


Departamento del Valle del Cauca  Gobernación	POLÍTICA DE SEGURIDAD DIGITAL	Código: PO-M11-P1-02
		Versión: 01
		Fecha de Aprobación: 06/11/2024
		Página: 1 de 10

POLÍTICA DE SEGURIDAD DIGITAL



Departamento del Valle del Cauca

Gobernación

CODIGO: PO-M11-P1-02

Versión: 01



Departamento del Valle del Cauca  Gobernación	POLÍTICA DE SEGURIDAD DIGITAL	Código:PO-M11-P1-02
		Versión: 01
		Fecha de Aprobación: 06/11/2024
		Página: 2 de 10

Tabla de Contenido

1. OBJETIVO.	3
2. ALCANCE	3
3. RESPONSABLES.	3
4. DEFINICIONES.	4
5. POLÍTICA DE SEGURIDAD DIGITAL DE LA GOBERNACIÓN DEL VALLE DEL CAUCA	5
5.1. Gestión de Riesgos de Seguridad de la Información:	5
5.2. Control de Acceso:	6
5.3. Protección de Datos:	6
5.4. Seguridad de Redes y Comunicaciones:	6
5.5. Seguridad de los endpoints:	7
5.6. Gestión de Incidentes de Seguridad:	7
5.7. Continuidad del Negocio:	8
5.8. Concienciación y Capacitación:	8
5.9. Cumplimiento y Auditoría:	9
6. CONDICIONES GENERALES	9
7. SOPORTE NORMATIVO Y DE REFERENCIA	9
8. REGISTROS Y ANEXOS	9

<p>Departamento del Valle del Cauca</p>  <p>Gobernación</p>	<p>POLÍTICA DE SEGURIDAD DIGITAL</p>	<p>Código:PO-M11-P1-02</p>
		<p>Versión: 01</p>
		<p>Fecha de Aprobación: 06/11/2024</p>
		<p>Página: 3 de 10</p>

1. OBJETIVO.

Establecer los lineamientos, principios, controles y responsabilidades para proteger los activos de información digital de la Gobernación del Valle del Cauca, garantizando su confidencialidad, integridad y disponibilidad, para minimizar los riesgos de seguridad digital, asegurar la continuidad de las operaciones y promover una cultura de ciberseguridad en la organización, en cumplimiento con las mejores prácticas y el marco legal vigente.

2. ALCANCE.

Inicia con la captura de datos en los sistemas de información de la Gobernación del Valle, a través de los medios digitales disponibles. También incluye la información recibida de fuentes externas, como ciudadanos, empresas, otras entidades gubernamentales o proveedores de servicios, finalizando con su disposición final o archivo.

Esta política aplica para todos las personas y entidades que interactúan con los sistemas de información y datos de la Gobernación del Valle del Cauca, incluyendo a todos los funcionarios públicos, empleados, contratistas, pasantes, proveedores de servicios externos y cualquier otra persona que tenga acceso a los recursos tecnológicos de la entidad, ya sea de forma directa o remota.

3. RESPONSABLES.

Todos los funcionarios, contratistas, pasantes, proveedores de servicios y demás personas naturales o jurídicas que interactúen con los sistemas de información y datos digitales de la Gobernación del Valle del Cauca, son responsables de cumplir con la presente Política. Este compromiso busca garantizar la confidencialidad, integridad y disponibilidad de la información digital en todas las actividades relacionadas con los planes, programas y proyectos de la entidad.


Roles y Responsabilidades

❖ Oficial de Seguridad de la Información (OSI):

- Liderar las actividades de seguridad digital en la entidad.
- Implementar y mantener los controles de seguridad digital.
- Gestionar los riesgos de seguridad digital.
- Gestionar los incidentes de seguridad digital.
- Reportar, a quien corresponda, el estado de la seguridad digital de la entidad.

❖ Personal directivo de la entidad:

- Asegurar que sus dependencias cumplan con la Política de Seguridad Digital.
- Implementar los controles de seguridad específicos en sus dependencias.
- Reportar al OSI cualquier incidente de seguridad digital.

<p>Departamento del Valle del Cauca</p>  <p>Gobernación</p>	<p>POLÍTICA DE SEGURIDAD DIGITAL</p>	Código:PO-M11-P1-02
		Versión: 01
		Fecha de Aprobación: 06/11/2024
		Página: 4 de 10

❖ **Funcionarios, Contratistas, Proveedores y Grupos de Valor:**

- Proteger los activos de información digital a los que tengan acceso autorizado.
- Reportar cualquier incidente de seguridad digital al OSI.

4. DEFINICIONES.

Activo de información digital: Cualquier información en formato electrónico que tenga valor para la Gobernación, incluyendo datos personales, información financiera, propiedad intelectual, registros públicos, software, hardware, servicios en la nube, etc.

