



RESOLUCIÓN VPR\_Nº- 114/19

**POR LA CUAL SE APRUEBA LAS POLÍTICAS PARA LA SEGURIDAD DE LA INFORMACIÓN DE LA VICEPRESIDENCIA DE LA REPÚBLICA.**

Asunción, 10 de junio de 2019

**VISTO:** El Memorandum VP\_IN/MEM-20/19 de fecha 06 de junio de 2019 de la Dirección de Tecnología de la Información y Comunicación – DTIC's de la Vicepresidencia de la República; y,

**CONSIDERANDO:** Que, por el memorandum precedentemente señalado, se solicita se dicte resolución por la cual se aprueba las Políticas para la Seguridad de la Información de la Vicepresidencia de la República, y así dar cumplimiento al Modelo Estándar de Control Interno para Instituciones Públicas del Paraguay.

Que, en la fundamentación de las Políticas de la Información se expresa que "la Vicepresidencia de la República está orientada a definir las medidas que resguarden la confidencialidad, integridad y disponibilidad de la información propia, el acceso a la información en conformidad con la Constitución Nacional, las leyes y demás normas jurídicas.." y que los procedimientos de seguridad asociados utilizarán como marco de referencia las normativas vigentes para el Gobierno Electrónico y las recomendadas por el Ministerio de Tecnología de la Información y Comunicación MITIC y las buenas prácticas definidas en la norma ISO 27001-2005 que es un estándar para la Seguridad de la Información, aprobado y publicado como estándar internacional.

Que, la Dirección de Tecnología de la Información y Comunicación – DTIC's de la Vicepresidencia de la República, asume la responsabilidad de implantar, mantener y mejorar continuamente la Política de Seguridad de la Información y que es imprescindible contar con un marco general en el cual encuadrar todos los subprocesos asociados a la Gestión de la Seguridad.

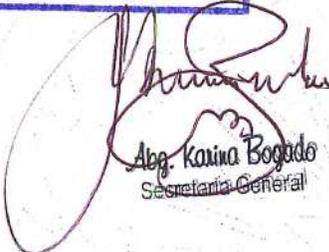
**POR TANTO,** en ejercicio de sus atribuciones legales vigentes,

**EL VICEPRESIDENTE DE LA REPÚBLICA DEL PARAGUAY**

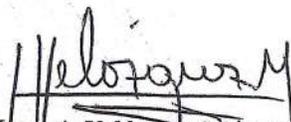
**RESUELVE:**

- Art. 1º** Aprobar las Políticas para la Seguridad de la Información de la Vicepresidencia de la República, de conformidad al considerando de la presente Resolución y al Anexo que forma parte de la misma.
- Art. 2º** Establecer que la Dirección de Tecnología de la Información y Comunicación de la Vicepresidencia de la República – DTIC's, bajo la supervisión del Director General de Administración y Finanzas, implemente de manera eficiente y eficaz las "Políticas para la Seguridad de la Información de la Vicepresidencia de la República", aprobadas por esta Resolución.
- Art. 3º** Comunicar a quienes corresponda y cumplido, archivar.

COPIA FIEL DEL ORIGINAL

  
Abg. Karina Bogado  
Secretaría General



  
Hugo A. Velázquez Moreno  
Vicepresidente de la República  
del Paraguay



RESOLUCIÓN VPR\_Nº- 114/19

**VICEPRESIDENCIA DE LA REPÚBLICA DEL PARAGUAY**  
**POLITICAS PARA LA SEGURIDAD DE LA INFORMACIÓN**

**1. INTRODUCCIÓN**

La Vicepresidencia de la República, creado en 1992 con la Constituyente de aquel entonces, reconoce la importancia y el valor de la información con respecto al funcionamiento eficiente y efectivo de la Institución. La información no es sólo crítica para el éxito de la organización, sino estratégica para su supervivencia a largo plazo.

LA VICEPRESIDENCIA DE LA REPÚBLICA, está orientada a definir las medidas que resguarden la confidencialidad, integridad y disponibilidad de la información propia, el acceso a la información en conformidad con la constitución, las leyes, y demás normas jurídicas, así como asegurar la continuidad de los servicios que le son propios.

