación y operación en relación directa a los riesgos reducidos;
   5. La necesidad de equilibrar las inversiones necesarias del proceso de mitigación contra el daño que podría resultar de las fallas de seguridad.

   Es necesario reconocer que algunos controles pueden no ser aplicables a todo sistema de información o a su ambiente, y podrían no ser aplicables en todos los Organismos.
   Se debe recordar que ningún conjunto de controles puede alcanzar la seguridad absoluta. Los controles implementados deben ser evaluados permanentemente para que puedan ser mejorados en eficiencia y efectividad.
b. **Aceptar** los riesgos de manera objetiva y consciente, siempre y cuando éstos satisfagan claramente la política y los criterios de aceptación de riesgos del GLP;
c. **Evitar** los riesgos, eliminando las acciones que dan origen a la ocurrencia de éstos;
d. **Transferir** los riesgos asociados a otras partes interesadas, por ejemplo: compañías de seguro o proveedoras/es.

3. **Seguridad Informática de los Recursos Humanos**

El personal de la Administración Pública Provincial es considerado un recurso central para la protección de la información.
Para las/los empleadas/os, contratistas y usuarias/os terceras partes, *se establece la obligatoriedad de la suscripción de compromisos de confidencialidad en función de las responsabilidades que correspondan y a las funciones que se desarrollen*. Los permisos de acceso son otorgados en función de cada perfil de trabajo y se mantienen actualizados.
El "Acuerdo de confidencialidad y de no divulgación de datos e información" -aprobado por Resolución N°47/20 del Ministerio de Conectividad y Modernización- que se celebre con los actores citados en el párrafo precedente, queda comprendido dentro de la facultad del Ministerio de Conectividad y Modernización de implementar herramientas y políticas de seguridad informática tendientes a garantizar la confidencialidad de la información generada en el ámbito de su competencia – Conforme lo establecido en el artículo 22, inciso 17) de la Ley N° 3170 —Ley de Ministerios y Secretarías de la Provincia de La Pampa—, según su T.O. aprobado por Decreto N° 6186/2023 y modificada por su Decreto Reglamentario N° 6187/23.

//5.-

OBJETIVO

- Establecer los lineamientos y responsabilidad ante la manipulación de activos de información por parte del Recurso Humano de la Administración Pública Provincial.
- Fortalecer la cultura de la seguridad de la información, mediante la incorporación de capacitaciones continuas en el marco del programa PROCAAP, garantizando que todo el personal cuente con los conocimientos necesarios para llevar a cabo la gestión ordenada de los activos de información, confirmar la Confidencialidad, Integridad y Disponibilidad de la información, y cumplir con las Políticas Internas.

3.1 Responsabilidades

El Gobierno de La Pampa y/o autoridad de aplicación debe solicitar a las/los empleadas/os, contratistas y usuarias/os de terceras partes que apliquen la seguridad en concordancia con las políticas y procedimientos establecidos por la organización, cumpliendo con lo siguiente:

a. Estar adecuadamente informados de sus roles y responsabilidades de seguridad de la información antes de que se le otorgue el acceso a información sensible o a los sistemas de información;
b. Alcanzar un nivel de conocimiento sobre la seguridad acorde con sus roles y responsabilidades en el ámbito de la Administración Pública Provincial;
c. Cumplir con la PSI y métodos adecuados de trabajo establecidos en las normativas vigentes.
d. Devolver todos los activos en su poder, pertenecientes al Gobierno de La Pampa (software, documentos corporativos, equipamiento, etc.) tras la culminación de su empleo, contrato, o acuerdo. En los casos los mismos tengan un conocimiento que es importante para las operaciones actuales, dicho conocimiento debe ser documentado y transferido.
e. La Autoridad de Aplicación de la presente política, designará a los Responsables de la Seguridad de la Información (RSI).
f. Para cada una de las instalaciones de procesamiento de información (repartición con funciones de implementación de soluciones tecnológicas), la Autoridad de Aplicación solicitará a las autoridades correspondientes, se designe el/los responsables de la seguridad operativa (RSO).

3.2 Autenticación, autorización y control de acceso

Solamente el personal autorizado accede a los activos de información críticos perteneciente al ámbito de la Administración Pública Provincial.

