



GOBERNACIÓN  
de BOLÍVAR

DESPACHO DEL GOBERNADOR

## RESOLUCION No. 261 2023

**"Por la cual se conforma el Comité de Seguridad de la Información, se definen sus funciones y se adopta la Estrategia de Seguridad Digital de la Gobernación de Bolívar"**

**EL GOBERNADOR DEL DEPARTAMENTO DE BOLÍVAR**

En uso de sus atribuciones legales y

### CONSIDERANDO

Que el Decreto 222 de 2022 de la Gobernación de Bolívar *"Por medio del cual se Actualiza el Modelo Integrado de Planeación y Gestión -MIPG en la Gobernación de Bolívar, establecido en el decreto No. 169 de 2018 y Decreto 489 de 2018"*, especifica que la Dirección de Tecnologías de la Información y las Comunicaciones es responsable de la Políticas de Gobierno Digital y de Seguridad Digital del equipo de trabajo de la dimensión Gestión con Valores para el Resultado.

Que la Resolución 247 de 2020 de la Gobernación de Bolívar, *"Por medio de la cual se adopta la actualización del Manual para la Administración del Riesgo de la Gobernación de Bolívar y se dictan otras disposiciones"* permitirá fortalecer la implementación y desarrollo de las prácticas de la Administración del Riesgo en la Gobernación de Bolívar, a través del adecuado tratamiento de los riesgos de gestión, de corrupción y de seguridad digital, controlando las situaciones que puedan impactar en el cumplimiento de su misión y sus objetivos institucionales.

Que en el Decreto 1008 de 2018, emanado del Ministerio de Tecnologías de la Información y las Comunicaciones, *"Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones"*, tiene por objeto *el uso y aprovechamiento de las tecnologías de la información y las comunicaciones para consolidar un Estado y ciudadanos competitivos, proactivos, e innovadores, que generen valor público en un entorno de confianza digital.*

Que en el mismo sentido, el Gobierno Nacional ha publicado varios documentos como el CONPES No. 3701, por medio del cual se establecieron los *"Lineamientos de Política para Ciberseguridad y Ciberdefensa"*, cuyo objetivo central es *"Fortalecer las capacidades del Estado para enfrentar las amenazas que atentan contra su seguridad y defensa en el ámbito cibernético (ciberseguridad y ciberdefensa), creando el ambiente y las condiciones necesarias para brindar protección en el ciberespacio."*

El CONPES No. 3854 *"Política Nacional de Seguridad Digital"*, cuyo objetivo general es *"Fortalecer las capacidades de las múltiples partes interesadas para identificar, gestionar, tratar y mitigar los riesgos de seguridad digital en sus actividades socioeconómicas en el entorno digital, en un marco de cooperación, colaboración y asistencia. Lo anterior, con el fin de contribuir al crecimiento de la economía digital nacional, lo que a su vez impulsará una mayor prosperidad económica y social en el país."*

El CONPES No. 3995 *"Política Nacional de Confianza y Seguridad Digital"*, el cual estableció las *"medidas para desarrollar la confianza digital a través de la mejora la seguridad digital de manera que Colombia sea una sociedad incluyente y competitiva en el futuro digital"*

**Bolívar  
primero**



GOBERNACIÓN  
de BOLÍVAR

DESPACHO DEL GOBERNADOR

## RESOLUCION No. 261 2023

**"Por la cual se conforma el Comité de Seguridad de la Información, se definen sus funciones y se adopta la Estrategia de Seguridad Digital de la Gobernación de Bolívar"**

*mediante el fortalecimiento de capacidades y la actualización del marco de gobernanza en seguridad digital, así como con la adopción de modelos con énfasis en nuevas tecnologías."*

Que la Resolución 500 de 2021 del Ministerio de Tecnologías de la Información y las Comunicaciones "*Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital*", en sus lineamientos Generales resolvió que "*... Las entidades deben contar con políticas, procesos, procedimientos, guías, manuales y formatos para garantizar el cumplimiento al ciclo PHVA del MSPI. En ese sentido, deben adoptar los lineamientos del MSPI, guía de riesgos y gestión de incidentes de seguridad digital que se relacionan en el Anexo 1 de la presente resolución.*" Además, "*Los sujetos obligados deben adoptar la estrategia de seguridad digital en la que se integren los principios, políticas, procedimientos, guías, manuales, formatos y lineamientos para la gestión de la seguridad de la información digital...*"

Que la Resolución 746 del 2022 "*Por la cual se fortalece el Modelo de Seguridad y Privacidad de la Información y se definen lineamientos adicionales a los establecidos en la Resolución No. 500 de 2021*" amplía el alcance de la Resolución No. 500 de 2021 de protección de datos personales, servicios de nube y relación con proveedores.

Que el día 28 de noviembre de 2021 los miembros del Comité Institucional de Gestión y Desempeño de la Gobernación de Bolívar se reunieron con el objetivo de presentar y aprobar los planes de acción de MIPG, y además establecer cómo se implementaría lo estipulado por el Ministerio de Tecnologías de la Información en la Resolución No. 500 de 2021.

Que en la mencionada reunión se decidió: **i)** adoptar la Resolución No. 500 de 2021 emanada del Ministerio de Tecnologías de la Información "*Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital*"; **ii)** Conformar el Comité de Seguridad de la Información y se definen sus funciones; y **iii)** Adoptar la Estrategia de Seguridad Digital de la Gobernación de Bolívar.

Que en mérito de lo expuesto.

