Haga clic aquí para escribir texto.

GOBERNACIÓN de BOLÍVAR

Plan de Seguridad y Privacidad de la Información.

Gobernación de Bolívar

Dirección de Tecnologías de la Información y las Comunicaciones

Vía Cartagena - Turbaco, km 3, Sector Bajo Miranda, El Cortijo
Teléfono: 57-5-6517444
e-mail: contactenos@bolivar.gov.co • www.bolivar.gov.co

FIRMAS Y REVISIONES

TITULO	Plan de Seguridad y Privacidad de la Información.
Autor	Dirección de las Tecnologías de la Información y las Comunicaciones - Gobernación de Bolívar
Tema	Política de Tecnología de Información y Comunicación, Estrategia Gobierno Digital
Fecha de Elaboración	Diciembre 2018
Formato	PDF
Versión	1.0
Palabras Relacionadas	Modelo de Gestión TI, Tecnología de Información – TI, Gobierno Digital

CONTROL DE CAMBIOS

Fecha	Autor	Versión	Cambio
28 de diciembre 2018	Dirección TIC	1.0	Versión Inicial
26 de diciembre 2019	Dirección TIC	2.0	• Cambio en la definición de la aplicabilidad y finalidad. • Se agregaron términos y definiciones. • Se incluyen tablas de referencias. • Se agregaron términos y definiciones. • Se agregó un objetivo general. • Se modificó el alcance, antes nombrado aplicabilidad. • Se sustituyó nivel de cumplimiento por los principios de seguridad y privacidad de la información. • Se definieron roles y responsabilidades.
30 de noviembre 2020	Dirección TIC	3.0	• Se cambió nombre del documento por “Plan de seguridad y privacidad de la Información”. • Se ajustaron los roles y responsabilidades de seguridad y privacidad de la información. • Se incluyeron las actividades a realizar.
06 de diciembre 2022	Dirección TIC	4.0	• Se agregaron responsables y fechas de ejecución a las actividades del plan.

TABLA DE CONTENIDO

2. ALCANCE 6

3. OBJETIVO 7

3.1 OBJETIVOS ESPECÍFICOS 7

4. PRINCIPIOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN. 8

5. ACTIVIDADES A DESAROLLAR 9

6. ROLES Y RESPONSABILIDADES 13

6.1 COMITÉ INSTITUCIONAL DE GESTIÓN Y DESEMPEÑO - Decreto Departamental 489 de 2018 13

6.2 LÍDER DE PROCESO 13

6.3 LÍDER DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN – DIRECTOR(A) TIC - Decreto Departamental 489 de 2018 14

6.4 OFICIAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 14

6.5 MESA DE TRABAJO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN. 15

6.6 FUNCIONARIOS Y CONTRATISTAS..... 15

7. TÉRMINOS Y DEFINICIONES 16

INTRODUCCIÓN

Teniendo en cuenta la importancia de la información y apoyados en su significado, como el conjunto organizado de datos generados, obtenidos, transformados o controlados que constituyen un mensaje sin importar el medio en que se contenga (digital y no digital); nace la necesidad de definir normativas y buenas prácticas para su tratamiento general dentro de la entidad.

El presente documento nos describe las medidas que implementará la **Gobernación de Bolívar**, para la seguridad y privacidad de la información que se maneja en la entidad, según lo establecido en el decreto 1008 del 14 de junio de 2018; 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.

2. ALCANCE

Mediante este plan se aplicará el Modelo de Seguridad y Privacidad de la Información que enmarcará todo activo de información integrado en los procesos de la Gobernación de Bolívar, los cuales incluyen: funcionarios, contratistas, sistemas de información, equipo de cómputo, servidores y todo lo que se incluya en el inventario de activos de información.

3. OBJETIVO

Establecer un plan que permitirá Instituir un Modelo de Seguridad y Privacidad de la información, el cual manifiesta la posición de la entidad con respecto a la importancia que tienen los activos de información para el cumplimiento de las funcionen misionales.