Es por ello que la DTICs asume la responsabilidad de implantar, mantener y mejorar continuamente la Política de Seguridad de la Información, que permita lograr niveles adecuados de seguridad para todos los activos de información institucional considerados relevantes, de manera tal de garantizar que los riesgos de la seguridad de la información sean conocidos, asumidos, gestionados y minimizados por la Institución de una forma documentada, sistemática, estructurada, repetible, eficiente y adaptada a los cambios que se produzcan en los riesgos, el entorno y las tecnologías.

Es imprescindible contar con un marco general en el cual encuadrar todos los subprocesos asociados a la Gestión de la Seguridad, comenzando por definir sus objetivos, el alcance o amplitud, los roles y responsabilidades y el marco general para elaboración y revisión de las políticas de seguridad específicas para la información de LA VICEPRESIDENCIA DE LA REPÚBLICA.

Esta política general, las políticas específicas y procedimientos de seguridad asociados utilizarán como marco de referencia las leyes nacionales para el Gobierno Electrónico y normativas recomendadas por el Ministerio de Tecnología de la Información y Comunicación – MITIC y las buenas prácticas definidas en la norma ISO 27001-2005, que es un Estándar para la Seguridad de la Información, aprobado y publicado como estándar internacional, la que adicionalmente deberá constituir el marco rector de todas las iniciativas de seguridad adoptadas por LA VICEPRESIDENCIA DE LA REPÚBLICA.

**2. OBJETIVOS**

Esta Política de Seguridad de la Información cubre los siguientes objetivos:

- ❖ Establecer las expectativas de la DTICs con respecto al correcto uso que el personal haga de los recursos de información de LA VICEPRESIDENCIA DE LA REPÚBLICA, así como de las medidas que se deben adoptar para la protección de los mismos.
- ❖ Establecer para todo el personal de la Vicepresidencia de la Republica, la necesidad de la seguridad de la información y promover la comprensión de sus responsabilidades individuales.
- ❖ Determinar las medidas esenciales de seguridad de la información que LA VICEPRESIDENCIA DE LA REPÚBLICA debe adoptar, para protegerse apropiadamente contra amenazas que podrían afectar en alguna medida la confidencialidad, integridad y disponibilidad de la información, ocasionando alguna de las siguientes consecuencias:
  - Pérdida o mal uso de los activos de información (datos, equipos, documentación impresa, y otros)
  - Pérdida de imagen como Institución.
- ❖ Proporcionar a todo el personal de LA VICEPRESIDENCIA DE LA REPÚBLICA una herramienta que facilite la toma de decisiones apropiada, en situaciones relacionadas con la preservación de la seguridad de la información.

COPIA FIEL DEL ORIGINAL

Abg. Karina Bogado  
Secretaría General



*[Handwritten signature]*



Para cumplir con estos objetivos la DTICs se basa en la identificación de los activos de información involucrados en los procesos de soporte de la institución, lo cual implica llevar a cabo junto a los responsables de los diferentes procesos de la institución las siguientes actividades esenciales:

- 1) Identificar, para todos los procesos, los activos de información involucrados, catalogados como información física, información digital, personas e infraestructura, clasificándolos según lo establezcan las leyes.
- 2) Para cada activo de información identificar un responsable que vele por su disponibilidad, confidencialidad e integridad.
- 3) Analizar el riesgo al cual están expuestos, con la ayuda del Comité de Comunicación para el MECIP.
- 4) Difundir en forma planificada entre todos los Funcionarios de la Institución el objetivo Institucional de preservación de la información, sus características y las responsabilidades individuales para lograrlo, inserto esto en los planes de capacitación anual de la institución como actividades permanentes y en el proceso de inducción del nuevo personal.

### 3. ALCANCE

Esta política se aplica a todo el personal de LA VICEPRESIDENCIA DE LA REPÚBLICA, Funcionarios Permanentes, Comisionados de otras Instituciones, Contratados, Voluntarios o Pasantes, y también al personal externo que preste o preste servicios, remunerados o no, a LA VICEPRESIDENCIA DE LA REPÚBLICA que tienen acceso privilegiado a la información.