El acceso a la información se establecerá en base a la "necesidad de saber", es decir que quienes accedan deben tener un interés válido para hacerlo en razón de su rol y/o funciones y usando una política de "Principio del 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 agentes públicos, funcionarios y demás usuarios, el uso responsable de los dispositivos y datos de autenticación otorgados por el organismo para el cumplimiento de sus funciones, que no los compartan y que los mantengan siempre seguros, tanto dentro como fuera del organismo.

3.2.1 Retiro de los derechos de acceso

Se deben revisar los derechos de acceso de un individuo a los activos asociados con los sistemas y servicios de información tras la desvinculación de su actividad laboral, y de ser necesario, removerlos.

Con el cambio de un empleo deben removerse todos los derechos de acceso que no fueron aprobados para el nuevo empleo, comprendiendo esto accesos lógicos y físicos.

Si una/un empleada/o, contratista o usuaria/o de tercera parte que se está desvinculando tiene conocimiento de contraseñas para cuentas que permanecen activas, éstas deben ser cambiadas tras la finalización o cambio de empleo, contrato o acuerdo.

///.-

//6.-

Se debe evaluar la reducción o eliminación de los derechos de acceso a los activos de la información y a las instalaciones de procesamiento de la información antes de que el empleo termine o cambie, dependiendo de factores de riesgos, tales como:

a. Si la terminación o cambio es iniciado por la/el empleada/o, contratista o usuaria/o de tercera parte, o por la gestión y la razón de la finalización;
b. Las responsabilidades actuales de la/el empleada/o, contratista o cualquier otra usuaria/o;
c. El valor de los activos accesibles actualmente.

4. **Gestión de Activos de Información**

Se debe realizar una gestión y protección efectiva de los activos de información de la Administración Pública Provincial en función de su clasificación por criticidad. 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.

OBJETIVO

- Garantizar que los activos de información reciban un apropiado nivel de protección.
- Clasificar la información para señalar su sensibilidad y criticidad.
- Definir niveles de protección y medidas de tratamiento especial acordes a su clasificación.

El Gobierno de La Pampa debe tener un conocimiento preciso sobre los activos digitales que posee como parte importante de la administración de riesgos. Algunas categorías son:

- **Recursos de información**: bases de datos y archivos, documentación de sistemas, información archivada, procedimientos operativos, entre otros.
- **Recursos de software**: software de aplicaciones, sistemas operativos, herramientas de desarrollo y publicación de contenidos, utilitarios, entre otros.
- **Activos físicos**: equipamiento informático, equipos de comunicaciones, equipos técnicos relacionados con el suministro eléctrico, mobiliario, entre otros.
- **Servicios**: servicios informáticos y de comunicaciones, utilitarios.

La información no necesariamente debe mantenerse invariable por siempre, puede cambiar de acuerdo con una política predeterminada, o bien, puede pasar a ser obsoleta y, por lo tanto, ser necesario eliminarla.

La destrucción de la información es un proceso que debe asegurar su confidencialidad hasta el momento de su eliminación.

4.2 Inventario de Activos Digitales de Información

Con la finalidad de aplicación de la PSI, en cada Unidad Organizacional perteneciente al Gobierno de La Pampa se deben identificar los activos digitales de información propios, y luego, elaborar y actualizar el inventario de Activos Digitales de Información.

Existen variedad de tipos de activos, que incluyen:

a. Información: bases de datos, archivos de datos, documentación, contratos, acuerdos, videos, presentaciones, tableros de comando;
b. Activos de software: software de aplicaciones, software de sistemas, herramientas de desarrollo, servicios en la nube, y utilitarios;
c. Activos intangibles: la reputación e imagen.

El inventario debe actualizarse ante cualquier modificación de los datos registrados y revisado con una periodicidad de SEIS (6) meses como mínimo.

4.2.1 Control: Propiedad de los activos

El conjunto de activos de información y su gestión comunicacional, corresponden a la órbita de un responsable/ o autoridad de cada Unidad Organizacional perteneciente al Gobierno de La Pampa.