3.1 OBJETIVOS ESPECÍFICOS

- ✓ Elevar los índices de transparencia como entidad pública del territorio colombiano.
- ✓ Crear las políticas y procedimientos en materia de seguridad y privacidad de la información.
- ✓ Mejorar los tiempos y la calidad de respuesta en los procesos de la entidad.
- ✓ Generar una cultura de seguridad y privacidad de la información en los funcionarios, contratistas y ciudadanos.
- ✓ Minimizar los riesgos asociados con los activos de información.
- ✓ Garantizar la continuidad del negocio frente a incidentes.

4. PRINCIPIOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN.

✓ Proteger la información creada, procesada, transmitida o resguardada por los procesos de la entidad, con el fin de minimizar impactos financieros, operativos, reputacionales o legales debido a un uso incorrecto de esta.

✓ Proteger la información de las amenazas originadas por parte de funcionarios o contratistas.

✓ Proteger las instalaciones de procesamiento y la infraestructura tecnológica que soporta los procesos críticos.

✓ Implementará control de acceso a la información, sistemas y recursos de red.

✓ Propender que la seguridad sea parte integral del ciclo de vida de los sistemas de información.

✓ Establecer una adecuada gestión de los eventos de seguridad y las debilidades asociadas con los sistemas de información para una mejora efectiva de su modelo de seguridad.

✓ Verificar la disponibilidad de sus procesos de negocio y la continuidad de su operación basada en el impacto que pueden generar los eventos.

✓ Dar cumplimiento de las obligaciones legales, regulatorias y contractuales establecidas.

✓ Definir, implementar, operar y mejorar de forma continua un modelo de seguridad y privacidad de la información, soportado en lineamientos claros alineados a las necesidades de las partes interesadas, y a los requerimientos regulatorios que le aplican a su naturaleza.

5. ACTIVIDADES A DESAROLLAR

FASE	ACTIVIDADES	ENTREGABLE / RESULTADO	Evidencia	Responsable	Fecha de ejecución
FASE DE DIAGNÓSTICO	Determinar el estado actual de la gestión de seguridad y privacidad de la información al interior de la entidad.	Documento del diagnóstico.	El documento del estado actual de la Gestión de seguridad y Privacidad de la Información se encuentra en custodia de la Dirección TIC	Dirección TIC	31/01/21
	Identificar el nivel de madurez de seguridad y privacidad de la información en la entidad		El documento de identificación del Nivel de Madurez de seguridad y Privacidad de la Información se encuentra en custodia de la Dirección TIC	Dirección TIC	31/01/21
	Identificar vulnerabilidades que sirvan como insumo para la fase de planificación.		El documento de identificación de Vulnerabilidades se encuentra en el Instructivo del Plan General de Gestión de Riesgos de seguridad y Privacidad de la Información se encuentra en custodia de la Dirección TIC	Dirección TIC	31/03/21
FASE DE PLANIFICACIÓN	Identificar el alcance y objetivos de seguridad y privacidad de la información	Documento con la política de seguridad de la información	El Alcance y los Objetivos de seguridad y privacidad de la información se encuentra definido en el Plan de Seguridad y Privacidad de la Información	Dirección TIC	31/03/21
	Política de seguridad y privacidad de la información		El documento de la política de seguridad y privacidad de la información se encuentra publicadas en la página www.bolivar.gov.co El documento de la actualización de la Política de seguridad y privacidad de la información fue revisado por parte del Comité Institucional de Gestión y Desempeño	Dirección TIC	31/12/22
	Roles y responsabilidades de seguridad y		El documento con la designación de roles y responsabilidades fue aprobado por parte del Comité Institucional de Gestión y	Comité Institucional de Gestión y Desempeño	31/12/22

