CIG.13.31.01 - 00279
Armenia, 13 de julio de 2022

Ingeniero
JHON MARIO LIEVANO FERNADEZ
Secretario de Tecnología de la Información y la Comunicación
Gobernación del Quindío
La Ciudad

ASUNTO: Auditoria Basada en Riesgos efectuada a la Secretaría TIC sobre **Política de Privacidad de Seguridad de la Información – Privacidad y Confidencialidad**

Cordial saludo

La Oficina de Control Interno de Gestión, en desarrollo de nuestro **ROL DE EVALUACION Y SEGUIMIENTO** y en cumplimiento del plan de auditorías internas aprobada en el comité de coordinación de control interno, procede a practicar auditoria Basada en Riesgos en la Secretaria TIC específicamente en el establecimiento de los lineamientos y procedimientos que permitan fortalecer y asegurar la Privacidad y Protección de Datos, el cual involucra entrevistas, inspección y rastreo a Políticas y Procedimientos establecidos en la Entidad, para la vigencia comprendidas entre el 1 de julio a 31 de 2022.

Inicio de la Auditoria Basada en Riesgos: 13 de Julio de 2022.
Hora: 3:00p.m

Atentamente;

JOSÉ DUVÁN LIZARAZO CUBILLOS
Jefe Oficina de Control Interno de Gestión.
Anexo: Carta de Compromiso, Plan de Auditoria N.04 y Plan de trabajo.

Diana
Julio 14
8:10

Reviso: José Duvan Lizarazo Cubillos. Jefe Oficina Control Interno de Gestión.
Proyecto y elaboro: Isabel Cristina Carvajal Ramos. – Auditor Contratista OCIG
Andrea Chacón Mellizo. – Auditor Contratista OCIG

PLAN AUDITORÍA INTERNA	Auditoría No. 04	Fecha	Día	Mes	Año
			11	07	2022

Auditor Líder:	José Duván Lizarazo Cubillos
Coordinador Auditoria:	Isabel Cristina Carvajal Ramos Andrea Chacón Mellizo
Equipo Auditor:	Contratistas

Consideraciones:	Para la presente auditoria se identificará la misión, visión y la política de tratamiento de datos personales adoptadas por la Secretaría de TIC Departamental, componente y línea estratégica del Plan de Desarrollo "Tú y Yo Somos Quindío 2020 -2023", objetivo específico de la misma, los productos, indicadores, unidades de medida, controles y riesgos relacionados con la protección de datos, dado que esta información es relevante para el alcance del objetivo de la auditoría. **Misión** Planificar y promover el desarrollo integral del Departamento, mediante la implementación de políticas, para mejorar las condiciones de vida de la población; apoyadas en el liderazgo público, la gestión estratégica institucional, institución y las leyes. **Visión** Quindío será en el 2032, un Departamento con una administración transparente, eficiente, planificada e incluyente; con un talento humano en constante desarrollo, con procesos articulados a través del uso de las TIC, con adecuados sistemas de planeación y gestión; que aúne esfuerzos para lograr un territorio ambientalmente sostenible; productivo y competitivo a partir de su vocación y aptitud; socialmente incluyente, equitativo y plural; con una institucionalidad fundamentada en la gobernabilidad y gobernanza, para construir ciudadanía y democracia, tendiente a mejorar la calidad de vida de los Quindianos. **Política de Privacidad de Seguridad de la Información – Privacidad y Confidencialidad** Adoptada por las TIC mediante formato POL-TIC-01, con fecha de actualización del 31 de enero de 2022, la cual tiene como fin proteger el derecho al Hábeas Data, actualizar y rectificar la información que se haya recogido en archivos y bancos de datos de naturaleza pública o privada garantizando a todos los ciudadanos poder de decisión y control sobre su información personal, teniendo en cuenta que para el desarrollo de su objeto, entiéndase tramites en línea, registros en plataformas, accesos a redes wifi, entre otros continuamente está recopilando información de los usuarios que interactúan con estas plataformas.

	Plan de Desarrollo "Tú y Yo Somos Quindío 2020 -2023" Componente Estratégico - Sector Tecnologías de la Información y las Comunicaciones Objetivos Específicos que le aplican - Capacitar personas y empresas a través de educación informal en competencias de TI en el Departamento del Quindío. - Capacitar personas en gestión TI y seguridad y privacidad de la información. - Elaborar documentos técnicos con el fin de llevar acabo el desarrollo de aplicaciones, contenidos digitales y apropiación de las TIC en el Departamento del Quindío. Programa 2302: Fomento del desarrollo de aplicaciones, software y contenidos para impulsar la apropiación de las Tecnologías de la Información y las Comunicaciones (TIC) "Quindío paraíso empresarial TIC-Quindío TIC" Producto: Servicio de educación informal en Gestión TI y en Seguridad y Privacidad de la Información Indicador: Personas capacitadas en Gestión TI y en Seguridad y Privacidad de la Información Riesgos: matriz de riesgo informáticos-2022 Controles: La dirección de Gobierno Digital socializará trimestralmente las leyes de protección de datos personales a los que administran o suben contenido a la página web
Objetivo:	Evaluar la efectividad de los controles que garantizan que la Información que maneja la entidad Territorial Departamento del Quindío en virtud de sus competencias, cumplan con la normatividad vigentes de protección de datos personales, para garantiza el derecho fundamental de Habeas Data consagrado en el artículo 15 de la Constitución Política.
Alcance:	La auditoría se realizará del 01 al 30 de julio de 2022, en las instalaciones de la Secretaría TIC del Departamento del Quindío y se enfocará tanto en los controles documentados en el Mapa de Riesgos Institucional, de corrupción, en el plan acción de la vigencia, así como en