///.-

//7.-

Los responsables de la gestión de los activos involucrados deben cumplir las siguientes funciones:

a. Informar sobre cualquier cambio que afecte el inventario de activos;
b. Clasificar los activos en función a su valor;
c. Definir los requisitos de seguridad de los activos;
d. Velar por la implementación y el mantenimiento de los controles de seguridad requeridos en los activos.

Los responsables designados pueden delegar la administración de sus funciones a personal idóneo a su cargo, sin embargo, conservaran la obligación de su cumplimiento. La delegación de la administración por parte de las/los propietarias/os de los activos debe ser documentada por éstos.

4.2.2 Control: Uso aceptable de los activos

Se deben identificar, documentar e implementar reglas para el uso aceptable de la información y los activos asociados con las instalaciones de procesamiento de la información.

Todas/os las/los agentes, contratistas y usuarias/os de terceras partes deben seguir las reglas y normativas para el uso aceptable de la información y los activos asociados con las instalaciones de su procesamiento, incluyendo entre otros:

- Correo electrónico,
- Sistemas de gestión,
- Estaciones de trabajo,
- Dispositivos móviles,
- Herramientas y equipamiento de publicación de contenidos, etc.

5. **Seguridad Operativa**

Considerando la infraestructura informática, las redes de comunicaciones, las instalaciones, los equipos auxiliares y las personas intervinientes, definimos los procesos de seguridad y gestión de riesgos, que evita que la información confidencial llegue a las personas equivocadas.

Se requiere del uso de activos tangibles que previamente fueron identificados e inventariados y que cuentan con su marco de seguridad propio. Entre estos activos se incluyen:

a. Activos físicos: equipamiento d computación, equipamiento de comunicaciones, medios removibles y otros equipamientos
b. Instalaciones: edificios, ubicaciones físicas, red eléctrica, entre otras.
c. Servicios: de cómputo y de comunicaciones, servicios generales.
d. Personas: sus calificaciones, habilidades y experiencia.

OBJETIVO

•Garantizar el funcionamiento correcto y seguro de las instalaciones de procesamiento de la información.

•Establecer responsabilidades y procedimientos para su gestión y operación, incluyendo instrucciones operativas, procedimientos para la respuesta a incidentes y separación de funciones.

Las operaciones se deben desarrollar en forma segura, en todas las instalaciones de procesamiento de información, asignándose las debidas responsabilidades, e implementando la administración de vulnerabilidades como un proceso continuo y proactivo, que busca proteger equipos, redes y aplicaciones organizacionales de ciberataques y vulneraciones de datos.

Los Responsables de la Seguridad de la Información (RSI) tienen a su cargo, entre otros:

a. Definir procedimientos para el control de cambios de los procesos operativos en las instalaciones de procesamiento de información;
b. Establecer criterios de código seguro para de aprobación para nuevos sistemas de

///.-

información, actualizaciones y nuevas versiones;

c. Definir procedimientos para el manejo de incidentes de seguridad y para la administración de los medios de almacenamiento;
d. Definir y documentar controles de detección y prevención del acceso no autorizado, y la protección contra software malicioso en las redes de la Administración Pública Provincial;
e. Desarrollar procedimientos adecuados de concientización de usuarias/os en materia de seguridad, controles de acceso al sistema y administración de cambios;
f. Verificar el cumplimiento de las normas, procedimientos y controles establecidos.

Los responsables de la seguridad operativa (RSO) tienen a su cargo:

a. Controlar la existencia de documentación actualizada relacionada con los procedimientos de operaciones;
b. Evaluar el posible impacto operativo de los cambios previstos a sistemas y equipamiento y verificar su correcta implementación, asignando responsabilidades;
c. Administrar los medios técnicos necesarios para permitir la segregación de los entornos de procesamiento;
d. Monitorear las necesidades de capacidad de los sistemas en operación y proyectar las futuras demandas de capacidad, a fin de evitar potenciales amenazas a la seguridad del sistema o a los servicios de la/el usuaria/o;
e. Controlar la realización de las copias de resguardo de información, así como la prueba periódica de su restauración;
f. Revisar y Documentar las fallas para prevenir su repetición o facilitar su resolución en caso de reincidencia;
g. Implementar los controles de seguridad definidos (software malicioso y accesos no autorizados);
h. Revisar las medidas correctivas para garantizar que los controles no fueron comprometidos, y que las medidas tomadas fueron autorizadas;
i. Definir e implementar procedimientos para la administración de medios informáticos de almacenamiento y para su eliminación segura.

