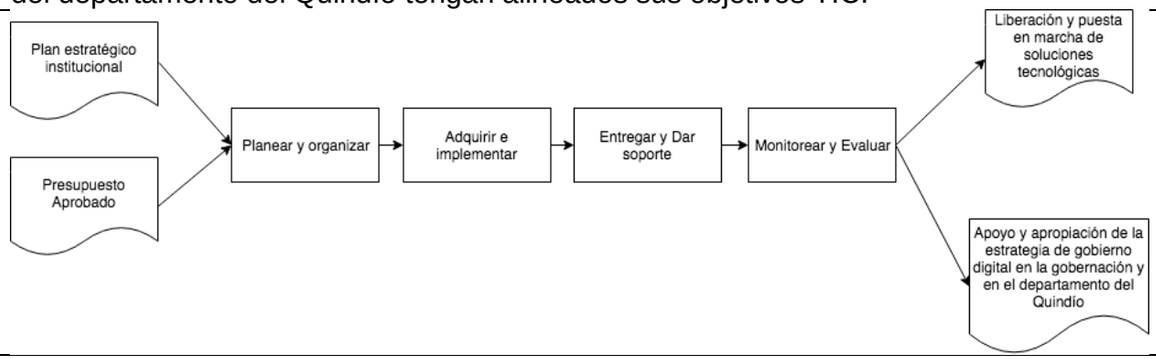
MAPA DE PROCESOS GESTION DE LAS TECNOLOGIAS DE LA INFORMACION Y COMUNICACIONES

GOBERNACIÓN DEL QUINDÍO
2019

TIPO DE PROCESO	ESTRATEGICO__X_____ MISIONALES _____ APOYO _____ EVALUACION _____
NOMBRE DEL PROCESO	Gestión de las tecnologías de la información y comunicaciones
RESPONSABLE DEL PROCESOS	Secretario de Tecnologías de la Información y comunicaciones
DEPENDENCIAS QUE INTEGRAN EL PROCESO	• Dirección de sistemas de información e infraestructura tecnológica • Dirección de Gobierno digital
OBJETIVO DEL PROCESO	Fortalecer el uso, la innovación y la apropiación de las Tecnologías de la Información y las Comunicaciones y la gestión de la información, con el fin de propiciar el cumplimiento de los objetivos de la institucionalidad gubernamental; promoviendo, aplicando y gestionando el ecosistema digital departamental, contribuyendo en el acercamiento permanente de la Administración Central Departamental con los ciudadanos mediante la implementación de la Política de Gobierno Digital.
ALCANCE	Adquirir, construir, actualizar, mantener y/o administrar los sistemas de información de la gobernación del Quindío y la infraestructura tecnológica sobre la que operan, así como brindar soporte técnico y solución a los requerimientos de los usuarios de las tecnologías de información. Por otra parte, y desde la dirección de gobierno digital, el alcance es brindar las herramientas necesarias para que los municipios del departamento del Quindío adopten la estrategia de gobierno digital, reconozcan el plan estratégico de tecnologías de la información desarrollado por la secretaría TIC de la gobernación y a través de crear sus propios planes, para que todas las entidades gubernamentales del departamento del Quindío tengan alineados sus objetivos TIC.
FLUJOGRAMA	

DESCRIPCIÓN DEL PROCESO

PHVA	No	ENTRADA			SUBPROCESOS ETAPAS	SALIDAS		
		PROVEEDOR		INSUMOS		PROCEDIMIENTOS ASOCIADOS		
		INTERNO	EXTERNO				SALIDAS	USUARIOS
PLANEAR	1	• Secretaría de Planeación • Secretaría TIC. • Secretaría de hacienda	• Ministerio de tecnologías de la información y comunicaciones MinTIC. • Leyes, decretos y/o actos administrativos que se expidan desde entes gubernamentales superiores.	• Plan estratégico institucional. • Políticas, lineamientos y normas en materia de Tecnología (Estrategia Gobierno digital Decreto 1008 del 14 de junio de 2018. • Plan operativo anual de inversiones POAI. • Plan de desarrollo departamental	Sistemas de la Información e Infraestructura Tecnológica	• Procedimientos de copias de seguridad y restauración de la información. • Procedimiento Adquisición y administración de la infraestructura tecnológica. • Procedimiento del portal web institucional. • Procedimiento de Mantenimiento preventivo y correctivo de equipos de cómputo. • Procedimiento de soporte técnico a usuarios	• Planes de adquisición de infraestructura tecnológica. • Plan de acción de la vigencia • Plan de capacidad TI. • Sistemas de restauración y recuperación de la información • Soporte técnico a usuario planificado de acuerdo a los tiempos establecidos según servicio. • Plan de mantenimiento preventivo y correctivo.	• Funcionarios de la administración central departamental. • Ciudadanos que consuman información de la gobernación del Quindío a través de sus diferentes portales web.

