INSTRUMENTO DE IDENTIFICACIÓN DE LA LINEA BASE DE SEGURIDAD
HOJA PORTADA

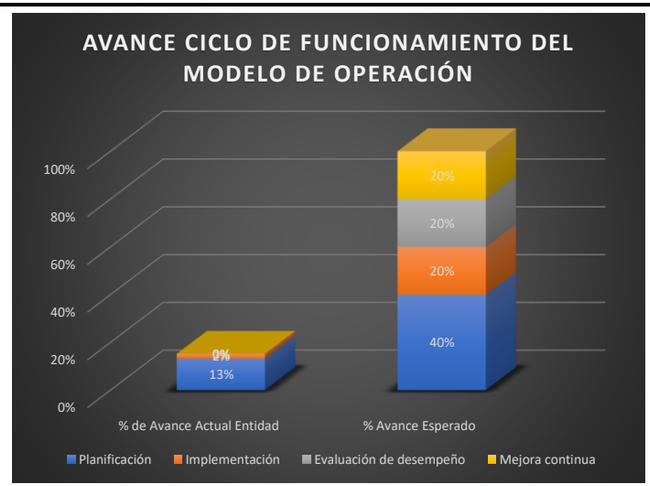
ENTIDAD EVALUADA	Alcaldía Municipal de Chía
FECHAS DE EVALUACIÓN	1/07/2020
CONTACTO	Jorge Ivan Ortiz- Jefe Oficina TIC
ELABORADO POR	Jorge Ivan Ortiz- Jefe Oficina TIC

EVALUACIÓN DE EFECTIVIDAD DE CONTROLES - ISO 27001:2013 ANEXO A

No.	Evaluación de Efectividad de controles			
	DOMINIO	Calificación Actual	Calificación Objetivo	EVALUACIÓN DE EFECTIVIDAD DE CONTROL
A.5	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	80	100	GESTIONADO
A.6	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	60	100	EFECTIVO
A.7	SEGURIDAD DE LOS RECURSOS HUMANOS	51	100	EFECTIVO
A.8	GESTIÓN DE ACTIVOS	47	100	EFECTIVO
A.9	CONTROL DE ACCESO	29	100	REPETIBLE
A.10	CRIPTOGRAFÍA	30	100	REPETIBLE
A.11	SEGURIDAD FÍSICA Y DEL ENTORNO	47	100	EFECTIVO
A.12	SEGURIDAD DE LAS OPERACIONES	33	100	REPETIBLE
A.13	SEGURIDAD DE LAS COMUNICACIONES	60	100	EFECTIVO
A.14	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	13	100	INICIAL
A.15	RELACIONES CON LOS PROVEEDORES	10	100	INICIAL
A.16	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	29	100	REPETIBLE
A.17	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	10	100	INICIAL
A.18	CUMPLIMIENTO	31	100	REPETIBLE
PROMEDIO EVALUACIÓN DE CONTROLES		38	100	REPETIBLE

AVANCE CICLO DE FUNCIONAMIENTO DEL MODELO DE OPERACIÓN (PHVA)

Año	AVANCE PHVA		
	COMPONENTE	% de Avance Actual Entidad	% Avance Esperado
2015	Planificación	13%	40%
2016	Implementación	2%	20%
2017	Evaluación de desempeño	0%	20%
2018	Mejora continua	0%	20%
TOTAL		15%	100%



NIVEL DE MADUREZ MODELO SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

NIVELES DE MADUREZ DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

	NIVEL DE CUMPLIMIENTO
Inicial	INTERMEDIO
Repetible	INTERMEDIO
Definido	CRÍTICO
Administrado	CRÍTICO
Optimizado	CRÍTICO

TOTAL DE REQUISITOS CON CALIFICACIONES DE CUMPLIMIENTO	
CRÍTICO	0% a 35%
INTERMEDIO	36% a 70%
SUFICIENTE	71% a 100%

CALIFICACIÓN FRENTE A MEJORES PRÁCTICAS EN CIBERSEGURIDAD (NIST)

MODELO FRAMEWORK CIBERSEGURIDAD NIST		
Etiquetas de fila	CALIFICACIÓN ENTIDAD	NIVEL IDEAL CSF
IDENTIFICAR	0	100
DETECTAR	0	100
RESPONDER	0	100
RECUPERAR	0	100
PROTEGER	0	100

INSTRUMENTO DE IDENTIFICACIÓN DE LA LINEA BASE DE SEGURIDAD ADMINISTRATIVA Y TÉCNICA
HOJA LEVANTAMIENTO DE INFORMACIÓN

Alcaldía Municipal de Chía

ID. ITEM	CARGO	ITEM	DESCRIPCIÓN	ISO	MSPI	CIBERSEGURIDAD	PRUEBA	EVIDENCIA	BRECHA	NIVEL DE CUMPLIMIENTO ANEXO A ISO 27001	RECOMENDACIÓN
SEGURIDAD DE LA INFORMACIÓN											
AD.1	**Responsable de SI**	**POLITICAS DE SEGURIDAD DE LA INFORMACIÓN**	**Orientación de la dirección para gestión de la seguridad de la información**	**A.5**	**Componente planificación y modelo de madurez nivel gestionado**					**80**	
AD.1.1	Responsable de SI	Documento de la política de seguridad y privacidad de la Información	Se debe definir un conjunto de políticas para la seguridad de la información aprobada por la dirección, publicada y comunicada a los empleados y a la partes externas pertinentes	A.5.1.1	Componente planificación y modelo de madurez inicial	ID.GV-1	Solicite la política de seguridad de la información de la entidad y evalúe: a) Si se definen los objetivos, alcance de la política b) Si esta se encuentra alineada con la estrategia y objetivos de la entidad c) Si fue debidamente aprobada y socializada al interior de la entidad por la alta dirección Revise si la política: a)Define que es seguridad de la información b) La asignación de las responsabilidades generales y específicas para la gestión de la seguridad de la información, a roles definidos; c) Los procesos para manejar las desviaciones y las excepciones. Indague sobre los responsables designados formalmente por la dirección para desarrollar, actualizar y revisar las políticas. Verifique cada cuanto o bajo que circunstancias se revisan y actualizan, verifique la ultima fecha de emisión de la política frente a la fecha actual y que cambios a sufrido, por lo menos debe haber una revisión anual. **Para la calificación tenga en cuenta que:** 1) Si se empiezan a definir las políticas de seguridad y privacidad de la información basada en el Modelo de Seguridad y Privacidad de la Información, están en 20. 2) Si se revisan y se aprueban las políticas de seguridad y privacidad de la información, , están en 40. 3) Si se divulgan las políticas de seguridad y privacidad de la información, están en 60.	La alcaldía municipal de Chía por medio del decreto 821 de 2019 estableció la política de seguridad de la información, donde se establecen procedimientos, lineamientos y políticas.		80	Monitorear el cumplimiento de la política de seguridad.
AD.1.2	Responsable de SI	Revisión y evaluación	Las políticas para seguridad de la información se deberían revisar a intervalos planificados o si ocurren cambios significativos, para asegurar su conveniencia, adecuación y eficacia continuas.	A.5.1.2	componente planificación					80	
ORGANIZACIÓN SEGURIDAD INFORMACIÓN											
A2	**Responsable de SI**	**ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN**	**Marco de referencia de gestión para iniciar y controlar la implementación y la operación de la seguridad de la información dentro de la organización Garantizar la seguridad del teletrabajo y el uso de los dispositivos móviles**	**A.6**						**60**	
AD.2.1	**Responsable de SI**	**Organización Interna**	**Marco de referencia de gestión para iniciar y controlar la implementación y la operación de la seguridad de la información dentro de la organización**	**A.6.1**	**Componente planificación y modelo de madurez gestionado**					**60**	
AD.2.1.1	Responsable de SI	Roles y responsabilidades para la seguridad de la información	Se deben definir y asignar todas las responsabilidades de la seguridad de la información	A.6.1.1	Componente planificación	ID.AM-6 ID.GV-2 PR.AT-2 PR.AT-3 PR.AT-4 PR.AT-5 DE.DP-1 RS.CO-1	Para revisarlo frente a la NIST verifique si 1) los roles y responsabilidades frente a la ciberseguridad han sido establecidos 2) los roles y responsabilidades de seguridad de la información han sido coordinados y alineados con los roles internos y las terceras partes externas 3) Los a) proveedores, b) clientes, c) socios, d) funcionarios, e) usuarios privilegiados, f) directores y gerentes (mandos senior), g) personal de seguridad física, h) personal de seguridad de la información entienden sus roles y responsabilidades, i) Están claros los roles y responsabilidades para la detección de incidentes Solicite el acto administrativo a través del cual se crea o se modifica las funciones del comité gestión institucional (o que haga sus veces), en donde se incluyan los temas de seguridad de la información en la entidad, revisado y aprobado por la alta Dirección. Revise la estructura del SGSI: 1) Tiene el SGSI suficiente apoyo de la alta dirección?, esto se ve reflejado en comités donde se discutan temas como la política de SI, los riesgos o incidentes. 2) Están claramente definidos los roles y responsabilidades y asignados a personal con las competencias requeridas?, 3) Están identificadas los responsables y responsabilidades para la protección de los activos? (Una práctica común es nombrar un propietario para cada activo, quien entonces se convierte en el responsable de su protección) 4)Están definidas las responsabilidades para la gestión del riesgo de SI y la aceptación de los riesgos residuales? 5) Están definidos y documentados los niveles de autorización? 6) Se cuenta con un presupuesto formalmente asignado a las actividades del SGSI (por ejemplo campañas de sensibilización en seguridad de la información)		No existe acto administrativo donde se establezcan los roles de seguridad de la información	60	Establecer por medio de acto administrativo roles de seguridad de la información