### RESUELVE

#### **ARTÍCULO PRIMERO: Conformación del Comité de Seguridad de la Información.**

Créase el Comité de Seguridad de la Información de la Gobernación de Bolívar. El Comité estará integrado así:

1. Secretario General Como encargado de la gestión de estas políticas
2. El Director de Tecnologías de la Información y de las Comunicaciones o su delegado.
3. El Secretario de Planeación o su delegado.
4. El Secretario Jurídico o su delegado.
5. El Director de Atención al Ciudadano y Gestión Documental o su delegado.
6. El Jefe de la Oficina de Control Interno o su delegado.

**Bolívar  
primero**



GOBERNACIÓN  
de BOLÍVAR

DESPACHO DEL GOBERNADOR

## RESOLUCION No. 261 2023

**“Por la cual se conforma el Comité de Seguridad de la Información, se definen sus funciones y se adopta la Estrategia de Seguridad Digital de la Gobernación de Bolívar”**

**Parágrafo:** El Comité podrá invitar a cada sesión, con voz y sin voto, a aquellas personas que considere necesarias por la naturaleza de los temas a tratar.

**ARTÍCULO SEGUNDO: Objetivo del Comité de Seguridad de la Información.** El Comité deberá asegurar que exista una dirección y apoyo gerencial para soportar la administración y desarrollo de iniciativas sobre seguridad de la información, a través de compromisos apropiados y uso de recursos adecuados en el organismo, así como de la formulación y mantenimiento de una política de seguridad de la información a través de todo el organismo.

**ARTÍCULO TERCERO: Funciones del Comité.** El Comité de Seguridad de la Información de la Gobernación de Bolívar tendrá dentro de sus funciones las siguientes:

1. Coordinar la implementación del Modelo de Seguridad y privacidad de la Información al interior de la entidad.
2. Revisar los diagnósticos del estado de la seguridad de la información en la Gobernación de Bolívar.
3. Acompañar e impulsar el desarrollo de proyectos de seguridad.
4. Coordinar y dirigir acciones específicas que ayuden a proveer un ambiente seguro y establecer los recursos de información que sean consistentes con las metas y objetivos de la Gobernación de Bolívar.
5. Recomendar roles y responsabilidades específicos que se relacionen con la seguridad de la información.
6. Aprobar el uso de metodologías y procesos específicos para la seguridad de la información.
7. Participar en la formulación y evaluación de planes de acción para mitigar y/o eliminar riesgos.
8. Realizar revisiones periódicas del SGSI y según los resultados de esta revisión definir las acciones pertinentes.
9. Promover la difusión y sensibilización de la seguridad de la información dentro de la entidad.
10. Poner en conocimiento de la entidad, los documentos generados al interior del comité de seguridad de la información que impacten de manera transversal a la misma.
11. Las demás funciones inherentes a la naturaleza del Comité.

**Parágrafo:** Una vez conformado el Comité de Seguridad de la Información, este expedirá su reglamento, en el cual fijará el alcance de cada una de las funciones operativas señaladas en el presente artículo.

**ARTÍCULO CUARTO: Secretaria Técnica:** La Secretaría Técnica será ejercida por el Director de Tecnologías de la Información y de las Comunicaciones o su delegado.

**ARTÍCULO QUINTO: Funciones de la Secretaría Técnica.** Las funciones de la Secretaría Técnica serán las siguientes:

1. Elaborar las actas de las reuniones del Comité y verificar su formalización por parte de sus miembros.
2. Citar a los integrantes del Comité a las sesiones ordinarias o extraordinarias
3. Remitir oportunamente a los miembros la agenda de cada comité.
4. Llevar la custodia y archivo de las actas y demás documentos soportados.

**Bolívar**  
**primero**



GOBERNACIÓN  
de BOLÍVAR

DESPACHO DEL GOBERNADOR

## RESOLUCION No. 2612023

**“Por la cual se conforma el Comité de Seguridad de la Información, se definen sus funciones y se adopta la Estrategia de Seguridad Digital de la Gobernación de Bolívar”**

5. Servir de interlocutor entre terceros y el Comité.
6. Realizar seguimiento a los compromisos y tareas pendientes del Comité.
7. Presentar los informes que requiera el Comité.
8. Las demás que le sean asignadas por el Comité.

### **ARTÍCULO SEXTO: Reuniones del Comité de Seguridad de la Información.**

El Comité de Seguridad de la Información deberá reunirse 1 vez cada 6 meses previa convocatoria del Secretario Técnico del Comité y de forma extraordinaria cuando sea necesario, de acuerdo con temas de riesgos, incidentes o afectaciones de continuidad dentro del Sistema de Gestión de Seguridad de la Información.

**ARTÍCULO SEPTIMO: Adopción de la Estrategia de Seguridad Digital:** Adóptese la Estrategia de Seguridad Digital en la que se integren los principios, políticas, procedimientos, guías, manuales, formatos y lineamientos del Modelo de Seguridad y Privacidad de la información.

**ARTÍCULO OCTAVO: Objetivo de la Estrategia de Seguridad Digital:** Adoptar la Resolución 500 de marzo 10 de 2021 “Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital” El objetivo deberá ser la protección de la información

**ARTÍCULO NOVENO: Acciones de la Estrategia de Seguridad Digital:** Las acciones a realizar en la Estrategia de Seguridad Digital están definidas en el Plan de Seguridad y Privacidad de la Información.

**ARTÍCULO DECIMO: Resultados de la Estrategia de Seguridad Digital:** Alcanzar el Nivel de Madurez **Definido** al finalizar la implementación de la Estrategia de Seguridad de la Información.

**ARTÍCULO DECIMO PRIMERO: Tiempos de la Estrategia de Seguridad Digital:** Los tiempos para realizar las actividades de la Estrategia de Seguridad Digital están articulados al Plan de Seguridad y Privacidad de la Información 2020-2023.