PLANEAR	2	• Secretaría de Planeación • Secretaría TIC. • Secretaría de hacienda	• Ministerio de tecnologías de la información y comunicaciones MinTIC. • Leyes, decretos y/o actos administrativos que se expidan desde entes gubernamentales superiores.	• Plan estratégico institucional. • Políticas, lineamientos y normas en materia de Tecnología (Estrategia Gobierno digital Decreto 1008 del 14 de junio de 2018. • Plan operativo anual de inversiones POAI. • Plan de desarrollo departamental	Gobierno Digital	• Procedimiento de Apoyo al desarrollo de aplicaciones y contenidos digitales en la industria del software regional. • Procedimiento de Gestión de recursos a nivel nacional e internacional para inversión en proyectos de gobierno digital. • Procedimiento de Asesoría técnica y acompañamiento a los municipios para fortalecer la Política de Gobierno Digital.	• Planes de Acción de la vigencia. • Presupuesto aprobado para la secretaría TIC • Plan estratégico de tecnología de la información y comunicaciones PETIC. • Portafolio de proyectos TIC para el cuatrienio. • Plan de tratamiento de riesgos de seguridad, privacidad de la información y seguridad digital. • Catálogo de servicios tecnológicos actualizados. • Plan de contingencias y continuidad del negocio.	• Funcionarios de la administración central departamental. • Entidades gubernamentales del departamento del Quindío.

							• Políticas de seguridad y privacidad de la información. • Arquitectura de sistemas de información.	
HACER	3	Planificación del subproceso de Sistemas de la Información e Infraestructura Tecnológica		• Planes de adquisición de infraestructura tecnológica. • Plan de acción de la vigencia • Plan de capacidad TI. • Sistemas de restauración y recuperación de la información • Soporte técnico a usuario planificado de acuerdo a los tiempos establecidos según servicio	Sistemas de la Información e Infraestructura Tecnológica	• Procedimientos de copias de seguridad y restauración de la información. • Procedimiento Adquisición y administración de la infraestructura tecnológica. • Procedimiento del portal web institucional. • Procedimiento de Mantenimiento preventivo y correctivo de equipos de cómputo. • Procedimiento de soporte técnico a usuarios	• Adquisición de sistemas de información, según requerimientos encontrados en el plan de capacidad TI. • Mantenimientos preventivos y correctivos realizados de acuerdo al plan de mantenimiento preventivo y correctivo de equipos de cómputo. • Actualización del portal web institucional de acuerdo a los requerimientos	

							de la estrategia de gobierno digital. • Copias de seguridad de los aplicativos misionales de la entidad realizadas y programas según las políticas de seguridad y privacidad de la información. • Controles y restricciones de a los equipos de cómputo de la entidad, según las políticas de seguridad y privacidad de la información	
		Planificación del subproceso de Gobierno Digital		• Planes de Acción de la vigencia. • Presupuesto aprobado para la secretaría TIC	Gobierno Digital	• Procedimiento de Apoyo al desarrollo de aplicaciones y contenidos digitales en la	• Implementación del plan estratégico de tecnología de la información y comunicaciones PETIC.	• Funcionarios de la administración central departamental. • Entidades gubernamentales del