	en cuenta los indicadores, la medición de los mismos y las conclusiones y recomendaciones consignados en los respectivos seguimientos.
Metodología:	Guía de auditoría interna basada en riesgos para entidades públicas – Versión 4 – Función Pública
Justificación:	La presente auditoría se proyecta conforme a la evaluación del riesgo que soporta el Plan de Auditoría de la Oficina de Control Interno de Gestión del Departamento del Quindío, dado que en el mapa de riesgo institucional se encuentra dentro del activo de las TIC "Página Web", el riesgo "pérdida de confidencialidad", como amenaza la "Información publicada en página web sin los correspondientes permisos y/o la correspondiente aplicación de la ley de protección de datos" por causa de un posible desconocimiento de la ley 1581 de 2012 "ley de protección de datos personales" y la ley 1712 del 2012 "Ley de transparencia, situación que amerita un proceso auditor para prevenir la configuración del riesgo que iría contra los intereses de la función pública que en la esencia es garantizar los derechos fundamentales de sus asociados..
Recursos necesarios:	Equipo auditor con formación en áreas de la ingeniería de sistemas y derecho.
Agenda de Auditoría	

Fecha de iniciación:	01 de julio de 2022	**Fecha de terminación:**	30 de julio de 2022
Plan de Trabajo:	Ver anexo 1.		

Nombre completo	Responsabilidad	Firma
José Duvan Lizarazo Cubillos	Auditor Líder	
Isabel Cristina Carvajal Ramos Andrea Chacón Mellizo	Coordinador Auditoria	

	FORMATO	**Código: F-CIG-11**
	Plan de Auditoría Interna	Versión: 04 Fecha: 01/12/2017
		Página 1 de 2

PROGRAMA DE TRABAJO									
TÍTULO AUDITORÍA: Auditoría a basada en riesgos gestión TIC									
OBJETIVO DE LA AUDITORÍA: Evaluar la efectividad de los controles que garantizan que la Información que maneja la entidad Territorial Departamento del Quindío en virtud de sus competencias, cumplan con la normatividad vigentes de protección de datos personales, para garantiza el derecho fundamental de Habeas Data consagrado en el artículo 15 de la Constitución Política.									
ALCANCE DE LA AUDITORÍA: La auditoría se realizará del 01 al 30 de julio de 2022, en las instalaciones de la Secretaría TIC del Departamento del Quindío y se enfocará tanto en los controles documentados en el Mapa de Riesgos Institucional, de corrupción, en el plan acción de la vigencia, así como en los procesos y procedimientos adoptados para el cumplimiento de sus funciones, teniendo en cuenta los indicadores, la medición de los mismos y las conclusiones y recomendaciones consignados en los respectivos seguimientos.									
RECURSOS: Equipo auditor con formación en áreas de TIC, derecho, otras.									
OBJETIVO	RIESGOS	CAUSA	NIVEL DEL RIESGO	CONTROL	PROCEDIMIENTO DE AUDITORÍA	AUDITOR	FECHA/HORAS O DIAS	PAPEL DE TRABAJO	OBSERVACIÓN O HALLAZGO
Estratégico: Fortalecer las capacidades institucionales de la administración departamental, para generar condiciones de gobernanza territorial, participación, administración eficiente y transparente, planificación y	Pérdida de confidencialidad. Información publicada en la página web sin los correspondientes permisos y/o la correspondiente aplicación de la ley de protección de datos	Desconocimiento de la ley 1581 de 2012 "ley de protección de datos personales" y la ley 1712 del 2012 "Ley de transparencia"	Alto	La dirección de Gobierno Digital socializará trimestralmente las leyes de protección de datos personales a los que administran o suben contenido a la página web.	Entrevistas	**Andrea Chacón Mellizo – Isabel Cristina Carvajal Ramos**	**11 de julio de2022**	Actas	

seguimiento de la gestión institucional y gobierno abierto.				Revisión de PQRSD, relacionadas con el manejo de datos que deben garantizarse su privacidad.	Inspecciones: Políticas y procedimientos objetos de capacitación		**12 – 13 de julio de2022**		
					Rastreo: Se realiza específicamente para probar la integridad de la información documentada o registrada		**14 – 20 de julio de 2022**		

CARTA DE COMPROMISO

Fecha: 11 de julio de 2022
Para: JHON MARIO LIEVANO FERNANDEZ - Secretario TIC
De: JOSE DUVAN LIZARAZO CUBILLOS - Jefe Oficina de Control Interno de Gestión
Asunto: Carta de Alcance "Auditoría basada en riesgos – Gestión TIC"

Respetado Ingeniero:

De acuerdo con el Plan General de Auditoría 2022, aprobado por el Comité de Coordinación de Control Interno, comunicamos el inicio del trabajo de auditoría al riesgo "Pérdida de confidencialidad de datos personales"

Objetivo y Alcance de la Auditoría

Evaluar la efectividad de los controles que garantizan que la Información que maneja la entidad Territorial Departamento del Quindío en virtud de sus competencias, cumplan con la normatividad vigentes de protección de datos personales, para garantiza el derecho fundamental de Habeas Data consagrado en el artículo 15 de la Constitución Política.

Metodología

1. Entendimiento y recorrido de:
   a) Política y procedimiento adoptado para la protección de datos
   b) Áreas involucradas en el proceso
   c) Actividades de control a nivel entidad

2. Identificación y valoración de riesgos y controles clave del proceso.

3. Planeación y ejecución de pruebas a controles (diseño, efectividad, detalle).

4. Identificación de posibles brechas de control y oportunidades de mejoramiento.

5. Discusión y validación del informe con el dueño del proceso o Jefe de dependencia relacionada con el aspecto evaluado y definición de planes de acción (plan de mejoramiento) estructurales para su remediación.