AD.2.1.2	Responsable de SI	Separación de deberes / tareas	Los deberes y áreas de responsabilidad en conflicto se debe separar para reducir las posibilidades de modificación no autorizada o no intencional, o el uso indebido de los activos de la organización.	A.6.1.2		PR.AC-4 PR.DS-5 RS.CO-3	Indague como evitan que una persona pueda acceder, modificar o usar activos sin autorización ni detección. La mejor práctica dicta que el inicio de un evento deber estar separado de su autorización. Al diseñar los controles se debería considerar la posibilidad de confabulación. Tenga en cuenta que para las organizaciones pequeñas la separación de deberes puede ser difícil de lograr, en estos casos se deben considerar controles compensatorios como revisión periódica de los rastros de auditoría y la supervisión de cargos superiores.	La alcaldía municipal de Chía tiene separado los deberes y funciones de cada persona, dependencia y direcciones. Teniendo en cuenta el acceso y modificación de los activos en algunos casos estos cuentan con un determinado propietario, custodio y usuarios, en algunos casos los activos están en computadores que tienen usuarios y contraseñas genéricas que pueden ser utilizadas por cualquier persona.		60	Capacitación a funcionarios y contratistas sobre la separación de deberes
AD.2.1.3	Responsable de SI	Contacto con las autoridades.	Las organizaciones deben tener procedimientos establecidos que especifiquen cuándo y a través de que autoridades se debe contactar a las autoridades (por ejemplo, las encargadas de hacer cumplir la ley, los organismos de reglamentación y las autoridades de supervisión), y cómo se debe reportar de una manera oportuna los incidentes de seguridad de la información	A.6.1.3		RS.CO-2	Solicite los procedimientos establecidos que especifiquen cuándo y a través de qué autoridades se debería contactar a las autoridades, verifique si de acuerdo a estos procedimientos se han reportado eventos o incidentes de SI de forma consistente.	La alcaldía municipal de Chía mediante la política de seguridad de la información, cuenta con un procedimiento para el contacto de autoridades nacionales son eventos de seguridad de la información		100	
AD.2.1.4	Responsable de SI	Contacto con grupos de interés especiales	Se deben mantener contactos apropiados con grupos de interés especial u otros foros y asociaciones profesionales especializadas en seguridad. Por ejemplo a través de una membresía	A.6.1.4		ID.RA-2	Pregunte sobre las membrecías en grupos o foros de interés especial en seguridad de la información en los que se encuentran inscritos las personas responsables de la SI.	La alcaldía municipal de Chía no cuenta con membrecías en grupos de interés de seguridad de la información. Sólo se contactan a los fabricantes en caso de soporte	No se cuentan con membrecías en grupos especiales de seguridad de la información	n/a	
AD.2.1.5	Responsable de SI	Seguridad de la información en la gestión de proyectos	La seguridad de la información se debe integrar al(los) método(s) de gestión de proyectos de la organización, para asegurar que los riesgos de seguridad de la información se identifiquen y traten como parte de un proyecto. Esto se aplica generalmente a cualquier proyecto, independientemente de su naturaleza, por ejemplo, un proyecto para un proceso del negocio principal, TI, gestión de instalaciones y otros procesos de soporte.	A.6.1.5		PR.IP-2	Pregunte como la Entidad integra la seguridad de la información en el ciclo de vida de los proyectos para asegurar que los riesgos de seguridad de la información se identifiquen y traten como parte del proyecto. Tenga en cuenta que esto no solamente aplica para proyectos de TI. Por ejemplo, puede aplicar en proyectos de traslado de activos de información, gestión de instalaciones, personal en outsourcing que soporta procesos de la organización. Las mejores prácticas sugieren: a) Que los objetivos de la seguridad de la información se incluyan en los objetivos del proyecto; b) Que la valoración de los riesgos de seguridad de la información se lleve a cabo en una etapa temprana del proyecto, para identificar los controles necesarios; c) Que la seguridad de la información sea parte de todas las fases de la metodología del proyecto aplicada.	No existe formalmente este lineamiento, queda a libre elección del líder o supervisor de cada proyecto si incluye temas relacionados con la seguridad de la información, por ejemplo en lo riesgos del proyecto.	No existe un lineamiento en los proyectos donde se integre la seguridad de la información, cada líder de proyecto es autónomo en decidir si desea integrar ese componente al ciclo de vida del proyecto a ejecutar.	20	Establecer un lineamiento para integrar la seguridad de la información en los proyectos a ejecutar en la alcaldía municipal de Chía.
AD.2.2	Responsable de SI	**Dispositivos Móviles y Teletrabajo**	**Garantizar la seguridad del teletrabajo y uso de dispositivos móviles**	**A.6.2**	**Modelo de Madurez Gestionado**					**60**	
AD.2.2.1	Responsable de SI	Política para dispositivos móviles	Se deberían adoptar una política y unas medidas de seguridad de soporte, para gestionar los riesgos introducidos por el uso de dispositivos móviles.	A.6.2.1			Pregunte si la entidad asigna dispositivos móviles a sus funcionarios o permite que los dispositivos de estos ingresen a la entidad. Revise si existe una política y controles para su uso, que protejan la información almacenada o procesada en estos dispositivos y el acceso a servicios te TI desde los mismos. De acuerdo a las mejores prácticas esta política debe considerar, teniendo en cuenta el uso que se le dé al dispositivo, lo siguiente: a) el registro de los dispositivos móviles; b) los requisitos de la protección física; c) las restricciones para la instalación de software; d) los requisitos para las versiones de software de dispositivos móviles y para aplicar parches; e) la restricción de la conexión a servicios de información; f) los controles de acceso; g) técnicas criptográficas; h) protección contra software malicioso; i) des habilitación remota, borrado o cierre; j) copias de respaldo; k) uso de servicios y aplicaciones web. Cuando la política de dispositivos móviles permite el uso de dispositivos móviles de propiedad personal, la política y las medidas de seguridad relacionadas también deben considerar: a) la separación entre el uso privado y de la Entidad de los dispositivos, incluido el uso del software para apoyar esta separación y proteger los datos del negocio en un dispositivo privado; b) brindar acceso a la información de la Entidad solo cuando los usuarios hayan firmado un acuerdo de usuario final, en el que se reconocen sus deberes (protección física, actualización del software, etc.), desistir de la propiedad de los datos de la	La Alcaldía Municipal de Chía cuenta con una política de dispositivos móviles la cual se encuentra en la política de seguridad de la información	Medición y aplicación de la norma en el 100% de los casos.	60	Medición y aplicación de la norma en el 100% de los casos.

AD.2.2.2	Responsable de TICs	Teletrabajo	Se deberían implementar una política y unas medidas de seguridad de soporte, para proteger la información a la que se tiene acceso, que es procesada o almacenada en los lugares en los que se realiza teletrabajo.	A.6.2.2		PR.AC-3	Definición de teletrabajo: El teletrabajo hace referencia a todas las formas de trabajo por fuera de la oficina, incluidos los entornos de trabajo no tradicionales, a los que se denomina "trabajo a distancia", "lugar de trabajo flexible", "trabajo remoto" y ambientes de "trabajo virtual". Indague con la entidad si el personal o terceros pueden realizar actividades de teletrabajo, si la respuesta es positiva solicite la política que indica las condiciones y restricciones para el uso del teletrabajo. Las mejores prácticas consideran los siguientes controles: a) la seguridad física existente en el sitio del teletrabajo b) los requisitos de seguridad de las comunicaciones, teniendo en cuenta la necesidad de acceso remoto a los sistemas internos de la organización, la sensibilidad de la información a la que se tendrá acceso y que pasará a través del enlace de comunicación y la sensibilidad del sistema interno; c) el suministro de acceso al escritorio virtual, que impide el procesamiento y almacenamiento de información en equipo de propiedad privada; d) la amenaza de acceso no autorizado a información o a recursos, por parte de otras personas que usan el mismo equipo, por ejemplo, familia y amigos; e) el uso de redes domésticas y requisitos o restricciones sobre la configuración de servicios de red inalámbrica; e) acuerdos de licenciamiento de software de tal forma que las organizaciones puedan llegar a ser responsables por el licenciamiento de software de los clientes en estaciones de trabajo de propiedad de los empleados o de usuarios externos; f) requisitos de firewall y de protección contra software malicioso. Las directrices y acuerdos que se consideren deberían incluir: g) el suministro de equipo adecuado y de muebles de	No se cuenta con una política de teletrabajo, debido a que la alcaldía municipal de Chía brinda servicios a la comunidad y la mayoría de funcionarios - contratistas viven en Chía.		60	
O DE LOS RECURSOS HUMANOS											
AD.3	**Responsable de SI/Gestión Humana/Líderes de los procesos**	**SEGURIDAD DE LOS RECURSOS HUMANOS**		**A.7**						**51**	
AD.3.1	**Responsable de SI**	**Antes de asumir el empleo**	**Asegurar que el personal y contratistas comprenden sus responsabilidades y son idóneos en los roles para los que son considerados.**	**A.7.1**	**Modelo de Madurez Definido**					**40**	
AD.3.1.1	Gestión Humana	Selección e investigación de antecedentes	Las verificaciones de los antecedentes de todos los candidatos a un empleo se deben llevar a cabo de acuerdo con las leyes, reglamentos y ética pertinentes, y deberían ser proporcionales a los requisitos de negocio, a la clasificación de la información a que se va a tener acceso, y a los riesgos percibidos.	A.7.1.1		PR.DS-5 PR.IP-11	Revise el proceso de selección de los funcionarios y contratistas, verifique que se lleva a cabo una revisión de: a) Referencias satisfactorias b) Verificación de la de la hoja de vida del solicitante incluyendo certificaciones académicas y laborales; c) Confirmación de las calificaciones académicas y profesionales declaradas; d) Una verificación más detallada, como la de la información crediticia o de antecedentes penales. Cuando un individuo es contratado para un rol de seguridad de la información específico, las organizaciones deberían asegurar que el candidato tenga la competencia necesaria para desempeñar el rol de seguridad; e) sea confiable para desempeñar el rol, especialmente si es crítico para la organización. f) Cuando un trabajo, ya sea una asignación o una promoción, implique que la persona tenga acceso a las instalaciones de procesamiento de información, y en particular, si ahí se maneja información confidencial, por ejemplo, información financiera o información muy confidencial, la organización debería también considerar verificaciones adicionales más detalladas (por ejemplo estudio de seguridad, polígrafo, visita domiciliaria) g) También se debería asegurar un proceso de selección para contratistas. En estos casos, el acuerdo entre la organización y el contratista debería especificar las responsabilidades por la realización de la selección, y los procedimientos de notificación que es necesario seguir si la selección no se ha finalizado, o si los resultados son motivo de duda o inquietud. h) La información sobre todos los candidatos que se consideran para cargos dentro de la organización, se debería recolectar y manejar apropiadamente de acuerdo con la ley de protección de datos personales.	En la alcaldía existen las modalidades de libre nombramiento y remoción, carrera (concurso de méritos), establecidos en la ley 909 de 2004, así como vinculación vía contratos (ley 80) Para los funcionarios contratados por ley 909, se validan los requisitos establecidos en el manual de funciones, requisitos y competencias, contra la información adjuntada por el candidato. A las personas contratadas por ley 80, se verifican durante el proceso contractual los requisitos establecidos por el área de la cual parte la necesidad de contratación.	No se ha establecido un procedimiento para la selección de personal en cuanto a seguridad de la información y verificación de antecedentes adicional cuando el cargo requiere el manejo de información confidencial.	40	Establecer un procedimiento para verificación de antecedentes cuando se va a desempeñar un cargo crítico.
AD.3.1.2	Gestión Humana	Términos y condiciones del empleo	Los acuerdos contractuales con empleados y contratistas, deben establecer sus responsabilidades y las de la organización en cuanto a la seguridad de la información.	A.7.1.2		PR.DS-5		En algunos de los apartes del manual de manual de funciones, requisitos y competencias, para determinados cargos, se realizan alusiones a temas relacionados a seguridad de la información; lo mismo ocurre en determinadas cláusulas de ciertos contratistas. Para ninguno de los casos existe un lineamiento formalmente establecido al respecto. En el manual de funciones, requisitos y competencias laborales, se establecen los requisitos de estudio, competencias comportamentales y conocimientos básicos esenciales.		40	Establecer las clausulas y responsabilidades de los funcionarios y contratistas en temas de seguridad de la información.