Amenaza de seguridad: Evento o acción que podría comprometer la seguridad de los activos de información digital, como ataques cibernéticos (malware, phishing, ransomware, denegación de servicio), errores humanos, fallos de hardware o software, desastres naturales, etc.

Autenticación: Proceso de verificación de la identidad de un usuario, dispositivo o sistema antes de permitirle acceder a recursos digitales protegidos.

Confidencialidad: Propiedad de la información que garantiza que solo las personas, entidades o procesos autorizados puedan acceder a ella, protegiéndola de la divulgación no autorizada.


Control de acceso: Conjunto de medidas y procedimientos que regulan quién puede acceder a recursos digitales, qué acciones pueden realizar y bajo qué condiciones, garantizando la confidencialidad, integridad y disponibilidad de la información.

Control de seguridad: Medida implementada para reducir el riesgo de una amenaza de seguridad digital, como firewalls, antivirus, contraseñas seguras, cifrado, autenticación de dos factores, copias de seguridad, actualizaciones de software, etc.

Disponibilidad: Propiedad de la información que garantiza que está accesible y utilizable cuando se necesita, asegurando la continuidad de las operaciones y servicios que dependen de ella.

Gestión de riesgos: Proceso sistemático de identificación, análisis, evaluación y tratamiento de los riesgos que amenazan la seguridad de la información y los sistemas, con el objetivo de minimizar su impacto y probabilidad de ocurrencia.

Incidente de seguridad: Evento que compromete la seguridad de los activos de información digital, como una violación de datos, una infección de malware, una denegación de servicio, una pérdida de datos, etc.

<p>Departamento del Valle del Cauca</p>  <p>Gobernación</p>	<p>POLÍTICA DE SEGURIDAD DIGITAL</p>	<p>Código:PO-M11-P1-02</p>
		<p>Versión: 01</p>
		<p>Fecha de Aprobación: 06/11/2024</p>
		<p>Página: 5 de 10</p>

Integridad: Propiedad de la información que garantiza que no ha sido modificada, alterada o destruida sin autorización, manteniendo su exactitud, consistencia y fiabilidad a lo largo del tiempo.

Mejora continua: Proceso cíclico de revisión, análisis y optimización constante de las medidas de seguridad digital, adaptándose a las nuevas amenazas y vulnerabilidades para garantizar la protección de la información y los sistemas.

No repudio: Garantía de que el autor de una acción o comunicación digital no puede negar su participación, ya que existen pruebas irrefutables de su origen y/o recepción.

Riesgo de seguridad: Probabilidad de que una amenaza explote una vulnerabilidad y cause daño a los activos de información digital.


Vulnerabilidad: Debilidad en un sistema, red, aplicación, proceso o comportamiento humano que puede ser explotada por una amenaza.

5. POLÍTICA DE SEGURIDAD DIGITAL DE LA GOBERNACIÓN DEL VALLE DEL CAUCA.

La Gobernación del Valle del Cauca, consciente de la importancia de la seguridad de la información digital y del papel fundamental que desempeña en la protección de los datos de los ciudadanos y la continuidad de los servicios públicos, establece la presente Política que promueve una cultura de seguridad en todos los niveles de la organización, basada en los lineamientos del Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC) y las mejores prácticas nacionales e internacionales en materia de seguridad de la información, a través de las siguientes acciones:

5.1. Gestión de Riesgos de Seguridad de la Información:

- **Identificación de Activos:** Generar y mantener actualizado un inventario exhaustivo de todos los activos de información de la Gobernación, incluyendo hardware, software, datos y servicios en la nube.
- **Análisis de Riesgos:** Realizar un análisis de riesgos para identificar y evaluar las amenazas y vulnerabilidades que podrían afectar la confidencialidad, integridad y disponibilidad de los activos de información.
- **Evaluación de Riesgos:** Evaluar el impacto potencial de los riesgos identificados, considerando la probabilidad de ocurrencia y las consecuencias para la Gobernación.

<p>Departamento del Valle del Cauca</p>  <p>Gobernación</p>	<p>POLÍTICA DE SEGURIDAD DIGITAL</p>	<p>Código:PO-M11-P1-02</p>
		<p>Versión: 01</p>
		<p>Fecha de Aprobación: 06/11/2024</p>
		<p>Página: 6 de 10</p>

- **Tratamiento de Riesgos:** Implementar medidas de control adecuadas para mitigar, transferir o aceptar los riesgos identificados, priorizando aquellos con mayor impacto potencial.
- **Monitoreo y Revisión:** Realizar un monitoreo continuo de los riesgos y se revisarán periódicamente las evaluaciones de riesgos para asegurar su vigencia y efectividad.