Cada etapa de auditoría (entendimiento del proceso, evaluación del riesgo y evaluación y prueba de controles) será desarrollada mediante:
1. Lectura de la documentación vigente del proceso;
2. Entrevistas/talleres con el dueño del proceso y el personal involucrado en el mismo;
3. Inspección de documentos relacionados con la ejecución del proceso;
4. Solicitud de información adicional, requerida dentro del análisis del proceso;

JHON MARIO LIEVANO FERNANDEZ
Secretario TIC

JOSE DUVAN LIZARAZO CUBILLOS
Jefe Oficina de Control Interno de Gestión

Julio 13
3:30

CIG 13.31.01 - 00326

Armenia, 18 de agosto de 2022

Doctor:
JHON MARIO LIEVANO FERNANDEZ
Secretario TIC
Gobernación del Quindío.
Ciudad.

Asunto: Remisión Informe Final de Auditoría Interna Basada en Riesgos de 2022 realizado a la **Política de Privacidad de Seguridad de la Información – Privacidad y Confidencialidad**

De manera respetuosa nos permitimos allegar el Informe Final de Auditoria Interna Especial No 001-2022 al proceso de la Secretaria TIC.

Lo anterior, en cumplimiento del Plan Anual de Audiotria adoptado por la Oficina de Control Interno de Gestión para la vigencia 2022.

Al respecto es perinente que se tenga encuenta la recomendación incluida en dicho informe:

"De conformidad al presente informe final de Audiotria se recomienda a la Secretaría TIC que adopte el Plan de Mejora conforme a los documentos adoptados para ello, el cual debe contener las accriones preventivas y corresctivas que ataquen la causa de los hallazgos Administrativos estructrados por la oficina de contro Interno de Gestion, en un plazo de quince (15) días hábiles siguientes a la fecha de recibido el Informe final de auditoría, salvo que involucre a otros procesos o dependencias, caso en el cual el término será veinte (20) días hábiles para su formulación y su remisión a la Oficina de Control Interno Interno de Gestion"

Cordialmente,

JOSE DUVAN LIZARAZO CUBILLOS
Jefe Oficina de Control Interno de Gestión.

Proyecto:
Andrea Chacón Mellizo – contratista OCIG
Aprobó: José Duván Lizarazo C. – Jefe de OCIG
Anexo: Informe Final Auditoría Basada en Riesgos 2022

Diana ago 18 10:23

FECHA DE EMISIÓN DEL INFORME	Día	Mes	Año
	18	08	2022

Aspecto Evaluable (Unidad Auditable):	**Auditoria Interna Basada en Riesgos al proceso Política de Privacidad de Seguridad de la Información – Privacidad y Confidencialidad** - Secretaría de Tecnología de la Información y las Comunicaciones
Líder de Proceso / jefe(s) **Dependencia(s):**	**ING. JHON MARIO LIEVANO FERNANDEZ**
Objetivo de la Auditoría	Evaluar la efectividad de los controles que garantizan que la Información que maneja la entidad Territorial Departamento del Quindío en virtud de sus competencias, cumplan con la normatividad vigentes de protección de datos personales, para garantiza el derecho fundamental de Habeas Data consagrado en el artículo 15 de la Constitución Política.
Alcance de la Auditoría	La auditoría se desarrollo entre el 01 al 30 de julio de 2022, en las instalaciones de la Secretaría TIC del Departamento del Quindío y se enfocará tanto en los controles documentados en el Mapa de Riesgos Institucional, de corrupción, en el plan acción de la vigencia, así como en los procesos y procedimientos adoptados para el cumplimiento de sus funciones, teniendo en cuenta los indicadores, la medición de los mismos, las conclusiones y recomendaciones consignados en los respectivos seguimientos.
Criterios de la Auditoría:	- Ley 527 del 1999. - Decreto 019 de 2012. - Ley 1226 de 2008. - Ley 1273 de 2009. - Ley 1349 de 2009. - Ley 1581 de 2012. - Ley 1712 del 2014. - Decreto 2573 de 2014, compilado por el decreto 1078 de 2015. - Decreto 103 de 2015. - Decreto 1008 de 2018.

	- Resolución de 00500 de 2021 de MinTIC - Decreto 00119 de 2021 de Gobernación del Quindío - Decreto 629 de 2021 de Gobernación del Quindío - Directiva presidencial 03 de 2021 - PR - TIC 01 Estrategia de Gobierno Digital. - PL - TIC 01 Plan de seguridad y privacidad de la información - PL - TIC 02 Plan de gestión del riesgo de seguridad y Privacidad de la Información y Seguridad Digital. - POL - TIC – 01 Política de tratamiento de datos - POL - TIC – 02 Política de seguridad de la información - P - TIC- 04 Administración del Portal web institucional. - PL - TIC - 05 Plan de capacitación, sensibilización y comunicación de la seguridad de la información. - GUIAS: a. Análisis de impacto de Negocio. b. Seguridad en la Nube. c. Evidencia Digital. d. Guía de aseguramiento del Protocolo IPV6. e. Guía de Transición de IPV4/IPV6.