	privacidad de la información.		Desempeño, además, ya hay responsabilidades asignadas por el Decreto 189 de 2018, el Decreto 531 de 2018, la Resolución 247 de 2020		
	Políticas de seguridad y privacidad de la información	Manual con las políticas y procedimientos de seguridad y privacidad de la información.	El documento de Políticas de seguridad y privacidad de la información fue revisado por parte del Comité Institucional de Gestión y Desempeño	Comité Institucional de Gestión y Desempeño	31/12/22
	Procedimientos de seguridad de la información.		Los documentos de Procedimientos, Instructivos y Formato están en construcción continua por parte de la Dirección TIC, ya se encuentran varios definidos	Dirección TIC	31/12/22
	Inventario de activos de información.	Documento con la metodología para identificación, clasificación y valoración de activos de información	Documento con la metodología para identificación, clasificación y valoración de activos de información se encuentra definido y en custodio de la Dirección TIC Versión 3	Dirección TIC	31/12/22
		Matriz con la identificación, valoración y clasificación de activos de información	El documento con la Matriz con la identificación, valoración y clasificación de activos de información se encuentra definido y en custodio de la Dirección TIC	Dirección TIC	28/04/23
	Identificación, valoración y tratamiento de riesgo.	Documento con el plan de tratamiento de riesgos	El documento Plan de Tratamiento de Riesgos nuevo está en espera de revisión por parte del Comité Institucional de Gestión y Desempeño El documento con el Manual de tratamiento de riesgos se encuentra definido en la Resolución 247 de 2020	Dirección TIC	31/12/22
		Documento con la declaración de aplicabilidad	El documento Declaración de Aplicabilidad hace parte de las Políticas de seguridad y privacidad de la información fue aprobado en Comité Institucional de Gestión y Desempeño	Dirección TIC	31/12/22
		Matriz de riesgos	La Matriz de Riesgo de Seguridad de la Información de la Dirección	Dirección TIC Dependencia	23/06/23

			TIC se encuentra en Construcción constante, se encuentra definido junto con el inventario de acitvos		
	Plan de comunicaciones	Documento con el plan de comunicación, sensibilización y capacitación para la entidad	El documento del Plan de comunicaciones está definido en el Plan Estratégico de Tecnologías de la Información 2020-2023	Dirección TIC Dependencia	31/12/22
FASE DE IMPLEMENTACIÓN	Planificación y control operacional	Documento con la estrategia de planificación y control operacional, revisado y aprobado por la alta Dirección	Socializar y aprobar la Visión de la Arquitectura Empresarial Socializar y aprobar los principios de negocio Arquitectura Empresarial	Dirección TIC Dependencia	21/07/23
	Implementación del plan de tratamiento de riesgos	Informe de la ejecución del plan de tratamiento de riesgos aprobado por el dueño de cada proceso	Este documento será entregado en la fase correspondiente	Dependencia	31/12/23
	Indicadores de gestión	Documento con la descripción de los indicadores de gestión de seguridad y privacidad de la información	Este documento será entregado en la fase correspondiente	Dirección TIC	31/12/23
FASE DE EVALUACIÓN DE DESEMPEÑO	Plan de revisión y seguimiento, a la implementación del MSPI	Documento con el plan de seguimiento y revisión del MSPI revisado y aprobado por	Este documento será entregado en la fase correspondiente	Dirección TIC	31/08/23

	ón TIC	la alta Dirección			
	Plan de ejecución de auditorias	Documento con el plan de ejecución de auditorías y revisiones independientes al MSPI, revisado y aprobado por la Alta Dirección	Este documento será entregado en la fase correspondiente	Dirección TIC	31/08/23
FASE DE MEJORA CONTINUA	Plan de mejora continua	Documento con el plan de mejoramiento	Este documento será entregado en la fase correspondiente	Dirección TIC Control Interno	28/02/24
		Documento con el plan de comunicación de resultados	Este documento será entregado en la fase correspondiente	Dirección TIC	28/02/24

6. ROLES Y RESPONSABILIDADES

A nivel general los funcionarios y contratistas de la **Gobernación de Bolívar** asumirán los siguientes roles y responsabilidades, una vez se formalice el MSPI al interior de la Entidad.

6.1 COMITÉ INSTITUCIONAL DE GESTIÓN Y DESEMPEÑO - Decreto Departamental 489 de 2018

- Aprobar y verificar del cumplimiento del Modelo de Seguridad y Privacidad de la Información, al interior de la entidad.
- Ser consciente de la criticidad de los activos de información para el desarrollo de los procesos de la Entidad.
- Divulgar las responsabilidades de seguridad y privacidad de la información de la entidad con base en los lineamientos del MSPI.
- Asignar los recursos necesarios para la implementación del MSPI al interior de la Gobernación de Bolívar.

