Pasantía – Alcaldía de Chaparral

Alejandro Garzón Cuellar

Director:

Juan Manuel Aldana Porras

Universidad Nacional Abierta Y A Distancia – UNAD-

Escuela De Ciencias Básicas, Tecnología E Ingeniería –ECBTI

Programa de Ingeniería Sistemas

Ibagué Tolima, 2022

Tabla de contenido

Lista de tablas

Lista de figuras

Introducción

Desde el 2018 se ha implementado la política de Gobierno Digital que aplica a entidades que hacen parte de la administración pública esta política tiene como objetivo fortalecer la gestión, los servicios existentes y los procesos de manera continua y transversal a las otras dependencias de la alcaldía.

El desarrollo de este proyecto es una pasantía, en la alcaldía de Chaparral – Tolima, en el área de informática a través de las siguientes actividades de apoyo: en primer lugar, se realizó un diagnóstico inicial sobre los parámetros de la seguridad informática; lo que permitió el establecimiento de estrategias de alcance para generar un proceso de concientización y planificación del desarrollo en pro de mitigar y subsanar los hallazgos de riesgo evidenciados. En segundo lugar, se efectuó la socialización sobre política de seguridad digital, gestión de riesgos de seguridad informática, diagnóstico y planificación del desarrollo, plan de tratamiento de riesgos de seguridad de la información, mantenimiento a computadores y disminución de amenazas, plan de acción de tratamientos de riesgos de seguridad y privacidad de la información.

Este documento tiene como propósito el mejoramiento en seguridad informática de la alcaldía de Chaparral, teniendo en cuenta, los requerimientos del Ministerio de las Tecnologías de la información y las Comunicaciones y la evaluación periódica departamental. De acuerdo a lo anterior, la alcaldía de chaparral se encuentra en transición al gobierno digital, razón por la que se describirán las actividades de apoyo y seguimiento al área TIC.

Inducción general

El tema de fortalecer la implementación de las estrategias programadas de las políticas públicas de Gobierno Digital y de Seguridad Digital en la Alcaldía municipal de Chaparral Tolima, las cuales se adoptaron en el Plan de Desarrollo Municipal “Más Progreso para Todos” y el Plan Estratégico de las Tecnologías de la Información PETI para la vigencia 2020 – 2023 (Alcaldia de Chaparral, 2021).

La administración municipal requiere el desarrollo de las siguientes actividades por parte de la pasantía, consistentes en:

- Análisis de componentes de la FURAG en la política de Seguridad Digital
- Contar con información permanente, actualizada
- Reducir y simplificar los reportes e informes
- Medir los avances y resultados
- Generar mecanismos de autoevaluación
- Apoyar, asesorar y retroalimentar a las entidades de la Rama Ejecutiva.

A continuación, se detalla cada una de las anteriores actividades para el análisis de diversos aspectos durante el acompañamiento y apoyo para el pasante, siendo:

- **Análisis de componentes del FURAG en la política de Seguridad Digital**

En esta actividad se analizarán diversos aspectos incluidos en la evaluación del FURAG especialmente aquellas que presentan debilidad o carencia de sus componentes, para tener en cuenta en la próxima versión, para su fortalecimiento.

- **Contar con información permanente, actualizada**

Se espera apoyar con el diseño y actualización de la información relacionada con SPI

- **Reducir y simplificar los reportes e informes**

Apoyar con la gestión para la reducción y simplificación de los reportes e informes.

- **Medir los avances y resultados**

Contribuir y apoyar con la medición de los avances y resultados.

- **Generar mecanismos de autoevaluación**

Actualizar la matriz de autodiagnóstico de SPI para verificar los alcances de cumplimiento de la política de Seguridad Digital

- **Apoyar, asesorar y retroalimentar a las entidades de la Rama Ejecutiva**

Se espera contribuir con el apoyo, asesoría y retroalimentación a las entidades de la Rama Ejecutiva

Al terminar este proyecto, se espera que la Alcaldía de Chaparral obtenga un mayor puntaje en los mecanismos de evaluación implementados por las Entidades de control como es el índice de Transparencia y Acceso a la información pública ITA y la evaluación del FURAG que se aplican anualmente a todas las entidades del orden territorial, permitiendo medir diversos aspectos como es el posicionamiento institucional, analizar el entorno participativo, entre otros importantes aspectos. De igual manera, con la ejecución del plan de acción se busca garantizar el aumento de la confianza de la ciudadanía en las entidades públicas, así como se desea tener un mayor acercamiento a la comunidad y que ésta participe activamente en la creación y modificación de las políticas públicas, así mismo se espera el fortalecimiento en cuanto al

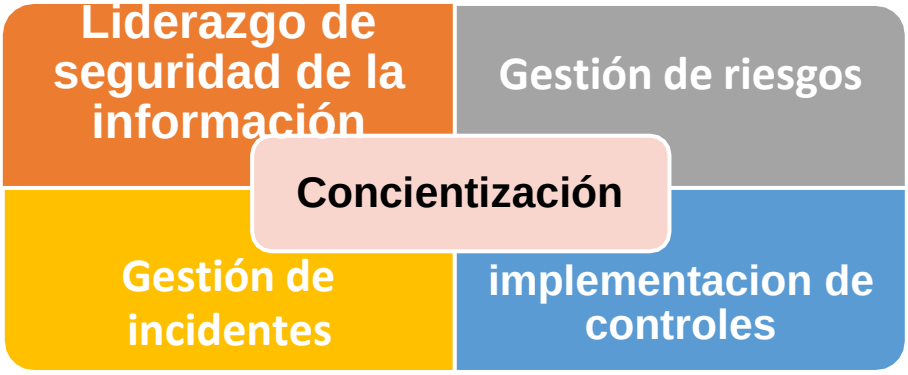
servicio a los ciudadanos, reconociendo cuales servicios se pueden prestar en línea y fomentando su uso, todo esto de acuerdo a las necesidades de la comunidad y su derecho al ejercicio de participación ciudadana.

Estrategias

Fortalecer la integridad, confidencialidad y disponibilidad de los activos de información de la Entidad, para reducir los riesgos a los que está expuesta la organización hasta niveles aceptables, a partir de la gestión de implementación de las estrategias de seguridad definidas.

Figura 1

Concientización de la seguridad informática



Fuente: el autor.

De la imagen anterior se puede decir que, la gestión de seguridad de la información es el proceso de identificar, comprender, evaluar y mitigar los riesgos –y sus vulnerabilidades subyacentes y el impacto en la información, los sistemas de información y las organizaciones que dependen de la información para sus operaciones. Además de identificar los riesgos y las medidas de mitigación, el método y el proceso de gestión del riesgo (Ministerio de Tecnológia de la Información y las Comunicaciones (MinTic), 2021).

Descripción de las estrategias

Liderazgo de seguridad de la información	Asegurar que se establezca el Modelo de Seguridad y Privacidad de la Información (MSPI) a través de la aprobación de las políticas general y demás lineamientos que se definan buscando proteger la confidencialidad, integridad y disponibilidad de la información teniendo como pilar fundamental el compromiso de la alta dirección y de los jefes de las diferentes dependencias de la Entidad.
Gestión de riesgos	Determinar los riesgos de seguridad de la información a través de la planificación y valoración que se defina buscando prevenir o reducir los efectos indeseados tendiendo como pilar fundamental la implementación de controles de seguridad para el tratamiento de los riesgos.
Concientización	Fortalecer la construcción de la cultura organizacional con base en la seguridad de la

	información para que convierta en un hábito, promoviendo las políticas, procedimientos, normas, buenas prácticas y demás lineamientos, la transferencia de conocimiento, la asignación y divulgación de responsabilidades de todo el personal de la entidad en seguridad y privacidad de la información.
Implementación de controles	Planificar e implementar las acciones necesarias para lograr los objetivos de seguridad y privacidad de la información y mantener la confianza en la ejecución de los procesos de la Entidad.
Gestión de incidentes	Garantizar una administración de incidentes de seguridad de la información con base a un enfoque de integración, análisis, comunicación de los eventos e incidentes y las debilidades de seguridad en pro de conocerlos y resolverlos para minimizar el impacto negativo de estos en la Entidad.

Videoconferencias de SPI

Figura 2

Videoconferencia de SPI

Fuente. **Ministerio de Tecnológia de la Información y las Comunicaciones (MinTic).**

Se cumple con la participación otorgadas por las MITIC que hace parte de la implementación de controles, donde se habla sobre la identificación de activos que es lo que podemos ver en la imagen a la que se referencia una de las clasificaciones a la que se podría definirse en la entidad (Alcaldía de chaparral), basa las características particularidades de la información, en el cual se hacía cada 3 días por semana de pendiendo de los horarios otorgados por la misma entidad encargada, con el fin de entregar información para poder mitigar los problemas presentados por la alcaldía y así dar una posible solución a estos.

Inducción específica

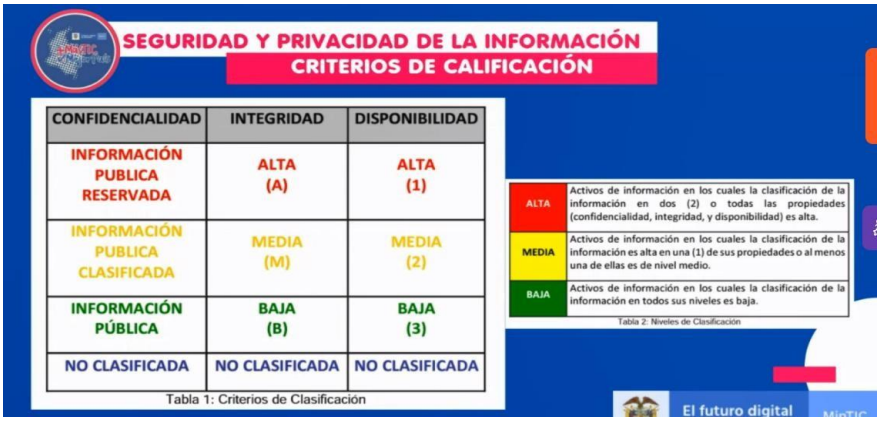
Políticas de seguridad física y del entorno

- La alcaldía municipal de Chaparral adoptará las medidas para el control de acceso físico a las instalaciones y áreas seguras con el fin de mitigar los riesgos asociados a la afectación de la confidencialidad, disponibilidad e integridad de la información.
- La alcaldía municipal de Chaparral definirá áreas seguras y los controles de acceso físico correspondientes para la protección de la información que allí se resguarda.
- Todas las personas que ingresen a las instalaciones de Alcaldía municipal de Chaparral deben cumplir con los lineamientos establecidos para el control de acceso físico sin excepción

Políticas de seguridad en las operaciones

Figura 3

Políticas de seguridad en las operaciones



Con el fin de asegurar las operaciones realizadas en los recursos tecnológicos que soportan la operación del negocio. Alcaldía municipal de Chaparral planea, gestiona, respalda y monitorea la

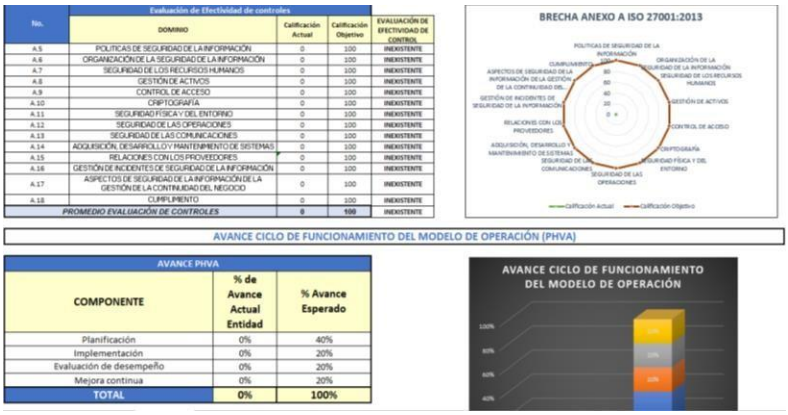
infraestructura tecnológica siguiendo los lineamientos establecidos en los procedimientos establecidos para el SGSI.

Se realizará el levantamiento información donde se identifiquen los procesos que se manejan en el área de operaciones para que posteriormente se pueda hacer el análisis y la evaluación de riesgos, teniendo en cuenta el impacto de cada uno de estos y las consecuencias que podría generar, con el objetivo de poder definir la manera en que se debe tratar cada uno.

Políticas de adquisición, desarrollo y mantenimiento de sistemas

Figura 4

Videoconferencia de SPI



No.	Evaluación de Efectividad de controles DOMINIO	Calificación Actual	Calificación Objetivo	EVALUACIÓN DE EFECTIVIDAD DE CONTROL
A.5	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	0	100	INEXISTENTE
A.6	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	0	100	INEXISTENTE
A.7	SEGURIDAD DE LOS RECURSOS HUMANOS	0	100	INEXISTENTE
A.8	GESTIÓN DE ACTIVOS	0	100	INEXISTENTE
A.9	CONTROL DE ACCESO	0	100	INEXISTENTE
A.10	CRIPTOGRAFÍA	0	100	INEXISTENTE
A.11	SEGURIDAD FÍSICA Y DEL ENTORNO	0	100	INEXISTENTE
A.12	SEGURIDAD DE LAS OPERACIONES	0	100	INEXISTENTE
A.13	SEGURIDAD DE LAS COMUNICACIONES	0	100	INEXISTENTE
A.14	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	0	100	INEXISTENTE
A.15	RELACIONES CON LOS PROVEEDORES	0	100	INEXISTENTE
A.16	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	0	100	INEXISTENTE
A.17	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	0	100	INEXISTENTE
A.18	CUMPLIMIENTO	0	100	INEXISTENTE
	PROMEDIO EVALUACIÓN DE CONTROLES	0	100	INEXISTENTE

AVANCE CICLO DE FUNCIONAMIENTO DEL MODELO DE OPERACIÓN (PHVA)

AVANCE PHVA COMPONENTE	% de Avance Actual Entidad	% Avance Esperado
Planificación	0%	40%
Implementación	0%	20%
Evaluación de desempeño	0%	20%
Mejora continua	0%	20%
TOTAL	0%	100%

- El Grupo/Oficina de Tecnológica y Comunicaciones, velara que los sistemas de información que sean implementados en la entidad cumplan con los requerimientos de seguridad y buenas prácticas.
- Todos los procesos de la entidad que realicen desarrollos deberán cumplir con los procedimiento y metodologías de desarrollo establecidos y formalizados para poder liberar sus aplicaciones.

- Todos los procesos de la entidad deberán informar al área de tecnología sobre sus proyectos de adquisición de sistemas de información, con el fin de brindar las observaciones correspondientes y revisar los aspectos técnicos necesario para su desarrollo e implementación.
- El Ministerio, debe establecer controles para cifrar la información que sea considerada sensible y evitar la posibilidad de repudio de una acción por parte de un usuario del 10 sistema. Se deben asegurar los archivos del sistema y mantener un control adecuado de los cambios que puedan presentarse.
- La información que se encuentra en los sistemas de producción no puede ser disminuida en los niveles de protección ni ser utilizada en ambientes de desarrollo y pruebas, tanto para mantenimiento como el desarrollo de soluciones.