Reunión de Apertura						**Ejecución de la Auditoria**					**Reunión de Cierre**				
Día	11	**Mes**	julio	**Año**	2022	**Desde**	11/07/2022 **D/M/A**	Hasta	30/07/2022 **D/M/A**	**Día**	18	**Mes**	08	**Año**	2022

Jefe Oficina de Control Interno	**Auditor Líder**
José Duvan Lizarazo Cubillos	**Isabel Cristina Carvajal Ramos** **Andrea Chacon Mellizo**

La información solicitada y aportada por la Oficina de Control Interno Gestion, así como la recolectada a través de las entrevistas y mesas de trabajo fue la base sobre la cual se desarrolló la **Auditoria Interna Basada en Riesgos al proceso Política de Privacidad de Seguridad de la Información – Privacidad y Confidencialidad**, por esta razón se deja explicito que la información evaluada a uno de los componentes de la Matriz de Riesgos Informaticos cuenta con las características de integridad requeridas para sustentar los hallazgos, las observaciones y las recomendaciones generadas en el presente informe.

La auditoría se desarrolló basada en el cumplimiento de las procedimientos, guias, politicas y procesos desarrolladas y en el Modelo de Seguridad y Privacidad de la Información establecido por MINTIC y dado que La Secretaria TIC es una entidad de naturaleza pública, está en la obligación de acoger su Sistema de Gestión de Seguridad de la Información de acuerdo a los lineamientos establecidos en las leyes,Decretros y resoluciones expedidas por ley, por lo anterior se presentan los resultados producto del análisis de las evidencias suministradas por la Secretaría TIC.

1. **REVISIÓN:** DECRETO 00119 DEL 23 DE FEBRERO DE 2021, "POR MEDIO DEL CUAL SE ACTUALIZA Y MODIFICA EL MANUAL ESPECIFICO DE FUNCIONES Y COMPETENCIAS LABORALES DE LA PLANTA DE EMPLEOS DE LA ADMINISTRACION CENTRAL DEPARTAMENTAL DEL QUINDIO"

   La revisión del manual de funciones, se hace con el fin de establecer si se encuentran asignadas responsabilidades que permita brindar servicios, controles y condiciones de protección de la privacidad de la información de la Entidad y los ciudadanos acorde con lo exigido en la Ley 1581 de 2012 y los decretos reglamentarios.

   Al respecto se encuentra lo siguiente:

a) Director Tributario

   Guardar la reserva tributaria de los datos consignados por los contribuyentes en su declaración, con excepción de la identificación y ubicación. Sólo podrán suministrarse a los contribuyentes o sus apoderados cuando lo soliciten por escrito, y a las autoridades que lo requieran conforme a la ley. El funcionario que viole esta reserva incurrirá en causal de mala conducta.

b) Técnico Administrativo – Secretaria de Hacienda
Vigilar y custodiar el archivo documental y bases de datos a cargo.

c) Auxiliar Administrativo - Secretaria de Hacienda
Vigilar y custodiar el archivo documental y bases de datos a cargo.

d) Profesional Universitario – Secretaria de Hacienda
Administrar la base de datos de terceros atendiendo los protocolos de sistemas y políticas de la administración.

e) Técnico operativo – Secretaría de Hacienda
Apoyar las actividades de registro y control de bases de datos en aplicación de las normas generales y específicas del sistema de contabilidad pública.

f) Técnico operativo – Secretaria de Salud
Ejecutar las políticas de seguridad informática según estándares internacionales y políticas institucionales en el manejo de las bases de datos de aseguramiento y prestación de servicios.

g) Director de Sistemas de Información e Infraestructura tecnológica
- Definir la arquitectura de datos, aplicaciones y de los diferentes sistemas de información de la Gobernación y su estrategia de administración.
- Soportar y mantener los sistemas de información existentes en la Gobernación aplicando las metodologías y mejores prácticas. Así como la administración y manutención de las bases de datos corporativas.
- Realizar la actualización de herramientas y medios para generar copias de respaldo de las bases de datos y herramienta tecnológica de mesa de ayuda.

h) Profesional Universitario – TIC
Consolidar el Centro de Datos a nivel departamental, que permita contar con información veraz, confiable y oportuna en cada uno de los sectores que constituyen la misión de la entidad.

i) Director Gobierno Digital – TIC
Realizar la asesoría y asistencia a entidades, dependencias y municipios para incorporación de información, datos, trámites y demás operaciones relacionadas con el Dirigir y velar por el funcionamiento de Gobierno Digital.

Observación: En el manual de funciones se le asignan responsabilidades de protección de datos a ciertos funcionarios, pero existen otros que manejan bases de datos, que no tienen asignada esta responsabilidad relacionada con la seguridad y privacidad de la información.

2. **REVISIÓN DE PROCESO**: GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES

2.1. PR-TIC-01 ESTRATEGIA DE GOBIERNO DIGITAL

OBJETIVO GENERAL: Promover 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.

OBJETIVO ESPECÍFICO
Lograr procesos internos seguros y eficientes a través del fortalecimiento de las capacidades de gestión de tecnologías de información.

LINEAS DE ACCIÓN

SEGURIDAD Y PRIVACIDAD
- Diagnostico seguridad y privacidad de la información
- Mejora continúa
- Planificación
- Implementación
- Evaluación y desempeño.

Observación: Este documento publicado en la Intranet como un documento de MIPG, tiene un formato denominado: **PROGRAMA - EDUCACIÓN INFORMAL PARA LA IMPLEMENTACIÓN DE LA ESTRATEGIA DE GOBIERNO DIGITAL,** denominación que no es coherente con la estrategia de gobierno digital, dado que esta es un conjunto de soluciones tecnológicas y procedimientos que brindan al Estado la capacidad para la transformación digital y lograr una adecuada interacción con el ciudadano.