HACER	4			• Plan estratégico de tecnología de la información y comunicaciones PETIC. • Portafolio de proyectos TIC para el cuatrienio. • Plan de tratamiento de riesgos de seguridad, privacidad de la información y seguridad digital. • Catálogo de servicios tecnológicos actualizados. • Plan de contingencias y continuidad del negocio. • Políticas de seguridad y privacidad de la información.		industria del software regional. • Procedimiento de Gestión de recursos a nivel nacional e internacional para inversión en proyectos de gobierno digital. • Procedimiento de Asesoría técnica y acompañamiento a los municipios para fortalecer la Política de Gobierno Digital.	• Proyectos TIC en fase de implementación en la entidad y en el departamento del Quindío. • Seguimiento a la matriz de riesgo de seguridad, privacidad de la información y seguridad digital. • Pruebas realizadas al plan e contingencias y continuidad de la entidad. • Seguimiento a la implementación de las políticas de seguridad y privacidad de la información.	departamento del Quindío.

				• Arquitectura de sistemas de información.				
VERIFICAR	El análisis de datos incluye: • Informe del Sistema Integrado de Gestión. • Informe del modelo integrado de planeación y gestión MIPG • Informes de auditorías internas y externas. • Informe de Auditoría Interna al Sistema Integrado de Gestión. • Informe de resultados a los proyectos implementados de acuerdo al plan estratégico de tecnológicas de la información y a la metodología de gestión de proyecto TI que adopto la secretaría TIC. • Plan de control operacional y declaración de aplicabilidad del modelo de seguridad y privacidad de la información. • Informe de seguimiento al soporte técnico a usuarios • Informe de verificación al seguimiento Plan Anticorrupción y de Atención al Ciudadano del proceso. • Informe de Peticiones, quejas, sugerencias y reclamos. • Información documentada, conservada y controlada. • Indicadores de gestión de seguridad y privacidad de la información.							
ACTUAR	• Planes de Mejoramiento. • Oportunidades de mejora. • Lecciones aprendidas de Proyectos TI							

SEGUIMIENTO Y/O MEDICION	RIESGOS Y/O OPORTUNIDADES	INFORMACION DOCUMENTADA	
• Indicadores incluidos en los planes, programas y proyectos. • Indicadores de gestión del modelo de seguridad y privacidad de la información • Tablero de control. • Cronogramas de mantenimiento preventivo y correctivo	• Mapa de Riesgos. • Matriz de riesgos de seguridad y privacidad de la información. • Valoración de riesgos. • Oportunidades de Mejora	**DOCUMENTOS** Listado Maestro de Documentos que incluye: Caracterizaciones, manuales, planes, programas y procedimientos, de la estrategia de gobierno digital	**CONTROLES** Los controles del proceso se encuentran establecidos en los diferentes procedimientos del proceso.

INDICADORES DE GESTION ASOCIADOS AL PETIC								
Cod identificación	**Nombre**	**Objetivos**	**Descripción**	**Frecuencia de medición**	**Línea Base**	**Metas**		
						Año 1	**Año 2**	**Año 3**
PR01	Alinear la gestión de TI con los procesos de la entidad	• Articular el soporte que ofrecen las TI con los procesos de la entidad.	Procesos de la entidad que pueden ser soportados con TI y cuentan con este apoyo tecnológico	Anual	4	4	4	6
		• Estrategia de TI - Ejecutar el Plan Anual de TI.	Porcentaje de ejecución anual del Plan Estratégico de TI (PETI)		0%	30%	80%	100%
		• Generación de información adecuada para la toma de decisiones en los procesos y servicios de la entidad.	Nivel de apoyo de la información en función de los acuerdos de servicio para los procesos que pueden ser soportados con TI		0	35	35	35
		• Servicios tecnológicos - Disponibilidad	Porcentaje de disponibilidad de los servicios de TI		98 %	95%	96%	98%
		• Apropiación de Internet y redes sociales en el edificio de la Gobernación del Quindío, de acuerdo a los estándares establecidos	Porcentaje de adopción por parte de las dependencias, de las guías para el acceso a los canales de Internet y las redes sociales		100%	100%	100%	100%
		• Desarrollo de Sistemas de Información con Capacidad de interoperabilidad	Nivel de integración e interoperabilidad entre sistemas de información (porcentaje de servicios que requieren interoperabilidad integrados sobre el universo de requerimientos de interoperabilidad)		2	0	1	2
		Gestión del conocimiento – Existencia de una base de Conocimiento sobre Activos y Servicios	Número de licencias disponibles en la Base de Conocimiento sobre Activos y Servicios		753	755	784	789
			Número de licencias utilizadas de la Base de Conocimiento de Activos y Servicios		678	680	709	714
PR02	Desarrollar proyectos de TI exitosos, según su planeación	• Servicios tecnológicos – Implementación de técnicas y manejo ágil de los proyectos para conseguir implementación rápida, con el fin de satisfacer los requerimientos y utilizar la tecnología adecuada	Número de proyectos que utilizan técnicas de herramientas para gestionar los proyectos del universo de proyectos de TI en ejecución.	Anual	NA	40%	70%	85%
PR03	Formar equipos de trabajo preparados para gestionar la estrategia de TI eficientemente	• Fortalecer la capacidad de los equipos de las áreas de tecnología - Reclutamiento y retención de graduados en carreras relacionadas con la gestión de TI	Cantidad de empleados reclutados que son graduados en carreras relacionados con la gestión de TI	Anual	70%	70%	72%	80%

