

Chía, 17 de diciembre de 2024

Dr.
CARLOS ANDRES RODRIGUEZ SANCHEZ
Jefe de oficina
Control interno
Alcaldía Chía

Asunto: Información para Auditoria interna 2024

Cordial saludo

Atendiendo la solicitud de información allegada a esta oficina mediante correo electrónico con fecha 04 de diciembre del 2024 nos permitimos dar respuesta a cada uno de los ítems citados así:

➤ **PLAN DE COMUNICACIONES MSPI Y SU EJECUCIÓN.**

- La aprobación del modelo de seguridad y privacidad de la información (MSPI) se dio mediante reunión del comité de gestión y desempeño, realizada el 17 de octubre del 2023.
- Teniendo en cuenta lo anterior, se estableció un plan de comunicación y/o socialización del MSPI, mediante circular informativa No. 009 del 27 de octubre del 2023, con el cronograma definido, cuya invitación se hizo extensiva a través de correo electrónicos de la Oficina TIC a todos los funcionarios y contratistas de la administración municipal.

Evidencias:

1. Correo programación sensibilizaciones MSPI
2. Circular No. 009 cronogramas MSPI y otros
3. Asistencia a sensibilizaciones MSPI, Políticas y Gobierno Digital
4. MSPI

➤ **SEGUIMIENTO A LOS INDICADORES ESTABLECIDOS EN EL MSPI.**

INDICADOR 01- ORGANIZACIÓN DE SEGURIDAD DE LA INFORMACIÓN.

INDICADOR 02 - TRATAMIENTOS DE EVENTOS RELACIONADOS EN MARCO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Se realiza el cálculo basándose en la cantidad de anomalías cerradas / cantidad de anomalías reportadas por la plataforma de administración de endpoint * 100
 $(8/8) * 100 = 100$

INDICADOR 03 – PLAN DE SENSIBILIZACIÓN

En la vigencia del 2024 se enviaron a través del correo electrónico de la Oficina TIC, dos circulares con las programaciones de cada semestre, en las cuales se impartieron sensibilizaciones sobre las políticas de seguridad digital, seguridad de la información, procedimientos de seguridad de la información, gobierno digital y arquitectura empresarial, las cuales relaciono a continuación:

- Circular informativa No. 02 del 06 de mayo del 2024, cuyo cronograma con las jornadas de sensibilización se realizaron el 9, 10, 16 y 17 de mayo del 2024. Los temas tratados fueron: Política de gobierno digital, Política de seguridad de información, Procedimientos de Seguridad de la Información, Datos abiertos y se dejó un espacio de preguntas y respuestas.
- Circular informativa No. 006 del 09 de octubre del 2024, cuyo cronograma con las jornadas de sensibilización se realizaron el 22, 23 y 24 de octubre del 2024. Los temas tratados fueron: Política de Gobierno Digital, Política de seguridad digital, Política de seguridad de información y Arquitectura Empresarial

Evidencias:

1. Circular 02 sensibilización-Políticas TI y Datos Abiertos – Mayo
2. Listado asistencia sensibilizaciones mayo 2024
3. Circular 06 sensibilización Política de Seguridad Digital y de la Información
4. Listado asistencia sensibilizaciones octubre 2024

INDICADOR 04 – ESTABLECER POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN EN LA ENTIDAD

Se elaboraron las nuevas políticas de seguridad digital y seguridad de la información alineadas al plan de desarrollo municipal 2024-2027 y a las normas ISO 27001:2022 e ISO 27002:2022, las cuales fueron expuestas y aprobadas en reunión de comité de gestión y desempeño el 01 de octubre del 2024.

Evidencias:

1. Presentación Unificada Políticas TIC
2. Política Seguridad Digital 2024-2027
3. Política de Seguridad de la Información_2024-2027
4. Citación comité de gestión y desempeño

INDICADOR 05 – IDENTIFICACIÓN DE LINEAMIENTOS DE SEGURIDAD DE LA ENTIDAD

En la vigencia del 2024, se elaboró el documento con los procedimientos de seguridad de la información, el cual fue aprobado por la jefa de la Oficina TIC del primer semestre y por el jefe de la Oficina TIC actual.

Evidencias:

1. Procedimientos de seguridad de la información

INDICADOR 06 – VERIFICACIÓN DEL CONTROL DE ACCESO

Teniendo en cuenta que la descripción de este indicador, hace referencia a establecer lineamientos, el cumplimiento se evidencia en los ítems: 5. Procedimiento de trabajo en áreas seguras y 6. Procedimiento de acceso a la red corporativa.

Evidencias:

1. Procedimientos de seguridad de la información

INDICADOR 07 – ASEGURAMIENTO EN LA ADQUISICIÓN Y MANTENIMIENTO DE SOFTWARE

Teniendo en cuenta que la descripción de este indicador, hace referencia a establecer lineamientos, el cumplimiento se evidencia en los ítems: 7. Procedimiento de instalación de software y 8. Procedimiento de propiedad intelectual y uso legal del software

Evidencias:

1. Procedimientos de seguridad de la información

INDICADOR 08 – IMPLEMENTACIÓN DE LOS PROCESOS DE REGISTRO Y AUDITORÍA

El registro y control de eventos que suceden sobre sistemas, redes y servicios son realizados de acuerdo a las Políticas de seguridad de la información establecidas adoptadas por la entidad, así como la documentación relacionada con la atención de requerimientos/eventos/incidentes de la oficina TIC, basándose en la caracterización de servicios y los respectivos tiempos de respuesta en que se deben atender estos.

INDICADOR 09 – IMPLEMENTACIÓN DE LOS PROCESOS DE REGISTRO Y AUDITORÍA

A nivel de redes se realiza análisis en tiempo real para detectar intentos de explotación de vulnerabilidades en la red, por medio de Sistemas de detección y prevención de intrusos (IDS/IPS), así mismo con el análisis/ escaneo que realiza el antivirus de la entidad, este se encuentra analizando vulnerabilidades y amenazas en tiempo real de servidores y equipos de cómputo.

A nivel de infraestructura de servidores con las actualizaciones de los sistemas de información la cual aplica parches de seguridad a vulnerabilidades encontradas por el fabricante del sistema operativo.

INDICADOR 10 – POLÍTICAS DE PRIVACIDAD Y CONFIDENCIALIDAD

Se encuentra dentro de la política de seguridad de la información en los ítems: 5.6 Política de compromiso de confidencialidad por parte de los funcionarios y 5.7 Política de confidencialidad y seguridad para contratistas.

Evidencias:

1. Política de Seguridad de la Información_2024-2027

INDICADOR 11 – VERIFICACIÓN DE LAS POLÍTICAS DE INTEGRIDAD DE LA INFORMACIÓN

Teniendo en cuenta que este indicador hace referencia a dar respuesta a los siguientes interrogantes: ¿La entidad ha implementado lineamientos contra modificación o pérdida accidental de información? ¿La entidad ha implementado lineamientos, normas y/o estándares para recuperar información en caso de modificación o pérdida intencional o accidental?, dentro de la política de seguridad de la información se encuentra el ítem 5.22 Políticas de gestión de incidentes de seguridad y en los procedimientos de seguridad de la información mediante el ítem 2. Procedimiento para el manejo de la información institucional, se da respuesta a estos interrogantes.