**ARTÍCULO DECIMO SEGUNDO: Métricas de la Estrategia de Seguridad Digital:** Las métricas a utilizar están descritas en el Anexo 1 Indicadores de Gestión de Seguridad de la Información de la Resolución 500 de 2021 del Ministerio de las Tecnologías de la Información y las Comunicaciones, y en la Tabla 6 - Características de los Niveles de Madurez del Modelo de Seguridad y Privacidad de la Información (MSPI).

### **INDICADOR 01- ORGANIZACIÓN DE SEGURIDAD DE LA INFORMACIÓN**

<b>INDICADOR 01- ORGANIZACIÓN DE SEGURIDAD DE LA INFORMACIÓN</b>	
<b>IDENTIFICADOR</b>	SGIN01
<b>DEFINICIÓN</b>	
El indicador permite determinar y hacer seguimiento, al compromiso de la dirección, en cuanto a seguridad de la información, en lo relacionado con la asignación de personas y responsabilidades relacionadas a la seguridad de la información al interior de la entidad	

**Bolívar  
primero**



GOBERNACIÓN  
de BOLÍVAR

DESPACHO DEL GOBERNADOR

## RESOLUCION No. 261 2023

**“Por la cual se conforma el Comité de Seguridad de la Información, se definen sus funciones y se adopta la Estrategia de Seguridad Digital de la Gobernación de Bolívar”**

<b>OBJETIVO</b>					
Hacer un seguimiento a la asignación de recursos y responsabilidades en gestión de seguridad de la información, por parte de la alta dirección.					
<b>TIPO DE INDICADOR</b>					
Indicador de Gestión					
<b>DESCRIPCIÓN DE VARIABLES</b>		<b>FORMULA</b>		<b>FUENTE DE INFORMACIÓN</b>	
VSI01: Número de personas con su respectivo rol definió según el modelo de operación capítulo 2.		(VSI01/VSI02) *100		Capítulo 2 de la guía del modelo de operación del marco de seguridad y privacidad de la información.	
VSI02: Número de personas con su respectivo rol definió después de un año.				Actas de asignación de personal.	
<b>METAS</b>					
<b>MÍNIMA</b>	75-80%	<b>SATISFACTORIA</b>	80- 90%	<b>SOBRESALIENTE</b>	100%
<b>OBSERVACIONES</b>					
De acuerdo a lo establecido en el capítulo 2 de la guía del modelo de operación del marco de seguridad y privacidad de la información, es necesario crear nuevos cargos y asignar responsabilidades en los actuales, por lo tanto, el indicador está enfocado, no solo a la contratación de nuevas personas, sí no a la asignación de responsabilidades.					

### INDICADOR 02 - CUBRIMIENTO DEL SGSI EN ACTIVOS DE INFORMACIÓN

<b>INDICADOR 02 - CUBRIMIENTO DEL SGSI EN ACTIVOS DE INFORMACIÓN.</b>		
<b>IDENTIFICADOR</b>	SGIN02	
<b>DEFINICIÓN</b>		
El indicador permite determinar y hacer seguimiento al cubrimiento que se realiza a nivel de activos <b>críticos</b> de información de una entidad y los controles aplicados.		
<b>OBJETIVO</b>		
Hacer un seguimiento a la inclusión de nuevos activos críticos de información y su control, dentro del marco de seguridad y privacidad de la información.		
<b>TIPO DE INDICADOR</b>		
Indicador de Gestión		
<b>DESCRIPCIÓN DE VARIABLES</b>	<b>FORMULA</b>	<b>FUENTE DE INFORMACIÓN</b>
VSI03: Número de activos críticos de información incluidos en el alcance de implementación del modelo, incluidos en la zona de riesgo inaceptable y la implementación del control no requiere adquisición de elementos de hardware o software.	(VSI03/VSI04) *100	Alcance del SGSI, Inventario de Activos de información, plan de tratamiento, matriz de riesgos
VSI04: Número de activos críticos de información incluidos en el alcance de		Inventario de Activos de información, nuevos

**Bolívar**  
**primero**



GOBERNACIÓN  
de BOLÍVAR

DESPACHO DEL GOBERNADOR

## RESOLUCION No. 261 2023

**“Por la cual se conforma el Comité de Seguridad de la Información, se definen sus funciones y se adopta la Estrategia de Seguridad Digital de la Gobernación de Bolívar”**

implementación del modelo; activos incluidos en la zona de riesgo inaceptable.		
<b>METAS</b>		
<b>MÍNIMA</b>	75-80%	<b>SATISFACTORIA</b> 80- 90% <b>SOBRESALIENTE</b> 100%
<b>OBSERVACIONES</b>		
El indicador de cada proceso debe ser recolectado y promediado para construir un indicador que refleje el estado a nivel empresa. El término “incluir un activo” debe ser entendido como realizar la correcta clasificación del activo, tratamiento, evaluación de riesgos sobre el mismo y determinación de controles para minimizar el riesgo calculado. Para este indicador, solo se tienen en cuenta los controles que no implican adquisición de hardware o software.		