Observación: El cronograma no arroja resultados del producto, no cuenta con fechas claras y especificas para lograr los resultados esperados, además algunas actividades no están programadas.

2.2. PL- TI – 01 PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

OBJETIVO GENERAL: Establecer el Plan de Seguridad y Privacidad de la Información, el cual está dirigido a la implementación del modelo de seguridad y privacidad de la información MSPI y a todas las etapas que lo componen. Lo anterior en atención al contexto organizacional de la entidad, las capacidades técnicas y recursos disponibles.

OBJETIVOS ESPECÍFICOS:

- Comunicar e implementar la estrategia de seguridad de la información.
- Identificar infraestructuras críticas en las entidades a través de la implementación de mejores prácticas de seguridad de la información.
- Implementar y apropiar el Modelo de Seguridad y Privacidad de la Información – MSPI, con el objetivo de proteger la información y los sistemas de información, de acceso, uso, divulgación, interrupción o destrucción no autorizada.
- Hacer uso eficiente y seguro de los recursos de TI (Humano, Físico, Financiero, Tecnológico, etc.), para garantizar la continuidad de la prestación de los servicios

MARCO LEGAL:
Revisado el marco legal, se tienen las siguientes

observaciones:

- Es pertinente mencionar que la ley 527 de 1999, fue modificado por el Decreto 19 de 2012, publicado en el Diario Oficial No. 48.308 de 10 de enero de 2012, 'Por el cual se dictan normas para suprimir o reformar regulaciones, procedimientos y trámites innecesarios existentes en la Administración Pública'.

- Importante incluir la ley 1341 de 2009 "Por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones –TIC–, se crea la Agencia Nacional de Espectro y se dictan otras disposiciones.

- El Decreto 2573 de 2014, fue compilado por el Decreto 1078 de 2015 *"Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones"*

- El Decreto 113 de 2015 mencionado, no corresponde a normatividad en la materia, al contrario, se debe incluir el Decreto 103 de 2015 "Por el cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones".

- Se debe incluir la Resolución 00500 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", expedido por el MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES.

- La Directiva presidencial No. 03 mencionada corresponde a la vigencia 2021 y no al 2022

2.3. PL- TI – 02 PLAN DE GESTIÓN DE RIESGOS DE SEGURIDAD, PRIVACIDAD DE LA INFORMACION Y SEGURIDAD DIGITAL

Consiste en el establecimiento, desarrollo de estrategias y procedimientos previos a la posible materialización del riesgo u ocurrencia de la emergencia, tendientes a la mitigación de los mismos, haciéndolos menos graves, reduciendo al máximo las consecuencias o posibles pérdidas., en el tema en particular se resumen a continuación:

Riegos por incidencia externa:

(…)

- Modificaciones a la constitución política: Ya sea por asamblea constituyente, referendo, consulta popular, plebiscito o mediante leyes orgánicas, reestructuración o supresión de entidades.

Riesgos por incidencia interna:

- Perdida de la información: Hace referencia a la seguridad de la información que maneja la gobernación del Quindío, ya que debido a los procesos que la entidad maneja, esta debe conservarse de manera confidencial, y así evitar que sea entregada accidentalmente, o bien, que sea objeto de robo.

(…)

- Procesos de capacitación constante del personal TI: Riesgo asociado a la falta de actualización y capacitación de los conocimientos en sistemas de información de la gobernación del Quindío.
- Accesos no autorizados a los sistemas de información: Hace referencia a accesos a las bases de datos no autorizados de los diferentes aplicativos misionales de la entidad y de computadores que manejen información confidencial de la misma.
- Equivocaciones humanas: Riesgo permanente que se genera por el desconocimiento, descuido, o mal uso de un sistema de información o aplicativo de la entidad.

Mitigación del riesgo

- Pérdida de Información: La Gobernación del Quindío, cuenta con una política de respaldo de la información de los servidores de la gobernación, este respaldo se realiza todos los días en discos duros externos que se encuentran en el data center.

- Procesos de capacitación constante del personal TI: La secretaria TIC, capacita en el manejo de los sistemas de información a todo el personal que ingresa a la dependencia, se realiza un proceso de aprendizaje en el cual el ingeniero, técnico o tecnólogo aprende a dominar las herramientas tecnológicas que se tienen en la gobernación. Por otra parte, a través de la estrategia de gobierno en línea, la secretaria TIC capacita constantemente a su personal en implementación de la misma.

- Accesos no autorizados a los sistemas de información: Como parte de las políticas de seguridad de la información aprobadas por la secretaría administrativa, la entidad cuenta con una política de bloqueo de cesión de los equipos cada 5 minutos de inactivad. Lo anterior con el fin de evitar accesos no autorizados a los sistemas cuando el funcionario responsable del equipo no se encuentre en el sitio de trabajo. Por otra parte, y con el fin de evitar acceso no autorizado a los sistemas de información por parte de personas tanto internas como externan a la gobernación del Quindío; La entidad cuenta con un firewall instalado y con un sistema de antivirus licenciado que brindan seguridad a la hora de bloquear intentos de ataques o accesos a sistemas de información de la entidad.

- Equivocaciones humanas: Si bien es cierto que este riesgo es difícil de mitigar, por la cantidad de funcionarios que laboran en la entidad, cabe decir que la Secretaria TIC, brinda capacitaciones continuas a los funcionarios de la entidad, sobre el manejo de los aplicativos de la entidad, además de eso, desde el área se generan copias de seguridad diarias de las bases de datos de los aplicativos de la entidad, lo anterior con el fin restaurar la información, ante cualquier perdida o daño que se haga en una base de datos.