- Evidencias:
- 1. Política de Seguridad de la Información_2024-2027
 - 2. Procedimientos de seguridad de la información

INDICADOR 12 – POLÍTICAS DE DISPONIBILIDAD DEL SERVICIO Y LA INFORMACIÓN

Se verifica que los lineamientos, normas y/o estándares orientados a la continuidad en la prestación de los servicios se cumplan a nivel de la realización de backups de las bases de datos de los sistemas de información alojados en el datacenter.

INDICADOR 14 – PORCENTAJE DE DISPONIBILIDAD DE LOS SERVICIO DE GOBIERNO DIGITAL QUE PRESTA LA ENTIDAD

INDICADOR 15 – PORCENTAJE DE IMPLEMENTACIÓN DE CONTROLES

➤ **MONITOREO A LOS CONTROLES DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN.**

En el Documento "Monitoreo de Riesgos" se revisa el cumplimiento de los controles a los riesgos de Seguridad de la Información.

Riesgo	Descripción del Riesgo	Controles	CUMPLE	NO CUMPLE
1	Posibilidad de pérdida económica y/o reputacional debido a la pérdida o alteración de la información originada por no contar	1. El profesional de gestión del área TIC debe velar por el cumplimiento y socialización de las políticas de seguridad de la información de la entidad.	X	

	con políticas o controles adecuados para proteger la información; o por amenazas tecnológicas emergentes o de ingeniería social que atenten la integridad, seguridad y disponibilidad de la información.	2. Reportar y documentar cada evento que atente ante la seguridad, integridad o disponibilidad de la información.	X	
		3. Utilizar herramientas informáticas de fuentes abiertas que permitan generar caracterización y clasificación de información mediante etiquetado, a través de palabras clave a los elementos de información (como documentos, imágenes y videos), Se pueden usar etiquetas como "alta prioridad", "confidencial" y "sensible"	X	
		4. Mantener copias de seguridad regulares o periódicas de toda la información crítica y sensible, almacenándola en ubicaciones seguras y separadas de los datos originales.	X	
2	Posibilidad de un impacto reputacional y/o económico debido a la carencia de un punto centralizado para trámite de peticiones de servicio técnico por causa del incremento en los tiempos de respuesta y resolución de fallas, falta de trazabilidad o seguimiento en los procesos de soporte iniciados a equipos y componentes, e incapacidad de cumplir los SLA y estándares de servicio	1. Seguimiento y control de reportes a incidentes mediante llamadas a la ext. del jefe de área de las TIC	X	
		2. Emplear módulos de software libre para la gestión en mesa de ayuda, que permita la recepción y asignación de tickets, así como la comprobación de tiempos y casos recurrentes.	X	
3	Probabilidad de un impacto económico y reputacional debido a deficiencia en los sistemas de seguridad informática por causa de controles físicos y	1. Realiza evaluaciones regulares de riesgos para identificar vulnerabilidades en los sistemas y redes.	X	
		2. Establecer políticas de seguridad informática que abarquen áreas como el	X	

	lógicos en equipos perimetrales, infraestructura tecnológica obsoleta, políticas de seguridad de la información, inexistentes o inapropiadas y falta de conocimiento de los profesionales asociados a los procesos de sistemas	uso de contraseñas seguras, acceso a sistemas y redes, manejo de datos sensibles, y responsabilidades del usuario.		
		3. Mantener actualizados los firewalls, sistemas de detección de intrusiones (IDS) y prevención de intrusiones (IPS), y realizar controles de acceso adecuados para proteger las redes internas y externas contra accesos no autorizados y ataques.	X	
		4. Utilizar herramientas de análisis de seguridad para identificar patrones de comportamiento sospechoso y establecer sistemas de monitoreo continuo para detectar actividades anómalas	X	
		5. Desarrollar plan de respuesta a incidentes que incluya procedimientos detallados para manejar y mitigar incidentes de seguridad cibernética	X	
4	Probabilidad de un impacto económico y reputacional con motivo de la ausencia de implementación de la política de gobierno digital y seguridad digital a causa de carencia en implementación de procesos y procedimientos internos seguros, falta de fortalecimiento de las capacidades de gestión de tecnologías de la información y omisión de habilitación y mejora de servicios digitales.	1. Crear y documentar políticas claras de gobierno digital y seguridad digital que definan los estándares y procedimientos para el uso seguro de las tecnologías de la información y comunicaciones (TIC).	X	
		2. Proporcionar capacitación regular sobre seguridad digital y buenas prácticas de gobierno digital a todos los empleados, contratistas y terceros que interactúen con los sistemas de la organización.	X	
		3. "Establecer un plan de respuesta a incidentes que incluya procedimientos detallados para manejar y mitigar las consecuencias	X	

		de un acontecimiento en seguridad."		
--	--	-------------------------------------	--	--

➤ **ACTIVIDADES TRATAMIENTO DE RIESGOS DE SEGURIDAD.**

En el Documento "Plan de Tratamiento de Riesgos" en el numeral 9 se indican las Actividades de tratamiento de riesgos de seguridad.

9. METODOLOGIA

El plan de tratamiento de riesgos contempla la definición de las actividades a desarrollar en aras de mitigar los riesgos sobre los activos, estas actividades se estructuraron de la siguiente manera, siguiendo las recomendaciones de la Guía de Gestión de Riesgos de Seguridad y Privacidad de la Información.

GESTION	ACTIVIDAD	TAREA	RESPONSABLE	FECHA DE INICIO	FECHA DE FIN
Gestión de Riesgos	Actualización de lineamientos de riesgo TIC	Actualizar política y metodología de gestión de riesgos TIC	Equipo de Gestión de Riesgos	Marzo 2024	Marzo 2027
	Sensibilización	Socialización guía y herramienta de gestión de riesgo de seguridad y privacidad de la información, seguridad digital y continuidad de la Operación.	Equipo de Gestión de Riesgos		
	Identificación de riesgos de seguridad y privacidad de la información, seguridad	Identificación, análisis y evaluación de riesgos – seguridad y privacidad de la información, seguridad	Equipo de Gestión de Riesgos	Marzo 2024	Marzo 2027

	digital y continuidad de la operación.	digital y continuidad de la operación.			
		Realimentación, revisión y verificación de los riesgos TIC, identificados (Ajustes)	Equipo de Gestión de Riesgos	Marzo 2024	Marzo 2027
	Aceptación de riesgos identificados	Aceptación, aprobación riesgos TIC identificados y planes de tratamiento	Equipo de Gestión de Riesgos	Marzo 2024	Marzo 2027
	Publicación	Publicación matriz de riesgos TIC	Equipo de Gestión de Riesgos	Marzo 2024	Marzo 2027
	Seguimiento fase de tratamiento	Seguimiento estado planes de tratamiento de riesgos TIC identificados y verificación de evidencias	Equipo de Gestión de Riesgos	Marzo 2024	Marzo 2027
	Evaluación de riesgos residuales	Evaluación de riesgos TIC residuales	Equipo de Gestión de Riesgos	Marzo 2024	Marzo 2027
	Mejoramiento	Identificación de oportunidades de mejora acorde a los resultados obtenidos durante la evaluación de riesgos TIC residuales	Equipo de Gestión de Riesgos	Marzo 2024	Marzo 2027
		Actualización Guía	Equipo de Gestión de	Marzo 2024	Marzo 2027

		gestión de Riesgos Seguridad de la información, de acuerdo a los cambios solicitados	Riesgos		
	Monitoreo y Revisión	Generación, presentación y reporte de indicadores	Equipo de Gestión de Riesgos	Marzo 2024	Marzo 2027

9.1 DESARROLLO METODOLOGICO

Fase 1: Análisis de la información

En esta etapa se evaluarán los resultados de las entrevistas con los colaboradores del proceso de TI, se desarrollarán las siguientes actividades:

Aplicar las políticas de tratamiento de riesgos.