Políticas de cumplimiento

Alcaldía municipal de Chaparral velara por el cumplimiento de la legislación vigente respecto a los requisitos establecidos en la seguridad y privacidad de la información, derechos de propiedad intelectual, protección de datos personales, transparencia y del derecho de acceso a la información pública.

- Cumplimiento de la normatividad y los controles relacionados con la seguridad de la información y los que son técnicamente compatibles con los diferentes ambientes o tecnologías de la entidad.
- Todos los productos de Software que se adquieran e instalen en los equipos de cómputo de la compañía deben contar con su respectiva licencia de uso.
- Realización de auditorías, para verificar la eficacia de los controles y asegurar la administración de los riesgos de seguridad de la información

Uso de usuarios y contraseñas

Cada funcionario o contratista cuyas funciones requieran de acceso a sistemas de información o correo electrónico, deberá asignársele un usuario y contraseña.

Las credenciales son personales e intransferibles.

Deben utilizarse esquemas de seguridad para la creación de contraseñas (uso de Mayúsculas, Minúsculas, Caracteres, Números).

Resultados de los indicadores propuestos

En la siguiente tabla de plan de acción se permite observar el rendimiento de los procesos internos que se hicieron en las pasantías, ya sea para medir el riesgo, productividad, calidad de servicio, gestión del tiempo, entre otros. Donde se puede utilizar para medir el desempeño global del estudio o el desempeño del área.

Por lo tanto, se implementaron diferentes tipos de indicadores con sus respectivos porcentajes. Hay que tener en cuenta que, los indicadores que se eligieron deben aportar información precisa, clara y confiable, para que así tengan fundamentos sólidos que permitan tomar decisiones efectivas.

Tabla 1.

Indicadores

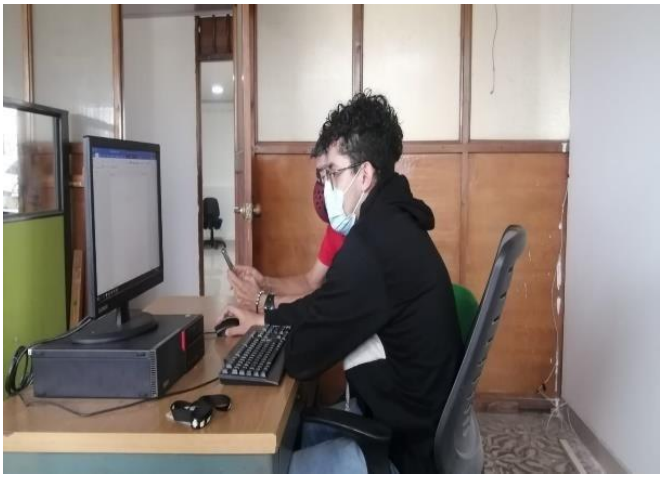
Resultado/producto esperado	Indicadores
Análisis de componentes de FURAG en la política de seguridad digital.	85% de componentes analizados del componente del FURAG.
Contar con información permanente, actualizada.	100% con información actualizada de seguridad digital.
Reducir y simplificar los reportes e informes	60% de reducción y simplicación de reportes ...
Apoyar, asesorar y retroalimentar a las entidades de la Rama Ejecutiva	100% De apoyo y asesoría, retroalimentación a los pasantes de CECONTEC y algunos del personal administrativo en el mantenimiento de computación.
Generar mecanismos de autoevaluación	99% Se lleva a cabo mantenimiento y procedimiento de seguridad de la información.

Análisis de componentes de FURAG en la política de seguridad digital.

Socialización de la política de gobierno y seguridad digital

Figura 5

SPGSD



Se comparte mi participacion donde se elaboro un texto guia para la elaboracion de la politicas generales de seguridad de la informacion aprendidas en dichas videoconferencias anteriormente, mediente el visto bueno del ingeniero encargado se contemplan los principios basicos a tener en cuenta su elaboracion dentro de la planeacion del sistema de gestion de seguridad de la informacion.

articles-176925_MPSGSI_Chaparral

Desarrollo Del **Manual** de políticas del sistema de gestión de seguridad de la información.

Figura 6

MPSI

MANUAL DE POLÍTICAS DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

Alcaldía municipal de Chaparral

2021

TABLA DE CONTENIDO

- Minimizar el riesgo en llas funciones mas importantes de la entidad.
- Cumplir con los principios de seguridad de la informacion.
- Cumplir con los principiopios de la funcion administrativas.
- Apoyar la innovacion tecnologica.

- Establecer las politicas, procedimientos e intrutivos en mateira de la seguridad informatica.

El tiempo habla de ciberseguridad, gestión de riesgos de seguridad de la información. Una vez que conocemos la definición de riesgo, pasamos a la seguridad de la información, que se puede definir como la protección de la información contra la divulgación, transferencia, modificación o destrucción no autorizada, ya sea voluntaria o accidental.

Figura 7

Ciberseguridad

Finalmente, la descripción general de otras políticas relevantes para el cumplimiento de los Objetivos planteados dentro del proyecto del SPGSD ya que éstas son el apoyo sobre el cual se desarrolla; éstas deben ser descritas de forma sencilla, puntual y muy efectiva.

Dentro de las temáticas que se tocan en este punto se encuentran por ejemplo la gestión de activos, seguridad física y ambiental, control de accesos, etc. Para abordar este punto es necesario remitirse a la “Guía de políticas específicas de seguridad y privacidad de la información” y mencionar aquellas que la Entidad haya establecido como necesarias y

primordiales, en las cuales no se pueden mostrar ya que son algunas de seguridad interna de la Alcaldía de chaparral (MINTIC, 2016).

Se utiliza el consentimiento informado para este ejercicio con el Apoyo de soporte técnico, por parte del estudiante (Anexo 1 gestión N.º 001).

Contar con información permanente, actualizada.

Diagnóstico

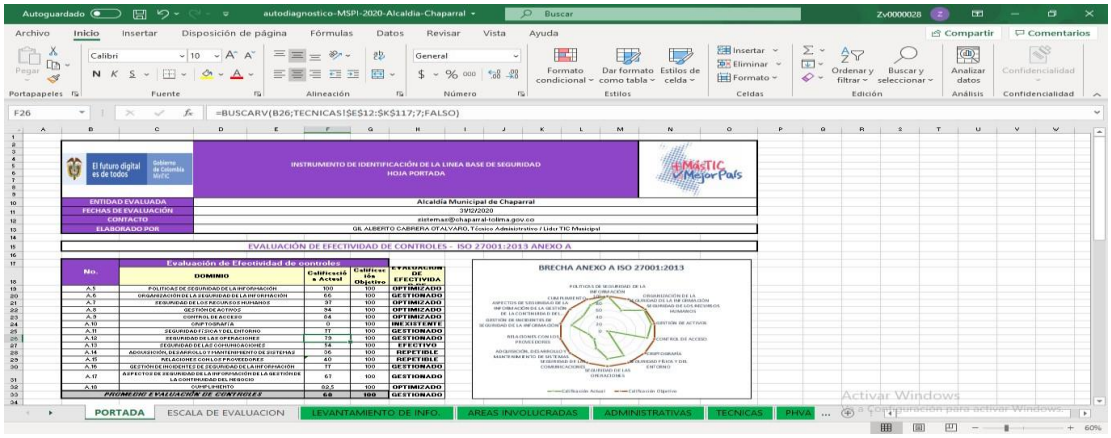
Figura 8

Diagnostico

La fase de diagnóstico permite establecer el estado actual de la implementación de la seguridad y privacidad de la información, se identifica de forma específica los controles implementados y faltantes para tener insumos fundamentales para la fase de planificación.

Figura 9

Autodiagnóstico MSPI 2021



Nota. Ministerio de Tecnología de la Información y las comunicaciones (MINTIC), (2016).

Se encontrará más información en el anexo 8: autodiagnóstico

Planificación del desarrollo

Para el desarrollo de esta fase se debe utilizar los resultados de la fase anterior (Diagnósticos) y proceder a elaborar el Plan de Seguridad y Privacidad de la Información con el objetivo de que la Entidad realice la planeación del tiempo, recursos y presupuesto de las actividades que va a desarrollar relacionadas con el MSPI.

Contexto

Comprensión de la organización y de su contexto

Se de determina los elementos externos e internos que son relevantes con las actividades que realiza la Entidad en el desarrollo de su misión y que podrían influir en las capacidades para lograr los objetivos del modelo, alineado con los objetivos estratégicos de la Entidad.

Necesidades y expectativas de los interesados

Se debe determinar partes interesadas internas o externas como las personas, entidades u organizaciones que pueden influir directamente en la seguridad y privacidad de la información de la Entidad o que pueden verse afectados en caso de que estas se vean comprometidas. Adicionalmente se deberán determinar sus necesidades y/o expectativas (intereses) relacionados con la seguridad y privacidad de la información.

Se encontrará más información en el anexo 9: plan estratégico de las tecnologías de la información y las comunicaciones PETI 2020

Definición del alcance del MSPI

Se realiza determinando los límites y la aplicabilidad del MSPI en el marco del modelo de operación por proceso de la Entidad. Determinando a qué procesos y recursos tecnológicos se realizará la implementación del MSPI.

Figura 10

Resolución 00061 2021 y PETI 2020 2023

RESOLUCION N° 00000061 DE 2021

(29 ENE 2021)

"Por la cual se adopta el Plan Estratégico de las Tecnologías de la Información y las Comunicaciones PETI 2020 – 2023 de la Alcaldía de Chaparral y se dictan otras disposiciones".

EL ALCALDE DEL MUNICIPIO DE CHAPARRAL TOLIMA
En uso de sus atribuciones que le confiere el Artículo 315-3 de la Constitución Política y,

CONSIDERANDO:

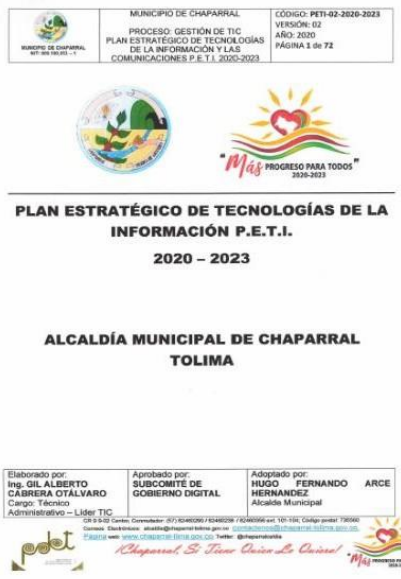
Que el Artículo N° 20 de la Constitución Política de Colombia de 1991 establece que "Se garantiza a toda persona la libertad de expresar y difundir su pensamiento y opiniones, la de informar y recibir información veraz e imparcial, y la de fundar medios masivos de comunicación." y el Artículo N° 67 dispuso que "la educación es un derecho de la persona y un servicio público que tiene una función social; con ella se busca el acceso al conocimiento, a la ciencia, a la técnica, y a los demás bienes y valores de la cultura. La educación formará al colombiano en el respeto a los derechos humanos, a la paz y a la democracia; y en la práctica del trabajo y la recreación, para el mejoramiento cultural, científico, tecnológico y para la protección del ambiente."

Que la Ley 1273 de 2009, por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones. Capítulo Primero: De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos. Capítulo Segundo: De las atentados informáticos y otras infracciones.

Que 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 en el artículo 38 sobre Masificación del uso de las TIC y cierre de la brecha digital establece que "El Ministerio de Tecnologías de la Información y las Comunicaciones, revisará, estudiará e implementará estrategias para la masificación de la conectividad, buscando sistemas que permitan llegar a las regiones más apartadas del país y que motiven a todos los ciudadanos a hacer uso de las TIC. Parágrafo: Las autoridades territoriales implementarán los mecanismos a su alcance para gestionar recursos a nivel nacional e internacional, para apoyar la masificación de las TIC, en sus respectivas jurisdicciones."

Que el Capítulo IV referente a la Gestión de Documentos Electrónicos de Archivo del Decreto 2809 de 2012, por el cual se reglamenta el Título V de la Ley 594 de 2000, parcialmente los artículos 58 y 59 de la Ley 1437 de 2011 y se dictan otras disposiciones en materia de Gestión Documental para todas las Entidades del Estado, establece que es necesario cumplir con los requisitos básicos de los documentos electrónicos de archivo y consideran la adecuada

Pág. 1



MUNICIPIO DE CHAPARRAL
PROCESO: GESTIÓN DE TIC
PLAN ESTRATÉGICO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES P.E.T.I. 2020-2023

CÓDIGO: PETI-02-2020-2023
VERSIÓN: 02
AÑO: 2020
PÁGINA 1 de 72

PLAN ESTRATÉGICO DE TECNOLOGÍAS DE LA INFORMACIÓN P.E.T.I.

2020 – 2023

ALCALDÍA MUNICIPAL DE CHAPARRAL TOLIMA

Elaborado por:	Aprobado por:	Adoptado por:
Ing. GIL ALBERTO CABRERA OTÁLVARO Cargo: Técnico Administrativo – Líder TIC	SUBCOMITÉ DE GOBIERNO DIGITAL	HUGO FERNANDO ARCE HERNANDEZ Alcalde Municipal

Fuente. Alcaldia de Chaparral.

Política de seguridad y privacidad de la información

Se debe establecer en la política de seguridad y privacidad de la información, que establezca el enfoque de la entidad, para ello debe tener en cuenta:

Misión de la Entidad

Normatividad vigente la cual se debe contar para el funcionamiento de la Entidad

Establecer compromiso del cumplimiento de los requisitos relacionados con la seguridad y privacidad de la información, así como también el de la mejora continua una vez el MSPI sea adoptado.

Estar alineada con el contexto de la Entidad, así como la identificación de las áreas que hacen parte de la implementación de seguridad de la información.

Se deben asignar los roles y responsabilidades que se identifiquen.

Ser incluidos y aprobados los temas de seguridad de la información y seguridad digital en el comité gestión y desempeño institucional, modificando el acto administrativo de conformación de este, aprobado por el mismo comité y expedido por el nominador o máxima autoridad de la Entidad.

Ser comunicada al interior de la Entidad y a los interesados que aplique.

Figura 11

Resolución 000637 de 2018 y PSPI 2021

RESOLUCION N° DE 2018

"Por la cual se aprueba e implementa el Plan de Seguridad y Privacidad de la Información PSPI de la Alcaldía de Chaparral y se dictan otras disposiciones".