Los responsables de la seguridad de la información (RSI), juntamente con los responsables de la seguridad operativa (RSO) tienen a su cargo:

a. Definir un plan de contingencia ante eventuales incidentes de seguridad;
b. Definir un esquema de requerimientos de resguardo de cada software o dato en función de su criticidad.
c. Verificar y probar periódicamente los procedimientos de restauración garantizando su eficacia y cumplimiento dentro del tiempo asignado a la recuperación en los procedimientos operativos.
d. Realizar pruebas necesarias contemplando el cumplimiento de los criterios de aprobación para nuevos sistemas de información, actualizaciones y nuevas versiones antes de su puesta en producción definitiva.

5.1. Separación entre Instalaciones de Desarrollo e Instalaciones Operativas.

Los entornos de Desarrollo, Prueba y Producción, siempre que sea posible, estarán separados preferentemente en forma física, y, se definirán y documentarán las reglas para la transferencia de software desde el estado de Desarrollo hacia el estado Producción. Para ello, se tendrán en cuenta los siguientes controles:

a. Ejecutar el software de Desarrollo y de Producción, en diferentes entornos de Producción, equipos, o directorios.
b. Separar las actividades de Desarrollo y Prueba, en entornos diferentes.
c. Impedir el acceso a los compiladores, editores y otros utilitarios del sistema en el ambiente Producción, cuando no sean indispensables para el funcionamiento del mismo.

d. Utilizar sistemas de autenticación y autorización independientes para los diferentes entornos, así como perfiles de acceso a los sistemas. Las interfaces de los sistemas identificarán claramente a qué instancia se está realizando la conexión.
e. Definir propietarios de la información para cada uno de los entornos de procesamiento existentes.
f. El personal de desarrollo no tendrá acceso al ambiente operativo Producción. De requerirse tal contingencia, el Responsable de la Seguridad Operativa (RSO) establecerá un procedimiento para la autorización, documentación y registro de dichos accesos.

5.2.Seguridad de las comunicaciones

Se adoptan las medidas necesarias para proteger adecuadamente la información que se comunica por sus redes informáticas y para minimizar los riesgos que pudieran afectar la infraestructura de soporte. Toda información que se transfiere, incluyendo la que se transmite a través de los servicios de correo electrónico es protegida de acuerdo a su nivel de criticidad.
Se asignan cuentas de correo electrónico institucionales a todos los empleados y funcionarios, quienes deben utilizarlas para toda comunicación vinculada a sus funciones, y dando cumplimiento a la normativa de uso vigente. En los casos en los que el organismo lo considere necesario, a los agentes públicos se les exige la firma de acuerdos de confidencialidad y no divulgación.

5.3.Adquisición de sistemas, desarrollo y mantenimiento de sistemas de información

Se adoptan los controles de seguridad necesarias para proteger por defecto y desde el diseño todas las aplicaciones que se desarrollen internamente, utilizando una metodología de desarrollo seguro, e incorporando requerimientos y evaluaciones de seguridad en el proceso de contratación de aplicaciones a terceros. Esto se ejecuta especialmente en aquellas aplicaciones que se utilicen para brindar servicios o realizar trámites por parte de la ciudadanía e involucren el tratamiento de datos personales.
Se evalúa la seguridad de las aplicaciones durante todo su ciclo de vida.

5.4.Relación con proveedores

El Gobierno de La Pampa incluye en sus pliegos de bases y condiciones particulares, cuando considera necesario, cláusulas vinculadas a la seguridad de la información, de cumplimiento efectivo y obligatorio por parte los involucrados. Estas disposiciones consideran los aspectos pertinentes a la protección de la información y los servicios que se brinden, desde el inicio del proceso contractual hasta su finalización. Los requisitos por incluir son acordes a la criticidad de la información y los servicios, a la evaluación de riesgos y al cumplimiento de todas las normas legales y contractuales aplicables.