Determinar los controles (se desprenden de las medidas) según los lineamientos del Ministerio TIC.

Determinar los riesgos que van a ser incluidos en el Plan de Tratamiento de Riesgos TIC.

Fase 2: Desarrollo de los proyectos

En esta fase se realizarán las actividades que permitan la estructuración de las medidas.

Determinar el nombre de la medida.

Definir los responsables de cada medida.

Establecer el objetivo de cada medida.

Elaborar la justificación de la medida.

Definir las actividades a realizar para el desarrollo de la medida.

Fase 3: Análisis de los proyectos

Definición de los controles relacionados con cada medida.

Validar los riesgos TIC mitigados por cada medida.

Análisis de la aplicabilidad de las medidas.

Priorización de las medidas.

Fase 4: Definición del organigrama de responsabilidad

En esta fase se realizará un organigrama y se definirán responsabilidades respecto a la administración y gestión del riesgo, esta etapa deberá ser definida por la Alcaldía Municipal de Chía, teniendo en cuenta su estructura organizacional para la gestión de riesgos.

Identificación de las funciones de la Alcaldía Municipal de Chía en materia de seguridad de la información.

Definición del grupo de trabajo de gestión de riesgo por parte de la Alcaldía Municipal de Chía.

Definición de las funciones del grupo de trabajo referentes a la aplicación y gestión de las medidas.

Fase 5: Ciclo de vida del tratamiento de riesgos

Definir las actividades a realizar por cada uno de los elementos del ciclo de vida del Plan de Tratamiento de Riesgo

Planear: Dentro de esta etapa se desarrollan las actividades definidas en la fase 1 de la metodología de tratamiento de riesgos.

Hacer: En este paso del ciclo de vida se desarrollarán las actividades enmarcadas en la fase 2 de la metodología del tratamiento de riesgos.

Verificar: En esta etapa se desarrollarán las actividades que permiten hacer seguimiento o auditorías a la ejecución de cada una de las medidas.

Actuar: Dentro de esta etapa se realizarán las mejoras teniendo en cuenta el seguimiento y los resultados de las auditorías de la ejecución de los proyectos.

➤ **CRONOGRAMA DE CAPACITACIÓN DE SEGURIDAD.**

En la vigencia del 2024, se realizaron programaciones e invitación a todos los funcionarios y contratistas de la alcaldía municipal de Chía, dando a conocer el cronograma establecido y los temas a tratar de la siguiente manera:

- Circular informativa No. 02 del 06 de mayo del 2024, cuyo cronograma con las jornadas de sensibilización se realizaron el 9, 10, 16 y 17 de mayo del 2024. Los temas tratados fueron: Política de gobierno digital, Política de seguridad de información, Procedimientos de Seguridad de la Información, Datos abiertos y se dejó un espacio de preguntas y respuestas.
- Circular informativa No. 006 del 09 de octubre del 2024, cuyo cronograma con las jornadas de sensibilización se realizaron el 22, 23 y 24 de octubre del 2024. Los temas tratados fueron: Política de Gobierno Digital, Política de seguridad digital, Política de seguridad de información y Arquitectura Empresarial

Evidencias:

1. Circular 02 sensibilización - Políticas TI y Datos Abiertos – Mayo
2. Circular 06 sensibilización - Política de TI y arquitectura empresarial – octubre

➤ **REGISTRO DONDE SE ENCUENTRE LOS CONSENTIMIENTOS POR ESCRITO DE LOS TITULARES DE LOS DATOS PARA EL TRATAMIENTO DE DATOS PERSONALES EN LAS DIFERENTES SITUACIONES.**

Dentro de los procesos de consentimiento por parte de los usuarios, nos remitimos en primera instancia a los términos legales, que como lo expresa MinTic: "... Las personas (en adelante Ciudadanos-Usuarios) al acceder, navegar o usar este sitio, reconocen que han leído, entendido y se obligan a cumplir con estos términos, leyes y reglamentos. Si el Ciudadano-Usuario no está de acuerdo con la presente política de privacidad, le sugerimos abstenerse de utilizar este sitio web..."

En el anterior entendido, las aplicaciones que se han generado desde la administración, cuenta con sus políticas de uso y tratamiento de datos, los cuales deben ser aceptados por el usuario para continuar con el uso del servicio digital dispuesto. En caso de no aceptarlo, pues es completa responsabilidad de los usuarios aceptarlos o no, no podría continuar con el uso del servicio, de acuerdo a lo contemplado en la ley.

Para las aplicaciones móviles y usos generales de registros, dichas políticas se encuentran publicadas en el sitio:

<https://chia-cundinamarca.gov.co/chiaapp/index.php>

Igualmente en el uso de la Ventanilla Única Virtual, en el momento de registro se realiza la aprobación de los términos y condiciones, los cuales citan:

TRATAMIENTO DE DATOS PERSONALES (REGISTRO VENTANILLA ÚNICA)**TÉRMINOS Y CONDICIONES**

Al momento de registrarse en la Ventanilla Única Virtual de Trámites y Servicios de la Alcaldía Municipal de Chía puede hacer uso de los diferentes trámites y servicios de la misma teniendo en cuenta los siguientes términos y condiciones, por favor léalos cuidadosamente ya que para continuar con el proceso es necesario aceptarlos (si usted no está de acuerdo con ellos por favor absténgase de continuar con el proceso de registro).

Declaración de privacidad: La ventanilla única virtual de trámites y servicios de la Alcaldía Municipal de Chía, realiza una declaración de privacidad donde garantiza el uso adecuado de los datos personales y la privacidad de los usuarios inscritos en la ventanilla, dado esto para cumplir con lo establecido en la ley estatutaria 1581 de 2012, decreto número 1377 de 2013 de protección de datos personales y basándose en la política de confidencialidad de datos donde se indica lo siguiente: “Para la Alcaldía Municipal de Chía los datos personales son privados y por tal motivo está en la obligación de proteger los datos e información suministrada mediante cifrados y detección de intrusos, para garantizar y asegurar el 90% de la información transmitida; también se recalca que estos datos se les da una categoría de confidencialidad y por esto solo ciertas personas tienen acceso a los datos personales.”