6.2 LÍDER DE PROCESO

- Liderar y apoyar la mejora continua del proceso, para la aplicación del MSPI.
- Alinear el proceso con los objetivos institucionales, con el fin de que su cumplimiento este apoyado por el MSPI.
- Asignar y verificar el cumplimiento de las funciones y responsabilidades de seguridad y privacidad de la información para los roles que actúan en el proceso.
- Apoyar la capacitación y entrenamiento requerido para que los funcionarios y contratistas que actúan en el proceso.
- Aplicar el proceso disciplinario ante los incidentes de seguridad y privacidad de la información originada por un funcionario o contratista que actúan en el proceso.

6.3 LÍDER DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN – DIRECTOR(A) TIC - Decreto Departamental 489 de 2018

- Liderar y apoyar la mejora continua para la aplicación del MSPI al interior de la gobernación de Bolívar.
- Asignar dentro de su equipo de trabajo quien servirá como oficial de seguridad y privacidad de la información.
- Apoyar las actividades relacionadas con el MSPI.

6.4 OFICIAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

- Apoyar en definir y actualizar el inventario de los activos de información.
- Realizar análisis de riesgos de seguridad y privacidad de la información con base en lo establecido en el MSPI.
- Apoyar en definir del plan de tratamiento de los riesgos de seguridad y privacidad de la información.
- Velar por la ejecución del plan de tratamiento de los riesgos de seguridad y privacidad de la información.
- Definir, actualizar y difundir las políticas, procedimientos y formatos del MSPI.
- Definir y generar las métricas de seguridad y privacidad de la información establecida en el MSPI.
- Propender una cultura de seguridad y privacidad de la información al interior de la entidad.

Lo anterior es responsabilidad del oficial de seguridad y privacidad de la información, pero debe contar con la participación de todos los funcionarios y contratistas de la Gobernación de Bolívar.

6.5 MESA DE TRABAJO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

- Validar y actualizar la documentación propia del MSPI dentro de la dependencia que representa.
- Fomentar dentro de su dependencia la práctica de directrices de seguridad y privacidad de información.
- Apoyar la identificación y actualización del inventario de activos de información y riesgos de estos.
- Apoyar la identificación e implementación de controles para la mitigación de riesgos de seguridad y privacidad de información.
- Participar en las jornadas de implementación, mantenimiento y mejora del MSPI.

6.6 FUNCIONARIOS Y CONTRATISTAS

Todos los funcionarios y contratistas vinculados a la Gobernación tendrán la responsabilidad de velar por la confidencialidad, integridad, disponibilidad y privacidad de la información que maneje, así mismo debe reportar los incidentes de seguridad, eventos sospechosos o un mal uso de los recursos que identifique.

El incumplimiento a la política general de seguridad y privacidad de la información traerá consigo, las consecuencias legales que apliquen a la normativa de la entidad, incluyendo lo establecido en las normas que competen al Gobierno Nacional y Territorial en cuanto a seguridad y privacidad de la información se refiere.

7. TÉRMINOS Y DEFINICIONES

Para efectos de entendimiento de la presente política general seguridad y privacidad de la información, es importante tener en cuenta los siguientes términos y definiciones:

✓ **Acceso remoto**: conexión con los recursos informáticos de la entidad desde una ubicación remota a través de una red pública.
✓ **Activos de información**: son aquellos recursos con los que cuenta una empresa. Es decir, todo elemento que compone el proceso completo de comunicación, partiendo desde la información, el emisor, el medio de transmisión y receptor.
✓ **Amenaza:** causa potencial de incidente no deseado, el cual puede resultar en daño al Sistema o a la Organización. [Fuente: ISO 27000].
✓ **Brecha**: se denomina al espacio o ruta a recorrer entre un estado actual y un estado deseado.
✓ **Calidad**: es la cualidad de un conjunto de información recogida, que reúne entre sus atributos la exactitud, completitud, integridad, actualización, coherencia, relevancia, accesibilidad y confiabilidad necesarias para resultar útiles al procesamiento, análisis y cualquier otro fin que un usuario quiera darles.
✓ **Confidencialidad:** propiedad que impide la divulgación de información a individuos, entidades o procesos no autorizados, asegurando el acceso a la información únicamente a aquellas personas que cuenten con la debida autorización.
✓ **Conservación:** mantener y cuidar la información para que no pierda sus características y propiedades con el paso del tiempo.
✓ **Disponibilidad:** característica, cualidad o condición de la información de encontrarse a disposición de quienes deben acceder a ella, ya sean personas, procesos o aplicaciones.
✓ **Dispositivo móvil:** son todos los equipos tecnológicos que acceden a Internet, tales como: portátiles, teléfonos IP, celulares, TV, tabletas, entre otros.
✓ **Entrenamiento**: proceso utilizado para enseñar habilidades, que permitan a una persona ejecutar funciones específicas asignadas su cargo u objeto contractual.
✓ **Equipos de cómputo:** se reconoce como los portátiles o computadores de escritorios que se le asigna a un funcionario o contratista de la entidad.

✓ **Estándar:** regla que especifica una acción o respuesta que se debe seguir a una situación dada. Los estándares son orientaciones obligatorias que buscan hacer cumplir las políticas. Los estándares son diseñados para promover la implementación de las políticas de alto nivel de la entidad antes de crear nuevas políticas.

✓ **Información:** conjunto organizado de datos generados, obtenidos, adquiridos, transformados o controlados que constituyen un mensaje sin importar el medio que lo contenga (digital y no digital).

✓ **Ingeniería social:** técnica que utilizan las personas para obtener información, acceso o privilegios en sistemas de información, permitiendo que algún acto perjudique o exponga a la persona o entidad.

✓ **Integridad:** propiedad que busca mantener los datos libres de modificaciones no autorizadas. A grosso modo, la integridad es mantener con exactitud la información tal cual fue generada, sin ser manipulada ni alterada por personas o procesos no autorizados.

✓ **Monitoreo**: verificación, supervisión, observación crítica o determinación continua del estado con el fin de identificar cambios con respecto al nivel de desempeño exigido o esperado.

✓ **MSPI:** Modelo Seguridad y Privacidad de la Información.

✓ **Política:** declaración de alto nivel que describe la posición de la entidad sobre un tema específico.

✓ **Privacidad de la información:** es el aspecto que se ocupa de la capacidad que una organización o individuo tiene para determinar qué datos pueden ser compartidos con terceros.

✓ **Procedimiento:** define específicamente como las políticas, estándares, mejores prácticas y guías que serán implementadas en una situación dada.

✓ **Propietario del activo:** persona o cargo que administra, autoriza el uso, regula o gestiona el activo de información. El propietario del activo aprueba el nivel de protección requerido frente a confidencialidad, integridad y disponibilidad.

✓ **Riesgo:** efecto de la incertidumbre sobre los objetivos. Un efecto es una desviación de aquello que se espera, sea positivo, negativo o ambos. Los objetivos pueden tener aspectos diferentes (económicos, de imagen, medio ambiente) y se pueden aplicar a niveles diferentes (estratégico, operacional, toda la organización). [Fuente: ISO 31000]

✓ **Sensibilización**: es un proceso que tiene como objetivo principal impactar sobre el comportamiento de una población o reforzar buenas prácticas sobre algún tema en particular.

✓ **Seguridad de la información:** preservación de la confidencialidad, integridad y disponibilidad de la información. NTC-ISO/IEC 27001.

✓ **Teletrabajo:** En Colombia, el teletrabajo se encuentra definido en la Ley 1221 de 2008 como: "Una forma de organización laboral, que consiste en el desempeño de actividades remuneradas o prestación de servicios a terceros utilizando como soporte las tecnologías de la información y comunicación -TIC- para el contacto entre el trabajador y la empresa, sin requerirse la presencia física del trabajador en un sitio especifico de trabajo".

✓ **TIC:** Tecnologías de la Información y Comunicaciones.

✓ **Vulnerabilidad:** debilidad identificada sobre un activo y que puede ser aprovechado por una amenaza para causar una afectación sobre la confidencialidad, integridad y/o disponibilidad de la información.