AD.3.2	**Responsable de SI/Líderes de los procesos**	**Durante la ejecución del empleo**	**Asegurar que los funcionarios y contratistas tomen consciencia de sus responsabilidades sobre la seguridad de la información y las cumplan.**	**A.7.1.2**	**Modelo de Madurez Definido**					**33**	
AD.3.2.1	Responsable de SI	Responsabilidades de la dirección	La dirección debe exigir a todos los empleados y contratistas la aplicación de la seguridad de la información de acuerdo con las políticas y procedimientos establecidos por la organización.	A.7.2.1		ID.GV-2	De acuerdo a la NIST los contratistas deben estar coordinados y alineados con los roles y responsabilidades de seguridad de la información. Indague y solicite evidencia del como la dirección se asegura de que los empleados y contratistas: a) Estén debidamente informados sobre sus roles y responsabilidades de seguridad de la información, antes de que se les otorgue el acceso a información o sistemas de información confidenciales. b) Se les suministren las directrices que establecen las expectativas de seguridad de la información de sus roles dentro de la Entidad. c) Logren un nivel de toma de conciencia sobre seguridad de la información pertinente a sus roles y responsabilidades dentro de la organización y estén motivados para cumplir con las políticas. d) Tengan continuamente las habilidades y calificaciones apropiadas y reciban capacitación en forma regular. e) Cuenten con un canal para reporte anónimo de incumplimiento de las políticas o procedimientos de seguridad de la información ("denuncias internas").	Las iniciativas relacionadas con seguridad de la información que se han llevado a cabo hasta ahora han sido particulares, no hay una directiva desde la alta dirección de la alcaldía	En la Alcaldía municipal de Chía se imparten sensibilizaciones sobre la politica de seguridad de la información 3 veces al año	0	Establecer lineamientos para capacitar a los funcionarios y contratistas en temas de seguridad de la información.
AD.3.2.2	Responsable de SI/Líderes de los procesos	Toma de conciencia, educación y formación en la seguridad de la información	Todos los empleados de la Entidad, y en donde sea pertinente, los contratistas, deben recibir la educación y la formación en toma de conciencia apropiada, y actualizaciones regulares sobre las políticas y procedimientos pertinentes para su cargo.	A.7.2.2	Componente planeación Modelo de Madurez Inicial	PR.AT-1 PR.AT-2 PR.AT-3 PR.AT-4 PR.AT-5	Entreviste a los líderes de los procesos y pregúnteles que saben sobre la seguridad de la información, cuales son sus responsabilidades y como aplican la seguridad de la información en su diario trabajo. Pregunte como se asegura que los funcionarios, Directores, Gerentes y contratistas tomen conciencia en seguridad de la información, alineado con las responsabilidades, políticas y procedimientos existentes en la Entidad. Solicite el documento con el plan de comunicación, sensibilización y capacitación, con los respectivos soportes, revisado y aprobado por la alta Dirección. Verifique que se han tenido en cuenta buenas prácticas como: a) Desarrollar campañas, elaborar folletos y boletines. b) Los planes de toma de conciencia y comunicación, de las políticas de seguridad y privacidad de la información, están aprobados y documentados, por la alta Dirección c) Verifique que nuevos empleados y contratistas son objeto de sensibilización en SI. d) Indague cada cuanto o con que criterios se actualizan los programas de toma de conciencia. e) Verifique que en las evidencias se puede establecer los asistentes al programa y el tema impartido. f) Incluir en los temas de toma de conciencia los procedimientos básicos de seguridad de la información (tales como el reporte de incidentes de seguridad de la información) y los controles de línea base (tales como la seguridad de las contraseñas, los controles del software malicioso, y los escritorios limpios). g) De acuerdo a NIST verifique que los funcionarios con roles privilegiados entienden sus responsabilidades y roles. **Para la calificación tenga en cuenta que:** Si Los funcionarios de la Entidad no tienen conciencia de la seguridad y privacidad de la información,	No se han realizado formalmente campañas de concienciación sobre seguridad de la información, ni capacitaciones sobre este tema. Se han llevado a cabo trasferencias de información a usuarios particulares cuando se presenta la oportunidad, por ejemplo, en un servicio de soporte.	No existen programas, capacitaciones o campañas de toma de conciencia sobre la seguridad de la información	20	Diseñar y establecer programas/capacitaciones de buenas prácticas y toma de conciencia en temas de seguridad de la información y política de seguridad y privacidad de la información.
AD.3.2.3	Responsable de SI	Proceso disciplinario	Se debe contar con un proceso disciplinario formal el cual debería ser comunicado, para emprender acciones contra empleados que hayan cometido una violación a la seguridad de la información.	A.7.2.3			Pregunte cual es el proceso disciplinario que se sigue cuando se verifica que ha ocurrido una violación a la seguridad de la información, quien y como se determina la sanción al infractor?	Existe una oficina de control interno disciplinario adscrita a la secretaria general y en el manual de políticas institucionales para el buen uso de tecnologías y seguridad de la información y las comunicaciones para la alcaldía municipal de Chía se hace alusión al incumplimiento de las políticas		80	Medir el cumplimiento de los procesos disciplinarios y establecer mejoras.
AD.3.3	**Responsable de SI**	**Terminación y cambio de empleo**	**Proteger los intereses de la Entidad como parte del proceso de cambio o terminación de empleo.**	**A.7.3**	**Modelo de Madurez Definido**					**80**	
AD.5.1.3	Responsable de SI	Terminación o cambio de responsabilidades de empleo	Las responsabilidades y los deberes de seguridad de la información que permanecen válidos después de la terminación o cambio de contrato se deberían definir, comunicar al empleado o contratista y se deberían hacer cumplir.	A.7.3.1		PR.DS-5 PR.IP-11	Revisar los acuerdos de confidencialidad, verificando que deben acordar que después de terminada la relación laboral o contrato seguirán vigentes por un periodo de tiempo.	Los contratos laborales se pueden terminar de manera unilateral, con declaratoria de insubsistencia, sin motivación para aquellos funcionarios de libre nombramiento y remoción o con un acto administrativo motivado para los de carrera. En el caso de los contratistas, finaliza al finalizar los términos de su contrato.	No se realiza medición o monitoreo del cumplimiento de los acuerdos de confidencialidad.	80	Medir y monitorear los acuerdos de confidencialidad de cada contrato y definir mejoras.
GESTIÓN DE ACTIVOS											
AD.4	**Responsable de SI**	**GESTIÓN DE ACTIVOS**		**A.8**						**47**	
AD.4.1	**Responsable de SI**	**Responsabilidad de los activos**	**Identificar los activos organizacionales y definir las responsabilidades de protección apropiadas.**	**A.8.1**	**Modelo de Madurez Gestionado**					**60**	