5.5.Gestión de incidentes de seguridad

Se adoptan las medidas necesarias para prevenir, detectar, gestionar, resolver y reportar los incidentes de seguridad que puedan afectar sus activos de información.
El responsable de la seguridad operativa (RSO) debe comunicar inmediatamente a la Autoridad de Aplicación de la presente política, cualquier evento detectado durante la ejecución de procesos, que constituya o que pueda constituir un incidente de seguridad.
Las vulnerabilidades detectadas deben ser comunicadas oportunamente de forma tal que se apliquen las acciones correctivas en el menor tiempo posible. Las mismas se registrarán teniendo presente el siguiente ordenamiento:

a) Revisión de registros de fallas para garantizar que las mismas fueron resueltas satisfactoriamente.
b) Revisión de medidas correctivas para garantizar que los controles no fueron comprometidos, y que las medidas tomadas fueron autorizadas.
c) Documentación de la falla con el objeto de prevenir su repetición o facilitar su resolución en caso de reincidencia.

//10.-

El responsable de la seguridad de la información (RSI), juntamente con el responsable de la seguridad operativa de procesos (RSO), desarrollarán procedimientos para comunicar las fallas en el procesamiento de la información o de los sistemas de comunicaciones, que permitan tomar medidas correctivas.
La autoridad de aplicación de la presente política verificará el cumplimiento de los procedimientos, identificando los controles de seguridad necesarios para el tratamiento del riesgo, llevando a un nivel aceptable, y detectando las oportunidades de mejora.

6. **Aspectos de la continuidad de gestión de la seguridad**

El concepto de continuidad de gestión de la seguridad de la información gira en torno a la capacidad de proteger y acceder de forma persistente a activos de información vitales, incluso durante eventos imprevistos o crisis.
En el ámbito de la seguridad de la información, la progresiva evolución de las amenazas, como el secuestro o robo de datos, la suplantación de identidad y las amenazas persistentes avanzadas (APT), demandan la adopción de un enfoque integral, riguroso y sostenido para la gestión continua de la seguridad. Estas amenazas ponen de relieve la necesidad de que la organización Gobierno de La Pampa mantenga medidas de ciberseguridad resilientes que puedan adaptarse a las tácticas cambiantes de los potenciales ataques.
OBJETIVO
Facilitar que el Gobierno de La Pampa pueda minimizar el impacto de eventos disruptivos y mantener la operatividad, garantizando la calidad y la seguridad de la información.
La gestión de la continuidad de la Seguridad debe contemplar todos los aspectos de seguridad requeridos en los procedimientos de persistencia de la gestión del Gobierno de La Pampa, especialmente cuando se trate de información, servicios o sistemas críticos. En consecuencia, se requieren ejecutar periódicamente, las siguientes acciones:

- Realizar análisis de impacto e identificar las ventanas de recuperación requeridas en los procesos críticos.
- Asegurar que todas las medidas preventivas y mecanismos de recuperación en caso de eventos desastrosos sean objeto de pruebas.
- Revisar si las medidas de prevención de desastres son acordes/coherentes con las percepciones de riesgo de pérdida de información o servicios.
- Dar continuidad a la implementación y actualización de tecnologías.
- Desarrollar políticas y procedimientos sobre seguridad de la información.

7. **Revisión y actualización**

El Gobierno de La Pampa debe adaptar sus planes de continuidad de seguridad de la información, en el marco de modernización del Estado Provincial, actualizando los protocolos existentes, invirtiendo en nuevas tecnologías de seguridad y garantizando que las iniciativas digitales estén alineadas con la postura de seguridad general de la organización.
La PSI será comunicada al personal de la Administración Pública Provincial, de manera pertinente, accesible y comprensible.

ANEXO DE DECRETO N° 167 /26.-

Alicia Susana MAYORAL
VICEGOBERNADORA DE LA PROVINCIA
EN EJERCICIO DEL PODER EJECUTIVO

DR. ANTONIO CURCIARELLO
MINISTRO DE CONECTIVIDAD
Y MODERNIZACIÓN

GLOSARIO

Política de Seguridad de la Información

Activo de información
Toda información o sistema relacionado con su tratamiento que tenga valor para la organización. Pueden consistir en documentos, datos, aplicaciones, equipos informáticos, personal o cualquier otro componente. Los activos de información son susceptibles de ataques deliberados o accidentales.