EL ALCALDE DEL MUNICIPIO DE CHAPARRAL TOLIMA
En uso de sus atribuciones que le confiere el Artículo 315-3 de la Constitución Política y,

CONSIDERANDO:

Que el Artículo N° 20 de la Constitución Política de Colombia de 1991 establece que "Se garantiza a toda persona la libertad de expresar y difundir su pensamiento y opiniones, la de informar y recibir información veraz e imparcial, y la de fundar medios masivos de comunicación." y el Artículo N° 67 dispuso que "la educación es un derecho de la persona y un servicio público que tiene una función social; con ella se busca el acceso al conocimiento, a la ciencia, a la técnica, y a los demás bienes y valores de la cultura. La educación formará al colombiano en el respeto a los derechos humanos, a la paz y a la democracia; y en la práctica del trabajo y la recreación, para el mejoramiento cultural, científico, tecnológico y para la protección del ambiente."

Que la Ley 1753 de 2015, por el cual se expide el Plan Nacional de Desarrollo 2014-2018, en el artículo 45 sobre los Estándares, modelos y lineamientos de tecnologías de la información y las comunicaciones para los servicios al ciudadano, contempla: "Bajo la plena observancia del derecho fundamental de hábeas data, el Ministerio de las Tecnologías de la Información y las Comunicaciones (MinTIC), en coordinación con las entidades responsables de cada uno de los trámites y servicios, definirá y expedirá los estándares, modelos, lineamientos y normas técnicas para la incorporación de las Tecnologías de la Información y las Comunicaciones (TIC), que contribuyan a le mejora de los trámites y servicios que el Estado ofrece al ciudadano."

Que el Decreto 2693 de 2012, por el cual se establecen los lineamientos generales de la estrategia de Gobierno en línea de la República de Colombia, se reglamentan parcialmente las Leyes 1341 de 2009 y 1450 de 2011, y se dictan otras disposiciones establece que "El representante legal de cada entidad pública será el responsable de coordinar con las instancias internas respectivas la implementación y desarrollo de la Estrategia de Gobierno en línea, designar el funcionario responsable de adelantar las actividades de líder de Gobierno en línea y Anti-trámites al interior de su entidad, y realizar el seguimiento y verificación del cumplimiento de lo establecido en el presente Decreto."

Pág. 1

Cr 9 9-02, Conmutador: (57) 8246029 0
Telefax: (57) 8246 1309, Código postal: 735560
www.chaparral-tolima.gov.co - alcalde@chaparral-tolima.gov.co -
Twitter: @chaparralcalda

MUNICIPIO DE CHAPARRAL | CÓDIGO: PSPI-ST-01 | VERSIÓN: 01
PROCESO: GESTIÓN DE TIC
PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN | PÁGINA 1 de 26

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION
PSPI

VERSIÓN 01

ALCALDÍA MUNICIPAL DE CHAPARRAL

CHAPARRAL – TOLIMA

JUNIO DE 2018

Elaborado por	Revisado por:	Aprobado por: HUMBERTO BUENAVENTURA LASSO
Ing. GIL ALBERTO CABRERA Cargo: Técnico Administrativo	COMITÉ DE GOBIERNO EN LÍNEA TERRITORIAL GELT	Alcalde Municipal

Cr 9 9-02 centro. Conmutador: (57) 8246029 / 258 / 356 ext 101 – 113 – 114
Telefax: (57) 8246 1309. Código postal: 735560
Página web: www.chaparral-tolima.gov.co
Email principal: Alcalde@chaparral-tolima.gov.co
Twitter: @chaparralcalda

Fuente: (Alcaldía de Chaparral)

Se encontrará más información en el anexo 10: aprobación e implementación.

Reducir y simplificar los reportes e informes

Roles y responsabilidades

Articular con las áreas o dependencias de la Entidad, los roles y responsabilidades necesarios para la adopción del MSPI, el monitoreo del desempeño y el reporte y seguimiento ante el comité institucional de gestión y desempeño, para que sean aprobados y comunicados dentro de la Entidad.

Planificación

Identificación de activos de información e infraestructura critica

Inventario y clasificación de activos de información Chaparral noviembre 2021.

Se debe definir y aplicar un proceso de identificación y clasificación de la información, que permita:

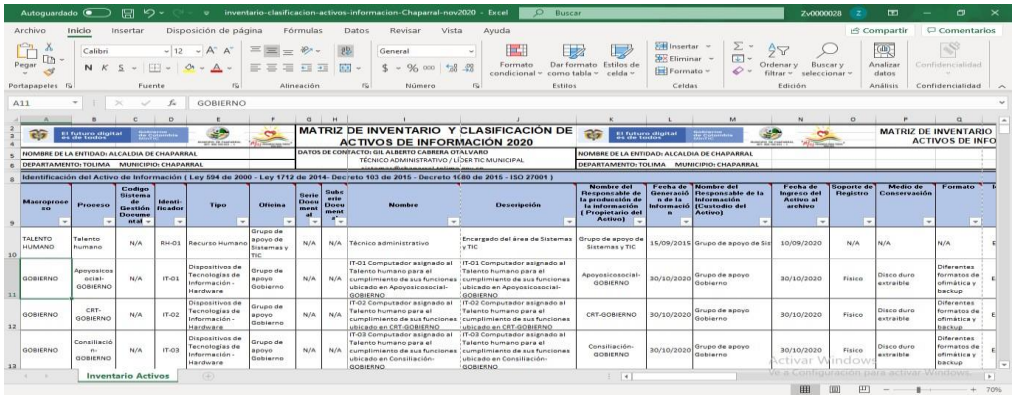
Determinar o identificar qué activos de información van a hacer parte del Inventario, que aportan valor agregado al proceso y por tanto necesitan ser protegidos de potenciales riesgos.

Clasificar los activos de información de acuerdo con los tres principios de seguridad de la información, integridad, confidencialidad y disponibilidad para garantizar que la información recibe los niveles de protección adecuados.

Actualizar el inventario y la clasificación de los activos por los propietarios y custodios de los activos de forma periódica o toda vez que exista un cambio en el proceso.

Figura 12

Identificación de activos



Valoración de los riesgos de seguridad de la información

Las entidades deben definir y aplicar un proceso de valoración de riesgos de la seguridad y privacidad de la información, que permita:

- Identificar los riesgos que causen la perdida de confidencialidad, integridad, disponibilidad, privacidad de la información, así como la continuidad de la operación de la Entidad dentro del alcance del MSPI.
- Identificar los dueños de los riesgos.
- Definir criterios para valorar las consecuencias de la materialización de los riesgos, y la probabilidad de su ocurrencia.
- Determinar el apetito de riesgos definido por la Entidad
- Establecer criterios de aceptación de los riesgos.
- Aplicar el proceso de valoración del riesgo que permita determinar los riesgos asociados a la perdida de confidencialidad, integridad y disponibilidad de la información que se encuentre dentro del alcance.
- Determinar los niveles de riesgo.
- Realizar la comparación entre los resultados del análisis y los criterios de los riesgos establecidos en este mismo numeral.
- Priorización de los riesgos analizados para su tratamiento.

Plan de tratamiento de los riesgos de seguridad de la información

La entidad debe definir y aplicar un proceso de tratamiento de riesgos de la seguridad de la información, que permita:

Seleccionar las opciones (controles) pertinentes y apropiadas para el tratamiento de riesgos.

Elaborar una declaración de aplicabilidad que contenga: los controles necesarios, su estado de implementación y la justificación de posible exclusión.

Definir un plan de tratamiento de riesgos que contenga, fechas y responsables con el objetivo de realizar trazabilidad.

Los dueños de los riesgos deben realizar la aprobación formal del plan de tratamiento de riesgos y esta aceptación debe llevarse a la revisión por dirección en el Comité Institucional y de Desempeño, o quien haga sus veces.

Figura 13

000624 de 2018 y PTRSPI

RESOLUCION N° DE 2018

"Por la cual se aprueba e implementa el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información PTRSPI de la Alcaldía de Chaparral y se dictan otras disposiciones".

EL ALCALDE DEL MUNICIPIO DE CHAPARRAL TOLIMA
En uso de sus atribuciones que le confiere el Artículo 315-3 de la Constitución Política y,

CONSIDERANDO:

Que el Artículo N° 20 de la Constitución Política de Colombia de 1991 establece que "Se garantiza a toda persona la libertad de expresar y difundir su pensamiento y opiniones, la de informar y recibir información veraz e imparcial, y la de fundar medios masivos de comunicación." y el Artículo N° 67 dispuso que "la educación es un derecho de la persona y un servicio público que tiene una función social; con ella se busca el acceso al conocimiento, a la ciencia, a la técnica, y a los demás bienes y valores de la cultura. La educación formará al colombiano en el respeto a los derechos humanos, a la paz y a la democracia; y en la práctica del trabajo y la recreación, para el mejoramiento cultural, científico, tecnológico y para la protección del ambiente."

Que la Ley 1753 de 2015, por el cual se expide el Plan Nacional de Desarrollo 2014-2018, en el artículo 45 sobre los Estándares, modelos y lineamientos de tecnologías de la información y las comunicaciones para los servicios al ciudadano, contempla: "Bajo la plena observancia del derecho fundamental de hábeas data, el Ministerio de las Tecnologías de la Información y las Comunicaciones (MinTIC), en coordinación con las entidades responsables de cada uno de los trámites y servicios, definirá y expedirá los estándares, modelos, lineamientos y normas técnicas para la incorporación de las Tecnologías de la Información y las Comunicaciones (TIC), que contribuyan a la mejora de los trámites y servicios que el Estado ofrece al ciudadano..."

Que el Decreto 2693 de 2012, por el cual se establecen los lineamientos generales de la estrategia de Gobierno en línea de la República de Colombia, se reglamentan parcialmente las Leyes 1341 de 2009 y 1450 de 2011, y se dictan otras disposiciones establece que "El representante legal de cada entidad pública será el responsable de coordinar con las instancias internas respectivas la implementación y desarrollo de la Estrategia de Gobierno en línea, designar al funcionario responsable de adelantar las actividades de líder de Gobierno en línea y Anti-trámites al interior de su entidad, y realizar el seguimiento y verificación del cumplimiento de lo establecido en el presente Decreto."

Cr 9 9-02, Conmutador: (57) 8246230 /
Telefax: (57) 8246130 Código postal: 735560
www.chaparral-tolima.gov.co - alcaldia@chaparral-tolima.gov.co -
Twitter: @chaparralcaldia

MUNICIPIO DE CHAPARRAL

	PROCESO: GESTIÓN DE TIC PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	CODIGO: PTRSPI-GT-01 VERSIÓN: 01 PÁGINA 1 de 47

PLAN DE TRATAMIENTO DE RIESTOS
DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION
PTRSPI

VERSIÓN 01

ALCALDIA MUNICIPAL DE CHAPARRAL

CHAPARRAL – TOLIMA

JUNIO DE 2018

Elaborado por:	Revisado por:	Aprobado por: HUMBERTO BUENAVENTURA LASSO
Ing. GIL ALBERTO CABRERA Cargo: Técnico Administrativo	COMITÉ DE GOBIERNO EN LÍNEA TERRITORIAL GELT	Alcalde Municipal

Cr 9 9-02 centro. Conmutador: (57) 8246230 / 288 / 308 ext 101 – 113 – 114
Telefax: (57) 8246130 Código postal: 735560
Página web: www.chaparral-tolima.gov.co
Email principal: alcaldia@chaparral-tolima.gov.co
Twitter: @chaparralcaldia

Competencia, toma de conciencia y comunicación

La entidad debe definir un plan de comunicación, capacitación, sensibilización y concientización para:

Asegurar que las personas cuenten con los conocimientos, educación y formación o experiencia adecuada para la implementación y gestión del modelo de seguridad y privacidad de la información.

Involucrar al 100% de los funcionarios de la entidad en la implementación y gestión del MSPI.

Concientizar a los funcionarios y partes interesadas en la importancia de la protección de la información.

Identificar las necesidades de comunicaciones internas y externas relacionadas con la seguridad y privacidad de la información. Se deberá definir qué será comunicado, cuándo, a quién, quién debe comunicar y finalmente definir los procesos para lograrlo.

Operación

Una vez culminada las actividades del MSPI de la fase de Planificación, se llevará a cabo la implementación de los controles, con el fin de dar cumplimiento con los requisitos del MSPI.

Los documentos que se deben generar en esta fase son:

- Plan de implementación de controles de seguridad y privacidad de la información
- Evidencia de la implementación de los controles de seguridad y privacidad de la información

Planificación e implementación

La Entidad debe realizar la planificación e implementación de las acciones determinadas en el plan de tratamiento de riesgos, esta información debe estar documentada por proceso según lo planificado. Estos documentos deben ser aprobados por el comité institucional de gestión y desempeño.

Evaluación y desempeño

Una vez culminada las actividades del MSPI, se evalúa la efectividad de las acciones tomadas a través de los indicadores definidos en la fase de implementación que debe incluir la correcta interacción entre el MSPI, MIPG y los requerimientos de la Ley 1581 de 2012 “Protección de

datos personales", Ley 1712 de 2014 "Ley de Transparencia y Acceso a la Información Pública", Decreto 2106 de 2019 o cualquier norma que las reglamente, adicione, modifique o derogue.

Seguimiento, medición, análisis y evaluación

Es importante que las Entidades conozcan de manera permanente los avances en su gestión, los logros de los resultados y metas propuestas, para la implementación del modelo habilitador de la Política de Gobierno Digital. Para tal fin es importante establecer los tiempos, recursos previstos para el monitoreo, desempeño, resultados y aceptación de estos en el comité de gestión institucional y desempeño, como lo establece el MIPG. Es importante incluir dentro del plan de auditorías los temas relacionados con seguridad digital como lo establece el MIPG.

Auditoría interna

Es de reiterar que en 2021 se programó una auditoría interna por parte de la oficina de Control Interno de la Alcaldía de Chaparral, la cual inició en julio y se culminó en diciembre del mismo año, como se puede apreciar en la siguiente imagen:

Figura 14

Programación de auditorias

PROGRAMACION DE AUDITORIAS 2021

PROCESO A AUDITAR	AREA RESPONSABLE	FECHA DE REALIZACION
Proyectos diseñados y aprobados para la ejecución de contratos relacionados con la atención de la Crisis por la pandemia de COVID19	Planeación- Oficina de Proyectos	Marzo 16 al 19
Contratos de Suministros para atender necesidades de la población con ocasión de la Pandemia	Almacén Municipal y/o a quien corresponda	3 al 7 de mayo
Plan de Seguridad y Privacidad de la Información y al Plan de SST con ocasión a la pandemia del COVID19	Oficina de Sistemas- presidente del COPASS	18 AL 21
Rubros presupuestales Dispuestos Para Cubrir Los Gastos Y/O Inversión En Tiempo De Crisis	Hacienda- Presupuesto	15 al 18 de junio
Auditoria de seguimiento a Planes de Mejoramiento suscritos con la CDT	Hacienda, planeación, gobierno	21 al 28 de junio
Auditoria de seguimiento a las Debilidades y amenazas que surjan de la evaluación del sistema de control interno Contable	Hacienda - Contabilidad	12 al 16 de julio

El principal objetivo de este ejercicio es obtener información sobre el cumplimiento del MSPI. Dicho cronograma del plan de auditorías 2021 se puede verificar en la página 04 y que se encuentra disponible en el siguiente enlace:

Se encontrará más información en el anexo 11: plan anual de las auditorias

Apoyar, asesorar y retroalimentar a las entidades de la rama ejecutiva

Plan de acción de tratamiento de riesgos de seguridad y privacidad de la información. En el presente plan de tratamiento de riesgos de seguridad y privacidad de la información se hace la verificación o revisión de dicho plan, en donde se busca inspeccionar las acciones que la oficina de sistemas está implementando para mitigar el riesgo, para que la información que se procesa y se publica en la Alcaldía, siga un derrotero de confiabilidad para los usuarios o consumidores (Función Público, 2021).