AD.4.1.1	Responsable de SI	Inventario de activos	Se deben identificar los activos asociados con la información y las instalaciones de procesamiento de información, y se debe elaborar y mantener un inventario de estos activos.	A.8.1.1	Componente Planificación Modelo de madurez inicial	ID AM-1 ID AM-2 ID.AM-5	Solicite el inventario de activos de información, revisado y aprobado por la alta Dirección y revise: 1) Ultima vez que se actualizó 2) Que señale bajo algún criterio la importancia del activo 3) Que señale el propietario del activo Indague quien(es) el(los) encargado(s) de actualizar y revisar el inventario de activos y cada cuanto se realiza esta revisión. De acuerdo a NIST se deben considerar como activos el personal, dispositivos, sistemas e instalaciones físicas que permiten a la entidad cumplir con su misión y objetivos, dada su importancia y riesgos estratégicos. **Tenga en cuenta para la calificación:** 1) Si Se identifican en forma general los activos de información de la Entidad, están en 40. 2) Si se cuenta con un inventario de activos de información física y lógica de toda la entidad, documentado y firmado por la alta dirección, están en 60. 3) Si se revisa y monitorean periódicamente los activos de información de la entidad, están en 80.	La Alcaldía Municipal de Chía, cuenta con un inventario de activos de información del año 2019, el cual cubrió toda la administración, en el cual se cubren las variables completas de un inventario de activos enfocado a seguridad de la información.		80	Revisar y monitorear periódicamente el inventario de activos de información.
AD.4.1.2	Responsable de SI	Propiedad de los activos	Los activos mantenidos en el inventario deben tener un propietario.	A.8.1.2		ID AM-1 ID AM-2	Solicite el procedimiento para asegurar la asignación oportuna de la propiedad de los activos. Tenga en cuenta que la propiedad se debería asignar cuando los activos se crean o cuando son entregados a la Entidad. De acuerdo a las mejores prácticas el propietario de los activos (individuo o entidad, que es responsable por el activo) tiene las siguientes responsabilidades: a) asegurarse de que los activos están inventariados; b) asegurarse de que los activos están clasificados y protegidos apropiadamente; c) definir y revisar periódicamente las restricciones y clasificaciones de acceso a activos importantes, teniendo en cuenta las políticas de control de acceso aplicables; d) asegurarse del manejo apropiado del activo cuando es eliminado o destruido.	El inventario de activos de información generado en mayo de 2019,cuenta con un propietario, responsable y custodio.	Existe un procedimiento para la realización del inventario de activos de información implementado desde el año 2018.	60	Realizar comunicación del procedimiento, monitoreo y medición.
AD.4.1.3	Responsable de SI	Uso aceptable de los activos	Se deben identificar, documentar e implementar reglas para el uso aceptable de información y de activos asociados con información e instalaciones de procesamiento de información.	A.8.1.3			Pregunte por la política, procedimiento, directriz o lineamiento que defina el uso aceptable de los activos, verifique que es conocida por los empleados y usuarios de partes externas que usan activos de la Entidad o tienen acceso a ellos.	Existen lineamientos en el manual de seguridad de la información, aunque más enfocado a la conservación y operación de los mismos, sin hacer énfasis en la seguridad de la información.	No existe un procedimiento para el uso aceptable de los activos.	20	Diseñar y establecer un procedimiento para el uso aceptable de los activos de información.
AD.4.1.4	Responsable de SI	Devolución de activos	Todos los empleados y usuarios de partes externas deben devolver todos los activos de la organización que se encuentren a su cargo, al terminar su empleo, contrato o acuerdo.	A.8.1.4		PR.IP-11	Revisar las políticas , normas , procedimientos y directrices relativas a los controles de seguridad de la información durante la terminación de la relación laboral por ejemplo, la devolución de los activos de información (equipos, llaves, documentos , datos, sistemas) , las llaves físicas y de cifrado, la eliminación de los derechos de acceso, etc. En caso de que un funcionario o tercero sea el dueño del activo indague como se asegura la transferencia de la información a la Entidad y el borrado seguro de la información de la Entidad. En caso en que un empleado o usuario de una parte externa posea conocimientos que son importantes para las operaciones regulares, esa información se debería documentar y transferir a la Entidad. Durante el período de notificación de la terminación, la Entidad debería controlar el copiado no autorizado de la información pertinente (por ejemplo, la propiedad intelectual) por parte de los empleados o contratistas que han finalizado el empleo.	Existe un acta de entrega de puesto que maneja la oficina de control interno que registra la entrega de información por parte de un funcionario, así como todos los elementos de su puesto y sus equipos de trabajo.	No se realiza medición o monitoreo en cuanto a la entrega completa de los activos de información que tenia a cargo el funcionario.	80	Medir el cumplimiento de este control y actualizar el procedimiento en cuanto al copiado y borrado de información no autorizada.
AD.4.2	**Responsable de SI**	**Clasificación de información**	**Asegurar que la información recibe un nivel apropiado de protección, de acuerdo con su importancia para la Entidad.**	**A.8.2**						**33**	
AD.4.2.1	Responsable de SI	Clasificación de la información	La información se debería clasificar en función de los requisitos legales, valor, criticidad y susceptibilidad a divulgación o a modificación no autorizada.	A.8.2.1	Modelo de Madurez Inicial		Solicite el procedimiento mediante el cual se clasifican los activos de información y evalué: 1) Que las convenciones y criterios de clasificación sean claros y estén documentados 2) Que se defina cada cuanto debe revisarse la clasificación de un activo 3) La clasificación debería valorarse analizando la confidencialidad, integridad y disponibilidad. Solicite muestras de inventarios de activos de información clasificados y evalué que se aplican las políticas y procedimientos de clasificación definidos. Evalué si los procesos seleccionados aplican de manera consistente estas políticas y procedimientos.	Se cuenta con una metodología para la realización de inventarios de activos de información, donde se indica como se debe realizar la clasificación de la información.	Existe un procedimiento para la realización del inventario de activos de información implementado desde el año 2018, en el cual se indica como se debe realizar la clasificación de la información en cuanto a la confidencialidad, integridad y disponibilidad.	80	Realizar monitoreo y medición.
AD.4.2.2	Responsable de SI	Etiquetado de la información		A.8.2.2		PR.DS-5 PR.PT-2	Solicite el procedimiento para el etiquetado de la información y evalúe: 1) Aplica a activos en formatos físicos y electrónicos (etiquetas físicas, metadatos) 2) Que refleje el esquema de clasificación establecido 3) Que las etiquetas se puedan reconocer fácilmente 4) Que los empleados y contratistas conocen el procedimiento de etiquetado Revise en una muestra de activos el correcto etiquetado	Existe un inventario de activos de información, donde se les clasifica en términos de confidencialidad, integridad y disponibilidad, pero no se hace mención al etiquetado, no hay procedimientos y en la oficina de TIC no están aún familiarizado con el término.	No existe etiquetado de los activos de información ni metodología para el mismo.	0	Diseñar metodología para el etiquetado de información tanto física como digital

AD.4.2.3	Responsable de SI	Manejo de activos		A.8.2.3		PR.DS-1 PR.DS-2 PR.DS-3 PR.DS-5 PR.IP-6 PR.PT-2	Solicite los procedimientos para el manejo, procesamiento, almacenamiento y comunicación de información de conformidad con su clasificación. De acuerdo a las mejores prácticas evidencie si se han considerado los siguientes asuntos: a) Restricciones de acceso que soportan los requisitos de protección para cada nivel de clasificación; b) Registro formal de los receptores autorizados de los activos; c) Protección de copias de información temporal o permanente a un nivel coherente con la protección de la información original; d) Almacenamiento de los activos de TI de acuerdo con las especificaciones de los fabricantes; e) Marcado claro de todas las copias de medios para la atención del receptor autorizado. f) De acuerdo a NIST la información almacenada (at rest) y en tránsito debe ser protegida.	Existen unas políticas de uso de hardware y software en el manual de políticas, aunque hace falta incorporar muchos aspectos relacionados con la seguridad de la información No hay un respaldo de la información del Drive asignado a cada funcionario, no hay control de lo que cada funcionario haga en su Drive	No existe un procedimiento para el manejo de los activos.	20	Modificar el manual de políticas en cuanto a seguridad de la información.
AD.4.3	**Responsable de TICs**	**Manejo de medios**	**Evitar la divulgación, la modificación, el retiro o la destrucción no autorizados de la información almacenada en los medios.**	**A.8.3**						**47**	
AD.4.3.1	Responsable de TICs	Gestión de medios removibles		A.8.3.1		PR.DS-3 PR.IP-6 PR.PT-2	Solicite las directrices, guías, lineamientos y procedimientos para la gestión de medios removibles, que consideren: a) Si ya no se requiere, el contenido de cualquier medio reusable que se vaya a retirar de la organización se debe remover de forma que no sea recuperable; b) cuando resulte necesario y práctico, se debe solicitar autorización para retirar los medios de la organización, y se debe llevar un registro de dichos retiros con el fin de mantener un rastro de auditoría; d) si la confidencialidad o integridad de los datos se consideran importantes, se deben usar técnicas criptográficas para proteger los datos que se encuentran en los medios removibles; f) se deben guardar varias copias de los datos valiosos en medios separados, para reducir aún más el riesgo de daño o pérdida casuales de los datos; h) sólo se deben habilitar unidades de medios removibles si hay una razón de valida asociada a los procesos la Entidad para hacerlo; i) En donde hay necesidad de usar medios removibles, se debería hacer seguimiento a la transferencia de información a estos medios (Por ejemplo DLP)	La Alcaldía Municipal de Chía cuenta con el procedimiento de gestión de medios removibles la cual se encuentra en la política de seguridad de la información	Medición y aplicación de la norma en el 100% de los casos.	60	Medición y aplicación de la norma en el 100% de los casos.
AD.4.3.2	Responsable de TICs	Disposición de los medios		A.8.3.2		PR.DS-3 PR.IP-6	Solicite los procedimientos existentes para garantizar que los medios a desechar o donar, no contienen información confidencial que pueda ser consultada y copiada por personas no autorizadas. Verifique si se ha realizado esta actividad y si existen registros de la misma.	La Alcaldía Municipal de Chía cuenta con el procedimiento de borrado seguro el cual se encuentra en la política de seguridad de la información, además todo equipo que se da de baja se hace a través de almacén, donde lo almacenan y lo llevan a un comité de bajas y lo subastan (pueden ir discos duros dañados en el equipo), antes se desarman en la oficina TIC para aprovechar las piezas, los discos buenos se almacenan en la bodega de las TIC.		80	Realizar mejoras y de acuerdo a las mediciones de los borrados seguros
AD.4.3.3	Responsable de TICs	Transferencia de medios físicos		A.8.3.3		PR.DS-3 PR.PT-2	Solicite las directrices definidas para la protección de medios que contienen información durante el transporte. Verifique de acuerdo a las mejores prácticas que se contemple: a) El uso de un transporte o servicios de mensajería confiables. b) Procedimientos para verificar la identificación de los servicios de mensajería. c) Indague y evidencie como es el embalaje el cual debe proteger el contenido contra cualquier daño físico que pudiera presentarse durante el tránsito, y de acuerdo con las especificaciones de los fabricantes, por ejemplo, protección contra cualquier factor ambiental que pueda reducir la eficacia de la restauración del medio, tal como exposición al calor, humedad o campos electromagnéticos; d) Solicite los registros que dejen evidencia del transporte donde se identifique el contenido de los medios, la protección aplicada, al igual que los tiempos de transferencia a los responsables durante el transporte, y el recibo en su destino.			0	
MACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO											
AD.5	**Responsable de la Continuidad**	**ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO**		**A.17**						**10**	
AD.5.1	**Responsable de la Continuidad**	**Continuidad de la seguridad de la información**	**La continuidad de la seguridad de la información debe incluir en los sistemas de gestión de la continuidad del negocio de la Entidad.**	**A.17.1**						**0**	