### **INDICADOR 03 - TRATAMIENTOS DE EVENTOS RELACIONADOS EN MARCO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN**

<b>INDICADOR 03 - TRATAMIENTOS DE EVENTOS RELACIONADOS EN MARCO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN</b>		
<b>IDENTIFICADOR</b>	SGIN03	
<b>DEFINICIÓN</b>		
El indicador permite determinar la eficiencia en el tratamiento de eventos relacionados la seguridad de la información. Los eventos serán reportados por los usuarios o determinadas en las auditorías planeadas para el sistema.		
<b>OBJETIVO</b>		
El objetivo del indicador es reflejar la gestión y evolución del modelo de seguridad y privacidad de la información al interior de una entidad		
<b>TIPO DE INDICADOR</b>		
Indicador de Gestión		
<b>DESCRIPCIÓN DE VARIABLES</b>	<b>FORMULA</b>	<b>FUENTE DE INFORMACIÓN</b>
VSI05: Número de anomalías cerradas.	$(VSI05/VSI06) * 100$	Auditorías internas, herramientas de monitoreo
VSI06: Número total de anomalías encontradas.		Auditorías internas, herramientas de monitoreo
<b>METAS</b>		
<b>MÍNIMA</b>	75-80%	<b>SATISFACTORIA</b> 80- 90% <b>SOBRESALIENTE</b> 100%
<b>OBSERVACIONES</b>		

### **INDICADOR 04 – PLAN DE SENSIBILIZACIÓN**

<b>INDICADOR 04 – PLAN DE SENSIBILIZACIÓN</b>	
<b>IDENTIFICADOR</b>	SGIN04
<b>DEFINICIÓN</b>	
El indicador permite medir la aplicación de los temas sensibilizados en seguridad de la información por parte de los usuarios finales. Estas mediciones se podrán realizar por medio de auditorías especializadas en el tema o de forma aislada por parte de los responsables de la capacitación y sensibilización.	

**Bolívar  
primero**



GOBERNACIÓN  
de BOLÍVAR

DESPACHO DEL GOBERNADOR

## RESOLUCION No. 261 2023

**“Por la cual se conforma el Comité de Seguridad de la Información, se definen sus funciones y se adopta la Estrategia de Seguridad Digital de la Gobernación de Bolívar”**

<b>OBJETIVO</b>					
El objetivo del indicador es establecer la efectividad de un plan de capacitación y sensibilización previamente definido como medio para el control de incidentes de seguridad.					
<b>TIPO DE INDICADOR</b>					
Indicador de Gestión					
<b>DESCRIPCIÓN DE VARIABLES</b>	<b>FORMULA</b>		<b>FUENTE DE INFORMACIÓN</b>		
VSI07: Número de fallas o no cumplimientos encontrados en las sensibilizaciones programadas o eventos realizados para evaluar el tema.	(VSI07/VSI08) *100		Oficial de Seguridad de la Información, auditorías internas, atención al usuario, listas de asistencia		
VSI08: Total de personal a capacitar.			Total de funcionarios de la entidad.		
<b>METAS</b>					
<b>MÍNIMA</b>	<b>75-80%</b>	<b>SATISFACTORIA</b>	<b>80- 90%</b>	<b>SOBRESALIENTE</b>	<b>100%</b>
<b>OBSERVACIONES</b>					
Para el levantamiento de la información que permita obtener datos para la medición el responsable debe idear planes, laboratorios o actividades periódicas que permitan medir lo capacitado o divulgado.					

### **INDICADOR 05 – CUMPLIMIENTO DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN EN LA ENTIDAD**

<b>INDICADOR 05 – CUMPLIMIENTO DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN EN LA ENTIDAD</b>		
<b>IDENTIFICADOR</b>	SGIN05	
<b>DEFINICIÓN</b>		
Cumplimiento de políticas de seguridad de la información en la entidad		
<b>OBJETIVO</b>		
Busca identificar el nivel de estructuración de los procesos de la entidad orientados a la seguridad de la información.		
<b>TIPO DE INDICADOR</b>		
Indicador de Cumplimiento		
<b>DESCRIPCIÓN DE VARIABLES</b>	<b>FORMULA</b>	<b>FUENTE DE INFORMACIÓN</b>
VSI09: ¿La entidad ha definido una política general de seguridad de la información?	VSI0X = 1 (Sí se evidencia) VSI0X = 0 (NO se evidencia)	Guía del Modelo de Operación / Usuarios Internos
VSI10: ¿La entidad ha definido una organización interna en términos de personas y responsabilidades con el fin de cumplir las políticas de seguridad de la información y documenta estas actividades?		Guía del Modelo de Operación / Usuarios Internos
VSI11: ¿La entidad cumple con los requisitos legales, reglamentarios y		Guía del Modelo de Operación / Usuarios Internos

**Bolívar  
primero**



GOBERNACIÓN  
de BOLÍVAR

DESPACHO DEL GOBERNADOR

## RESOLUCION No. 2612023

**“Por la cual se conforma el Comité de Seguridad de la Información, se definen sus funciones y se adopta la Estrategia de Seguridad Digital de la Gobernación de Bolívar”**

contractuales con respecto al manejo de la información?		
<b>METAS</b>		
<b>CUMPLE</b>	1	<b>NO CUMPLE</b> 0
<b>OBSERVACIONES</b>		