Observación: En la matriz de "RIESGOS INFORMÁTICOS", suministrada en el proceso de planeación del proceso auditor, solo se describe un riesgo, relacionada con la protección de datos personales para garantizar el derecho fundamental de Habeas Datas consagrado en el Articulo 15 de constitución, sin conocer el porque no se tienen en cuenta otros riesgos identificados en este documento como

2.5. POL-TIC-01 POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES

Observación: Analizada la política, se evidencia que no se designa de manera particular la persona responsable del tratamiento de datos, quien debe ser la encargada de decidir sobre las bases de datos y/o tratamiento de los mismos.

2.6. POL-TIC-02 POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

PRIVACIDAD Y CONFIDENCIALIDAD

Esta política contiene la descripción y los controles que la gobernación del Quindío realiza en el tratamiento de los datos personales. Dicha política está reglamentada conforme a la normatividad vigente.

Política de tratamiento de datos personales

La gobernación del Quindío, tiene adoptada una política de confidencialidad y protección de datos personales, con el objeto de proteger la privacidad de la información personal obtenida a través de sus diferentes sistemas de información, buscando salvaguardar la privacidad y seguridad de la información personal del usuario que interactúa con los diferentes sistemas de información de la entidad.

Finalidad y tratamiento al cual serán sometidos los datos personales de los usuarios

En relación con la naturaleza y las funciones propias de la gobernación del Quindío:

El tratamiento de los datos se realizará con la finalidad de las funciones propias del departamento, en las disposiciones contenidas en la ley 1581 de 20121 (Ministerio de tecnologías de la información y comunicaciones, 2013) y el decreto 1377 de 20132 (Ministerio de tecnologías de la información y comunicaciones, 2013) demás normas que los modifiquen, adicionen, sustituyan o complementen

El tratamiento de los datos se realizará para la vinculación, desempeño de funciones o prestación de servicios, retiro o terminación, dependiendo del tipo de relación jurídica entablada con el departamento del Quindío (incluye, entre otros, funcionarios, exfuncionarios, judicantes, practicantes y aspirantes a cargos).

El tratamiento de los datos se realizará para los fines relacionados con el desarrollo el proceso de gestión contractual de productos o servicios que la practicante requiere para su

funcionamiento de acuerdo a la normatividad vigente.

Observación: No se determina quien hace el control

RESPONSABILIDAD: La responsabilidad de privacidad y confidencialidad de la información, quedo enmarcada en:

- Director de Talento Humano
- Director de Recursos Físicos
- Secretario TIC
- Director de Gobierno digital
- Director de sistemas de información e infraestructura tecnológica
- Director Jurídico y de Contratación

Observación: Si bien es cierto se asignan unas responsabilidades no se concreta una persona responsable del tratamiento de datos, quien debe ser la encargada de decidir sobre las bases de datos y/o tratamiento de los mismos.

Al respecto es pertinente anotar "*Una entidad es **responsable** del tratamiento **cuando** controla y se responsabiliza de los datos que posee. Sin embargo, si una entidad almacena datos, pero otra decide sobre ellos, entonces es **encargado** del tratamiento.*"[1]

Observación: No se logró establecer las acciones implementadas por estos funcionarios para cumplir con las responsabilidades establecidas en la política, con excepción de las minutas de los contratos que tienen incorporada la cláusula de obligaciones del contratista, la reserva de la información y documentos que tenga conocimiento o a los que tenga acceso en virtud de la ejecución del contrato

2.7. P-TIC-04 ADMINISTRACIÓN DEL PORTAL WEB

Observación: Este procedimiento adoptado, no menciona responsabilidades relacionada con el tratamiento de datos, ni del personal encargado del tratamiento.

---

[1] https://www.sic.gov.co › preguntas-frecuentes-pdp

Objetivos:

- Evidenciar las debilidades informáticas que presenta la entidad.
- Socializar las políticas de seguridad de la información diseñadas por la dirección TIC de la gobernación del Quindío.
- Lograr que cada funcionario conozca sus roles y responsabilidades de seguridad y privacidad de la información dentro de la gobernación
- Evaluar, medir y cuantificar, si las políticas y el plan de sensibilización de seguridad de la información implementado generaron impacto en el desarrollo de las actividades de la Entidad.
- Mantener informados a los funcionarios, contratistas o terceros sobre las nuevas vulnerabilidades, actualizaciones a las plataformas y recomendaciones de seguridad informática.

Problemas identificados:

- Existe la mentalidad que no hay nada importante por proteger en su computador.
- Se tiene el concepto errado que la tecnología por si misma puede resolver los problemas de seguridad.
- Continuamente se generan nuevos métodos mediante engaños que buscan obtener información confidencial.
- Los funcionarios deben conocer tanto las amenazas externas como las internas.
- Es importante conocer las mejores prácticas en cuanto a seguridad en el manejo responsable del internet.