Amenaza informática
Causa potencial de un incidente no deseado, que puede causar daños en un sistema o proceso.

Ataque informático
Acción intencional de comprometer, destruir, exponer, alterar, inhabilitar, acceder sin permiso, hacer uso no autorizado y/o cualquier otra acción prohibida sobre un activo de información digital.

Autenticación
Procedimiento que se realiza para comprobar que alguien es quién dice ser cuando accede a un dispositivo o sistema.

Ciberataque
Intento deliberado de infiltración sin autorización, en sistemas informáticos, redes o dispositivos, sirviéndose de diferentes técnicas y vulnerabilidades, con la finalidad de acceder o dañar sistemas informáticos, redes, dispositivos o datos digitales; robar o manipular información confidencial o recursos digitales.

Confidencialidad
Propiedad que refiere a que los datos e información se mantengan inaccesibles y se revelen únicamente a personas, entes o procesos autorizados.

Control
Los medios para gestionar el riesgo, incluidos políticas, procedimientos, directrices, prácticas o estructuras organizativas, que pueden ser de naturaleza administrativa, técnica, de gestión o jurídica.

Control de acceso
Medios que se emplean para asegurar que el acceso a los activos de información se encuentre restringido a las personas autorizadas.

Disponibilidad
Propiedad que refiere a que los datos e información sean accesibles y se encuentren listos para su uso a demanda de una persona o ente autorizado.

Entorno de desarrollo
Espacio de trabajo que permite a los desarrolladores de sistemas crear una aplicación o realizar cambios en ella, sin afectar a la versión en el entorno de producción del software.

Entorno de producción
Ambiente donde el software está disponible para su uso por parte del público objetivo.

Incidente de seguridad de la información
Evento o serie de eventos de seguridad de la información, no deseados o inesperados, que comprometen la seguridad de la información y amenazan la operación de la organización.

Información
Es un conjunto de datos organizados que portan, transmiten o arrojan un significado.

Integridad
Propiedad que refiere a la exactitud y completitud de la información.

Principio del Mínimo privilegio (PoLP)
Es un concepto en ciberseguridad que se centra en limitar el acceso de usuarios y procesos al mínimo necesario para el desempeño de sus funciones. (https://identitymanagementinstitute.org/)

///.-

//2.-

Recurso
Cualquier activo que posibilite generar, almacenar, publicar o transmitir información.
Responsable de la seguridad de la información (RSI)
Persona encargada de diseñar, implementar y controlar diferentes medidas de seguridad con las que asegurar la protección de los datos de una empresa, organización, institución o persona. Desarrollar y gestionar la estrategia de seguridad de la información.
Responsable de la seguridad operativa (RSO)
Persona encargada de la implementación de políticas de seguridad, monitorizar los sistemas y redes en busca de actividad sospechosa, generar y responder a incidentes de seguridad.
Riesgo
La posibilidad de que un sistema sufra un incidente de seguridad y que una amenaza se materialice causando una serie de daños.
Sistema de información
Aplicaciones, servicios, activos de tecnología de la información y todo otro componente empleado para tratar información.
Uso Aceptable de Activos de Información
Práctica de utilizar los datos y recursos informáticos de la organización, de manera ética, legal, segura y responsable, evitando cualquier acción que pueda comprometer la confidencialidad, integridad o disponibilidad de la información. Implica adherirse a las políticas de la organización y cumplir con las leyes y regulaciones pertinentes.
Vulnerabilidad
Debilidad de un activo, grupo de activos o de un control que puede ser materializada por una o más amenazas.-

GLOSARIO DE ANEXO.-

DR. ANTONIO CURCIARELLO
MINISTRO DE CONECTIVIDAD
Y MODERNIZACION

Alicia Susana MAYORAL
VICEGOBERNADORA DE LA PROVINCIA
EN EJERCICIO DEL PODER EJECUTIVO