Verificado el plan que presenta el ingeniero de sistemas, se observó que está correcto el título del plan de tratamiento de riesgos de seguridad y privacidad de la información, por lo que la observación se ELIMINA y no hay objeciones.

En cumplimiento del indicador P3 , es válido y evidente el acompañamiento de MINTIC en la política de seguridad Digital, sin embargo se recomienda que de estos productos se guarden evidencias de la participación de los funcionarios, o en su defecto si no hay participación, guardar la evidencia de haberse informado, tomando el registro de notificación en el formato de asistencia, para con esas evidencias instar al Equipo Directivo para que se de operatividad al PIC, que entre otras no es funcional porque no hay quien se preocupe por su ejecución.

En el indicador H1 del plan de tratamiento de riesgos de seguridad y privacidad de la información, el titular del área de sistemas presenta como evidencia de la actualización de los

controles de SPI, planilla con el registro del mantenimiento de servicios tecnológicos con la fecha, la hora de inicio terminación de los controles y el tipo de mantenimiento realizado por cada dependencia, también se visualiza tableros de instrumentos de identificación de la línea base con los avances porcentuales y el nivel de madurez de los controles en el modelo de seguridad y privacidad de la información.

Otros controles que se visualizan en las evidencias reportadas por el titular Tic de la Entidad, es el calendario programador actualizado a noviembre de 2021 para la realización de los controles.

Es de resaltar en el presente informe de tratamiento de riesgos de SPI, la participación activa de algunos contratistas en la respuesta que se dio a la encuesta sobre seguridad y privacidad de la información, donde se observa la participación de 17 contratistas.

Así mismo, se observa la participación de funcionarios públicos en el diligenciamiento de la encuesta de SPI, en un total de 10 servidores públicos.

Por lo anterior y teniendo en cuenta las estrategias planteadas en dicha comunicación, es claro que esta entidad no cuenta con diversas herramientas tecnológicas para mejorar o mitigar los riesgos que se están viendo reflejados en lentitud de la red de internet, carencia del servidor que administre toda la red de internet de la alcaldía, y otra serie de inconsistencias o debilidades que el proveedor detectó al interior de identificación del Edificio.

Todos cuentan con la protección del antivirus «Defender», el cual está incluido en el sistema operativo «Windows», en sus diferentes versiones, en el caso de las estaciones de trabajo se cuenta con Windows 7, 8, 10 y 11; y para el caso de los servidores se cuenta con Windows Server 2012 y Server 2016.

Dicho activo se encuentra disponible en varias vigencias y en los formatos de Excel y pdf como lo exige el MinTIC, el cual se puede visualizar y/o descargar en los siguientes

Apoyos realizados

Se encontrará más información en el anexo 12: inventarios y clasificación

Las actividades que se llevaron a cabo son el mantenimiento de computadores y el mejoramiento de los controles SPI, también se elaboraron Folletos, Diapositivas cambios y recomendación de estas mismas. el ing. Gil Alberto nos da unas indicaciones, nombrándome como líder, con el objetivo de fortalecer el conocimiento de los compañeros CECONTEC

plan de acción del plan de seguridad y privacidad de la información código pa-pspi-04-2021 versión 04 vigencia 2021 en la etapa de “hacer”, en el cual se presentan los siguientes avances:

1. Oficio recibido de la empresa Morasystem para el Sr. alcalde, con radicado 01-001-DA-004999-E-2021 del 07-09-2021 con el siguiente asunto: Presentación propuesta mantenimiento red de datos y sistemas de video vigilancia; y desarrollo de aplicaciones móviles y web.

Es de reiterar que se está esperando la decisión del Señor alcalde para dar inicio a dicha necesidad.

2. Oficio recibido de la empresa Morasystem para el Sr. alcalde, con radicado 01-001-DA-005010-E-2021 del 07-09-2021 con el siguiente Asunto: Presentación propuesta para instalación de red de datos de la Alcaldía Municipal De Chaparral.

Es de reiterar que se está esperando la decisión del Señor alcalde para dar inicio a dicha necesidad.

3. Oficio recibido de Alejandro Garzón Cuellar para el Sr. alcalde, con radicado 01-110-SG-005022-E-2021 del 07-09-2021 con el siguiente Asunto: Solicitud pasantías semestre B de 2021 de la universidad UNAD.

Es de reiterar que este pasante ya se encuentra realizando diversas actividades de apoyo al grupo de Sistemas y TIC desde el mes de octubre de 2021, enfocado en el tema de "Seguridad y Privacidad de la Información.

4. Apoyo de soporte técnico, por parte de los estudiantes SENA de CECONTEC y de la universidad UNAD desde 12-noviembre-2021 hasta diciembre del 2021:

- Alejandro Garzon Cuellar (UNAD)
- Ingrid Yomara Quintero Bastidas (CECONTEC)
- Keisy Dariana Mendoza Serrano (CECONTEC)
- Kevin Smith Yate Rayo (CECONTEC)
- Lina María Tique Aguiar (CECONTEC)
- Sinndy Lorena Ramírez Portela (CECONTEC)
- Yulian Felipe Palomino (CECONTEC)

Procesos

- Mantenimiento de equipos
- Recomendaciones después de hacer el mantenimiento de computadores
- Folleto: importancia del mantenimiento y seguridad
- Diapositivas y presentación de la importancia sobre el proceso de mantenimiento de equipos

- Informe y avances del P.E.T.I 2021
- Cambios y mejoras a la página web únicos encargados ing. Gil y Alejandro Garzon Cuellar. (https://www.chaparraltolima.gov.co/Paginas/default.aspx)

Disminución de amenazas informáticas

Esta práctica permitió identificar cuales son aquellas amenazas de la organización susceptibles de mejora y así fijar los objetivos a alcanzar al respecto. La búsqueda de posibles mejoras se puede realizar con la participación del grupo de trabajo asignado, escuchando las opiniones de los compañeros y el encargado del grupo ing. Gil Alberto, buscando las mejoras mencionadas anterior mente.

Otras evidencias de elaboración del mantenimiento

Personal de mantenimiento de equipos:

Figura 15

Evidencias mantenimiento

El mantenimiento de computadoras Cuando se habla de Mantenimiento a una computadora, se refiere a las medidas y acciones que se toman para preservar una PC funcionando adecuadamente. Existen dos tipos de mantenimiento que se le puede aplicar a una computadora.

Mantenimiento preventivo

Consiste en crear un ambiente favorable para el sistema para que todo funcione correctamente y evitar posibles errores o fallos, es necesario realizar mantenimiento preventivo al equipo tanto para la parte física (hardware), que es conservar todas las partes físicas limpias como para la lógica (software), que es la ejecución de programas o utilidades que permitan mantener la computara en correcto funcionamiento. Se tiene en cuenta que el mantenimiento preventivo se debe realizar constantemente a nivel de software y hardware, según el ambiente en donde se encuentra la computadora, o si se encuentra en un lugar muy sucio debe preocupar más por la parte hardware y hacer el mantenimiento máximo cada 3 meses. Si el ordenador está trabajando constantemente con dispositivos de almacenamiento externos, en un grupo de trabajo, o dominio (en red) se debe preocupar más por la parte del software, revisar que el antivirus tenga actualizaciones automáticas y que esté actualizado, ya que la presencia de virus es inevitable. Además de antivirus se debe instalar en la computadora programas como que realiza mantenimiento a tu sistema operativo.

Mantenimiento correctivo

El mantenimiento correctivo es el que se llevará a cabo para reparar o cambiar un componente que está dañado o que ocasiona problemas de hardware. El mantenimiento correctivo se realizará cuando es necesario corregir o reparar algún problema que se esté sucediendo en una PC la cual puede corresponder a hardware o software respectivamente. También ocurre el mantenimiento correctivo cuando se necesite reemplazar un mouse, teclado, fuente de poder, parlantes, tarjeta de memoria o expansión o en el último de los casos se deba realizar una pequeña soldadura se habla de mantenimiento correctivo de hardware.

Algunos computadores de los que se le hicieron mantenimiento:

Figura 16

Evidencias mantenimiento

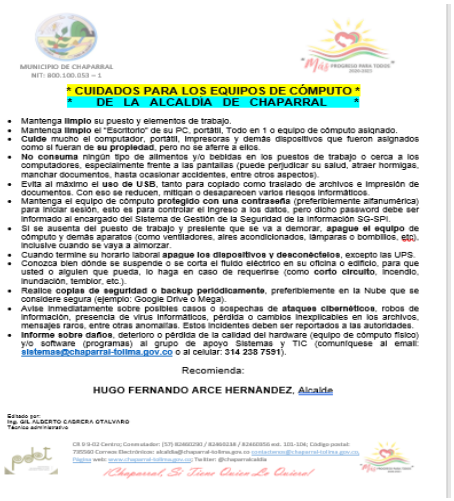
Se hace referencia en el (Anexo 7) Seguimiento y verificación de cumplimiento del plan de mantenimientos

Recomendaciones para mejorar el cuidado de los computadores:

En la siguiente imagen se aclara los cuidados de los equipos de cómputo para mantener un PC en buen estado se recomendable seguir una serie de pautas básicas que nos ayudarán no sólo a maximizar su vida útil, sino que además nos permitirán disfrutar de un buen nivel de rendimiento incluso tras el paso de algunos años.

Figura 17

Cuidados (2021)



MUNICIPIO DE CHAPARRAL
NIT: 800.100.053 – 1

*** CUIDADOS PARA LOS EQUIPOS DE CÓMPUTO ***
*** DE LA ALCALDIA DE CHAPARRAL ***

- Mantenga **limpio** su puesto y elementos de trabajo.
- Mantenga **limpio** el "Escritorio" de su PC, portátil. Todo en 1 o equipo de cómputo asignado.
- **Cuide** mucho el computador, portátil, impresoras y demás dispositivos que fueron asignados como si fueran de **su propiedad**, pero no se aferre a ellos.
- **No consuma** ningún tipo de alimentos y/o bebidas en los puestos de trabajo o cerca a los computadores, especialmente frente a las pantallas (puede perjudicar su salud, atraer hormigas, manchar documentos, hasta ocasionar accidentes, entre otros aspectos).
- Evita al máximo el **uso de USB**, tanto para copiado como traslado de archivos e impresión de documentos. Con esto se reducen, mitigan o desaparecen varios riesgos informáticos.
- Mantenga el equipo de cómputo **protegido con una contraseña** (preferiblemente alfanumérica) para iniciar sesión, esto es para controlar el ingreso a los datos, pero dicho password debe ser informado al encargado del Sistema de Gestión de la Seguridad de la Información SG-SPI.
- Si se ausenta del puesto de trabajo y presiente que se va a demorar, **apague el equipo** de cómputo y demás aparatos (como ventiladores, aires acondicionados, lámparas o bombillos, etc), inclusive cuando se vaya a almorzar.
- Cuando termine su horario laboral **apague los dispositivos y desconéctelos**, excepto las UPS.
- Conozca bien dónde se suspende o se corta el fluido eléctrico en su oficina o edificio, para que usted o alguien que pueda, lo haga en caso de requerirse (como **corto circuito**, incendio, inundación, temblor, etc.).
- Realice **copias de seguridad o backup periódicamente**, preferiblemente en la Nube que se considere segura (ejemplo: Google Drive o Mega).
- Avise inmediatamente sobre posibles casos o sospechas de **ataques cibernéticos**, robos de información, presencia de virus informáticos, pérdida o cambios inexplicables en los archivos, mensajes raros, entre otras anomalías. Estos incidentes deben ser reportados a las autoridades.
- **Informe sobre daños**, deterioro o pérdida de la calidad del hardware (equipo de cómputo físico) y/o software (programas) al grupo de apoyo Sistemas y TIC (comuníquese al email: sistemas@chaparral-tolima.gov.co o al celular: 314 238 7591).

Recomienda:

HUGO FERNANDO ARCE HERNÁNDEZ. Alcalde

Estado por:
Ing. GIL ALBERTO CABRERA OTALVARO
Técnico administrativo

¡Chaparral, Si Tiene Quien Le Quiera!

Consideraciones

- No exponer la PC a los rayos del sol.
- No colocar la PC en lugares húmedos.
- Limpiar con frecuencia el mueble donde se encuentra la PC, así como aspirar
- con frecuencia el área si es que hay alfombras.
- Evitar comer y beber cuando se esté usando la PC.
- Usar un UPS (Uninterruptible Power Supply, sistema de alimentación interrumpida)
- para regular la energía eléctrica y por si la energía se corta que haya tiempo de guardar la información.
- Cuando se deje de usar la PC, esperar a que se enfríe el monitor si es TRC
- (tubo de rayos catódicos), y si es LCD (pantalla de cristales líquidos) solo

- ponerle una funda protectora porque se enfría más rápido, así como al teclado y al chasis del CPU.
- Revisión de la instalación eléctrica de la casa u oficina, pero esto lo debe de hacer un especialista.

Folleto informativo sobre la importancia SPI (seguridad y privacidad de la información)

Se desarrolla un folleto informativo para hacer saber a los lectores qué importancia tiene el SPI (Seguridad y Privacidad de la información) el cual se hace un breve descripción de lo importante que es la mejora de esta como lo es el manejo de la computadora, asegurar datos entre otros, también hablando de las ventajas que tiene como lo es crear barreras de seguridad que no son más que técnicas, aplicaciones y dispositivos de seguridad, antivirus, anti espías, pero en lo personal lo más importante son los tips de seguridad que sería la capacitación al personal de la alcaldía para que comprendan la importancia de la seguridad tanto de las computadoras de las empresas como las personales.

Figura 18

Folleto preventivo (2021).