También es aplicable a todo activo de información que la organización posea en la actualidad o en el futuro, de manera que la no inclusión explícita en el presente documento, no constituye argumento para no proteger estos activos de información.

La política cubre toda la información, entre otros, la impresa o escrita en papel, almacenada electrónicamente, transmitida por correo o usando medios electrónicos, mostrada en videos, películas o hablada en una conversación.

La gestión de la seguridad de la información se realizará mediante un proceso sistemático, documentado y conocido por toda la organización basándose en metodologías de mejoramiento continuo. Este proceso de gestión deberá ser aplicado a todos los procesos de la Institución, iniciándose con los procesos propios.

Así también, como apoyo a esta política, cada dominio especificado por el estándar ISO 27001 tendrá una política específica, que complementará la presente y normará las particularidades de cada dominio.

Cada Política deberá contar con procedimientos asociados, mecanismos de control y sanciones asociadas al no cumplimiento.

### 3. DEFINICIONES

**Información:** Es la interpretación que se da a un conjunto de datos, pudiendo residir está en medios electromagnéticos, físicos o en el conocimiento de las personas. En el caso de la presente política, se entenderá como información a toda forma proveniente de datos relacionados con los procesos realizados, así como antecedentes proporcionados tanto por los usuarios internos como los externos, siempre que sea dentro del contexto del ejercicio de sus funciones y del cumplimiento de sus obligaciones.  
información Pública. toda aquella información no catalogada como secreta o reservada, tal como lo establece el ordenamiento jurídico vigente.

**Información Reservada (conocimiento reservado):** Son aquellos documentos cuyo conocimiento está circunscrito al ámbito de la respectiva unidad del órgano a que sean remitidos, en virtud de una ley o de una norma administrativa dictada en conformidad a ella, que les confiere tal carácter, cuando la naturaleza misma de la información requiera ser tratada de manera reservada.

**La información secreta (solamente a quien le atañe la información debe conocerlo):** Son aquellos documentos cuyo conocimiento está circunscrito a las autoridades o personas a las que vayan dirigidos y a quienes deban intervenir en su estudio y resolución, en virtud de una ley o de una norma administrativa dictada en conformidad a ella, que les confiere tal carácter. Una norma que establece restricciones claras es la ley de datos personales.

**Seguridad de la Información:** Es el nivel de confianza que la organización desea tener de su capacidad para preservar la confidencialidad, integridad y disponibilidad de la información. Tiene como objetivo proteger el

COPIA FIEL DEL ORIGINAL

Abg. Karina Bogado  
Secretaria General



[Handwritten signature]



recurso información de una amplia gama de amenazas, con el fin de asegurar la continuidad de los procesos de trámites, minimizar el daño y, cumplir su misión y objetivos estratégicos.

**Confidencialidad:** Es asegurar que la información, es accesible sólo para las personas autorizadas para ello.

**Integridad:** Es salvaguardar la exactitud y totalidad de la información en su procesamiento, transmisión y almacenamiento.

**Disponibilidad:** Es asegurar que los usuarios autorizados tengan acceso a la información y los activos asociados cuando estos sean requeridos.

**Buen Uso:** Se entiende por "buen uso" de los activos de información de la organización, a las expectativas que LA VICEPRESIDENCIA DE LA REPÚBLICA tiene con respecto al cuidado que su personal debe tener con los activos que la Institución les entregue para el desempeño de sus funciones.

**Personal:** Es toda persona a la cual se le concede autorización para acceder a la información y a los sistemas de LA VICEPRESIDENCIA DE LA REPÚBLICA. El personal puede ser interno o externo a la organización.

**Supervisor:** Es toda persona encargada de un grupo de personas, área, división, programa o departamento en LA VICEPRESIDENCIA DE LA REPÚBLICA.

**Tercero:** Se refiere a empresas prestadoras de servicios, las empresas contratistas, sub-contratistas y cualquiera que, por cuenta propia o de terceros, desarrolle trabajos para o por cuenta de LA VICEPRESIDENCIA DE LA REPÚBLICA.