AD.5.1.1	Responsable de la Continuidad	Planificación de la continuidad de la seguridad de la información		A.17.1.1	Modelo de Madurez Gestionado	ID.BE-5 PR.IP-9	Indagar si la Entidad cuenta con un BCP (Bussines Continuity Plan) o DRP (Disaster Recovery Plan). Determine si aplica para procesos críticos solamente o se han incluido otros procesos o por lo menos se ha reconocido la necesidad de ampliarlo a otros procesos (para determinar el nivel de madurez) Evalúe si se ha incluido en estos planes y procedimientos los requisitos de seguridad de la información. Tenga en cuenta que en ausencia de una planificación formal de continuidad de negocio y recuperación de desastres, la dirección de seguridad de la información debería suponer que los requisitos de seguridad de la información siguen siendo los mismos en situaciones adversas, en comparación con las condiciones operacionales normales. Como alternativa, una organización puede llevar a cabo un análisis de impacto en el negocio de los aspectos de seguridad de la información, para determinar los requisitos de seguridad de la información aplicables a situaciones adversas. De acuerdo a la NIST también se deben tener planes de respuesta a incidentes y recuperación de incidentes. **Tenga en cuenta para la calificación:** 1) Si existen planes de continuidad del negocio que contemplen los procesos críticos de la Entidad que garanticen la continuidad de los mismos. Se documentan tan y protegen adecuadamente los planes de continuidad del negocio de la Entidad, este de estar documentado y firmado, por la alta Dirección**, están en 40.** 2) Si se reconoce la importancia de ampliar los planes de continuidad de del negocio a otros procesos, pero aun no se pueden incluir ni trabajar con ellos, **están en 60.**	No existen planes ni infraestructura para recuperación desastres o continuidad del negocio, por tanto, no se han incorporado la continuidad en la seguridad de la información	No se cuenta con un plan de continuidad del negocio formalizado.	0	Diseñar y establecer un plan de continuidad del negocio.
AD.5.1.2	Responsable de la Continuidad	Implementación de la continuidad de la seguridad de la información	La organización debe establecer, documentar, implementar y mantener procesos, procedimientos y controles para garantizar el nivel necesario de continuidad para la seguridad de la información durante una situación adversa,	A.17.1.2	Modelo de Madurez Definido	ID.BE-5 PR.IP-4 PR.IP-9 PR.IP-9	Verifique si la entidad cuenta con a) Una estructura organizacional adecuada para prepararse, mitigar y responder a un evento contingente, usando personal con la autoridad, experiencia y competencia necesarias. b) Personal formalmente asignado de respuesta a incidentes con la responsabilidad, autoridad y competencia necesarias para manejar un incidente y mantener la seguridad de la información. c) Planes aprobados, procedimientos de respuesta y recuperación documentados, en los que se especifique en detalle como la organización gestionará un evento contingente y mantendrá su seguridad de la información en un límite predeterminado, con base en los objetivos de continuidad de seguridad de la información aprobados por la dirección. Revise si los controles de seguridad de la información que se han implementado continúan operando durante un evento contingente. Si los controles de seguridad no están en capacidad de seguir brindando seguridad a la información, se la Entidad debe establecer, implementar y mantener otros controles para mantener un nivel aceptable de seguridad de la información.	No se realiza porque no existe un plan de la continuidad de la seguridad de la información	No se cuenta con un plan de continuidad del negocio para la seguridad de la información.	0	Diseñar y establecer un plan de continuidad del negocio para la seguridad de la información.
AD.5.1.3	Responsable de la Continuidad	Verificación, revisión y evaluación de la continuidad de la seguridad de la información.		A.17.1.3	Modelo de Madurez Optimizado	PR.IP-4 PR.IP-10	Indague y solicite evidencias de la realización de pruebas de la funcionalidad de los procesos, procedimientos y controles de continuidad de la seguridad de la información, para asegurar que son coherentes con los objetivos de continuidad de la seguridad de la información; Tenga en cuenta que la verificación de los controles de continuidad de la seguridad de la información es diferente de las pruebas y verificación generales de seguridad de la información. Si es posible, es preferible integrar la verificación de los controles de continuidad de negocio de seguridad de la información con las pruebas de recuperación de desastres y de continuidad de negocio de la organización.	No se realiza porque no existe un plan de la continuidad de la seguridad de la información	No se cuenta con un plan de continuidad del negocio para la seguridad de la información.	0	Diseñar y establecer un plan de continuidad del negocio para la seguridad de la información.
AD.5.2	**Responsable de la Continuidad**	**Redundancias**	**Asegurar la disponibilidad de las instalaciones de procesamiento de la información.**	**A.17.2**						**20**	
AD.5.2.1	Responsable de la Continuidad	Disponibilidad de instalaciones de procesamiento de información		A.17.2.1		ID.BE-5	Verifique si la Entidad cuenta con arquitecturas redundantes, ya sea un centro de cómputo principal y otro alterno o componentes redundantes en el único centro de cómputo. Indague como se han definido las necesidades de los procesos para seleccionar que elementos deben ser redundantes. Solicite si aplica las pruebas aplicadas para asegurar que un componente redundante funciona de la forma prevista durante una emergencia o falla.	La Alcaldía no dispone de redundancia ni a nivel de servidores ni a nivel de infraestructura de red, seguridad o almacenamiento. No obstante, el centro de datos cuenta con sistema de extinción de incendio, aire acondicionado y UPS. Se cuenta con alta disponibilidad a nivel de los enlaces de Internet.	No se cuenta con un procedimiento o lineamiento para establecer la redundancia de los activos o elementos.	20	Diseñar y establecer un procedimiento o lineamiento de arquitectura redundantes.
CUMPLIMIENTO											
AD.6	**Responsable de SI/Responsable de TICs/Control Interno**	**CUMPLIMIENTO**		**A.18**						**31**	