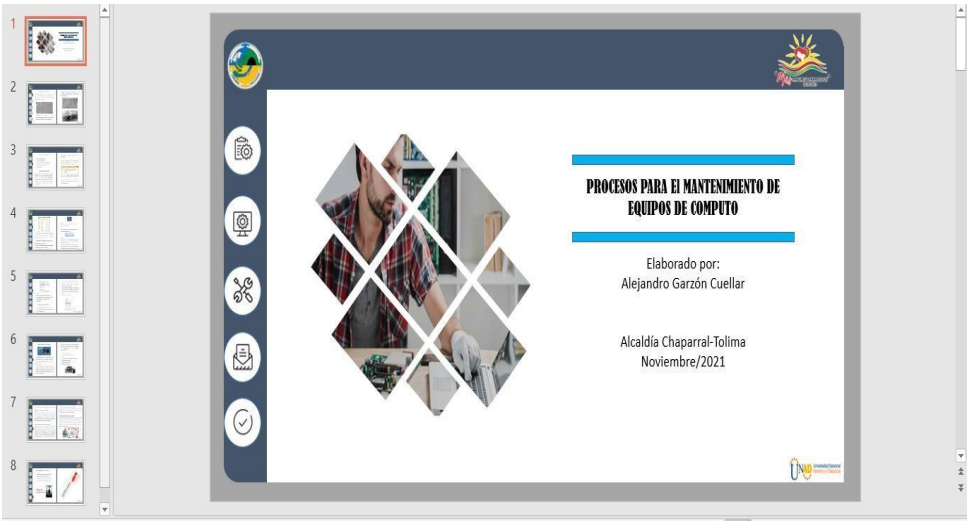
Diapositivas y presentación de la importancia sobre el proceso de mantenimiento de equipos en videoconferencias para el personal de la alcaldía. (Informativo):

Se dispone la siguiente diapositiva para anunciar los pasos a seguir del mantenimiento que se iban hacer en la empresa, por eso dijo con anterioridad las importancias se compartieron los folletos para informar al personal, en estas diapositivas se aclara que se llenaran unos formularios para cada computador y así llevar un registro o diagnóstico de cada uno para saber que errores o inseguridades presentan, también se hace el mantenimiento de los archivos ya que como se sabe los computadores guardan archivos basuras y en otros casos se descargan por cookies o documentos innecesarios, igualmente se trata el hardware de los computadores como es la limpieza de cada componente del computador para mejorar el rendimiento de la computadoras.

Se hace referencia en el (Anexo 2 y Anexo 3) plan de acción del plan de seguridad, mejoras del PSI y tratamiento a las amenazas informáticas.

Figura 19

Diapositivas (2021)



Cambios y mejoras en la página principal de Chaparral Tolima con su debida descripción y cambios:

- Implantacion del sitio local para la creacion de nuevos servicios y realizacion de pruebas

- Induccion por parte del ing. Gil a Alejandro Garzon para el manejo y utilizacion de la base de datos y pagina
- Familiarizacion con el etorno por parte de mi persona para el manejo del portal web

Figura 20

Informes de avances (2021)

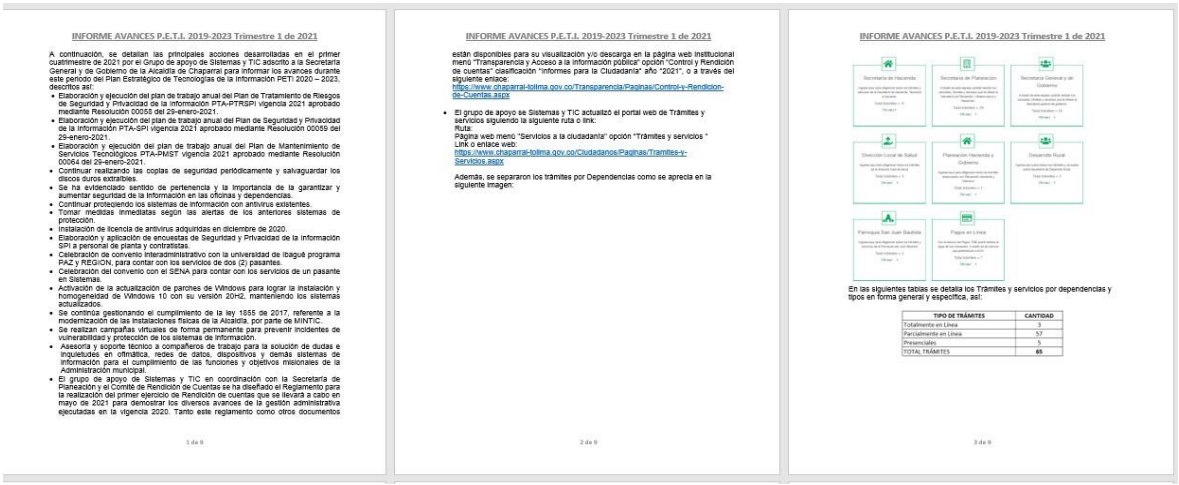
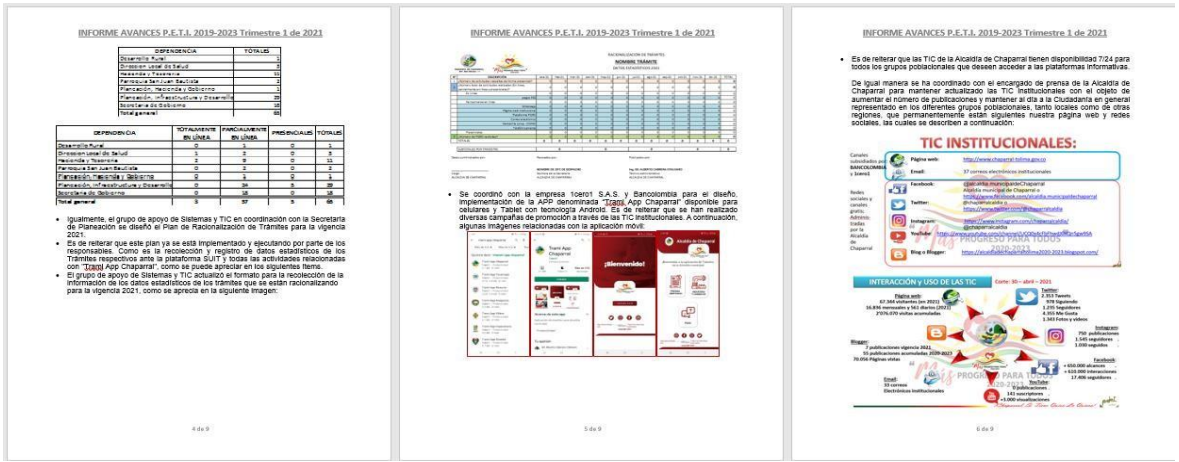


Figura 21

PETI (2021)



Generar mecanismos de autoevaluación

Liderazgo

Liderazgo y compromiso

Se debe incluir dentro del comité institucional de gestión y desempeño o quien haga sus veces, las funciones relacionadas con seguridad y privacidad de la información, adoptando, implementando, manteniendo y mejorando continuamente el MSPI, por medio de un acto administrativo. Con el propósito de garantizar el éxito de su implementación, que permita dar cumplimento entre otras, a las siguientes acciones:

Establecer y publicar la adopción de la política general, los objetivos y las políticas específicas de seguridad y privacidad de la información.

- Garantizar la adopción de los requisitos del MSPI en los procesos de la Entidad.
- Comunicar en la Entidad la importancia del MSPI.
- Planear y disponer de los recursos necesarios (presupuesto, personal, tiempo etc.) para la adopción del MSPI.
- Asegurar que el MSPI consiga los resultados previstos.
- Realizar revisiones periódicas de la adopción del MSPI (al menos dos veces por año y en las que el Nominador deberá estar presente).

Soporte

Recursos

Determinar y proporcionar los recursos necesarios para adoptar el MSPI, teniendo en cuenta que es un proceso transversal de la Entidad, se requiere que se disponga de los recursos financieros, humanos (dedicación de horas/hombre) de sus colaboradores y en general cualquier recurso que permita la adopción, implementación, mantenimiento y mejora continua del MSPI.

Revisión por la dirección

Los temas de seguridad y privacidad de la información, seguridad digital y en especial la Política y el Manual de Políticas de Seguridad y Privacidad de la Información deben ser tratados y aprobados en el comité institucional de gestión y desempeño, o cuando el nominador lo determine.

Mejoramiento continuo

Una vez culminada las actividades del MSPI de la fase evaluación y desempeño, se debe consolidar los resultados obtenidos de la fase de evaluación de desempeño y diseñar el plan de mejoramiento continuo de seguridad y privacidad de la información, tomando las acciones oportunas para mitigar las debilidades identificadas.

Mejora

Es importante que las Entidades elaboren un plan de mejoramiento continuo con el fin de realizar acciones correctivas, optimizar procesos o controles y mejorar el nivel de madurez del MSPI.

Conforme la anterior observación, se requieren acciones correspondientes para evitar o mitigar el riesgo de pérdida de la información institucional, toda vez que no se ha implementado

un procedimiento o protocolo de entrega de los activos de información por parte de los contratistas al momento de la terminación del contrato. Por tal razón, el proceso auditado deberá suscribir un PLAN DE MEJORAMIENTO, determinando un procedimiento para la entrega de la información y los dispositivos que se les haya entregado bajo la responsabilidad del contratista cuando se termine el contrato de prestación de servicios.

En los indicadores V3, V4, así como los indicadores A1 y A2, no se cuenta con evidencias de su ejecución, ya que las actividades fueron programadas para el mes de diciembre del año 2021. Por lo anterior, no hay información que observar ni reportar sobre estos indicadores.

Propuestas a nivel institucional

También se recomienda, además de la disposición de tiempo, la destinación de recursos que se requieren para evitar la ocurrencia de riesgos de pérdida de la información, adquiriendo las licencias de antivirus que menciono a continuación: Las versiones de Kaspersky están protegiendo los dos (2) servidores y las estaciones de trabajo de la dependencia de la Secretaría de Hacienda y los grupos de apoyo de Servicios administrativos y Almacén municipal.

La versión de McAfee protege los servidores y estaciones de trabajo de Centro Integrado de Servicios CIS de Chaparral.

Las versiones de Kaspersky y McAfee son renovadas anualmente y adquiridas con el contrato de adquisición del componente tecnológico que realiza la administración municipal y vence antes de terminarse el presente año 2021.

Es de reiterar que todos los antivirus antes descritos se encuentran activados y con la protección en tiempo real para evitar posibles ataque e infecciones que a diario intentan invadir las estaciones de trabajo con sus intereses particulares.

Se hace referencia en el (Anexo 4, Anexo 5, Anexo 6) Sobre los análisis de avances de seguridad digital

Conclusiones

Debido a la ausencia de personal para el área, los dispositivos no tenían ningún tipo de mantenimiento a la fecha, dicha situación fue subsanada

Durante el tiempo de la pasantía se mantuvo el 100% de la información actualizada de seguridad digital.

Complementar los dispositivos de la alcaldía de Chaparral-Tolima durante el periodo de la práctica se mantuvieron actualizados y con mantenimiento.

Se realizaron las actividades de apoyo según las indicaciones y necesidades del área de informática, soportado en los anexos.

Se realiza una actividad de apoyo en el documento del plan de seguridad y privacidad GT01, enfocado a la ciberseguridad y la garantía de la continuidad del servicio frente al incidente.

Referencias bibliográficas

Alcaldía de Chaparral (2018). *Resolución 000000637 del 2018.* Chaparral: Alcaldía Municipal de Chaparral.

Alcaldía de Chaparral (2020). *Gestión de l riesgo de seguridad digital G.R.S.D.* . Chaparral.

Alcaldia de Chaparral. (2021). *Resolución 000000611 de 2021.* Chaparral: Alcaldia .

Función Público. (10 de Septiembre de 2021). Socialización de la política de Gobierno y seguridad digital. Colombia.

Ministerio de Tecnología de la Información y las comunicaciones (MINTIC). (2016). *Seguiridad y privacidad de la información* . Vive Digital .

Ministerio de Tecnológia de la Información y las Comunicaciones (MinTic). (21 de Octubre de 2021). Es tiempo de hablar sobre ciberseguridad . Bogotá , Colombia .

ANEXOS

ANEXO 1: INFORME DE GESTION N.º 001 DE 2021

Chaparral, 22 de noviembre de 2021

En el presente informe se describen los avances del indicador H1 ““**Gestionar la Contratación de Personal Técnico para Mantenimiento Preventivos de Equipos de Cómputo”** del PLAN DE ACCION DEL PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION código PA-PSPI-04-2021 versión 04 vigencia 2021 en la etapa de “HACER”, en el cual se presentan los siguientes avances:

Oficio recibido de la empresa Morasystem para el Sr. alcalde, con radicado 01-001-DA-004999-E-2021 del 07-09-2021 con el siguiente asunto: Presentación propuesta mantenimiento red de datos y sistemas de video vigilancia; y desarrollo de aplicaciones móviles y web.

Es de reiterar que se está esperando la decisión del Señor alcalde para dar inicio a dicha necesidad.

Oficio recibido de la empresa Morasystem para el Sr. alcalde, con radicado 01-001-DA-005010-E-2021 del 07-09-2021 con el siguiente Asunto: Presentación propuesta para instalación de red de datos de la Alcaldía Municipal De Chaparral.

Es de reiterar que se está esperando la decisión del Señor alcalde para dar inicio a dicha necesidad.

Oficio recibido de Alejandro Garzón Cuellar para el Sr. alcalde, con radicado 01-110-SG-005022-E-2021 del 07-09-2021 con el siguiente Asunto: Solicitud pasantías semestre B de 2021 de la universidad UNAD.

Es de reiterar que este pasante ya se encuentra realizando diversas actividades de apoyo al grupo de Sistemas y TIC desde el mes de octubre de 2021, enfocado en el tema de “Seguridad y Privacidad de la Información.

Apoyo de soporte técnico, por parte de los estudiantes de SECONTEC y de la universidad UNAD desde 12-agosto-2021 hasta diciembre del 2021:

- Alejandro Garzon Cuellar
- Ingrid Yomara Quintero Bastidas
- Keisy Dariana Mendoza Serrano
- Kevin Smith Yate Rayo
- Lina María Tique Aguiar
- Sinndy Lorena Ramírez Portela
- Yulian Felipe Palomino

ANEXO 2: INFORME DE GESTIO N.º 002 DE 2021

Chaparral, 22 de noviembre de 2021

En el presente informe se presentan los avances del indicador H3 **"Promocionar la Política de Seguridad y Privacidad de la Información",** del PLAN DE ACCION DEL PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION código PA-PSPI-04-2021 versión 04 vigencia 2021 en la etapa de "HACER", en el cual se presentan los siguientes avances:

Se promociona periódicamente la política a través de email institucionales, grupos de WhatsApp y carteleras físicas.

Es de reiterar que la política de Seguridad y Privacidad de la Información se encuentra publicada en la página web institucional menú "Nuestra Alcaldía" opción "Gobierno Digital, TIC y Sistemas" sección "SEGURIDA Y PRIVACIDAD DE LA INFORMACIÓN" o a través del siguiente enlace:

Oficio enviado Sistemas@chaparral-tolima.gov.co Asunto: Volante Promocional de Seguridad y Privacidad de la Información SPI, recibido por "Lista 1-2019 Correos Institucionales Alcaldía", enviado el día miércoles, 17 de noviembre de 2021 5:43 p.m.