**Responsable de la Información:** Es el usuario a cargo de la información y de los procesos que la manipulan sean estos manuales, mecánicos o electrónicos.

**Encargado de Seguridad:** Es la persona que la autoridad máxima del servicio designa para la definición, diseño, implementación y supervisión de las medidas de seguridad de la información.

**Comité de Seguridad:** Es el equipo conformado por supervisores que representan a las áreas de la organización, responsable de la toma de decisiones en temas de la seguridad de la información.

**Activo de Información:** Todos aquellos elementos relevantes en la producción, emisión, almacenamiento, comunicación, visualización y recuperación de información de valor para la institución.

**Podemos distinguir 3 tipos de activos:**

- La Información propiamente tal, en sus múltiples formatos (papel o digital, texto, imagen, audio, video y otros.)
- Los Equipos/Sistemas que la soportan.
- Las Personas que la utilizan.

Los activos poseen valor para la organización, y necesitan por tanto ser protegidos adecuadamente, para que "los datos" no se vean perjudicados (implica detectar vulnerabilidades y establecer controles).

## 5. RESPONSABILIDADES Y CUMPLIMIENTOS

### 5.1. RESPONSABILIDADES

**Director(a) de LA VICEPRESIDENCIA DE LA REPÚBLICA:** En su calidad de tal, responde ante sus Superiores y el Sr. Vicepresidente de la República por la existencia y cumplimiento de las medidas que mantengan un nivel de Seguridad de la Información acorde con el rol de la organización y los recursos disponibles.

**Encargado de Seguridad:** Es el principal responsable en la definición de los criterios de Seguridad de la Información en LA VICEPRESIDENCIA DE LA REPÚBLICA, para lo cual deberá analizar periódicamente el nivel de riesgo existente, proponiendo soluciones. Una vez autorizada la implementación de las medidas, deberá coordinar con quienes corresponda su materialización oportuna y correcta.

**Comité de Seguridad:** Tiene por responsabilidad asesorar al Director(a) de LA VICEPRESIDENCIA DE LA REPÚBLICA, en temas de Seguridad de la Información, en coordinación con el Encargado de Seguridad.

**Responsable del Documento:** Tiene que mantener la aplicabilidad de este documento acorde a las prácticas operacionales de LA VICEPRESIDENCIA DE LA REPÚBLICA, por lo que es responsable de generar las modificaciones necesarias para que esté siempre actualizado. Además, es responsable de publicar y dar a conocer nuevas versiones del documento.

**Personal de LA VICEPRESIDENCIA DE LA REPÚBLICA:** tiene la responsabilidad de cumplir con lo formalizado en este documento y aplicarlo en su entorno laboral. Además, tiene la obligación de alertar de manera oportuna y adecuada, según lo determine las normas internas de la Institución, cualquier incidente que atente contra la Seguridad de la Información.

COPIA FIEL DEL ORIGINAL

Abg. Karina Bogado  
Secretaria General





## 5.2. CUMPLIMIENTOS

La presente Política de Seguridad de la Información entra en vigencia una vez oficializada las Autoridades de LA VICEPRESIDENCIA DE LA REPÚBLICA y, las jefaturas de los distintos Programas, Departamentos y Unidades de LA VICEPRESIDENCIA DE LA REPÚBLICA serán responsables de ponerlas en conocimiento de su personal subordinado.

Para el caso del personal que se contrate con posterioridad a la fecha de publicación, se le deberá entregar una copia del presente documento y hacer firmar una declaración de toma de conocimiento y aceptación de la misma.

La presente política está alineada con las directrices de las leyes y regulaciones existentes. Cualquier conflicto con estas regulaciones debe ser informado inmediatamente al responsable de este documento.