AD.6.1	**Responsable de SI**	**Cumplimiento de requisitos legales y contractuales**	**Evitar el incumplimiento de las obligaciones legales, estatutarias, de reglamentación o contractuales relacionadas con seguridad de la información y de cualquier requisito de seguridad.**	**A.18.1**		**ID.GV-3**	**De acuerdo a la NIST: Los requerimientos legales y regulatorios respecto de la ciberseguridad, incluyendo la privacidad y las libertades y obligaciones civiles, son entendidos y gestionados.**			**35**	
AD.6.1.1	Responsable de SI	Identificación de la legislación aplicable y de los requisitos contractuales.		A.18.1.1	**Modelo de Madurez Gestionado Cuantitativamente**		Solicite la relación de requisitos legales, reglamentarios, estatutarios, que le aplican a la Entidad (Normograma). Indague si existe un responsable de identificarlos y se definen los responsables para su cumplimiento.	Existen nomogramas para cada proceso que identifican la legislación aplicable, aunque algunos no están disponibles y en la mayoría no se toma en cuenta la legislación referente a seguridad de la información	Los normogramas establecidos en la alcaldía municipal de Chía no están alineados a la legislación actual referente a seguridad de la información; además no se cuenta con un responsable que monitoree los nomogramas.	40	Actualizar los nomogramas con la legislación actual referente a seguridad de la información solo si se necesita en el proceso. Definir un responsable del cumplimiento y verificación de los nomogramas.
AD.6.1.2	Responsable de TICs	Derechos de propiedad intelectual.		A.18.1.2			1) Solicite los procedimientos para el cumplimiento de los requisitos y contractuales relacionados con los derechos de propiedad intelectual y el uso de productos de software patentados. 2) Verifique si la Entidad cuenta con una política publicada sobre el cumplimiento de derechos de propiedad intelectual que defina el uso legal del software y de productos informáticos. Esta política debe estar orientada no solo al software, si no también a documentos gráficos, libros, etc. 3) Indague como se controla que no se instale software ilegal. 4) Indague si se tiene un inventario de software instalado y se compara con el número de licencias adquiridas para asegurar que no se incumplen los derechos de propiedad intelectual. Tenga en cuenta los controles que deben existir para asegurar que no se exceda ningún número máximo de usuarios permitido dentro de la licencia.	Se evidenciaron contratos firmados por la alcaldía donde, en primera instancia, se establece que los derechos de propiedad intelectual son de su autor y los derechos patrimoniales son de la alcaldía, aunque luego se aclara que los productos intelectuales enmarcados en el contrato, como por ejemplo el código fuente de las aplicaciones, son propiedad patrimonial de la alcaldía. Adicional a esto, la mayoría de la información es generado por la alcaldía, y el material audiovisual usado, así como el software comprado externamente, se adquiere a través de contratos formales que aseguran que se cuente con los derechos a uso y el licenciamiento dimensionado adecuadamente y con los soportes correspondientes, no obstante, no existe un procedimiento formal de verificación de derechos de autor que brinde los lineamientos que asegure que se está dando	No se cuenta con una política de propiedad intelectual, uso legal de software y productos informáticos.	20	Diseñar y establecer una política de propiedad intelectual, donde se especifique el uso de software legal, productos informáticos e inventario de software adquiridos por la alcaldía municipal de Chía.
AD.6.1.3	Responsable de SI	Protección de registros.	Se deben proteger los registros importantes de una organización de pérdida, destrucción y falsificación, en concordancia con los requerimientos estatutarios, reguladores, contractuales y comerciales	A.18.1.3		PR.IP-4	Revise si la Entidad cuenta con tablas de retención documental que especifiquen los registros y el periodo por el cual se deberían retener, además del almacenamiento, manejo y destrucción. Posibles tipos de registros pueden ser registros contables, registros de bases de datos, logs de transacciones, logs de auditoría y procedimientos operacionales, los medios de almacenamiento permitidos pueden ser papel, microfichas, medios magnéticos, medios ópticos etc.	La mayoría de los registros (logs) se almacenan en su punto de origen y no existe para ningún caso lineamientos formales para su protección, que incluyan, entre otros, los detalles de los periodos de retención, su categorización, la pertinencia y disponibilidad en el tiempo del medio de almacenamiento utilizado, las necesidades de cifrado y protección en el tiempo de las llaves criptográficas usadas	No se evidencia un lineamiento para la protección de los registros, cual es su tiempo de almacenamiento y como será su destrucción.	20	Diseñar y establecer un lineamiento para la protección de registros.
AD.6.1.4	Responsable de SI	Protección de los datos y privacidad de la información relacionada con los datos personales.	Se deben asegurar la protección y privacidad de la información personal tal como se requiere en la legislación relevante, las regulaciones y, si fuese aplicable, las cláusulas contractuales.	A.18.1.4		DE.DP-2	Indague sobre las disposiciones que ha definido la Entidad para cumplir con la legislación de privacidad de los datos personales, ley estatutaria 1581 de 2012 y decreto 1377 que reglamenta la ley de 2013. 1) Revise si existe una política para cumplir con la ley 2) Si están definidos los responsables 3) Si se tienen identificados los repositorios de datos personales 4) Si se ha solicitado consentimiento al titular para tratar los datos personales y se guarda registro de este hecho. 5) Si se adoptan las medidas técnicas necesarias para proteger las bases de datos donde reposan estos datos.	Existe una declaración de privacidad y tratamiento de datos establecida y firmada por la alta dirección		60	Realizar mediciones
AD.6.1.5	n/a	Reglamentación de controles criptográficos.		A.18.1.5			n/a			n/a	
AD.6.2	**Control interno**	**Revisiones de seguridad de la información**		**A.18.2**	**Modelo de Madurez Gestionado Cuantitativamente**					**27**	
AD.6.2.1	Control interno	Revisión independiente de la seguridad de la información		A.18.2.1			Investigue la forma como se realizan revisiones independientes (por personas diferentes o no vinculadas a un proceso o área que se revisa), de la conveniencia, la adecuación y la eficacia continuas de la gestionar la seguridad de la información. Para esto solicite: 1) El plan de auditorías del año 2015 2) El resultado de las auditorías del año 2015 3) Las oportunidades de mejora o cambios en la seguridad de la información identificados.	No se realiza una revisión independiente de la seguridad de la información, no existen planes de auditoria o planes para la revisión interna o externa de la operación y el cumplimiento de objetivos de seguridad de la información.	La alcaldía municipal de chía no cuenta con un SGSI, planes de auditoria de la seguridad de información, planes de seguimiento o cumplimiento de objetivos de seguridad de información.	0	Establecer auditorias de seguridad de la información cuando se defina y se adopte un sistema de gestión de seguridad de la información.
AD.6.2.2	Control interno	Cumplimiento con las políticas y normas de seguridad.	Asegurar el cumplimiento de los sistemas con las políticas y estándares de seguridad organizacional.	A.18.2.2		PR.IP-12	1) Verifique si los gerentes aseguran que todos los procedimientos de seguridad dentro de su área de responsabilidad se llevan a cabo correctamente para lograr el cumplimiento de las políticas y estándares de seguridad. 2) Verifique la revisión periódica del cumplimiento del centro de cómputo con las políticas y normas de seguridad establecidas. 3) Verifique si los sistemas de información son revisados regularmente para asegurar el cumplimiento de las normas de seguridad de la información	En el actual manual de políticas se especifican las sanciones por el incumplimiento de las mismas, no obstante, no hay registro de sanciones por este motivo y no se cuenta con métricas e indicadores al respecto.	No se realizan mediciones y/o monitoreo para el cumplimiento de las sanciones.	60	Realizar mediciones del cumplimiento de las sanciones establecidas en el manual de políticas.

AD.6.2.3	Responsable de SI	Revisión de cumplimiento técnico.	Los sistemas de información deben chequearse regularmente para el cumplimiento con los estándares de implementación de la seguridad.	A.18.2.3		ID.RA-1	Verifique si se realizan evaluaciones de seguridad técnicas por o bajo la supervisión de personal autorizado, apoyado en herramientas automáticas o con revisiones manuales realizadas por especialistas. Solicite evidencia de las últimas pruebas realizadas, sus resultados y seguimiento para asegurar que las brechas de seguridad fueron solucionadas.	Existe un plan de mantenimiento preventivo periódico durante el cual se revisan algunos aspectos de seguridad informática, por lo demás, no se hacen revisiones tanto en equipos como en aplicaciones para determinar el cumplimiento de las políticas y normas de seguridad de la información de la alcaldía	No existe un lineamiento para pruebas de seguridad de la información en los equipos y aplicaciones.	20	Diseñar y establecer un lineamiento para pruebas técnicas de seguridad de la información.
NES CON LOS PROVEEDORES											
AD.7	**Responsable de compras y adquisiciones**	**RELACIONES CON LOS PROVEEDORES**		**A.15**						**10**	
AD.7.1	Responsable de compras y adquisiciones	Seguridad de la información en las relaciones con los proveedores	Asegurar la protección de los activos de la entidad que sean accesibles para los proveedores	A.15.1	Modelo de Madurez Definido		1) Solicite la política de seguridad de la información para las relaciones con los proveedores, que indique los requisitos de SI para mitigar los riesgos asociados con el acceso de proveedores a los activos de la organización, esta política debe reflejarse en los acuerdos con los proveedores que deben estar documentados. 2) Verifique en la muestra de proveedores con acceso a los activos de información (no necesariamente son proveedores de tecnología de la información, por ejemplo pueden ser proveedores que tengan por ejemplo un proceso de nomina en outsourcing), se hayan suscrito acuerdos (ANS) formales donde se establezcan y acuerden todos los requisitos de seguridad de la información pertinentes con cada proveedor. 3) Verifique para los proveedores si se tiene en cuenta los riesgos de SI asociados a la cadena de suministro, por ejemplo para los proveedores en la nube es muy común que se apoyen en otros proveedores para proporcionar las instalaciones y se deben manejar los riesgos asociados a este tercero con el cual la entidad no tiene una relación comercial directa. Solicite que le indiquen como identifican para cada proveedor su cadena de suministro y obtenga evidencia de este hecho.	No existe en la Alcaldía una política de seguridad de la información para las relaciones con proveedores, aunque existen alusiones concretas en algunos contratos.	No existe una política de seguridad de la información que contenga la relación con los proveedores y cuáles son sus respectivos deberes y acuerdos en cuanto a la seguridad de la información.	0	Definir en la política de seguridad de la información la relación con los proveedores, donde se indique los deberes y los acuerdos que deben tener con la alcaldía municipal de Chía.
AD.7.2	Responsable de compras y adquisiciones	Gestión de la prestación de servicios de proveedores	Mantener el nivel acordado de seguridad de la información y de prestación del servicio en línea con los acuerdos con los proveedores	A.15.2	Modelo de Madurez Definido		1) Indague y solicite evidencia en una muestra de proveedores seleccionada, como la entidad hace seguimiento, revisa y audita con regularidad de acuerdo a la política la prestación de servicios de los proveedores y el cumplimiento de los compromisos respecto a la seguridad de la información. 2) Indague y evidencie como se gestionan los cambios en el suministro de servicios por parte de los proveedores, incluido el mantenimiento y la mejora de las políticas, procedimientos y controles de seguridad de la información existentes , teniendo en cuenta la criticidad de la información, sistemas y procesos del negocio involucrados, los incidentes de seguridad de la información y la revaloración de los riesgos. 2)	Los contratos con proveedores incorporan una cláusula de confidencialidad donde especifica las obligaciones generales del contratista frente a la protección de la confidencialidad de la información de la Alcaldía. Más allá de dicha cláusula, no se personalizan y/o concretan más acuerdos y requerimientos de seguridad de la información con los proveedores; no existe un lineamiento o una política de los aspectos que las áreas contratantes deben tener en cuenta	no existe una política de seguridad de la información que contenga la relación con los proveedores y cuáles son sus respectivos deberes y acuerdos en cuanto a la seguridad de la información.	20	Definir en la política de seguridad de la información la relación con los proveedores, donde se indique los deberes y los acuerdos que deben tener con la alcaldía municipal de Chía.