ANEXO 3: INFORME DE GESTION N.º 003 DE 2021

Chaparral, 22 de noviembre de 2021

En el presente informe se presentan los avances del indicador H4 “**“Mejorar los Controles de SPI”**, del PLAN DE ACCION DEL PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION código PA-PSPI-04-2021 versión 04 vigencia 2021 en la etapa de “HACER”, en el cual se presentan los siguientes avances:

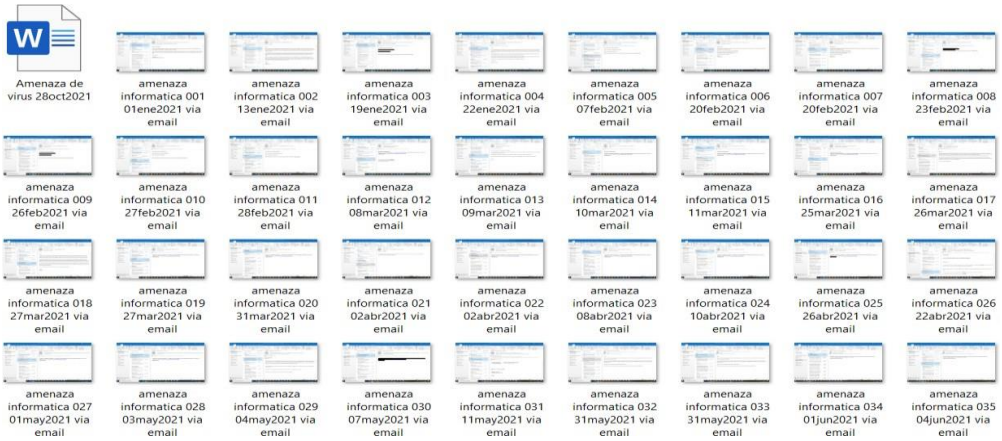
Oficio enviado por Ministerio TIC <ministeriotic@mintic.gov.co> Asunto: Alerta Preventiva de Ciberseguridad, recibido por Sistemas@chaparral-tolima.gov.co, enviado el día miércoles, 17 de noviembre de 2021 5:43 p.m. Permanentemente se reciben y comparten los boletines de seguridad emitidos por el Consejo de Seguridad Cibernética de Colombia CSIRGob, como se aprecian en las evidencias anexas a este informe.

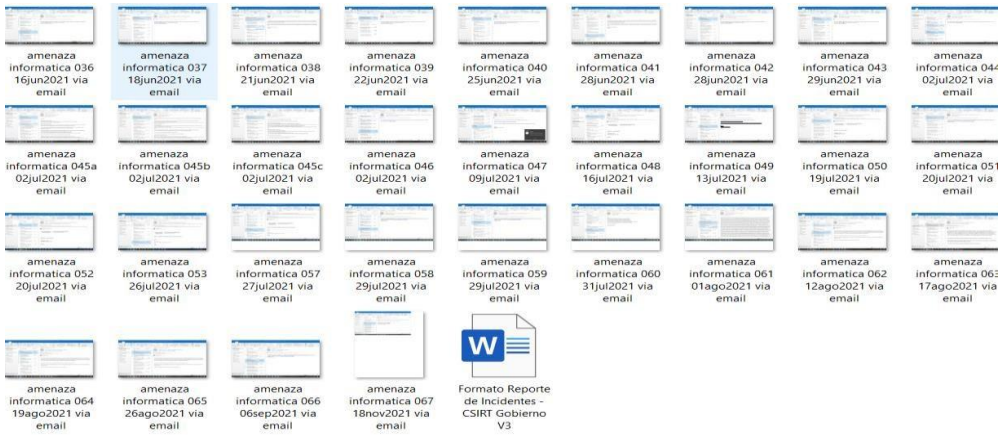
Se comparte vía WhatsApp y correos electrónicos de algunas amenazas cibernéticas para que las oficinas y dependencias de la Alcaldía estén alertas de posibles ataques informáticos.

Se actualizó el autodiagnóstico de Seguridad Digital, siendo una matriz compleja diseñada por el Ministerio de las TIC, el cual se anexa la portada evidenciando su avance y actualización de dicho control.

AMENAZAS INFORMÁTICAS

ALERTADAS INTERNAMENTE EN 2021


Amenaza de virus 28oct2021
amenaza informatica 001 01ene2021 via email
amenaza informatica 002 13ene2021 via email
amenaza informatica 003 19ene2021 via email
amenaza informatica 004 22ene2021 via email
amenaza informatica 005 07feb2021 via email
amenaza informatica 006 20feb2021 via email
amenaza informatica 007 20feb2021 via email
amenaza informatica 008 23feb2021 via email
amenaza informatica 009 26feb2021 via email
amenaza informatica 010 27feb2021 via email
amenaza informatica 011 28feb2021 via email
amenaza informatica 012 08mar2021 via email
amenaza informatica 013 09mar2021 via email
amenaza informatica 014 10mar2021 via email
amenaza informatica 015 11mar2021 via email
amenaza informatica 016 25mar2021 via email
amenaza informatica 017 26mar2021 via email
amenaza informatica 018 27mar2021 via email
amenaza informatica 019 27mar2021 via email
amenaza informatica 020 31mar2021 via email
amenaza informatica 021 02abr2021 via email
amenaza informatica 022 02abr2021 via email
amenaza informatica 023 08abr2021 via email
amenaza informatica 024 10abr2021 via email
amenaza informatica 025 26abr2021 via email
amenaza informatica 026 22abr2021 via email
amenaza informatica 027 01may2021 via email
amenaza informatica 028 03may2021 via email
amenaza informatica 029 04may2021 via email
amenaza informatica 030 07may2021 via email
amenaza informatica 031 11may2021 via email
amenaza informatica 032 31may2021 via email
amenaza informatica 033 31may2021 via email
amenaza informatica 034 01jun2021 via email
amenaza informatica 035 04jun2021 via email


amenaza informatica 036 16jun2021 via email
amenaza informatica 037 18jun2021 via email
amenaza informatica 038 21jun2021 via email
amenaza informatica 039 22jun2021 via email
amenaza informatica 040 25jun2021 via email
amenaza informatica 041 28jun2021 via email
amenaza informatica 042 28jun2021 via email
amenaza informatica 043 29jun2021 via email
amenaza informatica 044 02jul2021 via email
amenaza informatica 045a 02jul2021 via email
amenaza informatica 045b 02jul2021 via email
amenaza informatica 045c 02jul2021 via email
amenaza informatica 046 02jul2021 via email
amenaza informatica 047 09jul2021 via email
amenaza informatica 048 16jul2021 via email
amenaza informatica 049 13jul2021 via email
amenaza informatica 050 19jul2021 via email
amenaza informatica 051 20jul2021 via email
amenaza informatica 052 20jul2021 via email
amenaza informatica 053 26jul2021 via email
amenaza informatica 057 27jul2021 via email
amenaza informatica 058 29jul2021 via email
amenaza informatica 059 29jul2021 via email
amenaza informatica 060 31jul2021 via email
amenaza informatica 061 01ago2021 via email
amenaza informatica 062 12ago2021 via email
amenaza informatica 063 17ago2021 via email
amenaza informatica 064 19ago2021 via email
amenaza informatica 065 26ago2021 via email
amenaza informatica 066 06sep2021 via email
amenaza informatica 067 18nov2021 via email
Formato Reporte de Incidentes - CSIRT Gobierno V3

ANEXO 4: INFORME DE GESTION N.º 004 DE 2021

Chaparral, 22 de noviembre de 2021

En el presente informe se presentan los avances del indicador H5 ““**Gestionar La Implementación del Protocolo de Internet IPv6”** del PLAN DE ACCION DEL PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION código PA-PSPI-04-2021 versión 04 vigencia 2021 en la etapa de “HACER”, en el cual se presentan los siguientes avances:

Propuesta de Asistencia Técnica Especializada 18/enero/2021, Adjuntando él envió de lo relacionado en el asunto “DICITEC SEM SAS”. Con las propuestas económicas del 202,

Oficio enviado por DICITEC S.E.M. Asunto: Acompañamiento A La Implementación El Protocolo De IPV6, enviado de Bogotá D.C. diciembre 21 de 2020, Para el Señor alcalde y al Técnico administrativo con funciones de ingeniería de Sistemas.

Oficio enviado por DICITEC S.E.M. Asunto: Acompañamiento A La Implementación El Protocolo De IPV6, enviado de Bogotá D.C. junio 08 de 2021, Para el Señor alcalde y al Técnico administrativo con funciones de ingeniería de Sistemas.

Es de reiterar que se está esperando la decisión del Señor alcalde para dar inicio a dicha necesidad.

ANEXO 5: INFORME DE GESTION N.º 005 DE 2021

Chaparral, 22 de noviembre de 2021

En el presente informe se detallan los avances del indicador V2 ““**Actualizar Control Permanente de Medidas de Información”,** del PLAN DE ACCION DEL PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION código PA-PSPI-04-2021 versión 04 vigencia 2021 en la etapa de “VERIFICAR”, en el cual se presentan los siguientes avances:

En el mes de enero y julio de 2021 se han realizado las reuniones del Sub-Comité de Seguridad Digital, en la cual se analizan algunos temas relacionados, como son:

- Análisis del avance del estado del SG-SPI
- Análisis del avance de planes de acción 2021 de Seguridad digital
- Análisis y aprobación de tareas
- Asignación de tareas

Propuesta para la actualización del Plan de seguridad y privacidad de la información donde se quiere desarrollar los siguientes puntos: liderazgo de seguridad de la información, gestión de riesgo, gestión de incidentes, implementación de controles y concientización. Con ello Implementar el 100% del Modelo de Seguridad y Privacidad de la Información y gestionar la auditoría interna de cumplimiento. Se espera la socialización y respectiva aprobación por parte del Sub-Comité de Seguridad Digital, la cual está programada para el 01 de diciembre de 2021

ANEXO 6: INFORME DE GESTION N.º 007 DE 2021

Chaparral, 24 de noviembre de 2021

En el presente informe se detallan los avances del indicador H3 "**Gestión para vinculación de los sistemas digitales a las TRD de la Alcaldía",** del PLAN DE ACCION DEL PLAN DE MANTENIMIENTO DE SERVICIOS TECNOLÓGICOS código PA-PMST-02-2021 versión 02 vigencia 2021 en la etapa de "HACER", en el cual se presentan los siguientes aspectos:

Desde el mes de agosto se cuenta con el apoyo del Archivo General de la Nación AGN, donde se coordinan capacitaciones, diagnósticos, actualización del del Sistema de Gestión Documental, actualización de las TRD, entre otros elementos.

Desde el mes de agosto también se cuenta con el apoyo de la Función Pública para el acompañamiento de algunos temas e implementación de la política pública de Gobierno Digital enfocado al Plan de racionalización de trámites y servicios. Se gestionó el apoyo para la elaboración de las TRD de las políticas públicas de Gobierno Digital y Seguridad Digital, pero se confirmó que se concretaba dicho acompañamiento por parte de la AGN y el asesor departamental de MinTIC.

A la fecha aún se espera la visita del AGN a las instalaciones física de la Alcaldía de Chaparral para realizar los acompañamientos antes descritos y para programar el diseño e implementación de dichas TRD.

ANEXO 7: INFORME DE GESTION N.º 008 DE 2021

Chaparral, 24 de noviembre de 2021

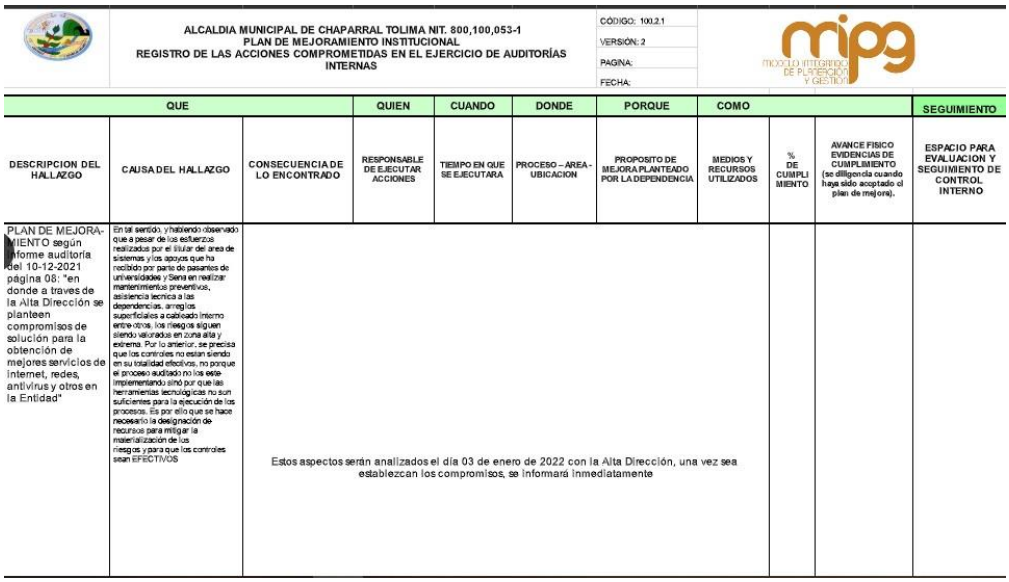
En el presente informe se detallan los avances del indicador V1 "**Seguimiento y verificación de cumplimiento del plan de mantenimientos 2021",** del PLAN DE ACCION DEL PLAN DE MANTENIMIENTO DE SERVICIOS TECNOLÓGICOS código PA-PMST-02-2021 versión 02 vigencia 2021 en la etapa de "VERIFICAR", en el cual se presentan los siguientes avances:

Se realizó convenio con el SENA y CECONTEC desde agosto de 2021 hasta diciembre de 2021, para contar con el apoyo para soporte técnico, en calidad de pasantes (quienes aceptaron de forma voluntaria y sin remuneración). Dichos estudiantes son:

- Alejandro Garzon Cuellar
- Ingrid Yomara Quintero Bastidas
- Keisy Dariana Mendoza Serrano
- Kevin Smith Yate Rayo
- Lina María Tique Aguiar
- Sinndy Lorena Ramírez Portela
- Yulian Felipe Palomino

Se realizó la programación para realizar el mantenimiento a los 227 dispositivos identificados y en uso al servicio de la Administración municipal, como se puede apreciar en los anexos.