INDICADORES MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

INDICADORES 01 – ORGANIZACIÓN DE SEGURIDAD DE LA INFORMACION					
IDENTIFICADOR	SGIN01				
DEFINICION					
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					
OBJETIVO					
Hacer un seguimiento a la asignación de recursos y responsabilidades en gestión de seguridad de la información, por parte de la alta dirección.					
TIPO DE INDICADOR					
Indicador de gestión					
DESCRIPCIÓN DE VARIABLES		**FORMULA**		**FUENTES DE INFORMACION**	
VSI01: Número de personas con su respectivo rol definIdo según el MSPI (6 personas)		(VSI01/VSI02)*100 (3/6)*100 = 50%		Documento comité de seguridad de la información modelo MSPI	
VSI02: Número de personas con su respectivo rol definió después de un año (3 personas)				Actas de asignación de personal	
METAS					
MINIMA	**50%**	SATISFACTORIA		SOBRESALIENTE	
OBSERVACIONES					
El indicador de cada proceso debe ser recolectado y promediado para construir un indicador que refleje el estado a nivel empresa. El terminó “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					
De acuerdo a lo anterior y teniendo en cuenta que la dirección TIC se convirtió en Secretaría TIC, se definieron los roles y responsabilidades de seguridad del Director de sistemas de información e infraestructura tecnología, el director de gobierno digital y del Secretario TIC.					

INDICADORES 02 - CUBRIMIENTO DEL MSPI EN ACTIVOS DE INFORMACION
IDENTIFICADOR: SGIN02
DEFINICION
El indicador permite determinar y hacer seguimiento al cubrimiento que se realiza a nivel de activos críticos de información de una entidad y los controles aplicados.
OBJETIVO
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.
TIPO DE INDICADOR
Indicador de gestión

DESCRIPCIÓN DE VARIABLES	FORMULA	FUENTES DE INFORMACION
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. 4 riesgos identificados de la matriz de riesgos	(VSI03/VSI04)*100 (4/6)*100=66.66%	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 implementación del modelo; activos incluidos en la zona de riesgo inaceptable.6 activos de información desactualizados.		Inventario de Activos de información, catálogo de servicios

METAS					
MINIMA	**66.66 %**	SATISFACTORIA		SOBRESALIENTE	

OBSERVACIONES

El terminó “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.

Los datos se tomaron de los riesgos identificados de la matriz de riesgos de la entidad:

- Calentamiento de la sala de computo (Data center)
- Falla de equipos electrónicos
- Falta de actualización de la infraestructura tecnológica
- Activos de la información desactualizados.

VSI04: se tomo del catalogo de servicios tecnológicos de la gobernación del Quindío.

INDICADORES 03 - TRATAMIENTOS DE EVENTOS RELACIONADOS EN MARCO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	
IDENTIFICADOR	SGIN03

DEFINICION

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.