Si el usuario acepta los términos y condiciones, está dando su autorización para el tratamiento de los datos. Basándonos en esta política de confidencialidad es de recalcar que la persona que viole esta declaración de privacidad se verá expuesto a las sanciones infringidas en la ley 1273 de 2009 artículo 269F que indica lo siguiente: “Violación de datos personales. El que, sin estar facultado para ello, con provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique o emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes, incurrirá en pena de prisión de 48 a 96 meses y en multa de 100 a 1.000 salarios mínimos.”

Manejo de contraseñas: Teniendo en cuenta la seguridad de la información la ventanilla única de trámites y servicios no cuenta con la creación de contraseñas, para esto cuenta con un código único que es enviado al correo electrónico inscrito por el usuario para verificar datos y salvaguardar la información suministrada por el usuario.

Propiedad intelectual: La Ventanilla Única Virtual de Trámites y Servicios de la Alcaldía Municipal de Chía cuenta con contenido original y funcionalidades que son de propiedad de la Alcaldía Municipal de Chía y por tal motivo está prohibido la reproducción total o parcial de dicho contenido a través de otro medio analógico o digital en Colombia o cualquier otro país. El usuario debe saber y reconocer que el contenido que está visualizando desde la Ventanilla Única Virtual de Trámites y Servicios son de propiedad de la Alcaldía Municipal de Chía. La Alcaldía Municipal de Chía no se hará responsable por daños que se puedan ocasionar en los dispositivos por causas de terceros o archivos maliciosos.

Modificaciones de la Ventanilla Única Virtual de Trámites y Servicios: La Alcaldía Municipal de Chía tiene los siguientes derechos sobre la Ventanilla Única Virtual de Trámites y Servicios:

- Negar o restringir trámites y servicios a los usuarios.
- Utilizar la información suministrada por los usuarios.
- Modificar el contenido.

Atención al usuario: La Ventanilla Única Virtual de Trámites y Servicios de la Alcaldía Municipal de Chía cuenta con un canal de PQRS para el usuario, así mismo los canales de atención de la Alcaldía Municipal de Chía.

Deberes del usuario: El usuario tiene el deber de utilizar de la mejor forma la Ventanilla Única Virtual de Trámites y Servicios, así mismo se hace responsable de su comportamiento en este sitio. No dar información o datos falsos en la ventanilla única virtual de trámites y servicios para actividades ilegales o no autorizadas tanto en Colombia, como en cualquier otro país.

Por lo anterior, el registro en la base de datos del despliegue de las aplicaciones y demás servicios digitales, se dan en el entendido que los registros existentes, cuentan con la aprobación expresa de los términos de aceptación de los mismos. (El registro de un usuario, es la manera expresa de su aprobación en el uso de los términos y condiciones de uso y tratamiento de la información).

• IDENTIFICACIÓN Y CLASIFICACIÓN DE ACTIVOS DE INFORMACIÓN.

Para la vigencia 2024, se inició el proceso con el envío de la Circular Informativa 004, en la cual se solicitó a las diferentes dependencias un enlace para capacitar y diligenciar la Matriz de Actividad de la Información.

Debido a temas contractuales, el proceso fue retomado en el mes de octubre. Se volvió a enviar la solicitud a las dependencias para que designaran un enlace.

El 6 de noviembre se llevó a cabo una capacitación virtual dirigida a los enlaces asignados también se realizó envío de un correo tanto a las oficinas como a sus enlaces con material de apoyo para el diligenciamiento de la matriz y se estableció como fecha límite para la entrega de la matriz el 29 de noviembre.

A corte del 10 de diciembre, se observa lo siguiente:

Solo 8 oficinas reportaron sus matrices dentro de los tiempos establecidos.

Otras 3 oficinas han presentado sus matrices, incluso después de la fecha límite.

➤ ACUERDOS SUSCRITOS DE CONFIDENCIALIDAD O DE NO DIVULGACIÓN PARA SALVAGUARDAR LA INFORMACIÓN CON ENTIDADES, EMPRESAS O PERSONAL EXTERNO PARA ACCEDER A LA INFORMACIÓN SENSIBLE O CRÍTICA DE LA ENTIDAD.

Desde la Oficina TIC se lidera la proyección de los acuerdos de confidencialidad dirigidos a funcionarios, contratistas personas naturales y jurídicas. En este sentido, se han enviado los borradores iniciales de dichos acuerdos a la Oficina Jurídica para su respectiva revisión, con el propósito de garantizar su cumplimiento normativo y la alineación con los lineamientos legales vigentes.

No obstante, es importante mencionar que la construcción de estos acuerdos requiere un enfoque colaborativo que involucre a diversas áreas de la entidad, ya que su contenido debe reflejar las necesidades particulares de la Oficina de Contratación y Dirección de Función Pública, por ser su competencia las actuaciones hacia los funcionarios y contratistas de la entidad. Por esta razón, se tiene previsto presentar los acuerdos preliminares ante el Comité de Seguridad de la Información, en una sesión programada en el mes de diciembre de 2024.

Cabe resaltar que este comité, establecido mediante el Decreto 545 de 2024, tiene como función principal la coordinación de la implementación del Modelo de Seguridad y privacidad de la información al interior de la entidad. Su participación en este proceso es clave para asegurar que los acuerdos de confidencialidad estén alineados a las necesidades de seguridad y a la normatividad nacional en esta materia.

➤ **CONTROLES REALIZADOS PARA EL CUMPLIMIENTO DE LAS POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN.**

La entidad cuenta con el autodiagnóstico del Modelo de Seguridad y Privacidad de la Información (MSPI) debidamente diligenciado, en el cual se evalúa y documenta el cumplimiento de los controles establecidos en las políticas de seguridad de la información. Este documento permite verificar el grado de adherencia a las políticas, identificar oportunidades de mejora y garantizar que los controles implementados estén alineados con los lineamientos de seguridad establecidos por la organización y las normativas aplicables.

En las hojas llamadas “ADMINISTRATIVAS” y “TÉCNICAS” y en la columna “EVIDENCIA” se describen las evidencias con las que cuenta la entidad para dar cumplimiento a cada uno de los controles del MSPI las cuales corresponden a los 113 controles de la norma ISO 27001:2013.

➤ **REGISTRO DE CONTROLES A LA CREACIÓN, EDICIÓN Y BAJA DE USUARIOS EN LOS SISTEMAS DE INFORMACIÓN EN PRODUCCIÓN.**

La captura de datos es realizada de acuerdo a su aceptación de términos, por los mismos usuarios, quienes son los responsables de la veracidad de los datos que se diligencian en cada una de las diferentes aplicaciones. Es importante destacar que de acuerdo a la arquitectura de base de datos, existe una dependencia de datos exclusiva para los usuarios, para generar de acuerdo a lo dispuesto por el ministerio de las TIC, un único repositorio de usuario donde reposa la información, de acuerdo los ítems de seguridad anteriormente expuestos. Para los procesos de actualización y bajas de usuario, se tiene habilitado los procesos de solicitudes a través del canal ventanillaunicavirtual@chia.gov.co, el cual se evalúa el trámite y se realiza de acuerdo al registro de los datos en el sistema para corroborar la autenticidad de la solicitud. Igualmente, es importante destacar que los datos de contacto pueden ser actualizados por el usuario, desde su sesión, la cual solamente podrá ingresar a través de sus credenciales de acceso, creadas en el momento del registro a las aplicaciones respectivas.