- Plan anual de auditoria, Informe definitivo de auditoria y Plan de mejoramiento de auditoria



ALCALDIA MUNICIPAL DE CHAPARRAL TOLIMA NIT. 800,100,053-1
PLAN DE MEJORAMIENTO INSTITUCIONAL
REGISTRO DE LAS ACCIONES COMPROMETIDAS EN EL EJERCICIO DE AUDITORÍAS INTERNAS

CÓDIGO: 100.2.1
VERSIÓN: 2
PAGINA:
FECHA:

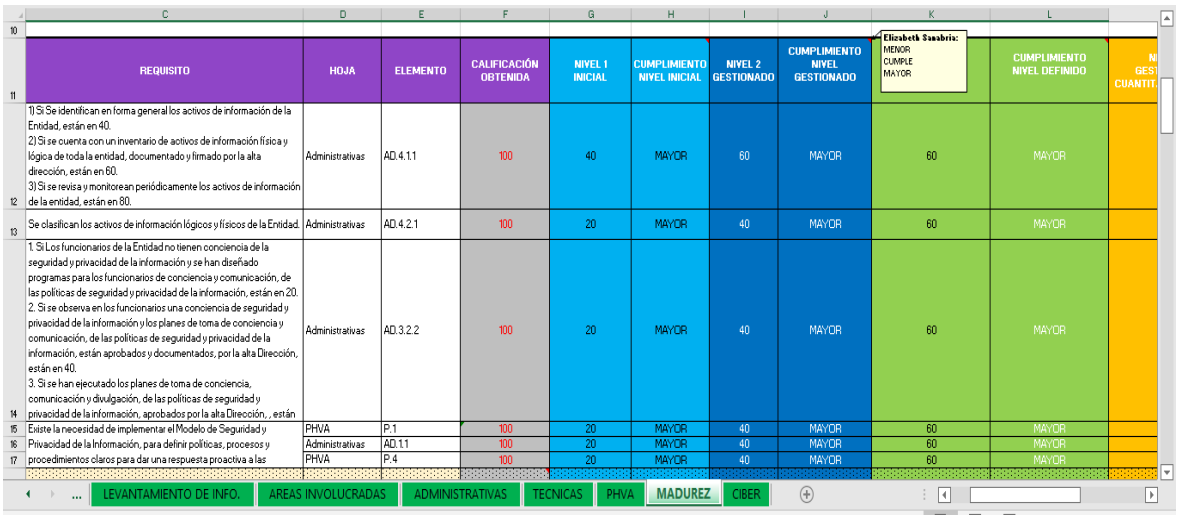
QUE			QUIEN	CUANDO	DONDE	PORQUE	COMO			SEGUIMIENTO
DESCRIPCION DEL HALLAZGO	CAUSA DEL HALLAZGO	CONSECUENCIA DE LO ENCONTRADO	RESPONSABLE DE EJECUTAR ACCIONES	TIEMPO EN QUE SE EJECUTARA	PROCESO - AREA - UBICACION	PROPOSITO DE MEJORA PLANTEADO POR LA DEPENDENCIA	MEDIOS Y RECURSOS UTILIZADOS	% DE CUMPLIMIENTO	AVANCE FISICO EVIDENCIAS DE CUMPLIMIENTO (se diligencia cuando haya sido aceptado el plan de mejora).	ESPACIO PARA EVALUACION Y SEGUIMIENTO DE CONTROL INTERNO
PLAN DE MEJORAMIENTO según informe auditoria del 10-12-2021 pagina 08: "en donde a traves de la Alta Dirección se planteen compromisos de solución para la obtención de mejores servicios de internet, redes, antivirus y otros en la Entidad"	En tal sentido, y habiendo observado que a pesar de los esfuerzos realizados por el titular del area de sistemas y los apoyos que ha recibido por parte de pasantes de universidades y Sena en realizar mantenimientos preventivos, asistencia tecnica a las dependencias, arreglos superficiales a cableado interno entre otros, los riesgos siguen siendo valorados en zona alta y extrema. Por lo anterior, se precisa que los controles no estan siendo en su totalidad efectivos, no porque el proceso auditado no los este implementando sinó por que las herramientas tecnológicas no son suficientes para la ejecución de los procesos. Es por ello que se hace necesario la designación de recursos para mitigar la materialización de los riesgos y para que los controles sean EFECTIVOS	Estos aspectos serán analizados el día 03 de enero de 2022 con la Alta Dirección, una vez sea establezcan los compromisos, se informará inmediatamente								

Alejandro Garzon, PAAID. (2021). [Imagen]. Chaparral-Tolima.

- Palabras, buen desempeño de pasantes y compromiso por la entrega de sus deberes.

Alejandro Garzon, DPC. (2021). [Imagen]. Chaparral-Tolima.

ANEXO 8: AUTODIAGNÓSTICO



REQUISITO	HOJA	ELEMENTO	CALIFICACIÓN OBTENIDA	NIVEL 1 INICIAL	CUMPLIMIENTO NIVEL INICIAL	NIVEL 2 GESTIONADO	CUMPLIMIENTO NIVEL GESTIONADO	Elizabeth Sanabria: MENOR CUMPLE MAYOR	CUMPLIMIENTO NIVEL DEFINIDO	NI GEST CUANTIT
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.	Administrativas	AD.4.1.1	100	40	MAYOR	60	MAYOR	60	MAYOR	
Se clasifican los activos de información lógicos y físicos de la Entidad.	Administrativas	AD.4.2.1	100	20	MAYOR	40	MAYOR	60	MAYOR	
1. Si Los funcionarios de la Entidad no tienen conciencia de la seguridad y privacidad de la información y se han diseñado programas para los funcionarios de conciencia y comunicación, de las políticas de seguridad y privacidad de la información, están en 20. 2. Si se observa en los funcionarios una conciencia de seguridad y privacidad de la información y 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, están en 40. 3. Si se han ejecutado los planes de toma de conciencia, comunicación y divulgación, de las políticas de seguridad y privacidad de la información, aprobados por la alta Dirección, , están	Administrativas	AD.3.2.2	100	20	MAYOR	40	MAYOR	60	MAYOR	
Existe la necesidad de implementar el Modelo de Seguridad y	PHVA	P.1	100	20	MAYOR	40	MAYOR	60	MAYOR	
Privacidad de la Información, para definir políticas, procesos y	Administrativas	AD.1.1	100	20	MAYOR	40	MAYOR	60	MAYOR	
procedimientos claros para dar una respuesta proactiva a las	PHVA	P.4	100	20	MAYOR	40	MAYOR	60	MAYOR	

LEVANTAMIENTO DE INFO. | AREAS INVOLUCRADAS | ADMINISTRATIVAS | TECNICAS | PHVA | MADUREZ | CIBER

Instrumento de identificación de la línea base de seguridad, nos mostrara en la forma que se organizó el autodiagnóstico como lo es: escala de valoración de controles, levantamiento de información, otras áreas involucradas, técnicas, PHVA, madurez entre otros.

ANEXO 9: PLAN ESTRATÉGICO DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES PETI 2020

La resolución en la cual se adopta el Plan Estratégico de las Tecnologías de la Información y las Comunicaciones PETI 2020 — 2023 de la Alcaldía de Chaparral y se dictan otras disposiciones.

EL ALCALDE DEL MUNICIPIO DE CHAPARRAL TOLIMA
En uso de sus atribuciones que le confiere el Artículo 315-3 de la Constitución Política y,

CONSIDERANDO:

Que el Artículo N° 20 de la Constitución Política de Colombia de 1991 establece que "Se garantiza a toda persona la libertad de expresar y difundir su pensamiento y opiniones, la de informar y recibir información veraz e imparcial, y la de fundar medios masivos de comunicación." y el Artículo N° 67 dispuso que "la educación es un derecho de la persona y un servicio público que tiene una función social; con ella se busca el acceso al conocimiento, a la ciencia, a la técnica, y a los demás bienes y valores de la cultura. La educación formará al colombiano en el respeto a los derechos humanos, a la paz y a la democracia; y en la práctica del trabajo y la recreación, para el mejoramiento cultural, científico, tecnológico y para la protección del ambiente."

Que la Ley 1273 de 2009, por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones. Capítulo Primero: De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos. Capítulo Segundo: De las atentados informáticos y otras infracciones.

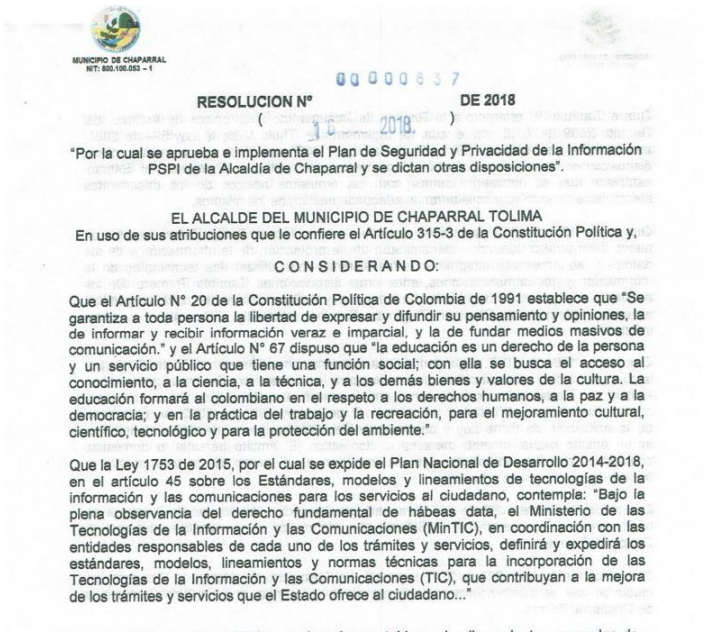
Que la Ley 1341 de 2009 Por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones –TIC–, se crea la Agencia Nacional de Espectro y se dictan otras disposiciones en el artículo 38 sobre Masificación del uso de las TIC y cierre de la brecha digital establece que "El Ministerio de Tecnologías de la Información y las Comunicaciones, revisará, estudiará e implementará estrategias para la masificación de la conectividad, buscando sistemas que permitan llegar a las regiones más apartadas del país y que motiven a todos los ciudadanos a hacer uso de las TIC. Parágrafo: Las autoridades territoriales implementarán los mecanismos a su alcance para gestionar recursos a nivel nacional e internacional, para apoyar la masificación de las TIC, en sus respetivas jurisdicciones."

Que el Capítulo IV referente a la Gestión de Documentos Electrónicos de Archivo del Decreto 2609 de 2012, por el cual se reglamenta el Título V de la Ley 594 de 2000, parcialmente los artículos 58 y 59 de la Ley 1437 de 2011 y se dictan otras disposiciones en materia de Gestión Documental para todas las Entidades del Estado, establece que es necesario cumplir con los requisitos básicos de los documentos electrónicos de archivo y consideran la adecuada

CR 9 9-02 Centro; Conmutador: (57) 82460290 / 82460238 / 82460356 ext. 101-104. Código postal: 735560
Correos Electrónicos: alcaldia@chaparral-tolima.gov.co contactenos@chaparral-tolima.gov.co.
Pág. 1

ANEXO 10: APROBACIÓN E IMPLEMENTACIÓN

Se mostrará la Resolución donde se aprobó e implemento el plan de seguridad y privacidad de la información PSPI de la alcaldía que hace parte del proceso de Gestión de TIC.



MUNICIPIO DE CHAPARRAL
NIT: 800.100.093 – 1

00 000637

RESOLUCION Nº **DE 2018**

(10 ENE 2018)

"Por la cual se aprueba e implementa el Plan de Seguridad y Privacidad de la Información PSPI de la Alcaldía de Chaparral y se dictan otras disposiciones".

EL ALCALDE DEL MUNICIPIO DE CHAPARRAL TOLIMA
En uso de sus atribuciones que le confiere el Artículo 315-3 de la Constitución Política y,

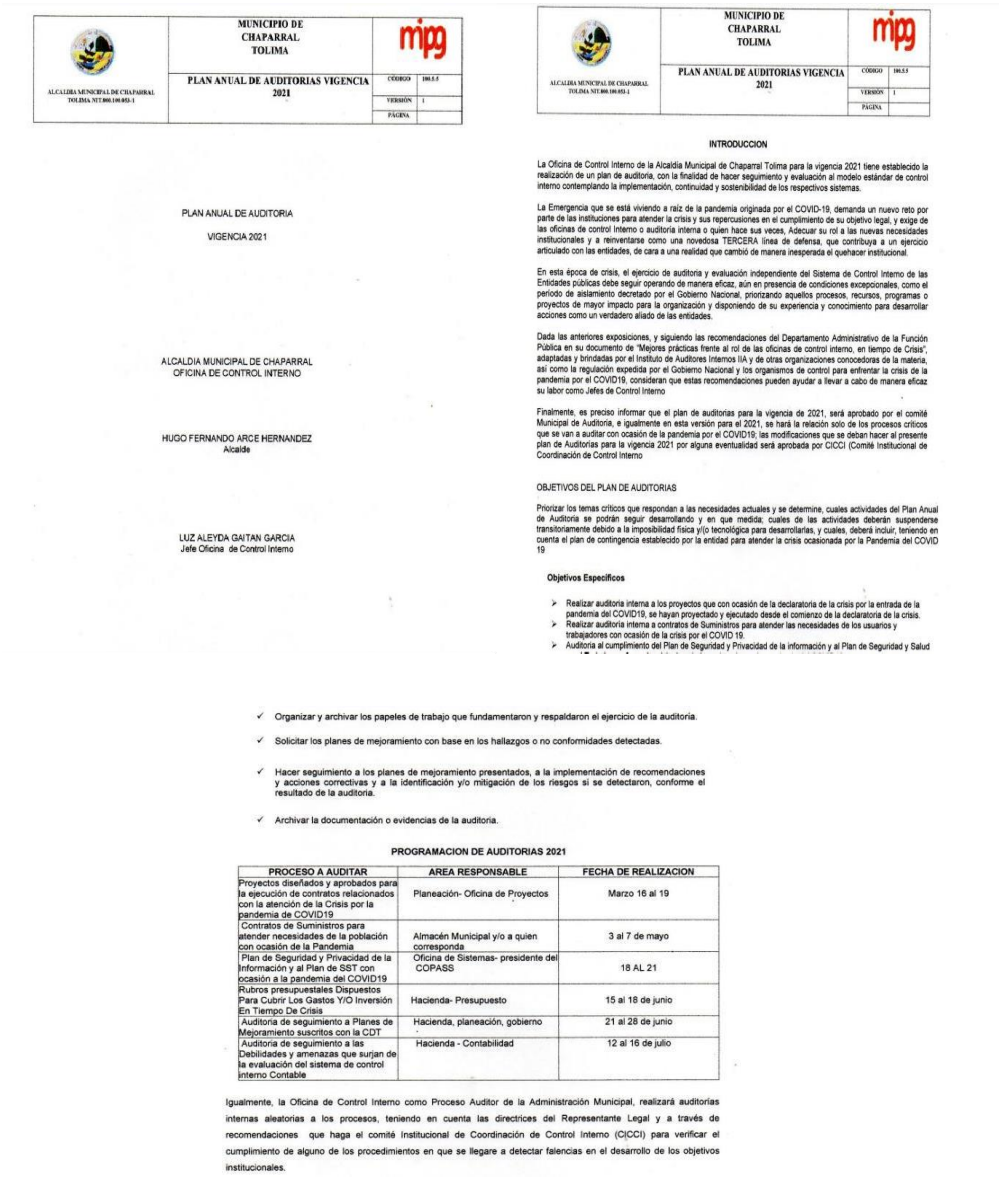
CONSIDERANDO:

Que el Artículo N° 20 de la Constitución Política de Colombia de 1991 establece que "Se garantiza a toda persona la libertad de expresar y difundir su pensamiento y opiniones, la de informar y recibir información veraz e imparcial, y la de fundar medios masivos de comunicación." y el Artículo N° 67 dispuso que "la educación es un derecho de la persona y un servicio público que tiene una función social; con ella se busca el acceso al conocimiento, a la ciencia, a la técnica, y a los demás bienes y valores de la cultura. La educación formará al colombiano en el respeto a los derechos humanos, a la paz y a la democracia; y en la práctica del trabajo y la recreación, para el mejoramiento cultural, científico, tecnológico y para la protección del ambiente."