OBJETIVO

El objetivo del indicador es reflejar la gestión y evolución del modelo de seguridad y privacidad de la información al interior de una entidad

TIPO DE INDICADOR

Indicador de gestión

DESCRIPCIÓN DE VARIABLES	FORMULA	FUENTES DE INFORMACION
VSI05: Número de anomalías cerradas.		Auditorías internas, herramientas de

	(VSI03/VSI04)*100 (4/6)*100=66.66%	monitoreo, mesa de ayuda, informes de Fortinet y antivirus
VSI06: Número total de anomalías encontradas.		Auditorías internas, herramientas de monitoreo, mesa de ayuda, informes de Fortinet y antivirus

METAS					
MINIMA	**66.66 %**	SATISFACTORIA		SOBRESALIENTE	

OBSERVACIONES
El terminó “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.
Los datos se tomaron de los riesgos identificados de la matriz de riesgos de la entidad: • Calentamiento de la sala de computo (Data center) • Falla de equipos electrónicos • Falta de actualización de la infraestructura tecnológica • Activos de la información desactualizados. VSI04: se tomo del catalogo de servicios tecnológicos de la gobernación del Quindío.

INDICADORES 04 – CUMPLIMIENTO DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN EN LA ENTIDAD	
IDENTIFICADOR	SGIN04
DEFINICION	
Cumplimiento de políticas de seguridad de la información en la entidad	
OBJETIVO	
Busca identificar el nivel de estructuración de los procesos de la entidad orientados a la seguridad de la información.	
TIPO DE INDICADOR	
Indicador de cumplimiento	

DESCRIPCIÓN DE VARIABLES	**FORMULA**	**FUENTES DE INFORMACION**
VSI07: ¿La entidad ha definido una política general de seguridad de la información?	VS0X = 1 (SÍ se evidencia) VS0X = 0 (NO se evidencia) VS07 = 1 VS08 = 1 VS09 = 1	Política de seguridad de la información establecida y aprobada
VSI08: ¿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?		Roles y responsabilidades de seguridad de la información definidos
VSI09: ¿La entidad cumple con los requisitos legales, reglamentarios y contractuales con respecto al manejo de la información?		Política de seguridad de la información establecida y aprobada

METAS			
CUMPLE	**1%**	NO CUMPLE	0%
OBSERVACIONES			

INDICADORES 05 – IDENTIFICACIÓN DE LINEAMIENTOS DE SEGURIDAD DE LA ENTIDAD			
IDENTIFICADOR	SGIN05		
DEFINICION			
Grado de la seguridad de la información y los equipos de cómputo.			
OBJETIVO			
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.			
TIPO DE INDICADOR			
Indicador de cumplimiento			
DESCRIPCIÓN DE VARIABLES		**FORMULA**	**FUENTES DE INFORMACION**
VSI10: ¿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?		VS1X = 1 (SÍ se evidencia) VS1X = 0 (NO se evidencia) VS10 = 1 VS11 = 1	Roles y responsabilidades de seguridad de la información definidos
VSI11: ¿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?			Control de acceso físico en las políticas de seguridad y privacidad de la información
METAS			
CUMPLE	**1%**	NO CUMPLE	0%
OBSERVACIONES			

INDICADORES 06 – VERIFICACIÓN DEL CONTROL DE ACCESO			
IDENTIFICADOR	SGIN06		
DEFINICION			
Grado control de acceso en la entidad.			
OBJETIVO			
Busca identificar la existencia de lineamientos, normas o estándares en cuanto al control de acceso en la entidad.			
TIPO DE INDICADOR			
Indicador de cumplimiento			
DESCRIPCIÓN DE VARIABLES		**FORMULA**	**FUENTES DE INFORMACION**
VSI12: ¿La entidad ha definido lineamientos, normas y/o estándares para controlar el acceso de los usuarios a sus servicios de Gobierno digital y a sus redes de comunicaciones?		VS1X = 1 (SÍ se evidencia) VS1X = 0 (NO se evidencia) VS12 = 1 VS13 = 1	Política de seguridad de la información establecida y aprobada
VSI13: ¿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?			Política de seguridad de la información establecida y aprobada, Catalogo de servicios tecnologicos