De acuerdo a lo anterior, en el caso de las bajas, el usuario a nivel de base de datos se inactivará mas no eliminará, de acuerdo a las normas técnicas de conservación de historial de datos, respecto a los trámites realizados por la entidad.

➤ **QUE HERRAMIENTA DE ENCRIPCIÓN DE DATOS CUENTA LA ALCALDÍA DE CHÍA.**

1. Que herramienta de encriptación de datos cuenta la Alcaldía de Chía.

Para realizar el proceso de encriptación de datos, no solo se contempla las capas de datos sino también de infraestructura. De acuerdo a lo anterior se realiza la descripción de cada una de ellas:

Protocolo de seguridad a nivel de datos: Para ello, dentro de las estrategias de seguridad implementadas para el desarrollo de aplicaciones, se realiza autenticación por medio de un código único en el registro, con el cual se verifica el acceso al correo diligenciado, además de usuario y contraseña para el ingreso a las

plataformas. La contraseña está encriptada en 3 capas con dos algoritmos (MD5), el cual es una codificación de 128 bits que se compone de 32 caracteres hexadecimales. Igualmente se cuenta con las políticas de contraseñas seguras en las que se definen los lineamientos en longitud de caracteres, tipos de caracteres numéricos, alfabéticos y especiales, caracteres adyacentes, repeticiones, cambios periódicos, entre otros. El almacenamiento de la información se realiza mediante bases de datos divididas por dependencias y procesos para el control de acceso a la información donde la información del usuario se encuentra en un esquema propio con el cual se comunican los demás servicios. La consulta, ingreso y actualización de información se cuentan con el esquema de perfiles asociados a los usuarios, y estos a su vez tienen permisos que habilitan o inhabilitan funcionalidad. Finalmente la comunicación con las bases de datos se realiza por medio de procedimientos almacenados, lo que garantiza que las operaciones se realicen en el servidor, controlando los procesos que se llevan a cabo además de blindar el sistema contra ataques de inyección de código.

Lo anterior, establece que las encriptaciones se realizan a través de programación, que para el particular se realizan en lenguaje PHP V8 y C#.

2. Seguridad desde la capa de infraestructura

La entidad cuenta con herramientas y mecanismos de cifrado de datos que propenden por la seguridad de su infraestructura tecnológica. Entre ellas, se destacan:

Solución de seguridad perimetral:

- Utiliza algoritmos de cifrado avanzados en la configuración de VPN IPsec bajo el protocolo IPsec, la cual crea túneles cifrados en Internet asegurando la confidencialidad e integridad de la comunicación entre la red local y puntos remotos.
- Además, se implementa VPN SSL, que permite conexiones seguras desde dispositivos externos a los recursos internos de la entidad utilizando el protocolo Secure Socket Layer (SSL).

Protocolos de administración segura:

El protocolo SSH (Secure Shell) se utiliza para establecer conexiones cifradas hacia servidores, equipos de red y dispositivos de seguridad, como el UTM (Unified Threat Management). Esto protege las credenciales y los datos transmitidos durante las sesiones de administración de estos dispositivos o equipos.

➤ QUE PROCESO SEGUROS GARANTIZA EL DATACENTER PARA EL RESPALDO DE LA INFORMACIÓN SENSIBLE DE LAS BASES DE DATOS

Desde la Oficina de Tecnología de la Información y las Comunicaciones (TIC) se ha implementado un proceso de custodia y respaldo de las copias de seguridad para los sistemas de la entidad. Con el fin de alinearnos con las mejores prácticas en seguridad de la información, en particular en lo que respecta al almacenamiento de copias de seguridad en ubicaciones externas a la infraestructura donde se ejecutan los aplicativos, se ha establecido un mecanismo de traslado de las copias de seguridad, realizando un respaldo en un ambiente de nube privada proporcionado por la empresa Tigo-Une. Este proceso se realiza mediante una conexión segura a través de una VPN (Red Privada Virtual) site-to-site, que establece un canal cifrado entre la red interna de la entidad y la infraestructura de nube. Adicionalmente, como

medida de control de acceso, se requiere autenticación mediante dirección IP, usuario y contraseña, datos que están restringidos exclusivamente a los profesionales autorizados del datacenter de la entidad.

➤ **QUE PARCHES DE ACTUALIZACIONES DEL SISTEMA OPERATIVO Y OFIMÁTICA SE HAN IMPLEMENTADO O APLICADO**

Para los equipos de la administración que tienen instalado Windows 10, Windows 11 y Windows 8 o 8.1, los parches que se instalan son los proporcionados por Microsoft a través del servicio de Windows Update, los cuales siempre se indica al usuario final que las realice dado que estas actualizaciones no son automáticas siempre esperan la aceptación o descarga por parte del usuario, en cuanto a los equipos que tienen instalado Windows 7 se instalan unos parches descargados de la plataforma de Microsoft que son los Windows6.1-KB2999226 y Windows6.1-KB3138612 los cuales hacen que el sistema operativo se fuerce a actualizar adicional a estos se instala el KB3033929 el cual es un paquete que permite la actualización del antivirus de Microsoft Essenciales para Windows 7 cabe indicar que esta actualizaciones hacen que el equipo entre a descargar las actualizaciones por Windows Update las cuales en muchas ocasiones demoran de 2 a 3 días haciendo este proceso, dado que la cantidad de paquetes es alta, y hay que reiniciar varias veces para que siga con el proceso.

En cuanto a los parches de seguridad de Microsoft Office se realiza igualmente a través del servicio de Microsoft Update, esto cuando el equipo encuentra paquetes de actualización a descargar, e igual a las actualizaciones de sistema operativo estas se realizan de manera manual por parte de los funcionarios que usan los equipos.

➤ **METODOLOGÍA DE DESARROLLO SEGURO DE SOFTWARE.**

El desarrollo seguro es una práctica esencial para garantizar la integridad, confidencialidad y disponibilidad de las aplicaciones. Este documento describe una metodología basada en el desarrollo back-end utilizando Blazor Server y Open PHP con enfoque en el testing, la documentación técnica y las mejores prácticas de seguridad.

Desarrollo Back-End con Blazor Server

Arquitectura y Tecnologías

Lenguaje: C#

- Framework: Blazor Server
- Base de datos: SQL Server 2019
- Modelo: API REST
- Metodología: SCRUM
- Framework CSS: Bootstrap

Prácticas de Seguridad

1. Validación y sanitización de entradas: Asegurar que todas las entradas sean válidas y estén libres de contenido malicioso.

2. Gestión segura de credenciales: Uso de Identity Server para autenticar usuarios validando por número de documento y contraseña en BD.
3. Cifrado de datos sensibles: Método EncryptSHA512 para cifrar información confidencial (contraseñas).
4. Uso de sesiones: Se maneja un inicio de sesión único por usuario, el cual permite la generación de trámites para el ID del usuario registrado en BD.
5. Actualización continua: Asegurar que el framework Blazor Server y las dependencias estén actualizados.