## 6. POLÍTICA

### 6.1. DE LA INFORMACIÓN INTERNA

- La información es un activo vital y todos sus accesos, usos y procesamiento, deberán ser consistentes con las políticas y estándares emitidos por LA VICEPRESIDENCIA DE LA REPÚBLICA en cada ámbito en particular.
- La información debe ser protegida, por sus custodios, de una manera consistente con su importancia, valor y criticidad, siguiendo las reglas establecidas en las políticas específicas de seguridad de la información, sus procedimientos asociados y en las recomendaciones dadas por el responsable designado de dicha información. Para ello, la DTICs de LA VICEPRESIDENCIA DE LA REPÚBLICA deberá proveer los recursos que permitan implementar los controles necesarios para otorgar el nivel de protección correspondiente al valor de los activos.
- Toda la información creada o procesada por la organización debe ser considerada como "Pública", a menos que se determine otro nivel de clasificación, pudiendo ser "Reservada" o "Secreta" de acuerdo a lo establecido en las leyes vigentes. Periódicamente se deberá revisar la clasificación, con el propósito de mantenerla o modificarla según se estime apropiado.
- LA VICEPRESIDENCIA DE LA REPÚBLICA proveerá los mecanismos para que la información sea accedida y utilizada por el personal que de acuerdo a sus funciones así lo requiera. Sin embargo, se reserva el derecho de revocar al personal, el privilegio de acceso a la información y tecnologías que la soportan, si la situación y las condiciones lo ameritan.

### 6.2. DE LA INFORMACIÓN DE LOS USUARIOS EXTERNOS

- Si la institución procesa y mantiene información de usuarios externos que sean datos personales y/o sensibles de acuerdo a la normativa vigente, la organización se compromete a asegurar que esta información no será divulgada sin previa autorización y estará protegida de igual manera que la información interna.
- En el caso que la información de usuarios externos que se procese y mantenga y que no tenga las características anteriormente mencionadas, esta podrá ser divulgada sin previa autorización.
- Si se requiere compartir información de los usuarios externos de LA VICEPRESIDENCIA DE LA REPÚBLICA con instituciones externas, con motivo de externalizar servicios, a éstas se le exigirá la firma de un contrato de confidencialidad y no divulgación, previo a la entrega de la información.

### 6.3. DE LAS AUDITORÍAS

- Con el fin de velar por el correcto uso de los activos de información de su propiedad, LA VICEPRESIDENCIA DE LA REPÚBLICA se reserva el derecho de auditar en todo momento y sin previo aviso, el cumplimiento de las políticas vigentes y que dicen relación con el acceso y uso que los usuarios hacen de los activos de información.
- LA VICEPRESIDENCIA DE LA REPÚBLICA se reserva el derecho de tomar medidas administrativas en contra del personal que no dé cumplimiento a lo dispuesto en la presente política, las políticas específicas que se deriven y en su documentación de referencia, acciones que pueden ser solicitadas por el responsable de la Dirección de Talento Humano o el Encargado de Seguridad.

COPIA FIEL DEL ORIGINAL

Abg. Karina Bogado  
Secretaría General



H.



#### 6.4. DEL COMPROMISO DE LA DTICS

- La DTICS velará por la existencia de un plan formal de difusión de esta política y las políticas específicas que la sustenten.
- Mediante la estructura que se defina en la política específica "Aspectos Organizativos de la Seguridad de la Información", procurará que todo el personal reciba un entrenamiento suficiente en materia de seguridad, consistente con sus necesidades y su rol dentro de LA VICEPRESIDENCIA DE LA REPÚBLICA.
- La DTICS propiciará la existencia de mecanismos o procedimientos formales que permitan asegurar la continuidad de los procesos ante situaciones que impidan el acceso a la información imprescindible para el funcionamiento de la Institución.

#### 6.5. DEBERES DEL PERSONAL

- La información y las tecnologías de información deben ser usadas sólo para propósitos relacionados con el servicio y autorizados por los supervisores, debiéndose aplicar criterios de buen uso en su utilización.
- Las claves de acceso a la información y a las tecnologías de información son individuales, intransferibles y de responsabilidad única de su propietario.
- El personal está en la obligación de alertar, de manera oportuna y adecuada, cualquier incidente que atente contra lo establecido en esta política según procedimientos establecido en las normas de la Institución.
- Está absolutamente prohibido al personal de la organización divulgar cualquier información que según el ordenamiento jurídico esté catalogada como "Reservada" o "Secreta", Organización y Mantenimiento de las Políticas

Con el objetivo de garantizar el cumplimiento de la Política de Seguridad de la Información y las políticas específicas que se definan posteriormente, LA VICEPRESIDENCIA DE LA REPÚBLICA ha establecido una estructura organizacional que contempla la definición de funciones específicas en el ámbito de seguridad, las cuales serán ejecutadas por el personal designado por las alta autoridades.