VSI14: ¿La entidad ha definido lineamientos, normas y/o estándares para controlar las terminales móviles y accesos remotos a los recursos de la entidad?	VS14 = 1	Política de seguridad de la información establecida y aprobada

METAS			
CUMPLE	**1%**	NO CUMPLE	0%
OBSERVACIONES			

INDICADORES 07 – ASEGURAMIENTO EN LA ADQUISICIÓN Y MANTENIMIENTO DE SOFTWARE	
IDENTIFICADOR	SGIN07
DEFINICION	
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**	**FUENTES DE INFORMACION**
VSI15: ¿La entidad ha definido lineamientos, normas y/o estándares para el desarrollo o adquisición de software, sistemas y aplicaciones?	VS1X = 1 (SÍ se evidencia) VS1X = 0 (NO se evidencia)	Política de seguridad de la información establecida y aprobada y lineamientos para la adquisición de sistemas de información y software
VSI16: ¿La entidad ha definido lineamientos, normas y/o estándares para la gestión de incidentes relacionados con el servicio?	VS15 = 1 VS16 = 1	Plan de gestión de incidentes de seguridad de la información

METAS			
CUMPLE	**1%**	NO CUMPLE	0%
OBSERVACIONES			

INDICADORES 08 – IMPLEMENTACIÓN DE LOS PROCESOS DE REGISTRO Y AUDITORÍA	
IDENTIFICADOR	SGIN08
DEFINICION	
Grado de existencia de lineamientos, normas o estándares en cuanto registro y auditoría para la seguridad de la información.	
OBJETIVO	
Busca identificar la existencia de lineamientos, normas o estándares en cuanto registro y auditoría para la seguridad de la información.	
TIPO DE INDICADOR	
Indicador de cumplimiento	

DESCRIPCIÓN DE VARIABLES	**FORMULA**	**FUENTES DE INFORMACION**
VSI17: ¿La entidad ha definido lineamientos, normas y/o estándares para el registro y control de eventos que sucedan	VS1X = 1 (SÍ se evidencia)	Fase de implementación del modelo de seguridad y privacidad de la

sobre sus sistemas, redes y servicios?	VS1X = 0 (NO se evidencia) VS17 = 1 VS18 = 0	información MSPI, seguimiento a riesgos.
VSI18: ¿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?		Plan de auditorias de la fase de mejora continua (No existe)

METAS			
CUMPLE	**1% VS17**	NO CUMPLE	**0% VS18**
OBSERVACIONES			

INDICADOR 09 – IMPLEMENTACIÓN DE LOS PROCESOS DE REGISTRO Y AUDITORÍA		
IDENTIFICADOR	SGIN09	
DEFINICION		
Grado de implementación de los mecanismos encaminados a la detección de anomalías e irregularidades.		
OBJETIVO		
Busca medir el nivel de mecanismos encaminados a la detección de anomalías e irregularidades.		
TIPO DE INDICADOR		
Indicador de Cumplimiento		
DESCRIPCIÓN DE VARIABLES	**FORMULA**	**FUENTES DE INFORMACION**
VSI19: VAPRSG005: ¿La entidad ha implementado mecanismos para detectar Periódicamente 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?	VSI0X = 1 (SÍ se evidencia) VSIOX = 0 (NO se evidencia) VS19= 1	Auditorías internas, herramientas de monitoreo PRTG Network, informes Firewall perimetral (Fortinet) e informes de antivirus.
METAS.		Auditorías externas expertos en seguridad informática, herramientas de monitoreo de trafico de red, informes de herramienta firewall perimetral Fortinet y análisis de datos por experto e informes de antivirus y acciones ante posibles amenazas.

CUMPLE			
OBSERVACIONES	**1**	**NO CUMPLE**	
OBSERVACIONES			
El indicador de este proceso es medido mediante la implementación de los diferentes mecanismos que utiliza la entidad para detectar periódicamente las			

vulnerabilidades de seguridad de la información en su infraestructura, redes de datos, sistemas de información y aplicativos con los que cuenta el CAD; esto se realiza a través de auditorías internas, herramientas de monitoreo PRTG Network, informes Firewall perimetral (Fortinet) e informes de antivirus, con el fin de tener un control a la detección de anomalías e irregularidades.
La información se toma de los informes mensuales de seguridad realizados por el ISP de turno y de la auditoria externa realizada por el experto de seguridad, además de los informes mensuales realizados por parte del equipo de trabajo de la secretaria tic en cada uno de los ítems relacionados.