### INDICADOR 06 – IDENTIFICACIÓN DE LINEAMIENTOS DE SEGURIDAD DE LA ENTIDAD

<b>INDICADOR 06 – IDENTIFICACIÓN DE LINEAMIENTOS DE SEGURIDAD DE LA ENTIDAD</b>		
<b>IDENTIFICADOR</b>	SGIN06	
<b>DEFINICIÓN</b>		
Grado de la seguridad de la información y los equipos de cómputo.		
<b>OBJETIVO</b>		
Busca medir el nivel de preparación del recurso humano y su apropiación en cuanto a la seguridad de la información y los equipos de cómputo.		
<b>TIPO DE INDICADOR</b>		
Indicador de Cumplimiento		
<b>DESCRIPCIÓN DE VARIABLES</b>	<b>FORMULA</b>	<b>FUENTE DE INFORMACIÓN</b>
VSI12: ¿La entidad ha definido lineamientos de trabajo a través del comité o responsable de seguridad para que sus funcionarios cumplan las políticas de seguridad y evalúa periódicamente su pertinencia?	VSI0X = 1 (Sí se evidencia) VSI0X = 0 (NO se evidencia)	Usuarios Internos.
VSI13: ¿La entidad ha definido lineamientos en cuanto a la protección de las instalaciones físicas, equipos de cómputo y su entorno para evitar accesos no autorizados y minimizar riesgos de la información de la entidad?		Usuarios Internos.
<b>METAS</b>		
<b>CUMPLE</b>	1	<b>NO CUMPLE</b> 0
<b>OBSERVACIONES</b>		

### INDICADOR 07 – VERIFICACIÓN DEL CONTROL DE ACCESO

<b>INDICADOR 07 – VERIFICACIÓN DEL CONTROL DE ACCESO</b>	
<b>IDENTIFICADOR</b>	SGIN07
<b>DEFINICIÓN</b>	
Grado control de acceso en la entidad.	
<b>OBJETIVO</b>	
Busca identificar la existencia de lineamientos, normas o estándares en cuanto al control de acceso en la entidad.	
<b>TIPO DE INDICADOR</b>	
Indicador de Cumplimiento	

**Bolívar**  
**primero**



GOBERNACIÓN  
de BOLÍVAR

DESPACHO DEL GOBERNADOR

## RESOLUCION No. 261 2023

**“Por la cual se conforma el Comité de Seguridad de la Información, se definen sus funciones y se adopta la Estrategia de Seguridad Digital de la Gobernación de Bolívar”**

DESCRIPCIÓN DE VARIABLES	FORMULA	FUENTE DE INFORMACIÓN
VS14: ¿La entidad ha definido lineamientos, normas y/o estándares para controlar el acceso de los usuarios a sus servicios de Gobierno en línea y a sus redes de comunicaciones?	VSIOX = 1 (Sí se evidencia) VSIOX = 0 (NO se evidencia)	Usuarios Internos.
VS15: ¿La entidad ha definido lineamientos, normas y/o estándares para controlar el uso y el acceso a los sistemas de información, las aplicaciones y los depósitos de información con las que cuenta la entidad?		Usuarios Internos.
VS16: ¿La entidad ha definido lineamientos, normas y/o estándares para controlar las terminales móviles y accesos remotos a los recursos de la entidad?		
<b>METAS</b>		
<b>CUMPLE</b>	1	<b>NO CUMPLE</b> 0
<b>OBSERVACIONES</b>		

### INDICADOR 08 – ASEGURAMIENTO EN LA ADQUISICIÓN Y MANTENIMIENTO DE SOFTWARE

INDICADOR 08 – ASEGURAMIENTO EN LA ADQUISICIÓN Y MANTENIMIENTO DE SOFTWARE		
IDENTIFICADOR	SGIN08	
DEFINICIÓN		
Grado de protección de los servicios de la entidad.		
OBJETIVO		
Busca identificar la existencia de lineamientos, normas o estándares en cuanto a la adquisición o desarrollo de aplicaciones.		
TIPO DE INDICADOR		
Indicador de Cumplimiento		
DESCRIPCIÓN DE VARIABLES	FORMULA	FUENTE DE INFORMACIÓN
VS17: ¿La entidad ha definido lineamientos, normas y/o estándares para el desarrollo o adquisición de software, sistemas y aplicaciones?	VSIOX = 1 (Sí se evidencia) VSIOX = 0 (NO se evidencia)	Usuarios Internos.
VS18: ¿La entidad ha definido lineamientos, normas y/o estándares para la gestión de incidentes relacionados con el servicio?		Usuarios Internos.
<b>METAS</b>		
<b>CUMPLE</b>	1	<b>NO CUMPLE</b> 0
<b>OBSERVACIONES</b>		

**Bolívar  
primero**

*[Handwritten signature]*



GOBERNACIÓN  
de BOLÍVAR

DESPACHO DEL GOBERNADOR

## RESOLUCION No. 261 2023

**“Por la cual se conforma el Comité de Seguridad de la Información, se definen sus funciones y se adopta la Estrategia de Seguridad Digital de la Gobernación de Bolívar”**

### INDICADOR 09 – IMPLEMENTACIÓN DE LOS PROCESOS DE REGISTRO Y AUDITORÍA

<b>INDICADOR 09 – IMPLEMENTACIÓN DE LOS PROCESOS DE REGISTRO Y AUDITORÍA</b>		
<b>IDENTIFICADOR</b>	SGIN09	
<b>DEFINICIÓN</b>		
Grado de existencia de lineamientos, normas o estándares en cuanto registro y auditoría para la seguridad de la información.		
<b>OBJETIVO</b>		
Busca identificar la existencia de lineamientos, normas o estándares en cuanto registro y auditoría para la seguridad de la información.		
<b>TIPO DE INDICADOR</b>		
Indicador de Cumplimiento		
<b>DESCRIPCIÓN DE VARIABLES</b>	<b>FORMULA</b>	<b>FUENTE DE INFORMACIÓN</b>
VSI19: ¿La entidad ha definido lineamientos, normas y/o estándares para el registro y control de eventos que sucedan sobre sus sistemas, redes y servicios?	VSI0X = 1 (Sí se evidencia) VSI0X = 0 (NO se evidencia)	Usuarios Internos.
VSI20: ¿La entidad verifica de manera interna y/o a través de terceros, periódicamente sus procesos de seguridad de la información y sistemas para asegurar el cumplimiento del modelo?		Usuarios Internos.
<b>METAS</b>		
<b>CUMPLE</b>	1	<b>NO CUMPLE</b> 0
<b>OBSERVACIONES</b>		