INSTRUMENTO DE IDENTIFICACIÓN DE LA LINEA BASE DE SEGURIDAD
HOJA LEVANTAMIENTO DE INFORMACIÓN

Alcaldía Municipal de Chía

RESPONSABLE / AREA	TEMA	FUNCIONARIO	Funciones de la dependencia
Control interno	Revisiones de seguridad de la información	Jefe Oficina de Control Interno	Realizar el seguimiento a la implementación de la politica de la seguridad de la información
	Revisión independiente de la seguridad de la información		
	Cumplimiento con las políticas y normas de seguridad.		
	CUMPLIMIENTO		
	Auditoría Interna Plan		
	Auditoría Interna Ejecución y Subsanación de hallazgos y brechas		
Gestión humana	Selección e investigación de antecedentes	Directora de Función Pública	
	Términos y condiciones del empleo		
PROCESOS ESTRATÉGICOS			
Líder de Proceso: Director(a) Departamento Administrativo de Planeación.	**PROCESO 1:**	**PLANIFICACIÓN ESTRATÉGICA**	
	DESCRIPCIÓN DEL PROCESO	Definir estrategias y líneas de accion que den rumbo y destino a la Alcaldía, con el fin de cumplir con los planes, programas y proyectos, así como con la plataforma estratégica adoptada por la entidad. Asimismo, busca proporcionar información estadística y geográfica municipal para la toma de decisiones y la formulación de políticas, programas, planes y proyectos que requieran las dependencias y entidades del Municipio.	
Líder de Proceso: Secretario(a) General	**PROCESO 2**	**Sistema Integral de Gestión**	
	DESCRIPCIÓN DEL PROCESO	Mantener el funcionamiento y operatividad del sistema de gestión de calidad para mejorar continuamente los procesos y contribuir al cumplimiento de competencias, políticas y objetivos Municipales.	
Líder de Proceso Oficina de TIC	**PROCESO 3**	**Tecnologías de la Información y Comunicaciones**	
	DESCRIPCIÓN DEL PROCESO	Dotar a la Alcaldía de tecnología de punta para la información y la comunicación en todos los procesos, con el propósito de mejorar la gestión y obtener resultados en menor tiempo y con mayor calidad. Responder y administrar el sistema integrado de información que requiere la Alcaldía para el desarrollo eficiente de todos sus procesos. Garantizar que cada uno de los integrantes o personal asignado a los procesos asimile la tecnología, la utilice adecuadamente para desarrollar sus actividades y compromisos laborales. Propender por la creación de una cultura y conciencia para aplicar, utilizar, adaptar, aprovechar y darle adecuado y buen uso a las tecnologías. Asimismo, lograr más y mejores recursos tecnológicos y de conectividad para la ciudadanía del Municipio de Chía.	
Líder de Proceso Jefe Oficina de Participación Ciudadana	**PROCESO 4**	**Participación Ciudadana**	
	DESCRIPCIÓN DEL PROCESO	Formular e implementar las políticas, planes, programas, proyectos de formación y generación de cultura política para la participación democrática ciudadana que conduzca a la cualificación y el surgimiento de liderazgos, así como los procesos de presupuesto participativo que propendan por la adecuada distribución de los recursos públicos.	
Líder de Proceso Jefe Oficina Asesora de Comunicación y Prensa	**PROCESO 5**	**Comunicación Estratégica**	
	DESCRIPCIÓN DEL PROCESO	Formular y desarrollar una estrategia que dimensione los diferentes componentes del proceso comunicativo y supere el alcance de socialización y de mantenimiento de una imagen institucional favorable de la entidad en la opinión pública.	
PROCESOS MISIONALES			
Líder de Proceso Secretario(a) de Salud	**PROCESO 1:**	**Gestión en Salud**	
	DESCRIPCIÓN DEL PROCESO	Dirigir y coordinar el sector salud y el sistema general de seguridad social en salud mediante el aseguramiento, la prestación de servicios de salud, la gestión de la salud pública y la vigilancia y control, para mejorar las condiciones de salud de la población del Municipio de Chía.	
Líder de Proceso Secretario(a) de Educación	**PROCESO 2**	**Gestiòn Educativa**	
	DESCRIPCIÓN DEL PROCESO	Garantizar que la prestación del servicio educativo se realice con la calidad, pertinencia y cobertura establecidas mediante la dirección, administración evaluación y control del sistema educativo municipal para contribuir al mejoramiento de las condiciones de vida de la población en condiciones de equidad y género establecidas en el plan de desarrollo.	
Líder de Proceso Secretario(a) de Gobierno	**PROCESO 3**	**Gestión de Gobierno y Seguridad**	
	DESCRIPCIÓN DEL PROCESO	Mejorar los niveles de seguridad, participación y convivencia ciudadana, y el control del espacio público, mediante estrategias y acciones de promoción de la cultura de la legalidad, control, defensa, protección, recuperación y prevención para el fortalecimiento institucional, con el fin de garantizar las libertades civiles, la convivencia y el disfrute de la comunidad.	
Líder de Proceso Director(a) de Urbanismo	**PROCESO 4**	**Gestión Urbanística**	
	DESCRIPCIÓN DEL PROCESO	Efectuar las actividades relacionadas con la expedición de licencias urbanísticas y demás actuaciones competentes, de manera ágil, confiable y efectiva.	
Líder de Proceso Secretario(a) de Obras Públicas	**PROCESO 5**	**Gestión de Obra Pública**	
	DESCRIPCIÓN DEL PROCESO	Diseñar, construir y mantener la obra pública a cargo del Municipio de Chía de acuerdo con las normas y especificaciones técnicas, para contribuir con la prestación de los servicios y con la satisfacción de las necesidades de la comunidad.	
Líder de Proceso Secretario(a) de Movilidad	**PROCESO 6**	**Gestión de Movilidad**	
	DESCRIPCIÓN DEL PROCESO	Garantizar la circulación de los diferentes actores Mediante la aplicación de mecanismos de planeación y control de tránsito y transporte que permitan la movilidad de forma cómoda, segura, ágil y oportuna en el Municipio de Chía.	
Líder de Proceso Director(a) de Derechos y Resolución de Conflictos	**PROCESO 7**	**Gestión de Derechos y Resolución de Conflictos**	
	DESCRIPCIÓN DEL PROCESO	Promover la protección y recuperación de los derechos de los individuos, así adelantar e implementar estrategias y mecanismos de resolución de conflictos.	
Líder de Proceso Secretario(a) de Desarrollo Social	**PROCESO 8**	**Gestión Social para el Desarrollo**	
	DESCRIPCIÓN DEL PROCESO	Promover el desarrollo con equidad de la ciudadanía, mediante estrategias de bienestar y cultura para contribuir al mejoramiento de la calidad de vida de los habitantes del Municipio.	
Líder de Proceso Jefe Oficina Centro de Atención al Ciudadano	**PROCESO 9**	**Gestión de Atención a la Ciudadanía**	
	DESCRIPCIÓN DEL PROCESO	Garantizar la calidad de la atención, la oportunidad y capacidad de respuesta a la ciudadanía mediante la definición e implementación de políticas de servicio, protocolos de atención, la estructuración de canales de atención y un modelo de servicio a la comunidad para satisfacer de manera efectiva la demanda de servicios y trámites en el municipio.	
Líder de Proceso Secretario(a) para el Desarrollo Económico	**PROCESO 10**	**Gestión de Desarrollo Económico**	
	DESCRIPCIÓN DEL PROCESO	Promover el desarrollo económico, turístico y agropecuario del municipio de Chía mediante la implementación de estrategias, planes, programas, productos y proyectos que mejoren la competitividad y revierta sobre los sectores del Municipio ingresos en su desarrollo humano.	
Líder de Proceso Secretario de Gobierno	**PROCESO 11**	**Gestión del Riesgo y Atención de Desastres**	
	DESCRIPCIÓN DEL PROCESO	Garantizar la protección de personas y colectividades de los efectos negativos de desastres de origen natural o antrópico, mediante la generación de políticas, estrategias y normas que promuevan capacidades orientadas a identificar, analizar, prevenir y mitigar riesgos para enfrentar y manejar eventos de desastre.	
Líder de Proceso Jefe Oficina Centro de Atención al Ciudadano	**PROCESO 12**	**Gestión del Medio Ambiente**	
	DESCRIPCIÓN DEL PROCESO	Garantizar la calidad de la atención, la oportunidad y capacidad de respuesta a la ciudadanía mediante la definición e implementación de políticas de servicio, protocolos de atención, la estructuración de canales de atención y un modelo de servicio a la comunidad para satisfacer de manera efectiva la demanda de servicios y trámites en el municipio.	
PROCESOS DE APOYO			