5.2. Control de Acceso:

- **Autenticación:** Implementar mecanismos de autenticación robustos, como contraseñas fuertes, autenticación de dos factores y certificados digitales, para garantizar que solo el personal autorizado pueda acceder a los sistemas y datos.
- **Autorización:** Establecer reglas de autorización claras y específicas para cada rol y función, definiendo los permisos de acceso y las acciones permitidas en cada sistema y recurso de información.
- **Gestión de Identidades:** Implementar un sistema de gestión de identidades para controlar el ciclo de vida de las cuentas de usuario, desde su creación y modificación hasta su eliminación, asegurando la correcta asignación de permisos y el cumplimiento de la política de contraseñas.

5.3. Protección de Datos:

- **Clasificación de Datos:** Clasificar los datos según su nivel de sensibilidad, aplicando medidas de protección proporcionales al riesgo.
- **Cifrado:** Implementar mecanismos de cifrado robustos para asegurar la confidencialidad de los datos durante su transmisión, evitando que puedan ser leídos o utilizados por personas no autorizadas en caso de interceptación o pérdida.
- **Consentimiento y Derechos de los Titulares:** Respetar los derechos de los titulares de los datos personales, como el acceso, rectificación, cancelación y oposición, de acuerdo con la Ley 1581 de 2012 y demás normativa aplicable.

5.4. Seguridad de Redes y Comunicaciones:

<p>Departamento del Valle del Cauca</p>  <p>Gobernación</p>	<p>POLÍTICA DE SEGURIDAD DIGITAL</p>	Código:PO-M11-P1-02
		Versión: 01
		Fecha de Aprobación: 06/11/2024
		Página: 7 de 10


- **Segmentación de Redes:** Segmentar la red en diferentes zonas de seguridad, separando los sistemas y datos críticos de aquellos menos sensibles, y aplicando controles de acceso específicos para cada zona.
- **Firewalls:** Implementar equipos cortafuegos para controlar el tráfico de red entrante y saliente, permitiendo solo las comunicaciones autorizadas y bloqueando el acceso no autorizado.
- **Seguridad de las aplicaciones:** Garantizar la seguridad de las aplicaciones mediante la implementación de un firewall de aplicaciones web (WAF) que brinde protección contra ataques de tipo web. Así mismo, se debe mantener actualizadas las aplicaciones con los últimos parches de seguridad.
- **Seguridad en la nube:** Gestionar la seguridad en la nube mediante una evaluación rigurosa de los proveedores de servicios, verificando su cumplimiento con los requisitos de seguridad establecidos por la Gobernación del Valle del Cauca, así como configurar de manera segura los servicios en la nube para minimizar los riesgos y monitorear constantemente la actividad en la nube para detectar anomalías.
- **Redes Privadas Virtuales (VPN):** Utilizar VPN para asegurar las comunicaciones a través de redes públicas, como Internet, garantizando la confidencialidad e integridad de los datos transmitidos.

5.5. Seguridad de los endpoints:

- **Software antivirus y antimalware actualizado:** Mantener el software de protección contra virus y malware actualizado para detectar y eliminar las últimas amenazas.
- **Control de aplicaciones:** Restringir la ejecución de software no autorizado en los dispositivos para prevenir la instalación de programas maliciosos.
- **Gestión de parches:** Aplicar actualizaciones de seguridad de manera regular para corregir vulnerabilidades conocidas en los sistemas operativos y aplicaciones.

5.6. Gestión de Incidentes de Seguridad:

- **Detección y Reporte:** Establecer mecanismos para detectar y reportar incidentes de seguridad de manera oportuna, incluyendo canales de comunicación claros y accesibles para todo el personal.

<p>Departamento del Valle del Cauca</p>  <p>Gobernación</p>	<p>POLÍTICA DE SEGURIDAD DIGITAL</p>	Código:PO-M11-P1-02
		Versión: 01
		Fecha de Aprobación: 06/11/2024
		Página: 8 de 10


- **Análisis y Contención:** Llevar a cabo un análisis exhaustivo de cada incidente para determinar su causa, alcance e impacto, y se deben implementar medidas de contención para limitar los daños y prevenir la propagación.
- **Erradicación y Recuperación:** Eliminar las causas del incidente y restaurar los sistemas y datos afectados a su estado original, utilizando copias de seguridad y otros mecanismos de recuperación.
- **Lecciones Aprendidas:** Documentar las lecciones aprendidas de cada incidente e implementar mejoras en los procesos y controles de seguridad para prevenir futuros incidentes similares.