Testing

Se debe emplear una combinación de pruebas automatizadas y manuales:

- Testeo en local: para verificar la funcionalidad del código.
- Pruebas de integración: para asegurar la correcta interacción entre componentes.
- Pruebas de seguridad: utilizando herramientas como OWASP ZAP para identificar vulnerabilidades.

Desarrollo Back-End con Open PHP y MVC

Arquitectura y Tecnologías

- Lenguaje: PHP 8.2
- Framework: MVC personalizado
- Base de datos: MySQL 5.2 y 8.1
- Metodología: SCRUM
- Framework CSS: Bootstrap

Prácticas de Seguridad

1. Uso de prepared statements: Evitar inyecciones SQL mediante el uso de PDO o MySQLi.
2. Gestión de sesiones: Asegurar que las sesiones sean seguras utilizando cookies marcadas como HttpOnly y Secure.
3. Protección contra XSS y CSRF: Implementar tokens CSRF y escapar datos en vistas.
4. Control de acceso: Aplicar políticas de autorización basadas en roles y privilegios mínimos.
5. Registro y monitoreo: Implementar un sistema de logs seguro para rastrear eventos críticos.

Testing

El enfoque de pruebas para PHP incluye:

- Pruebas unitarias utilizando PHPUnit.
- Pruebas funcionales para validar interacciones del usuario.
- Pruebas de carga para evaluar el rendimiento de la aplicación bajo estrés.

Documentación Técnica

La documentación técnica debe ser clara, estructurada y mantener la trazabilidad del desarrollo. Para la definición de los requerimientos, nos basamos en la descripción del estándar ISO/EIC/IEEE 29148 de Ingeniería de Requisito Recomendaciones:

- Crear diagramas UML para ilustrar la arquitectura del sistema.
- Mantener un registro de versiones y cambios en el código.

Esta metodología proporciona un enfoque sólido para el desarrollo seguro, abarcando prácticas clave en seguridad, pruebas y documentación. La implementación rigurosa de estas estrategias asegura la entrega de aplicaciones confiables y robustas.

➤ CUALES SON LOS PROVEEDORES DE TI.

De acuerdo a los procesos contractuales realizados en la actual vigencia, se establecen como proveedores de servicios de TI, los correspondientes a Servicio de Internet, Almacenamiento en la Nube privada, servicio de Hosting de Almacenamiento de página institucional, servicio de proveedores de servicios de comunicación (cuentas de correo electrónico), dentro de los que tenemos :

Item	Tipo de Servicio	Proveedor	Nit del Proveedor
1	Servicio de Internet Dedicado	UNE EPM TELECOMUNICACIONES S.A	900092385
2	Servicio de Icloud (Nube Privada)	UNE EPM TELECOMUNICACIONES S.A	900092385
3	Servicio de comunicación móvil	COLOMBIA MOVIL S.A. ESP.	830114921
4	Servicio de Hosting	CREAR IMAGEN S.A.S.	900457310
5	Servicio de Correo electrónico	Electrocom S.A.S.	800229279

➤ REVISIONES PERIÓDICAS AL CUMPLIMIENTO DE LAS POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN A LOS PROVEEDORES.

Dentro de los procesos de políticas de seguridad y privacidad de la información, el seguimiento a proveedores está acompañado en primera instancia desde el aspecto contractual, donde en los contratos establecidos se especifican dentro de las obligaciones del contrato “Garantizar la confidencialidad de la información obtenida con ocasión de la labor de supervisión de la red.”, las cuales especifican el cumplimiento de las políticas de seguridad y privacidad de la información, en las que en los cumplimiento contractuales realizados a través de los formatos de GEC-FT-62-V3 (Informe de Supervisión), se realiza la validación del cumplimiento de las obligaciones, a través de informes presentados donde se especifican las acciones propias de cada uno de los proveedores. Igualmente, de los servicios TI de proveedores, se solicitan las consolas de administración que permiten el total control de las cuentas y acceso a la información, aplicando también las políticas

de los grandes prestadores de servicios como en el caso de Microsoft, donde a través de TEMUT, (Administración de aplicaciones), se realiza y conserva la información. En el caso puntual de la información asociada a los correos electrónicos, desde el administrador no es posible por políticas no solo contractuales entre la administración y proveedores, sino del fabricante (en éste caso Microsoft), no es posible el acceso a la información de ninguna cuenta así como de sus cuentas OneDrive, por lo que se garantiza la privacidad de la información. Es importante destacar que con pruebas constantes y control de accesos, se verifica la no intrusión a los datos de la administración.

➤ **CUAL ES MÉTODO DE REPORTE DE EVENTOS E INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN.**

En el Documento "Procedimientos de seguridad de la información en el numeral 1 se indica el Procedimiento para reportar incidentes de seguridad de la información.

1. PROCEDIMIENTO PARA REPORTAR INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

Objetivo:

Gestionar de manera adecuada los eventos, incidentes y vulnerabilidades de seguridad de la información en la Alcaldía Municipal de Chía con el fin de prevenir y limitar su impacto.

Aplicabilidad:

Este procedimiento debe ser aplicado por la alta dirección, secretarios, jefes, funcionarios y contratistas de la Alcaldía Municipal de Chía, es responsabilidad de los usuarios cumplir con los procedimientos de seguridad informática.

Identificación del incidente:

Cualquier persona que detecte un incidente de seguridad de la información debe reportarlo de inmediato. Los incidentes pueden incluir, pero no se limitan a, accesos no autorizados, malware, pérdida de datos, o cualquier actividad sospechosa que pueda comprometer la seguridad de la información.

1.1 Notificación inmediata

El incidente debe ser reportado de manera oportuna a la Oficina de Tecnologías de la Información y las Comunicaciones (TIC) utilizando los medios establecidos para la comunicación de incidentes (p.ej., el formulario en línea, correo electrónico, teléfono de Oficina TIC). De acuerdo a lo establecido en la mesa de ayuda.

1.2 Recolección de evidencia

El usuario que reporta debe proporcionar toda la información y evidencia relevante sobre el incidente. Esto puede incluir screenshots, registros de sistema, descripciones detalladas del incidente, y cualquier otra información que pueda ayudar en la investigación y resolución del mismo.

1.3 Documentación de incidentes

La Oficina TIC debe documentar todos los detalles del incidente, incluyendo la descripción, la evidencia recopilada, la fecha y hora del incidente, y las personas involucradas o afectadas, a través de la plataforma de gestión de la mesa de ayuda.

1.4 Registro de incidentes

Mantener un registro actualizado de todos los incidentes de seguridad, vulnerabilidades y eventos reportados, junto con su respectiva solución y seguimiento.

1.5 Evaluación y respuesta

La Oficina TIC evaluará la gravedad del incidente y determinará las medidas necesarias para mitigar el incidente y prevenir futuras ocurrencias. Esto puede incluir la actualización de software, el cambio de contraseñas, y la implementación de controles adicionales de seguridad.

1.6 Comunicación con entidades de control

Dependiendo de la naturaleza y gravedad del incidente, la Oficina TIC será la única autorizada para contactar con las entidades de control pertinentes (ColCert y/o CSIRT) para reportar el incidente y obtener asistencia adicional si es necesario.