### INDICADOR 10 – DETECCIÓN DE ANOMALÍAS EN LA PRESTACIÓN DE LOS SERVICIOS DE LA ENTIDAD

<b>INDICADOR 10 – DETECCIÓN DE ANOMALÍAS EN LA PRESTACIÓN DE LOS SERVICIOS DE LA ENTIDAD</b>		
<b>IDENTIFICADOR</b>	SGIN10	
<b>DEFINICIÓN</b>		
Grado de implementación de los mecanismos encaminados a la detección de anomalías e irregularidades.		
<b>OBJETIVO</b>		
Busca medir el nivel de mecanismos encaminados a la detección de anomalías e irregularidades		
<b>TIPO DE INDICADOR</b>		
Indicador de Cumplimiento		
<b>DESCRIPCIÓN DE VARIABLES</b>	<b>FORMULA</b>	<b>FUENTE DE INFORMACIÓN</b>
VSI21: VAPRSG005: ¿La entidad ha implementado mecanismos para detectar periódicamente	VSI0X = 1 (Sí se evidencia) VSI0X = 0 (NO se evidencia)	Usuarios Internos, No Conformidades

**Bolívar**  
**primero**



GOBERNACIÓN  
de BOLÍVAR

DESPACHO DEL GOBERNADOR

## RESOLUCION No. 261 2023

**“Por la cual se conforma el Comité de Seguridad de la Información, se definen sus funciones y se adopta la Estrategia de Seguridad Digital de la Gobernación de Bolívar”**

vulnerabilidades de seguridad en el funcionamiento de: a) su infraestructura, b) redes, c) sistemas de información, d) aplicaciones y/o e) uso de los servicios?		
<b>METAS</b>		
<b>CUMPLE</b>	1	<b>NO CUMPLE</b> 0
<b>OBSERVACIONES</b>		

### INDICADOR 11 – POLÍTICAS DE PRIVACIDAD Y CONFIDENCIALIDAD

<b>INDICADOR 11 – POLÍTICAS DE PRIVACIDAD Y CONFIDENCIALIDAD</b>		
<b>IDENTIFICADOR</b>	SGIN11	
<b>DEFINICIÓN</b>		
Grado de implementación de políticas privacidad y confidencialidad de la entidad.		
<b>OBJETIVO</b>		
Busca identificar el nivel de implementación de políticas privacidad y confidencialidad de la entidad.		
<b>TIPO DE INDICADOR</b>		
Indicador de Cumplimiento		
<b>DESCRIPCIÓN DE VARIABLES</b>	<b>FORMULA</b>	<b>FUENTE DE INFORMACIÓN</b>
VSI22: ¿La entidad ha implementado lineamientos, normas y/o estándares para proteger la información personal y privada de los ciudadanos que utilicen sus servicios?	VSI0X = 1 (Sí se evidencia) VSI0X = 0 (NO se evidencia)	Usuarios Internos.
VSI23: ¿La entidad ha implementado lineamientos, normas y/o estándares para proteger la información privada de las entidades que utilicen sus servicios?		Usuarios Internos.
<b>METAS</b>		
<b>CUMPLE</b>	1	<b>NO CUMPLE</b> 0
<b>OBSERVACIONES</b>		

### INDICADOR 12 – VERIFICACIÓN DE LAS POLÍTICAS DE INTEGRIDAD DE LA INFORMACIÓN

<b>INDICADOR 12 – VERIFICACIÓN DE LAS POLÍTICAS DE INTEGRIDAD DE LA INFORMACIÓN</b>	
<b>IDENTIFICADOR</b>	SGIN12
<b>DEFINICIÓN</b>	
Grado de implementación de mecanismos para la integridad de la información de la entidad.	
<b>OBJETIVO</b>	

**Bolívar**  
**primero**



GOBERNACIÓN  
de BOLÍVAR

DESPACHO DEL GOBERNADOR

## RESOLUCION No. 2612023

**“Por la cual se conforma el Comité de Seguridad de la Información, se definen sus funciones y se adopta la Estrategia de Seguridad Digital de la Gobernación de Bolívar”**

Busca identificar el nivel de implementación de políticas privacidad y confidencialidad de la entidad.			
<b>TIPO DE INDICADOR</b>			
Indicador de Cumplimiento			
<b>DESCRIPCIÓN DE VARIABLES</b>	<b>FORMULA</b>		<b>FUENTE DE INFORMACIÓN</b>
VSI24: ¿La entidad ha implementado lineamientos contra modificación o pérdida accidental de información?	VSI0X = 1 (Sí se evidencia) VSI0X = 0 (NO se evidencia)		Usuarios Internos.
VSI25: ¿La entidad ha implementado lineamientos, normas y/o estándares para recuperar información en caso de modificación o pérdida intencional o accidental?			Usuarios Internos.
<b>METAS</b>			
<b>CUMPLE</b>	1	<b>NO CUMPLE</b>	0
<b>OBSERVACIONES</b>			