Líder de Proceso **Director(a) de Servicios Administrativos**	**PROCESO 1**	**Gestión de Servicios Administrativos**
	DESCRIPCIÓN DEL PROCESO	Administrar y mantener adecuadamente los recursos físicos y optimizar la calidad y la oportunidad en la adquisición y suministro de bienes, mediante la ejecución del plan de compras de funcionamiento, con el fin de mantener la eficiencia en la prestación de servicios de apoyo a la gestión de la Alcaldía.
Líder de Proceso **Director(a) de Contratación**	**PROCESO 2**	**Gestión de Contratación**
	DESCRIPCIÓN DEL PROCESO	Organizar, coordinar, controlar y ejecutar los procesos, procedimientos y actividades propias de las etapas precontractuales, contractuales y post contractuales que se adelante en la Alcaldía para la adquisición de los bienes y servicios requeridos para el desarrollo y cumplimiento de la misión y operación de la entidad, a través de la celebración de contratos y/o convenios, acorde con el procedimiento previsto en la Ley 80 de 1993, Ley 1150 de 2007 y sus decretos reglamentarios y hacer el seguimiento a la ejecución de los mismos.
Líder de Proceso **Director(a) de Función Pública**	**PROCESO 3**	**Gestión del Talento Humano**
	DESCRIPCIÓN DEL PROCESO	Administrar de manera eficiente el recurso humano como base fundamental del desarrollo y posicionamiento de la Alcaldía, desde el momento de su ingreso a la entidad, pasando por su permanencia en la misma, hasta su retiro, desarrollando estrategias administrativas y operativas que permitan el adecuado y eficiente manejo.
Líder de Proceso **Director(a) de Servicios Administrativos**	**PROCESO 4**	**Gestión Documental**
	DESCRIPCIÓN DEL PROCESO	Garantizar que los documentos recibidos, tramitados y enviados en el municipio se conserven adecuadamente mediante las actividades de correspondencia y gestión de archivo para asegurar la eficacia y eficiencia en la gestión de correspondencia y archivo.
Líder de Proceso **Jefe Oficina Asesora Jurídica**	**PROCESO 5**	**Gestión Jurídica**
	DESCRIPCIÓN DEL PROCESO	Garantizar el apoyo jurídico necesario para la adecuada operación, que incluye atención de solicitudes, requerimientos, tutelas, demandas, así como emisión de conceptos jurídicos necesarios para apoyar trámites y procesos misionales, estratégicos, habilitadores y de evaluación y control de la Alcaldía y en general del talento humano, en ejercicio de sus funciones
Líder de Proceso **Secretario(a) de Hacienda**	**PROCESO 6**	**Gestión Financiera**
	DESCRIPCIÓN DEL PROCESO	Gestionar, controlar y hacer seguimiento a la ejecución de los recursos apropiados a la Alcaldía y a los fondos cuenta, o transferidos a organismos de cooperación a través de la suscripción de convenios, que permita conocer en forma oportuna y veraz el nivel de ejecución y el cumplimiento de las tareas encomendadas, mediante el registro de las operaciones y su presentación a través de informes intermedios y emisión de estados financieros. Vigilancia y control de los recursos. Ejercicio responsable de registros contables y presentación de estados financieros y balances; así como de tesorería para atender pagos de compromisos institucionales.
Líder de Proceso **Director(a) Banco de Maquinaria**	**PROCESO 7**	**Gestión de Maquinaria y Equipo**
	DESCRIPCIÓN DEL PROCESO	Garantizar las condiciones de funcionamiento de la maquinaria y equipo pesado a cargo del municipio, mediante programas de mantenimiento preventivo y correctivo, para asegurar su disponibilidad y uso.
Líder de Proceso **Jefe Oficina de Control Disciplinario**	**PROCESO 8**	**Gestión Disciplinaria**
	DESCRIPCIÓN DEL PROCESO	Investigar la conducta de los servidores y exservidores públicos de la Alcaldía que incurran en transgresión a las normas disciplinarias.
PROCESOS DE EVALUACIÓN Y MEJORA		
Líder de Proceso **Jefe Oficina de Control Interno**	**PROCESO 1**	**Evaluación Independiente**
	DESCRIPCIÓN DEL PROCESO	A través de instrumentos y sistemas confiables y debidamente validados, hacer seguimiento, control y evaluación de la gestión de las dependencias de la Alcaldía, para tomar correctivos y proponer planes de mejoramiento orientados a fortalecer la capacidad de las áreas y obtener de ellas productos y servicios de mejor calidad. Evaluar la planeación, ejecución y control en la gestión de los procesos, programas, planes y proyectos de la entidad, desde la perspectiva del evaluador independiente. Su finalidad es generar información, recomendaciones, alertas y aprendizajes dirigidos a lograr la eficacia y la eficiencia en la toma de decisiones oportunas que contribuyan al mejoramiento de la gestión.
Responsable de compras y adquisiciones	RELACIONES CON LOS PROVEEDORES	Lider de cada proceso
	Seguridad de la información en las relaciones con los proveedores	
	Gestión de la prestación de servicios de proveedores	
Responsable de la continuidad	ASPECTOS DE SEGURIDAD DE LA	Ingeniero Jorge Ivan Ortiz Ardila Jefe oficina TIC.
	Continuidad de la seguridad de la información	
	Planificación de la continuidad de la seguridad de la información	
	Implementación de la continuidad de la	
	Verificación, revisión y evaluación de la continuidad de la seguridad de la información.	
	Redundancias	
	Disponibilidad de instalaciones de	
Responsable de la seguridad física	SEGURIDAD FÍSICA Y DEL ENTORNO	Ingeniero Jorge Ivan Ortiz Ardila Jefe oficina TIC.
	ÁREAS SEGURAS	
	Perímetro de seguridad física	
	Áreas de despacho y carga	
	Visita al Centro de Computo	
Responsable de SI	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	Ingeniero Jorge Ivan Ortiz Ardila Jefe oficina TIC.
	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	
	SEGURIDAD DE LOS RECURSOS HUMANOS	
	Antes de asumir el empleo	
	Durante la ejecución del empleo	
	Terminación y cambio de empleo	
	GESTIÓN DE ACTIVOS	
	CUMPLIMIENTO	
	Cumplimiento de requisitos legales y contractuales	
	CONTROL DE ACCESO	
	CRIPTOGRAFÍA	
	SEGURIDAD FÍSICA Y DEL ENTORNO	
	SEGURIDAD DE LAS OPERACIONES	
	PROCEDIMIENTOS OPERACIONALES Y RESPONSABILIDADES	
	Procedimientos de operación documentados	
	Gestión de cambios	
	Gestión de capacidad	
	Separación de los ambientes de desarrollo, pruebas y operación	
	PROTECCIÓN CONTRA CÓDIGOS MALICIOSOS	
	COPIAS DE RESPALDO	
	REGISTRO Y SEGUIMIENTO	
	Registro de eventos	
	Protección de la información de registro	
	Registros del administrador y del operador	
	Sincronización de relojes	
	CONTROL DE SOFTWARE OPERACIONAL	
	Instalación de software en sistemas operativos	
	GESTIÓN DE LA VULNERABILIDAD TÉCNICA	
	Gestión de las vulnerabilidades técnicas	
	Restricciones sobre la instalación de software	
	CONSIDERACIONES SOBRE AUDITORÍAS DE SISTEMAS DE INFORMACIÓN	
	Controles sobre auditorías de sistemas de información	
	SEGURIDAD DE LAS COMUNICACIONES	
	GESTIÓN DE LA SEGURIDAD DE LAS REDES	
	TRANSFERENCIA DE INFORMACIÓN	
	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	
	REQUISITOS DE SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN	
	SEGURIDAD EN LOS PROCESOS DE DESARROLLO Y DE SOPORTE	
	DATOS DE PRUEBA	
	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	

	Alcande MSPI (Modelo de Seguridad y Privacidad de la Información)	
	Identificación y valoración de riesgos	
	Tratamiento de riesgos de seguridad de la información	
	Toma de conciencia, educación y formación en la seguridad de la información	
	Planificación y control operacional	
	Implementación del plan de tratamiento de riesgos	
	Indicadores de gestión del MSPI	
	Plan de seguimiento, evaluación y análisis del MSPI	
	Evaluación del plan de tratamiento de riesgos	
	Plan de seguimiento, evaluación y análisis del MSPI	
	Tratamiento de temas de seguridad y privacidad de la información en los comités del modelo integrado de gestión, o en los comités directivos interdisciplinarios de la Entidad	
	Con base en el inventario de activos de información clasificado, se establece la caracterización de cada uno de los sistemas de información.	
	La entidad conoce su papel dentro del estado Colombiano, identifica y comunica a las partes interesadas la infraestructura crítica.	
	Las prioridades relacionadas con la misión, objetivos y actividades de la Entidad son establecidas y comunicadas.	
	La gestión de riesgos tiene en cuenta los riesgos de ciberseguridad	
	Detección de actividades anómalas	
	Respuesta a incidentes de ciberseguridad, planes de recuperación y restauración	
Responsable de TICs	Teletrabajo	Ingeniero Jorge Ivan Ortiz Ardila Jefe oficina TIC.
	Manejo de medios	
	Derechos de propiedad intelectual.	
	CONTROL DE ACCESO	
	SEGURIDAD DE LAS OPERACIONES	
	PROCEDIMIENTOS OPERACIONALES Y RESPONSABILIDADES	
	COPIAS DE RESPALDO	
	CONTROL DE SOFTWARE OPERACIONAL	
	CONSIDERACIONES SOBRE AUDITORÍAS DE SISTEMAS DE INFORMACIÓN	
	SEGURIDAD DE LAS COMUNICACIONES	
	GESTIÓN DE LA SEGURIDAD DE LAS REDES	
	TRANSFERENCIA DE INFORMACIÓN	
	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	
	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	
	Plan y Estrategia de transisicón de IPv4 a IPv6	
	Implementación del plan de estrategia de transición de IPv4 a IPv6	
	Redundancias	
Calidad	Procedimientos de control documental del MSPI	Ingeniero Jorge Ivan Ortiz Ardila Jefe oficina TIC.