INDICADORES 10 – POLÍTICAS DE PRIVACIDAD Y CONFIDENCIALIDAD			
IDENTIFICADOR	SGIN10		
DEFINICION			
Grado de implementación de políticas privacidad y confidencialidad de la entidad.			
OBJETIVO			
Busca identificar el nivel de implementación de políticas privacidad y confidencialidad de la entidad.			
TIPO DE INDICADOR			
Indicador de cumplimiento			
DESCRIPCIÓN DE VARIABLES		**FORMULA**	**FUENTES DE INFORMACION**
VSI20: ¿La entidad ha implementado lineamientos, normas y/o estándares para proteger la información personal y privada de los ciudadanos que utilicen sus servicios?		VS2X = 1 (SÍ se evidencia) VS2X = 0 (NO se evidencia) VS20 = 1 VS21 = 0	Política de seguridad de la información establecida y aprobada
VSI21: ¿La entidad ha implementado lineamientos, normas y/o estándares para proteger la información privada de las entidades que utilicen sus servicios?			Política de seguridad de la información establecida y aprobada
METAS			
CUMPLE	**1%**	NO CUMPLE	0%
OBSERVACIONES			

INDICADORES 11 – VERIFICACIÓN DE LAS POLÍTICAS DE INTEGRIDAD DE LA INFORMACIÓN			
IDENTIFICADOR	SGIN11		
DEFINICION			
Grado de implementación de mecanismos para la integridad de la información de la entidad.			
OBJETIVO			
Busca identificar el nivel de implementación de políticas privacidad y confidencialidad de la entidad.			
TIPO DE INDICADOR			
Indicador de cumplimiento			
DESCRIPCIÓN DE VARIABLES		**FORMULA**	**FUENTES DE INFORMACION**
VSI22 ¿La entidad ha implementado lineamientos contra modificación o pérdida accidental de información?		VS2X = 1 (SÍ se evidencia)	Política de seguridad de la información establecida y aprobada, Plan de recuperación ante desastres (DRP)

VSI23: ¿La entidad ha implementado lineamientos, normas y/o estándares para recuperar información en caso de modificación o pérdida intencional o accidental?	VS2X = 0 (NO se evidencia) VS22 = 1 VS23 = 1	Política de seguridad de la información establecida y aprobada, Plan de recuperación ante desastres (DRP)
METAS		
CUMPLE	**1%**	NO CUMPLE	0%
OBSERVACIONES		

INDICADORES 12 – POLÍTICAS DE DISPONIBILIDAD DEL SERVICIO Y LA INFORMACIÓN			
IDENTIFICADOR	SGIN12		
DEFINICION			
Grado de cumplimiento de las políticas de disponibilidad del servicio y la información.			
OBJETIVO			
Busca identificar el nivel de implementación de políticas de disponibilidad del servicio y la información.			
TIPO DE INDICADOR			
Indicador de cumplimiento			
DESCRIPCIÓN DE VARIABLES		**FORMULA**	**FUENTES DE INFORMACION**
VSI24 ¿La entidad verifica que los lineamientos, normas y/o estándares orientados a la continuidad en la prestación de los servicios se cumplan?		VS2X = 1 (SÍ se evidencia) VS2X = 0 (NO se evidencia) VS22 = 1 VS23 = 0	Política de seguridad de la información establecida y aprobada, Plan de recuperación ante desastres (DRP)
VSI25: ¿La entidad ha implementado mecanismos para que los servicios de Gobierno digital tengan altos índices de disponibilidad?			Política de seguridad de la información establecida y aprobada, Plan de recuperación ante desastres (DRP)
METAS			
CUMPLE	**1%**	NO CUMPLE	**0%**
OBSERVACIONES			