### INDICADOR 13 – POLÍTICAS DE DISPONIBILIDAD DEL SERVICIO Y LA INFORMACIÓN

<b>INDICADOR 13 – POLÍTICAS DE DISPONIBILIDAD DEL SERVICIO Y LA INFORMACIÓN</b>			
<b>IDENTIFICADOR</b>	SGIN13		
<b>DEFINICIÓN</b>			
Grado de cumplimiento de las políticas de disponibilidad del servicio y la información.			
<b>OBJETIVO</b>			
Busca identificar el nivel de implementación de políticas de disponibilidad del servicio y la información.			
<b>TIPO DE INDICADOR</b>			
Indicador de Cumplimiento			
<b>DESCRIPCIÓN DE VARIABLES</b>	<b>FORMULA</b>		<b>FUENTE DE INFORMACIÓN</b>
VSI26: ¿La entidad verifica que los lineamientos, normas y/o estándares orientados a la continuidad en la prestación de los servicios se cumplan?	VSI0X = 1 (Sí se evidencia) VSI0X = 0 (NO se evidencia)		Usuarios Internos.
VSI27: ¿La entidad ha implementado mecanismos para que los servicios de Gobierno en línea tengan altos índices de disponibilidad?			Usuarios Internos.
<b>METAS</b>			
<b>CUMPLE</b>	1	<b>NO CUMPLE</b>	0
<b>OBSERVACIONES</b>			

**Bolívar  
primero**



GOBERNACIÓN  
de BOLÍVAR

DESPACHO DEL GOBERNADOR

## RESOLUCION No. 261 2023

**“Por la cual se conforma el Comité de Seguridad de la Información, se definen sus funciones y se adopta la Estrategia de Seguridad Digital de la Gobernación de Bolívar”**

### INDICADOR 14 – ATAQUES INFORMÁTICOS A LA ENTIDAD

INDICADOR 14 – ATAQUES INFORMÁTICOS A LA ENTIDAD			
IDENTIFICADOR		SGIN14	
DEFINICIÓN			
Porcentaje de ataques informáticos recibidos en la entidad que impidieron la prestación de alguno de sus servicios.			
OBJETIVO			
Busca conocer el número de ataques informáticos que recibe la entidad			
TIPO DE INDICADOR			
Indicador de Cumplimiento			
DESCRIPCIÓN DE VARIABLES	FORMULA	FUENTE DE INFORMACIÓN	
VSI28: ¿Cuántos ataques informáticos recibió la entidad en el último año?	VSI0X = 1 (Sí se evidencia) VSI0X = 0 (NO se evidencia)	Herramientas de Monitoreo/Usuarios Internos.	
VSI29: ¿Cuántos ataques recibió la entidad en el último año que impidieron la prestación de algunos de los servicios que la entidad ofrece a los ciudadanos y empresas?		Herramientas de Monitoreo/Usuarios Internos.	
METAS			
CUMPLE		1	NO CUMPLE
			0
OBSERVACIONES			

### INDICADOR 15 – PORCENTAJE DE DISPONIBILIDAD DE LOS SERVICIO DE GOBIERNO EN LÍNEA QUE PRESTA LA ENTIDAD

INDICADOR 15 – PORCENTAJE DE DISPONIBILIDAD DE LOS SERVICIO DE GOBIERNO EN LÍNEA QUE PRESTA LA ENTIDAD			
IDENTIFICADOR		SGIN15	
DEFINICIÓN			
Porcentaje de disponibilidad de los servicios que presta la entidad			
OBJETIVO			
Busca identificar el nivel de disponibilidad del servicio y la información.			
TIPO DE INDICADOR			
Indicador de Cumplimiento			
DESCRIPCIÓN DE VARIABLES	FORMULA	FUENTE DE INFORMACIÓN	
VSI30: La entidad tiene definidos ANS para los servicios de Gobierno en Línea que presta	VSI0X = 1 (Sí se evidencia) VSI0X = 0 (NO se evidencia)	Usuarios Internos.	
VSI31: Porcentaje de disponibilidad de los servicios de Gobierno en línea que presta la entidad en base a los ANS del punto anterior.		Usuarios Internos.	
METAS			
CUMPLE		1	NO CUMPLE
			0

**Bolívar**  
**primero**



GOBERNACIÓN  
de BOLÍVAR

DESPACHO DEL GOBERNADOR

## RESOLUCION No. 261 2023

**“Por la cual se conforma el Comité de Seguridad de la Información, se definen sus funciones y se adopta la Estrategia de Seguridad Digital de la Gobernación de Bolívar”**

<b>OBSERVACIONES</b>

### INDICADOR 16 – PORCENTAJE DE IMPLEMENTACIÓN DE CONTROLES

<b>INDICADOR 16 – PORCENTAJE DE IMPLEMENTACIÓN DE CONTROLES</b>			
<b>IDENTIFICADOR</b>	SGIN16		
<b>DEFINICIÓN</b>			
Grado de avance en la implementación de controles de seguridad			
<b>OBJETIVO</b>			
Busca identificar el grado de avance en la implementación de controles de seguridad			
<b>TIPO DE INDICADOR</b>			
Indicador de Gestión			
<b>DESCRIPCIÓN DE VARIABLES</b>	<b>FORMULA</b>	<b>FUENTE DE INFORMACIÓN</b>	
VSI32: Número de Controles Implementados	$(VSI032/VSI33) * 100$	Plan de tratamiento de riesgos	
VSI33: Número de Controles que se planearon implementar		Plan de tratamiento de riesgos	
<b>METAS</b>			
<b>MÍNIMA</b>	75-80%	<b>SATISFACTORIA</b> 80- 90%	<b>SOBRESALIENTE</b> 100%
<b>OBSERVACIONES</b>			

**TABLA 6 – CARACTERÍSTICAS DE LOS NIVELES DE MADUREZ - MINISTERIO DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES**