Las características de esta instancia organizacional y roles se detallan en el documento organizacional de la Institución.

#### 6.6. DIFUSIÓN DE LA POLÍTICA

Resulta clave para que la presente política se integre en la cultura organizacional, la existencia de un plan formal de difusión, capacitación y sensibilización en torno a la seguridad de la información.

Los Directores de LA VICEPRESIDENCIA DE LA REPÚBLICA serán los responsables de la existencia permanente y el cumplimiento de un plan formal de difusión, capacitación y sensibilización de la Seguridad de la Información.

El personal designado para la Seguridad de la Información es el responsable de la ejecución del plan y el cumplimiento de sus objetivos, así como la existencia de un plan comunicacional que lo complementa.

### 7. FORMATO Y MANTENCIÓN DE LAS POLÍTICAS

#### 7.1. FORMATO DE LAS POLÍTICAS

Toda política debe contener las siguientes secciones.

1. Introducción
2. Propósito
3. Alcance
4. Definiciones
5. La política en si
6. Aplicación de la política y responsabilidades
7. Historial de revisión

Asociada a cada política se deben emitir los mecanismos de control y las sanciones cuando se viola la política respectiva.

#### 7.2. MANTENCIÓN DE LA POLÍTICA

- La mantención de la presente política será realizada por el Personal Encargado de Seguridad de la Información y sus cambios aprobados por las Autoridades de LA VICEPRESIDENCIA DE LA REPÚBLICA.
- Las políticas específicas asociadas a la presente política y los procedimientos, deberán ser aprobadas por las Autoridades de la Institución.

COPIA FIEL DEL ORIGINAL

Abg. Karina Bogado  
Secretaria General





- El presente documento debe ser revisado a lo menos una vez al año y actualizado cada vez que se realicen cambios relevantes en LA VICEPRESIDENCIA DE LA REPÚBLICA, que afecten la adecuada protección de la información, considerando como tales entre otros, cambios en la misión, objetivos estratégicos, infraestructura, personal y/o procedimientos relacionados con la protección de la información.
- La DTICs solicitará al área de comunicaciones interna que difunda la política dependiendo del alcance de la misma y su importancia para la Institución.

### 1.1. DOCUMENTACIÓN DE REFERENCIA

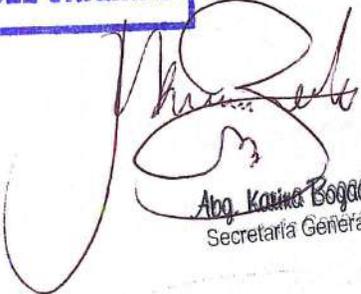
El presente documento constituye una Política de Alto Nivel, destinada a normar los aspectos más relevantes de la Gestión de Seguridad de la Información, con una vigencia de largo plazo, por lo cual la Vicepresidencia de la República emitirá Resoluciones de documentos adicionales que explicitan en mayor detalle las medidas de Seguridad de Alto Nivel dispuestas en el presente documento.

Dichos documentos deberían estar asociados a los dominios definidos en la ISO/IEC 27001- 2005 y su versión 2013, los cuales son:

- Organización de la Seguridad de la Información.
- Gestión de Activos.
- Seguridad de Talento Humano.
- Seguridad Física y del Ambiente.
- Gestión de las Operaciones y de las Comunicaciones.
- Control de Acceso.
- Adquisición, Desarrollo y Mantenimiento de Sistemas de Información.
- Gestión de Incidentes de la Seguridad de la Información.
- Gestión de Continuidad de Procesos Documentales.
- Cumplimiento.

COPIA FIEL DEL ORIGINAL



  
Abg. Karina Bogado  
Secretaría General