1.7 Revisión y mejora

Una vez resuelto el incidente, se debe realizar una revisión post-incidente para evaluar la respuesta y mejorar las políticas y procedimientos de seguridad basados en las lecciones aprendidas y generar un plan de mejora.

Este procedimiento establece un marco claro para la gestión de incidentes de seguridad de la información en la Alcaldía Municipal de Chía, asegurando una respuesta coordinada y eficaz que protege los activos informativos y reduce el impacto de los incidentes de seguridad.

➤ **CAPACITACIONES O SENSIBILIZACIONES REALIZADAS EN SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN.**

En la vigencia del 2024, se realizaron 8 jornadas de sensibilizaciones, distribuidas de la siguiente manera:

- Mayo 09 del 2024, en la sala de gobierno
- Mayo 10 del 2024, en el auditorio del palacio municipal
- Mayo 16 del 2024, en el punto vive digital – piso 1
- Mayo 17 del 2024, en la sede Curubito – sala piso 2
- Octubre 22 del 2024 – jornada 9 a 11 am, en el auditorio del palacio municipal
- Octubre 22 del 2024 – jornada 3 a 5 pm, en el punto vive digital – piso 1
- Octubre 23 del 2024, salón acción social sede gobierno
- Octubre 24 del 2024, en la sede Curubito – sala piso 2

Evidencias:

1. Listado asistencia sensibilizaciones mayo 2024
2. Listado asistencia sensibilizaciones octubre 2024



➤ **PROGRAMACIÓN Y EJECUCIÓN DE MANTENIMIENTOS PREVENTIVOS Y CORRECTIVOS A LOS RECURSOS TECNOLÓGICOS EN TODOS LOS PROCESOS DE LA ALCALDÍA.**

Dada la programación por la oficina TIC según la circular informativa No. 001 del 30 de mayo del 2024 se dejó estipulado el siguiente cronograma.

SEDE - DEPENDENCIAS	JUNIO 2024
<ul style="list-style-type: none">✓ Dirección de ordenamiento territorial✓ Secretaría de salud✓ Secretaría de educación✓ Secretaría para el desarrollo económico✓ Consejo territorial de planeación	1, 2,3 y 4 semana
SEDE - DEPENDENCIAS	JULIO 2024
<ul style="list-style-type: none">✓ Secretaría de gobierno✓ Secretaría de participación ciudadana y acción comunitaria✓ Oficina de prensa✓ Oficina TIC✓ Secretaría de medio ambiente✓ Dirección de acción social	1,2 y 3 semana
<ul style="list-style-type: none">✓ Secretaría general✓ Oficina de control interno✓ Despacho alcaldía✓ Secretaría de hacienda✓ Oficina asesora jurídica✓ Oficina de contratación✓ Datacenter	1, 2,3 y 4 semana
SEDE - DEPENDENCIAS	AGOSTO 2024
<ul style="list-style-type: none">documental)✓ Dirección centro de atención al ciudadano (Paco 1 y 2)	1, 2,3 y 4 semana
<ul style="list-style-type: none">✓ Control interno disciplinario✓ Almacén general	
<ul style="list-style-type: none">✓ Secretaría de obras públicas✓ Secretaría de movilidad	1, 2,3 y 4 semana
SEDE - DEPENDENCIAS	SEPTIEMBRE 2024
<ul style="list-style-type: none">✓ Central de emergencias✓ Inspección quinta de policía✓ Comisaría segunda de familia	1 y 2 semana
<ul style="list-style-type: none">✓ Biblioteca Hoqabiga✓ Punto vive digital✓ Secretaría de desarrollo social	1, 2,3 y 4 semana
<ul style="list-style-type: none">✓ Casa de justicia Centro	1, 2,3 y 4 semana

No se logró iniciar en las fechas estipuladas por falta de personal técnico y de elementos necesarios para realizar los mantenimientos preventivos, elementos tales como pasta térmica pero después de tener el personal y que llegaran los elementos necesarios se inició el proceso de los mantenimientos preventivos, lo que resume lo siguiente:

Dependencia	Cantidad
Agencia pública de empleo	7
Casa de la Mujer	18
CTP	2
Dirección Administrativa y Financiera	2
Dirección Centro de Atención al Ciudadano	2

Dirección de Desarrollo Agropecuario y Empresarial	19
Dirección de Gestión y Fomento a la Educación – Calidad	8
Dirección de Gestión y Fomento a la Educación – FOES	5
Dirección de Inspección y Vigilancia	7
Dirección de Ordenamiento Territorial y Plusvalía "DOT"	14
Dirección de Salud Pública	9
Dirección de Urbanismo	23
Dirección de Vigilancia y Control	12
Inspección Quinta de Policía	4
Comisaria Segunda de Familia	6
Central de Emergencias 123	7
Plaza de Mercado	2
Secretaría de educación	21
Secretaría de salud	16
Terminal de Transporte	6

Dando como un total hasta el momento de 190 equipos intervenidos con mantenimientos preventivos.

Atendiendo las solicitudes provenientes de los funcionarios de la Administración Municipal ante alguna falla a nivel de hardware o software que llegaran a presentar los equipos de cómputo. Se han atendido hasta el 30 de noviembre **433** solicitudes las cuales han sido resueltas satisfactoriamente. Se resaltan los casos atendidos en la Biblioteca HOQABIGA asociados a los equipos de cómputo de consulta, como también los casos en el Punto Vive Digital asociados a los equipos de cómputo donde se dictan cursos de ofimática básica, media y avanzada entre otros, elementos que son usados por la comunidad de Chía.

La instalación de 1 memoria RAM de 8 GB en la oficina de Servicios públicos.

➤ **REGISTRO DEL CONTROL DE LAS AUTORIZACIONES DE ACCESO A UN SISTEMA DE INFORMACIÓN O A LA RED INFORMÁTICA INSTITUCIONAL DE LOS SERVIDORES PÚBLICOS Y CONTRATISTAS.**

Los sistemas de Información tales como Hasnet, Corrycom, Kawak, entre otros, cuentan con sus respectivos administradores, los cuales son de las áreas funciones de cada sistema de información, estas personas son los encargados de crear y asignar contraseñas y por ende son los responsables del acceso a dichos sistemas, así como la dada de baja de los usuarios una vez finalice la vinculación laboral con la entidad ya sean funcionarios o contratistas.

En lo relacionado con el acceso a la red informática institucional se tienen protocolos de acceso a través de la asignación de una dirección IP única para cada equipo de cómputo que le permite la navegación. Adicionalmente se cuenta con un archivo donde se registran los datos del computador, placa, dirección MAC de la tarjeta de red, nombre del funcionario, dependencia e ip asignada. Por ello sin este parámetro es imposible el acceso a la red, lo que me permite a la oficina TIC tener el control de las conexiones alámbricas.