5.7. Continuidad del Negocio:

- **Evaluación de riesgos:** Identificar y evaluar los riesgos que podrían causar una interrupción, como desastres naturales, fallos tecnológicos, ciberataques, pandemias, etc.
- **Estrategias de recuperación:** Desarrollar estrategias y planes para recuperar las funciones críticas del negocio en caso de una interrupción, incluyendo la identificación de recursos alternativos, acuerdos con proveedores, equipos de emergencia, etc.
- **Planes de comunicación:** Establecer estrategias de comunicación para mantener informados a los empleados, clientes, proveedores y otras partes interesadas durante una interrupción.
- **Pruebas y Ejercicios:** Realizar pruebas y ejercicios periódicos para validar la efectividad de los planes de continuidad y recuperación, identificar áreas de mejora y asegurar que el personal esté preparado para responder a una emergencia.

5.8. Concienciación y Capacitación:

- **Programa de Concienciación:** Implementar un programa de concienciación sobre seguridad de la información para todo el personal, incluyendo charlas, talleres, boletines informativos y campañas de comunicación, para fomentar una cultura de seguridad y promover las buenas prácticas.
- **Capacitación en Seguridad:** Proporcionar capacitación específica en seguridad de la información a los empleados, contratistas y proveedores de servicios, adaptada a sus roles y responsabilidades, para que puedan identificar y responder a las amenazas de seguridad de manera efectiva.

<p>Departamento del Valle del Cauca</p>  <p>Gobernación</p>	<p>POLÍTICA DE SEGURIDAD DIGITAL</p>	<p>Código:PO-M11-P1-02</p>
		<p>Versión: 01</p>
		<p>Fecha de Aprobación: 06/11/2024</p>
		<p>Página: 9 de 10</p>

- **Evaluación y Refuerzo:** Evaluar periódicamente la efectividad de las actividades de concienciación y capacitación, realizando ajustes y refuerzos según sea necesario para asegurar un nivel adecuado de conocimiento y conciencia sobre la seguridad de la información en toda la organización.

5.9. Cumplimiento y Auditoría:

La Gobernación del Valle del Cauca, en cumplimiento de su política de seguridad digital, se compromete a monitorear y medir de manera continua el cumplimiento y la eficacia de los controles de seguridad digital implementados. Se realizarán auditorías internas y externas periódicas para identificar y corregir cualquier no conformidad con la política, así como para revisar y actualizar los controles de seguridad digital según sea necesario, asegurando así su relevancia y eficacia frente a las amenazas en constante evolución.


6. CONDICIONES GENERALES

- El incumplimiento de esta Política podrá dar lugar a acciones disciplinarias, de acuerdo con la normativa interna de la Gobernación y la legislación aplicable.
- Se espera que todos los empleados y partes interesadas colaboren activamente en el cumplimiento de esta Política, reportando cualquier incidente de seguridad o vulnerabilidad que detecten.
- Cualquier excepción a esta Política deberá ser solicitada por escrito al Oficial de Seguridad de la Información, quien evaluará la solicitud y determinará si se justifica la excepción, teniendo en cuenta los riesgos de seguridad involucrados.
- Las excepciones aprobadas deberán ser documentadas y revisadas periódicamente para garantizar que sigan siendo necesarias y que no comprometan la seguridad digital de la Gobernación.
- Esta Política entra en vigencia a partir de la fecha de su aprobación y se mantendrá vigente hasta que sea modificada o reemplazada por una nueva política.

7. SOPORTE NORMATIVO Y DE REFERENCIA

Ver Normograma del proceso.

8. REGISTROS Y ANEXOS

Departamento del Valle del Cauca  Gobernación	POLÍTICA DE SEGURIDAD DIGITAL	Código: PO-M11-P1-02
		Versión: 01
		Fecha de Aprobación: 06/11/2024
		Página: 10 de 10

No aplica.

CONTROL DE CAMBIOS		
Versión	Descripción del cambio	Fecha
1	creación del documento donde se establecen los lineamientos básicos de seguridad digital, conforme a la norma fundamental de la documentación del MIPG/SGC/SCI.	06/11/2024

ELABORÓ	REVISÓ	APROBÓ
Nombre: Carlos Marino Santacruz, Valentina Duarte España, Waldor Drada	Nombre: Héctor Fabio Bedoya Bedoya	Mesa de Trabajo con el Proceso M1-P3 Administración del MIPG. Acta No. 053 del 06 de noviembre del 2024.
Cargo: Profesional Universitario, Contratista	Cargo: Líder de Programa	Comité Institucional de Gestión y Desempeño. Acta No. 009 del 26 de noviembre del 2024.
Firma: 	Firma: 	
Fecha: 06/11/2024	Fecha: 06/11/2024	Fecha: 06/11/2024