Que la Ley 1753 de 2015, por el cual se expide el Plan Nacional de Desarrollo 2014-2018, en el artículo 45 sobre los Estándares, modelos y lineamientos de tecnologías de la información y las comunicaciones para los servicios al ciudadano, contempla: "Bajo la plena observancia del derecho fundamental de hábeas data, el Ministerio de las Tecnologías de la Información y las Comunicaciones (MinTIC), en coordinación con las entidades responsables de cada uno de los trámites y servicios, definirá y expedirá los estándares, modelos, lineamientos y normas técnicas para la incorporación de las Tecnologías de la Información y las Comunicaciones (TIC), que contribuyan a la mejora de los trámites y servicios que el Estado ofrece al ciudadano..."

ANEXO 11: PLAN ANUAL DE LAS AUDITORIAS

Se presenta el plan anual de las auditorias con sus debidas fechas, el cual se presentará en el cumplimiento del código de ética.



	MUNICIPIO DE CHAPARRAL TOLIMA	
ALCALDIA MUNICIPAL DE CHAPARRAL TOLIMA NIT:800.100.953-1	PLAN ANUAL DE AUDITORIAS VIGENCIA 2021	CÓDIGO 100.1.5 VERSIÓN 1 PÁGINA

PLAN ANUAL DE AUDITORIA

VIGENCIA 2021

ALCALDIA MUNICIPAL DE CHAPARRAL
OFICINA DE CONTROL INTERNO

HUGO FERNANDO ARCE HERNANDEZ
Alcalde

LUZ ALEYDA GAITAN GARCIA
Jefe Oficina de Control Interno

	MUNICIPIO DE CHAPARRAL TOLIMA	
ALCALDIA MUNICIPAL DE CHAPARRAL TOLIMA NIT:800.100.953-1	PLAN ANUAL DE AUDITORIAS VIGENCIA 2021	CÓDIGO 100.1.5 VERSIÓN 1 PÁGINA

INTRODUCCION

La Oficina de Control Interno de la Alcaldía Municipal de Chaparral Tolima para la vigencia 2021 tiene establecido la realización de un plan de auditoria, con la finalidad de hacer seguimiento y evaluación al modelo estándar de control interno contemplando la implementación, continuidad y sostenibilidad de los respectivos sistemas.

La Emergencia que se está viviendo a raíz de la pandemia originada por el COVID-19, demanda un nuevo reto por parte de las instituciones para atender la crisis y sus repercusiones en el cumplimiento de su objetivo legal, y exige de las oficinas de control Interno o auditoria interna o quien hace sus veces, Adecuar su rol a las nuevas necesidades institucionales y a reinventarse como una novedosa TERCERA línea de defensa, que contribuya a un ejercicio articulado con las entidades, de cara a una realidad que cambió de manera inesperada el quehacer institucional.

En esta época de crisis, el ejercicio de auditoria y evaluación independiente del Sistema de Control Interno de las Entidades públicas debe seguir operando de manera eficaz, aún en presencia de condiciones excepcionales, como el período de aislamiento decretado por el Gobierno Nacional, priorizando aquellos procesos, recursos, programas o proyectos de mayor impacto para la organización y disponiendo de su experiencia y conocimiento para desarrollar acciones como un verdadero aliado de las entidades.

Dada las anteriores exposiciones, y siguiendo las recomendaciones del Departamento Administrativo de la Función Pública en su documento de "Mejores prácticas frente al rol de las oficinas de control interno, en tiempo de Crisis", adaptadas y brindadas por el Instituto de Auditores Internos IIA y de otras organizaciones conocedoras de la materia, así como la regulación expedida por el Gobierno Nacional y los organismos de control para enfrentar la crisis de la pandemia por el COVID19, consideran que estas recomendaciones pueden ayudar a llevar a cabo de manera eficaz su labor como Jefes de Control Interno

Finalmente, es preciso informar que el plan de auditorias para la vigencia de 2021, será aprobado por el comité Municipal de Auditoria, e igualmente en esta versión para el 2021, se hará la relación solo de los procesos críticos que se van a auditar con ocasión de la pandemia por el COVID19; las modificaciones que se deban hacer al presente plan de Auditorias para la vigencia 2021 por alguna eventualidad será aprobada por CICCI (Comité Institucional de Coordinación de Control Interno

OBJETIVOS DEL PLAN DE AUDITORIAS

Priorizar los temas críticos que respondan a las necesidades actuales y se determine, cuales actividades del Plan Anual de Auditoria se podrán seguir desarrollando y en que medida; cuales de las actividades deberán suspenderse transitoriamente debido a la imposibilidad física y/o tecnológica para desarrollarlas, y cuales, deberá incluir, teniendo en cuenta el plan de contingencia establecido por la entidad para atender la crisis ocasionada por la Pandemia del COVID 19

Objetivos Específicos

- Realizar auditoria interna a los proyectos que con ocasión de la declaratoria de la crisis por la entrada de la pandemia del COVID19, se hayan proyectado y ejecutado desde el comienzo de la declaratoria de la crisis.
- Realizar auditoria interna a contratos de Suministros para atender las necesidades de los usuarios y trabajadores con ocasión de la crisis por el COVID 19.
- Auditoria al cumplimiento del Plan de Seguridad y Privacidad de la información y al Plan de Seguridad y Salud

- ✓ Organizar y archivar los papeles de trabajo que fundamentaron y respaldaron el ejercicio de la auditoria.
- ✓ Solicitar los planes de mejoramiento con base en los hallazgos o no conformidades detectadas.
- ✓ Hacer seguimiento a los planes de mejoramiento presentados, a la implementación de recomendaciones y acciones correctivas y a la identificación y/o mitigación de los riesgos si se detectaron, conforme el resultado de la auditoria.
- ✓ Archivar la documentación o evidencias de la auditoria.

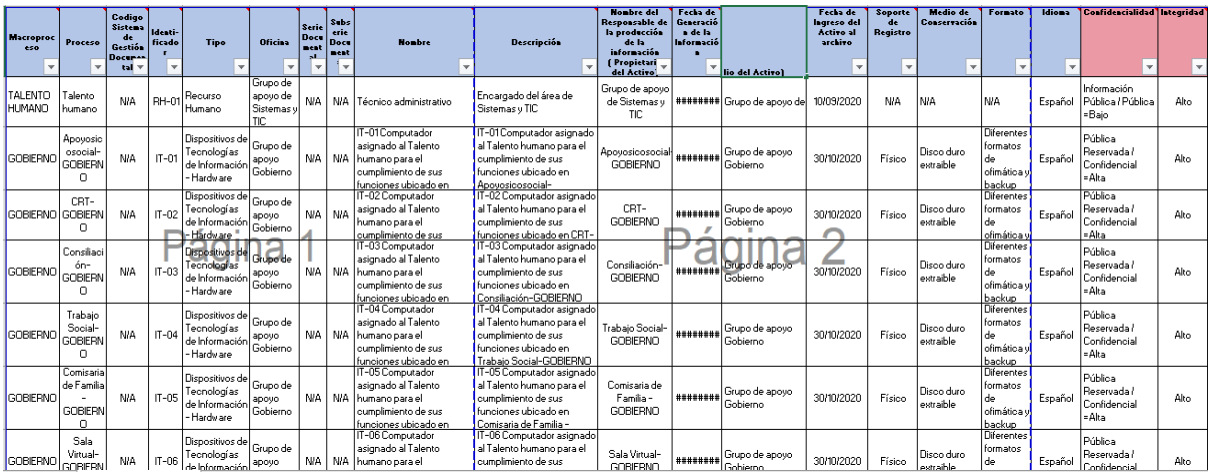
PROGRAMACION DE AUDITORIAS 2021

PROCESO A AUDITAR	AREA RESPONSABLE	FECHA DE REALIZACION
Proyectos diseñados y aprobados para la ejecución de contratos relacionados con la atención de la Crisis por la pandemia de COVID19	Planeación- Oficina de Proyectos	Marzo 16 al 19
Contratos de Suministros para atender necesidades de la población con ocasión de la Pandemia	Almacén Municipal y/o a quien corresponda	3 al 7 de mayo
Plan de Seguridad y Privacidad de la Información y al Plan de SST con ocasión a la pandemia del COVID19	Oficina de Sistemas- presidente del COPASS	18 AL 21
Rubros presupuestales Dispuestos Para Cubrir Los Gastos Y/O Inversión En Tiempo De Crisis	Hacienda- Presupuesto	15 al 18 de junio
Auditoria de seguimiento a Planes de Mejoramiento suscritos con la CDT	Hacienda, planeación, gobierno	21 al 28 de junio
Auditoria de seguimiento a las Debilidades y amenazas que surjan de la evaluación del sistema de control interno Contable	Hacienda - Contabilidad	12 al 16 de julio

Igualmente, la Oficina de Control Interno como Proceso Auditor de la Administración Municipal, realizará auditorias internas aleatorias a los procesos, teniendo en cuenta las directrices del Representante Legal y a través de recomendaciones que haga el comité Institucional de Coordinación de Control Interno (CICCI) para verificar el cumplimiento de alguno de los procedimientos en que se llegare a detectar falencias en el desarrollo de los objetivos institucionales.

ANEXO 12: INVENTARIOS Y CLASIFICACION

Documentos clasificación de activos



Macroproceso	Proceso	Codigo Sistema de Gestión Documental	Ideatificador	Tipo	Oficina	Serie Documental	Subserie Documental	Nombre	Descripción	Nombre del Responsable de la producción de la información (Propietario del Activo)	Fecha de Generación de la Información	tio del Activo)	Fecha de Ingreso del Activo al archivo	Soporte de Registro	Medio de Conservación	Formato	Idioma	Confidencialidad	Integridad
TALENTO HUMANO	Talento humano	N/A	RH-01	Recurso Humano	Grupo de apoyo de Sistemas y TIC	N/A	N/A	Técnico administrativo	Encargado del área de Sistemas y TIC	Grupo de apoyo de Sistemas y TIC	########	Grupo de apoyo de	10/09/2020	N/A	N/A	N/A	Español	Información Pública / Pública =Bajo	Alto
GOBIERNO	Apoyosicosocial-GOBIERNO	N/A	IT-01	Dispositivos de Tecnologías de Información - Hardware	Grupo de apoyo Gobierno	N/A	N/A	IT-01 Computador asignado al Talento humano para el cumplimiento de sus funciones ubicado en	IT-01 Computador asignado al Talento humano para el cumplimiento de sus funciones ubicado en Apoyosicosocial-	Apoyosicosocial GOBIERNO	########	Grupo de apoyo Gobierno	30/10/2020	Físico	Disco duro extraible	Diferentes formatos de ofimática y backup	Español	Pública Reservada / Confidencial =Alta	Alto
GOBIERNO	CRT-GOBIERNO	N/A	IT-02	Dispositivos de Tecnologías de Información - Hardware	Grupo de apoyo Gobierno	N/A	N/A	IT-02 Computador asignado al Talento humano para el cumplimiento de sus	IT-02 Computador asignado al Talento humano para el cumplimiento de sus funciones ubicado en CRT-	CRT-GOBIERNO	########	Grupo de apoyo Gobierno	30/10/2020	Físico	Disco duro extraible	Diferentes formatos de ofimática y	Español	Pública Reservada / Confidencial =Alta	Alto
GOBIERNO	Consiliación-GOBIERNO	N/A	IT-03	Dispositivos de Tecnologías de Información - Hardware	Grupo de apoyo Gobierno	N/A	N/A	IT-03 Computador asignado al Talento humano para el cumplimiento de sus funciones ubicado en	IT-03 Computador asignado al Talento humano para el cumplimiento de sus funciones ubicado en Consiliación-GOBIERNO	Consiliación-GOBIERNO	########	Grupo de apoyo Gobierno	30/10/2020	Físico	Disco duro extraible	Diferentes formatos de ofimática y backup	Español	Pública Reservada / Confidencial =Alta	Alto
GOBIERNO	Trabajo Social-GOBIERNO	N/A	IT-04	Dispositivos de Tecnologías de Información - Hardware	Grupo de apoyo Gobierno	N/A	N/A	IT-04 Computador asignado al Talento humano para el cumplimiento de sus funciones ubicado en	IT-04 Computador asignado al Talento humano para el cumplimiento de sus funciones ubicado en Trabajo Social-GOBIERNO	Trabajo Social-GOBIERNO	########	Grupo de apoyo Gobierno	30/10/2020	Físico	Disco duro extraible	Diferentes formatos de ofimática y backup	Español	Pública Reservada / Confidencial =Alta	Alto
GOBIERNO	Comisaria de Familia - GOBIERNO	N/A	IT-05	Dispositivos de Tecnologías de Información - Hardware	Grupo de apoyo Gobierno	N/A	N/A	IT-05 Computador asignado al Talento humano para el cumplimiento de sus funciones ubicado en	IT-05 Computador asignado al Talento humano para el cumplimiento de sus funciones ubicado en Comisaria de Familia -	Comisaria de Familia - GOBIERNO	########	Grupo de apoyo Gobierno	30/10/2020	Físico	Disco duro extraible	Diferentes formatos de ofimática y backup	Español	Pública Reservada / Confidencial =Alta	Alto
GOBIERNO	Sala Virtual-GOBIERN	N/A	IT-06	Dispositivos de Tecnologías de Información	Grupo de apoyo	N/A	N/A	IT-06 Computador asignado al Talento humano para el	IT-06 Computador asignado al Talento humano para el cumplimiento de sus	Sala Virtual-GOBIERNO	########	Grupo de apoyo Gobierno	30/10/2020	Físico	Disco duro extraible	Diferentes formatos de	Español	Pública Reservada / Confidencial	Alto

Inventarios y clasificación e información sobre los elementos asignados a cada usuario de la empresa como son computadores y otros elementos electrónicos para el cumplimiento de sus funciones.