En cuanto al control de las conexiones Wifi, el proceso de control y autenticación de estas se realiza por medio del portal cautivo, en nuestro caso este portal es administrado desde el dispositivo de seguridad perimetral – UTM de la entidad. Este proceso inicia desde la solicitud formal de la conexión la cual es realizada por el jefe de la oficina con la necesidad, una vez validada la vinculación del usuario con la

entidad, así como el propósito de este acceso, se procede con la creación de un usuario y contraseña específico para cada persona que solicita acceso, se realiza la asignación de permisos y grupos dentro de la plataforma de administración y se procede a informar al usuario como debe ser la forma de conexión.

Al conectarse, el usuario es dirigido al portal cautivo, donde debe aceptar los términos y condiciones para proceder con la conexión. Es importante tener en cuenta que el dispositivo UTM de la entidad, que administra el portal cautivo, realiza un monitoreo constante de las conexiones. Esto permite visualizar información clave como el usuario conectado, la dirección IP asignada, el consumo de ancho de banda y los sitios web visitados durante la sesión en la red, estableciendo así registro, control y monitoreo de las conexiones a la red.

➤ **QUE MECANISMOS O HERRAMIENTAS HAY PARA LA DEVOLUCIÓN DE LOS ACTIVOS DE INFORMACIÓN ASIGNADOS A CARGO DE LOS SERVIDORES PÚBLICOS Y CONTRATISTAS UNA VEZ FINALICE LA RELACIÓN CONTRACTUAL CON LA ENTIDAD.**

Los lineamientos establecidos sobre la gestión de los activos de información se encuentran detallados dentro de la política de seguridad de la información en el ítem: 5.10 Política gestión de activos de información, sub-item: 5.10.5 Devolución de activos de información

Evidencia:

1. Política de Seguridad de la Información_2024-2027

➤ **LA ENTIDAD CUENTA CON CENTRO DE OPERACIONES DE SEGURIDAD SOC**

El SOC (Security Operations Center) es un equipo interno o subcontratado de profesionales de seguridad de TI dedicados a monitorizar 24x7 toda la infraestructura informática de la organización. Su misión es detectar, analizar y responder a incidentes de seguridad en tiempo real. En este sentido, la Alcaldía Municipal de Chía no cuenta con este servicio tal como está descrito aquí, sin embargo, es necesario tener en cuenta que si se realiza monitoreo de las conexiones y actividades de red por medio del dispositivo de seguridad perimetral UTM de la entidad. Este monitoreo incluye entre otros:

- Análisis de tráfico de red
- Identificación de posibles amenazas y el registro de eventos relacionados con la seguridad, como intentos de acceso no autorizados.
- Consumo de ancho de banda
- Control de aplicaciones y filtrado web
- Detección de amenazas avanzadas por medio de motor de inspección profunda de paquetes (DPI) y el sistema de prevención de intrusos (IPS).
- Supervisión de conexiones en VPN

Estas funcionalidades son consultadas por medio de logs y reportes centralizados, proporcionando una supervisión y control para la protección de la infraestructura informática municipal.

- **LISTADO DE CONTACTOS DE ENTIDADES REGULADORAS, AUTORIDADES Y ORGANISMOS CON CONOCIMIENTO Y EXPERTICIA EN SEGURIDAD DE LA INFORMACIÓN, A LOS CUALES SE PUEDA ACUDIR EN CASO DE UN INCIDENTE DE SEGURIDAD DE LA INFORMACIÓN.**

Grupo de Interés	Correo Electrónico	Teléfono
Comando Conjunto Cibernético (CCOC) - Infraestructura crítica	contacto@ccoc.mil.co	57 (1) 2216336
Ministerio de Tecnologías de la Información y las comunicaciones	minticresponde@mintic.gov.co https://www.mintic.gov.co/portal/inicio/	601 344 34 60 601 692 89 99
CSIRT-CCIT – Centro de Coordinación Seguridad Informática Colombia	https://cc-csirt.policia.gov.co csirt@ccit.org.co	(571) 5159090 / 5159586 601 6207799
ColCERT – Grupo de Respuesta a Emergencias Cibernéticas en Colombia	contacto@colcert.gov.co	601 2959897 601 3442222
Centro Cibernético Policial	https://www.ccp.gov.co/	601 5159711
FIRST (Forum of Incident Response and Security Teams)	first-sec@first.org	

- **PROCEDIMIENTO Y/O PLAN DE RESPUESTA A INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN, EN EL CUAL SE CONTEMPLAN CADA UNA DE LAS FASES DE ATENCIÓN DE UN INCIDENTE (PREPARACIÓN, DETECCIÓN Y ANÁLISIS, CONTENCIÓN, ERRADICACIÓN, RECUPERACIÓN Y ACTIVIDAD POSTINCIDENTE)**

En el Documento “Protocolo MDS” en el numeral 2.4 se indica cómo se da respuesta a los incidentes de seguridad de la Información.

2.4 Gestión seguridad de la información

Corresponden al cuarto nivel de atención, escalado al equipo que hace parte del comité institucional de seguridad de la información, quienes realizarán la gestión requerida o escalamiento a los entes nacionales ColCERT o CSirt, según sea el caso y serán los facilitadores en todo el proceso de investigación a que haya lugar.

Corresponden al presente ítem, sin limitarse a ello:

- Uso inadecuado de la información institucional
- Uso inadecuado de datos personales
- Fuga de información
- Acceso no autorizado a un recurso TIC de forma remota o física
- Manipulación inadecuada de los activos de información
- Uso inadecuado de credenciales de acceso a plataformas de la alcaldía municipal de Chía y/o a los equipos de cómputo, servidores y demás activos de información



- Equipo informático de usuario desatendido
- Pérdida o robo de los recursos TIC
- Distribución no autorizada, robo o pérdida de la información
- Infección única o masiva con software malicioso como virus, gusanos, troyanos, ransomware, rootkits, etc.
- Cambios o daños físicos no autorizados en los recursos TIC y en el sistema
- Abuso indiscriminado en los permisos concedidos a la información y recursos TIC.
- Accesos a los recursos TIC para realizar envíos masivos de phishing
- Incumplimiento a las políticas de seguridad de la información y seguridad digital, establecidas en la alcaldía municipal de Chía
- Cualesquiera otros eventos que puedan vulnerar los recursos TIC.

En la herramienta de gestión debe quedar registrada toda la trazabilidad de los incidentes, siguiendo el presente protocolo:

- El responsable de Seguridad se encargará de gestionar el registro de incidentes.
- Los incidentes serán registrados incluyendo al menos:
 - a. Fecha, hora y lugar de detección del incidente.
 - b. Categorización del incidente por su gravedad.
 - c. Lista de recursos TIC afectados.
 - d. Posible causa del incidente.
 - e. Acciones realizadas para resolver el incidente y la identificación del personal que las originó.
 - f. El registro de incidentes servirá para una retroalimentación para una mejora continua en la seguridad de la información de la alcaldía municipal de Chía
 - g. Se capacitará al personal para concientizarlos sobre la seguridad de la información, en detección y reporte de incidentes encontrados.

GUSTAVO CARVAJA MILLAN
Jefe Oficina TIC

Elaboró: Cindi Yuliet Latorre Bernal-Contratista-Oficina TIC
Revisó: Ing. Gustavo Carvajal Millán – Jefe de Oficina TIC