MAPA DE RIESGO								
PROCESO: Tecnologías de la información y las comunicaciones								
OBJETIVO DEL PROCESO: Dotar a la Alcaldía de tecnología de punta para la información y la comunicación en todos los procesos, con el propósito de mejorar la gestión y obtener resultados en menor tiempo y con mayor calidad. Responder y administrar el sistema integrado de información que requiere la Alcaldía para el desarrollo eficiente de todos sus procesos. Garantizar que cada uno de los integrantes o personal asignado a los procesos asimile la tecnología, la utilice adecuadamente para desarrollar sus actividades y compromisos laborales. Propender por la creación de una cultura y conciencia para aplicar, utilizar, adaptar, aprovechar y darle adecuado y buen uso a las tecnologías. Asimismo, lograr más y mejores recursos tecnológicos y de conectividad para la ciudadanía del Municipio de Chía.								
RIESGO	**CALIFICACIÓN**		**CONTROLES**	**NUEVA CALIFICACIÓN**		**ACCIONES**	**RESPONSABLE**	**INDICADORES**
	PROBABILIDAD	**IMPACTO**		**PROBABILIDAD**	**IMPACTO**			
R-42 Alteración de base de datos	4	5	Procedimientos para la gestión de acceso de los usuarios.	4	5	1. Elaborar e implementar procedimiento de gestión de acceso de los usuarios, donde se establezca el registro y cancelación de usuarios, la asignación de los permisos o roles para el ingreso a las aplicaciones o sistemas de información y la revisión de los derechos de acceso, perfiles y roles de los usuarios en las aplicaciones o sistemas de información.	Oficina de las tecnologías de la información y comunicaciones.	· Número de acceso a aplicaciones, sistemas de información y equipos de cómputo vs accesos anormales. · Número de mantenimientos realizados vs Número de mantenimientos programados. · Contraseñas actualizadas vs contraseñas genéricas. · Permisos y roles de usuarios vs permisos y roles de usuarios inscritos.
R-43 Falla de seguridad	2	4	Procedimiento para la protección de los sistemas contra código malicioso. Lineamiento general para realizar pruebas de seguridad, funcionamiento y aceptación de las aplicaciones o sistemas de información empleados en las diferentes dependencias de la alcaldía municipal de Chía. Establecer una política de control de acceso físico a las instalaciones	2	4	1. Elaborar e implementar procedimiento para la protección de los aplicativos y sistemas de información en contra de código malicioso. 2. Lineamiento para realizar las respectivas pruebas de seguridad, funcionamiento y aceptación de las aplicaciones y sistemas de información. 3. Establecer una política de control de acceso físico a las instalaciones	Oficina de las tecnologías de la información y comunicaciones	· Vulnerabilidades detectadas vs vulnerabilidades establecidas. · Accesos autorizados a la dependencia vs total de accesos a la dependencia.
R-44 Pérdida de información	3	5	Procedimiento establecido para la actualización y mantenimiento de los equipos de cómputo. Procedimiento general para el ingreso seguro y sistema de gestión de contraseñas en los equipos de cómputo, aplicaciones y sistemas de información de la alcaldía municipal de Chía.	2	4	1. Elaborar e implementar un procedimiento para el ingreso seguro y sistema de gestión de contraseñas en los equipos de cómputo, aplicaciones y sistemas de información.	Oficina de las tecnologías de la información y comunicaciones	· Contraseñas actualizadas vs contraseñas genéricas. · Número de personal vinculado vs personal informado y con contraseña diferente a la genérica
R-45 Alteración de usuarios y contraseñas	4	5	Lineamiento para la gestión de contraseñas.	3	4	1. Elaborar e implementar lineamiento para la gestión de contraseñas en las aplicaciones, sistemas de información y equipos de cómputo.	Oficina de las tecnologías de la información y comunicaciones	· Número de personal vinculado vs personal informado y con contraseña diferente a la genérica. · Contraseñas actualizadas vs contraseñas genéricas.
R-46 Acceso no autorizado a los sistemas	2	4	Política de control de acceso. política de escritorio y pantalla limpia, lineamiento para asegurar el bloqueo de pantallas de equipo de cómputo desatendidos.	2	4	1. Elaborar e implementar una política de control de acceso, donde se establezca un procedimiento para el ingreso seguro, cifrado y gestión de contraseñas, procedimiento para el acceso, privilegios de usuarios y la revisión periódica de los derechos de acceso de usuarios. 2. Implementar política de escritorio y pantalla limpia.	Oficina de las tecnologías de la información y comunicaciones	· Número de equipos bloqueados, pantallas y escritorios limpios vs número de equipos de la alcaldía municipal de Chía. · Permisos y roles de usuarios vs permisos y roles de usuarios inscritos. · Accesos autorizados a la dependencia vs total de accesos a la dependencia
R-47 Pérdida económica	3	5	Lineamiento para la gestión de contraseñas.	3	5	1. Elaborar e implementar un lineamiento para la gestión de contraseñas dentro de las aplicaciones, sistemas de información y equipos de cómputo, donde se exija la robustez de las contraseñas y se controle el cambio periódico de las contraseñas.	Oficina de las tecnologías de la información y comunicaciones	· Número de personal vinculado vs personal informado y con contraseña diferente a la genérica
R-48 Penetración a los sistemas	4	5	Lineamiento para la gestión de contraseñas.	4	5	1. Elaborar e implementar un lineamiento para la gestión de contraseñas dentro de las aplicaciones, sistemas de información y equipos de cómputo, donde se exija la robustez de las contraseñas y se controle el cambio periódico de las contraseñas.	Oficina de las tecnologías de la información y comunicaciones	· Número de personal vinculado vs personal informado y con contraseña diferente a la genérica. · Contraseñas actualizadas vs contraseñas genéricas.