2.8. PLAN Código: PL-TIC-05 PLAN DE IDENTIFICACIÒN DE NECESIDADES DE CAPACITACIÒN

Problemas identificados

Temáticas involucradas en las capacitaciones

- Manejo responsable del internet, riesgos asociados.
- Seguridad en redes wifi-privadas y públicas.
- Uso adecuado del correo electrónico empresarial, redes sociales y aplicativos misionales de la entidad.
- Manejo adecuado de contraseñas.
- Copias de seguridad y su importancia para dar continuidad a las actividades a causa de pérdida o daño del equipo de cómputo.
- Software permitido y no permitido en la entidad

- Ingeniería social.
- Protección contra los virus.
- Sanciones por incumplimiento de las políticas.
- Gestión de incidentes (que reportar, donde puedo reportar).
- Spam.
- Seguridad En El Puesto De Trabajo

Problemas identificados

- La mayoría de las vulnerabilidades provienen desde el interior de las propias empresas (empleados descontentos, fraude interno, accesos no autorizados, poca motivación, carencia de entrenamiento organizacional y desconocimientos de las políticas de seguridad)
- Uso inadecuado de las contraseñas de los equipos, correos electrónicos y demás aplicativos que se emplean en la entidad.
- Mal uso del internet no existe conciencia sobre mejores prácticas a la hora de navegar en la web.
- Mal uso del correo electrónico empresarial, el cual es utilizado muchas veces para actividades personales e inscripción en páginas web de dudosa procedencia.
- Falta control de acceso a sitios restringidos para las personas, se evidencia muchas veces fácil acceso a computadores de funcionarios públicos.
- Uso inadecuado de dispositivos USB, como discos duros, memorias, etc.
- Copias de seguridad de los equipos de cómputo de los funcionarios, que respalden la información contra perdida o daños.
- Falta de capacitación y sensibilización de la política de escritorio y pantalla limpios en los equipos de los funcionarios.

Cronograma de capacitaciones

Se define un cronograma de capacitación, sensibilización y comunicación de las políticas de seguridad informática de la entidad, el cual incluirá todas las secretarias de despacho de la entidad.

Cronograma Capacitaciones 2022 Gobernación Del Quindio							
Secretarias	Fechas						
	Abril	Mayo	Junio	Julio	Septiembre	Octubre	Noviembre
Secretaria Tics	X						
Secretaria Juridica		X					
Planeación		X					
Hacienda y Finanzas Públicas			X				
Salud			X				
Interior				X			
Turismo Industria y Comercio				X			
Aguas e Infraestructura					X		
Educación					X		
Privada					X		
Agricultura, Desarrollo Rural y Medio Ambiente						X	
Representación Judicial y Defensa del Departamento						X	X
Administrativa						X	
Familia							X
Cultura							X
Control interno de Gestión					X		

Observación: El cronograma de capacitaciones no se está siguiendo con rigor

Las evidencias muestran lo siguiente:

- 18 DE MARZO DE 2022:
  Tema: Ética en el contexto digital y manejo digital de datos
  Personas capacitadas: 56 (44 contratistas y 12 funcionarios de la planta)

- 11 DE MAYO DE 2022 – Secretaria Jurídica y de Contratación
  Tema: Ética en el contexto digital y manejo digital de datos
  Personas capacitadas: 6 (5 contratistas y 1 funcionario de la planta)
- 13 DE JUNIO DE 2022 – Secretaria de Salud
  Tema: Datos Abiertos
  Personas capacitadas: No aportan listado de asistencia

Observación: No se evidencia la socialización de los procesos adoptados, guías e instructivos en materia de Seguridad y Privacidad de la Información

Observación: El material pedagógico aportado y que es utilizado en los procesos de capacitación, no evidencia que cubra las necesidades en razón a los problemas identificados en el "Plan de Capacitación Sensibilización y Comunicación de Seguridad de la Información"

3. OTROS DOCUMENTOS VALORADOS

Con el fin de lograr la trazabilidad de la información, se revisaron los siguientes documentos adoptados y publicados por la Secretaría TIC:

- ANALISIS DE IMPACTO DE NEGOCIOS
- SEGURIDAD EN LA NUBE
- EVIDENCIA DIGITAL
- GUIA DE ASEGURAMIENTO DEL PROTOCOLO IP V 6
- GUIA DE TRANSICIÓN DE IP Y 4 A IP V 6

Observación: La secretaría TIC cuenta con las Guías implementadas para garantizar la protección del Derecho a la Protección del Habeas Data.

4. REVISIÓN DEL DECRETO 629 DE OCTUBRE DE 2021 – PUBLICADO EN LA GACETA No. 145 DEL19 DE NOVIEMBRE DE 2021

Observación: En el decreto no se tiene en cuenta las directrices emanadas de la Resolución No.00500 de marzo 10 de 2022

4.1 PÁGINA WEB GOBERNACIÓN DEL QUINDÍO – DECRETO 1008 DE 2018

Tiene publicada la política de Seguridad y Privacidad de la siguiente manera:

Seguridad y privacidad: Busca preservar la confidencialidad, integridad y disponibilidad de los activos de información de las entidades del Estado, garantizando su buen uso y la privacidad de los datos a través de un Modelo de Seguridad y Privacidad de la información.

HALLAZGOS

HALLAZGO N.1: POLÍTICAS, PROCESOS, PROCEDIMIENTOS, GUÍAS, MANUALES Y FORMATOS SIN AJUSTAR DE CONFORMIDAD CON LA RESOLUCIÓN 00500 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".

CONDICIÓN: una vez revisadas, verificadas y analizados los documentos adoptados en la vigencia 2022, por la secretaria de las TIC y publicadas en la Intranet conforme a MIPG, así como el Decreto 629 de octubre de 2021 expedido por la Gobernación del Quindío, relacionados con el Modelo de Seguridad y Privacidad de la Información (MSPI), la Guía de Gestión del Riesgo de Seguridad de la Información y el Procedimiento para la gestión de incidentes de la Gestión Digital, se evidencia que los mismos no fueron ajustados conforme a la Resolución 0050 del 10 de marzo de 2021, teniendo en cuenta que dicho acto administrativo es vinculante según el artículo 2.2.9.1.1.2. del Decreto 1078 de 2015.