NIVEL	DESCRIPCIÓN
Inexistente	<ul style="list-style-type: none"> <li>Se han implementado controles en su infraestructura de seguridad física, seguridad de recursos humanos entre otros, embargo, no están alineados a un Modelo de Seguridad.</li> <li>No se reconoce la información como un activo importante para su misión y objetivos estratégicos.</li> <li>No se tiene conciencia de la importancia de la seguridad de la información en la entidad.</li> </ul>
Inicial	<ul style="list-style-type: none"> <li>Se han identificado las debilidades en la seguridad de la información.</li> <li>Los incidentes de seguridad de la información se tratan de forma reactiva.</li> <li>Se tiene la necesidad de implementar el MSPI, para definir políticas, procesos y procedimientos que den respuesta proactiva a las amenazas sobre seguridad de la información que presentan en la Entidad.</li> </ul>
Repetible	<ul style="list-style-type: none"> <li>Se identifican en forma general los activos de información.</li> <li>Se clasifican los activos de información.</li> <li>Los servidores públicos de la entidad tienen conciencia sobre la seguridad de la información.</li> </ul>

**Bolívar  
primero**



GOBERNACIÓN  
de BOLÍVAR

DESPACHO DEL GOBERNADOR

## RESOLUCION No. 261 2023

**“Por la cual se conforma el Comité de Seguridad de la Información, se definen sus funciones y se adopta la Estrategia de Seguridad Digital de la Gobernación de Bolívar”**

	<ul style="list-style-type: none"><li>• Los temas de seguridad y privacidad de la información se tratan en los comités del modelo integrado de gestión.</li><li>• La entidad cuenta con un plan de diagnóstico para IPv6.</li></ul>
Definido	<ul style="list-style-type: none"><li>• La Entidad ha realizado un diagnóstico que le permite establecer el estado actual de la seguridad de la información.</li><li>• La Entidad ha determinado los objetivos, alcance y límites de seguridad de la información.</li><li>• La Entidad ha establecido formalmente políticas de Seguridad de la información y estas han sido divulgadas.</li><li>• La Entidad tiene procedimientos formales de seguridad de Información</li><li>• La Entidad tiene roles y responsabilidades asignados en seguridad y privacidad de la información.</li><li>• La Entidad ha realizado un inventario de activos de información aplicando una metodología.</li><li>• La Entidad trata riesgos de seguridad de la información a través de una metodología.</li><li>• Se implementa el plan de tratamiento de riesgos.</li><li>• La entidad cuenta con un plan de transición de IPv4 a IPv6.</li></ul>
Administrado	<ul style="list-style-type: none"><li>• Se revisa y monitorea periódicamente los activos de información de la Entidad.</li><li>• Se utilizan indicadores para establecer el cumplimiento de políticas de seguridad y privacidad de la información.</li><li>• Se evalúa la efectividad de los controles y medidas necesarias para disminuir los incidentes y prevenir su ocurrencia en el futuro.</li><li>• La entidad cuenta con ambientes de prueba para el uso del protocolo IPv6.</li></ul>
Optimizado	<ul style="list-style-type: none"><li>• En este nivel se encuentran las entidades en las cuales la seguridad es un valor agregado para la organización.</li><li>• Se utilizan indicadores de efectividad para establecer si la entidad encuentra retorno a la inversión bajo la premisa de mejora en el cumplimiento de los objetivos misionales.</li><li>• La entidad genera tráfico en IPv6.</li></ul>

**ARTÍCULO DECIMO TERCERO: Establecimiento un Sistema de Gestión de Seguridad de la Información:** Establecer un **Sistema de Gestión de Seguridad de la Información (SGSI)** y adóptese el Modelo de Seguridad y Privacidad de la Información (MSPI) como lineamiento de la Estrategia de Seguridad Digital.

**ARTÍCULO DECIMO CUARTO: Alcance del Sistema de Gestión de Seguridad de la Información:** El Alcance de la adopción de la Estrategia de Seguridad Digital, la Adopción del Modelo de Seguridad y Privacidad de la Información y el Establecimiento de un Sistema de Gestión de Seguridad de la Información basado en el Modelo de Seguridad y Privacidad de la Información está definido para todos los procesos que conforman la entidad.

**ARTÍCULO DECIMO QUINTO: Roles y Responsabilidades:** El Comité de Seguridad de la Información será el encargado de dirigir la Adopción de la Estrategia de Seguridad Digital y realizará conjuntamente con la Secretaría de Planeación las actuaciones necesarias para

**Bolívar  
primero**



GOBERNACIÓN  
de BOLÍVAR

DESPACHO DEL GOBERNADOR

## RESOLUCION No. 261 2023

**“Por la cual se conforma el Comité de Seguridad de la Información, se definen sus funciones y se adopta la Estrategia de Seguridad Digital de la Gobernación de Bolívar”**

la adopción del Modelo de Seguridad y Privacidad de la Información y el establecimiento del Sistema de Gestión de Seguridad de la Información de la Gobernación de Bolívar.

**ARTÍCULO DECIMO SEXTO: Vigencia.** La presente Resolución regirá a partir de su publicación y derogan las normas que le sean contrarias.

**PUBLÍQUESE, COMUNÍQUESE Y CÚMPLASE**

24 de marzo 2023

Dado en Cartagena de Indias, a los

**VICENTE ANTONIO BLEL SCAFF**  
Gobernador de Bolívar

**RUDY JOEL NIETO HENRÍQUEZ**  
Director de TIC

Revisor: Juan Mauricio González Negrete  
Secretario Jurídico

Revisor: Alba Margarita Elles Arnedo

Directora de Conceptos, Actos Administrativos y Personería Jurídica(E)

Proyecto: Tairo Elías Mendoza Piedrahita  
Profesional Especializado

**Bolívar  
primero**