INDICADOR 13 – ATAQUES INFORMÁTICOS A LA ENTIDAD.			
IDENTIFICADOR	SGIN13		
DEFINICION			
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**	**FUENTES DE INFORMACION**
VSI26: ¿Cuántos ataques informáticos recibió			Auditorías internas, herramientas de

la entidad en el último año?	VSI0X = 1 (SÍ se evidencia) VSIOX = 0 (NO se evidencia)	monitoreo PRTG Network, informes Firewall perimetral (Fortinet) e informes de antivirus.
METAS.		Auditorías externas expertos en seguridad informática, herramientas de monitoreo de trafico de red, informes de herramienta firewall perimetral Fortinet y análisis de datos por experto e informes de antivirus y acciones ante posibles amenazas.

CUMPLE			
OBSERVACIONES	**1**	**NO CUMPLE**	

OBSERVACIONES
El indicador de este proceso es medido mediante la implementación de los diferentes mecanismos que utiliza la entidad para detectar periódicamente las vulnerabilidades de seguridad de la información en su infraestructura, redes de datos, sistemas de información y aplicativos con los que cuenta el CAD; esto se realiza a través de auditorías internas, herramientas de monitoreo PRTG Network, informes Firewall perimetral (Fortinet) e informes de antivirus, con el fin de tener un control a la detección de anomalías e irregularidades.
La información se toma de los informes mensuales de seguridad realizados por el ISP de turno y de la auditoria externa realizada por el experto de seguridad, además de los informes mensuales realizados por parte del equipo de trabajo de la secretaria tic en cada uno de los ítems relacionados.

INDICADORES 14 – PORCENTAJE DE DISPONIBILIDAD DE LOS SERVICIO DE GOBIERNO EN LÍNEA QUE PRESTA LA ENTIDAD	
IDENTIFICADOR	SGIN14
DEFINICION	
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**	**FUENTES DE INFORMACION**
VSI27 La entidad tiene definidos ANS para los servicios de Gobierno en Línea que presta.	VS2X = 1 (SÍ se evidencia) VS2X = 0 (NO se evidencia) VS22 = 0 VS23 = 0	No se tiene
VSI28: Porcentaje de disponibilidad de los servicios de Gobierno digital que presta la entidad en base a los ANS del punto anterior.		No se tiene

METAS			
CUMPLE	1%	NO CUMPLE	**0%**
OBSERVACIONES			
La entidad no ha definido las ANS de los servicios que presta de gobierno digital.			

INDICADORES 15 – PORCENTAJE DE IMPLEMENTACIÓN DE CONTROLES					
IDENTIFICADOR	SGIN15				
DEFINICION					
Grado de avance en la implementación de controles de seguridad					
OBJETIVO					
Busca identificar el grado de avance en la implementación de controles de seguridad					
TIPO DE INDICADOR					
Indicador de cumplimiento					
DESCRIPCIÓN DE VARIABLES		**FORMULA**		**FUENTES DE INFORMACION**	
VSI29 Número de Controles Implementados		(VSI029/VSI30)*100		Plan de tratamiento de riesgos, declaración de aplicabilidad del MSPI	
VSI30: Número de Controles que se planearon implementar		(15/19)*100 = 78.94%		Plan de tratamiento de riesgos, declaración de aplicabilidad del MSPI	
METAS					
MINIMA	**75%-80%**	SATISFACTORIA	80%-90%	SOBRESALIENTE	100%
OBSERVACIONES					
La entidad no ha definido las ANS de los servicios que presta de gobierno digital.					

1. CONTROL DE CAMBIOS		
VERSION	**FECHA DE APROBACIÓN**	**DESCRIPCION DE CAMBIOS REALIZADOS**
01	01/10/2019	Se crea la primera versión del documento

2. REGISTROS

IDENTIFICACION		ALMACENAMIENTO Y RECUPERACION			ACCESO	CONSERVACION	DISPOSICIÓN FINAL
CODIGO	NOMBRE	RESPONSABLE	LUGAR DE ALMACENAMIENTO	CLASIFICACION	PERSONAL AUTORIZADO	TEMPO DE RETENCION	METODO