CRITERIO:

- Artículo 39 de la Ley 489 de 1998
- Artículo 2.2.9.1.1.2 del Decreto 1078 de 2015.
- Resolución 00500 de 10 de marzo de 2021.
- Artículo 17 de la Ley 1341 de 2009 modificado por el artículo 13 de la Ley 1978 de 2019, y el Decreto 1064 de 2020.

CAUSA: Falta de gestión en la actualización del Normograma de la Secretaría TIC

EFECTO:

- Incumplimiento con directrices de Normatividad Vigente.
- Configuración de riesgos en materia de Seguridad y Privacidad de la Información.

HALLAZGO N. 2
PLAN DE CAPACITACIÒN QUE NO CONTEMPLA LA SOCIALIZACIÒN DE POLÌTICAS, PROCESOS, PROCEDIMIENTOS, GUÌAS, MANUALES Y FORMATOS ADOPTADOS POR LA SECRETARIA EN LA VIGENCIA 2022.

CONDICIÒN:
Las evidencias aportadas en el curso de la etapa de la ejecución de la auditoria dan cuenta de capacitaciones realizadas, sobre la normatividad vigente en materia de Seguridad y Privacidad de la informacion, pero se ha omitido la socialización de POLíTICAS, PROCESOS, PROCEDIMIENTOS, GUÍAS, MANUALES Y FORMATOS adoptados por la secretaria de las tic en la vigencia 2022 al cliente interno (Funcionarios y contratistas de la Gobernación del Quindío), quienes son los llamados a garantizar la Seguridad y privacidad de la informacion que en virtud de sus funciones manejan como por ejemplo las Bases de Datos.

CRITERIO:

- PL-TIC-05 PLAN DE IDENTIFICACIÒN DE NECESIDADES DE CAPACITACIÒN

CAUSA:

- En la PL-TIC-05 PLAN DE IDENTIFICACIÒN DE NECESIDADES DE CAPACITACIÒN, no se identifica como problema que los funcionarios y contratistas desconozcan lo referente a los procesos, procedimientos, guías, manuales y formatos establecidos por la secretaria TIC.

EFECTO:

- Incumplimiento de la Normatividad interna adoptada por la secretaría TIC

HALLAZGO N. 3
RIESGOS RELACIONADOS CON LA SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN QUE NO SON VALORADOS EN LA CONTRUCCIÒN DE LA MATRIZ DEL RIESGO INFORMATICO.

CONDICIÒN: revisada toda la documentación que soporta el proceso auditor se tiene que en algunos de dichos documentos se asignan responsabilidad en el tratamiento y control de la informacion que manejan las diferentes áreas y la cual está en cabeza de la Secretarias y direcciones: TIC, Jurídica y de Contratación, Talento Humano y Recursos Físicos, todas estas en representación de la Entidad Territorial Departamento del Quindio, no obstante, no se encuentra determinado la responsabilidad de las Funcionarios y/o Contratistas que deciden sobre las Bases Datos almacenados por la Entidad para la prestación del servicio Público.

CRITERIO:

- Ley 87 de 1993.
- Ley 1273 de 2009 Articulo 269f
- Matriz de Riesgos Informáticos.

CAUSA:

- Desconocimiento de las responsabilidades por la violación de Datos Personales.

EFECTO:

- Denuncias ciudadanas.
- Hallazgos con incidencia Penal.

RECOMENDACIONES

De conformidad al presente informe final de Audiotria se recomienda a la Secretaría TIC que adopte el Plan de Mejora conforme a los documentos adoptados para ello, el cual debe contener las acciones preventivas y correctivas que ataquen la causa de los Hallazgos Administrativos estructrados por la oficina de contro Interno de Gestion, en un plazo de quince (15) días hábiles siguientes a la fecha de recibido el Informe final de auditoría, salvo que involucre a otros procesos o dependencias, caso en el cual el término será veinte (20) días hábiles para su formulación y su remisión a la Oficina de Control Interno Interno de Gestion.

CONCLUSION DE LA AUDITORIA

En el resultado general de la evaluación **al proceso Política de Privacidad de Seguridad de la Información – Privacidad y Confidencialidad** se evidenció lo siguiente:
La Secretaría TIC, refleja en la información aportada, el adecuado desarrollo y trabajo realizado evidenciado en **ciertos** elementos como son la política general de seguridad de la información, políticas específicas de seguridad informática, Matrix de Riesgo de Seguridad de Informatica, Modelo de Seguridad y Privacidad de la Información e indicadores de gestión entre otros.
Así mismo, se identificaron diferentes herramientas tecnológicas que le han permitido a la Secretaría TIC cumplir con los objetivos de asegurar y mantener la confidencialidad, integridad y disponibilidad de la información. Aun así, se identifica el Plan de Mejora relacionada con la elaboración, formalización, actualización de la documentación de algunos procedimientos, políticas, procesos, guías, manuales y formatos, donde se identificaron falencias en la operatividad de dichos controles, asi mismo se evidencia una falta de valoración de situaciones que pueden vulnerar los datos personales que pueden ser manejados con la mayor pulcritud para garantizar el Derecho Fundamental al Habeas Data.

Para constancia se firma en Armenia Quindío, a los dieciocho (18) días de agosto de 2022

APROBACIÓN DEL INFORME DE AUDITOÍIA		
Nombre completo	**Responsabilidad (Cargo)**	**Firma**
JOSÉ DUVÁN LIZARAZO CUBILLOS	Jefe Oficina Control Interno de Gestión	
	Contratistas – O. C.I.G	
Andrea Chacón Mellizo		