R-49 Alteración de la información	3	5	Procedimientos para la gestión de acceso de los usuarios.	3	5	1. Elaborar e implementar un procedimiento para la gestión de acceso de los usuarios, donde se establezca el registro y cancelación de usuarios, la asignación de los permisos o roles para el ingreso a las aplicaciones o sistemas de información y la revisión de los derechos de acceso, perfiles y roles de los usuarios en las aplicaciones o sistemas de información.	Oficina de las tecnologías de la información y comunicaciones	· Número de acceso a aplicaciones, sistemas de información y equipos de cómputo vs accesos anormales · Contraseñas actualizadas vs contraseñas genéricas · Permisos y roles de usuarios vs permisos y roles de usuarios inscritos.
R-50 Alteración de la información	3	5	Lineamiento para la gestión de contraseñas.	3	5	1. Elaborar e implementar lineamiento para la gestión de contraseñas dentro de las aplicaciones, sistemas de información y equipos de cómputo, donde se exija la robustez de las contraseñas y se controle el cambio periódico de las contraseñas.	Oficina de las tecnologías de la información y comunicaciones	· Número de personal vinculado vs personal informado y con contraseña diferente a la genérica · Contraseñas actualizadas vs contraseñas genéricas.
R-51 Daños del sistema	4	5	Política para realizar copias de seguridad o respaldo de la información almacenada en los servidores de la alcaldía municipal de Chía. Procedimiento para el registro de eventos de ingresos y cambios en servidores y equipos de cómputo.	3	4	1. Elaborar e Implementar política para realizar copias de seguridad o respaldo de la información almacenada en los servidores de la alcaldía municipal de Chía. 2. Elaborar e implementar procedimiento para el registro de eventos de ingresos y cambios en servidores y equipos de cómputo.	Oficina de las tecnologías de la información y comunicaciones	· Copias de seguridad realizadas vs copias de seguridad programadas · Cambios y eventos registrados vs total de cambios y eventos
R-52 Daños del sistema por borrado de información	4	5	Procedimientos para la gestión de acceso de los usuarios. Establecer una política de control de acceso físico a las instalaciones	4	5	1. Elaborar e implementar procedimientos para la gestión de acceso de los usuarios, donde se establezca el registro y cancelación de usuarios, la asignación de los permisos o roles para el ingreso a las aplicaciones o sistemas de información y la revisión de los derechos de acceso, perfiles y roles de los usuarios en las aplicaciones o sistemas de información. 2. Establecer una política de control de acceso físico a las instalaciones	Oficina de las tecnologías de la información y comunicaciones	· Accesos autorizados a la dependencia vs total de accesos a la dependencia. · Número de acceso a aplicaciones, sistemas de información y equipos de cómputo vs accesos anormales · Contraseñas actualizadas vs contraseñas genéricas · Permisos y roles de usuarios vs permisos y roles de usuarios inscritos.
R-53 Denegación de servicios	3	4	Procedimiento para implementar controles contra código malicioso, en desarrollo de software, además de la toma de conciencia por parte de los usuarios.	3	4	1. Elaborar Procedimiento para implementar controles contra código malicioso, en desarrollo de software, además de la toma de conciencia por parte de los usuarios.	Oficina de las tecnologías de la información y comunicaciones	· Vulnerabilidades detectadas vs vulnerabilidades establecidas.
R-55 código malicioso	2	4	Procedimiento para implementar controles contra código malicioso, en desarrollo de software, además de la toma de conciencia por parte de los usuarios.	2	4	1. Elaborar procedimiento para implementar controles contra código malicioso, en desarrollo de software, además de la toma de conciencia por parte de los usuarios.	Oficina de las tecnologías de la información y comunicaciones	· Vulnerabilidades detectadas vs vulnerabilidades establecidas.
R-57 Caída de los sistemas	2	3	procedimiento para realizar las respectivas pruebas de seguridad en los sistemas, servicios o aplicaciones de la alcaldía municipal de Chía	2	3	1. Elaborar e implementar procedimiento para realizar las respectivas pruebas de seguridad en los sistemas, servicios o aplicaciones de la alcaldía municipal de Chía	Oficina de las tecnologías de la información y comunicaciones	· Pruebas documentadas vs pruebas realizadas.
R-58 Caída de los sistemas	3	4	Realizar la verificación y monitoreo de la autonomía de las UPS de la alcaldía municipal de Chía, procedimiento para el registro de eventos o logs de los servidores, sistemas de información, aplicaciones y equipos de cómputo.	3	4	1. Realizar la verificación y monitoreo de la autonomía de las UPS de la alcaldía municipal de Chía. 2. Procedimiento para el registro de eventos o logs de los servidores, sistemas de información, aplicaciones y equipos de cómputo.	Oficina de las tecnologías de la información y comunicaciones Obras públicas	· Número de ups vs ups monitoreadas · Cambios y eventos registrados vs total de cambios y eventos

R-59 Indisponibilidad de los sistemas	4	4	Política de control de acceso. Controles de detección y prevención para la protección contra los códigos maliciosos. Política de control de acceso físico a las instalaciones	4	4	1. Diseñar e implementar una política de control de acceso donde se documenten los procesos de acceso seguro a aplicaciones, permisos en red, logs de acceso y modificación de usuarios y contraseñas en el directorio activo; además un procedimiento para el acceso y privilegios de usuarios. 2. Controles de detección y prevención para la protección contra los códigos maliciosos. 3. Establecer una política de control de acceso físico a las instalaciones	Oficina de las tecnologías de la información y comunicaciones	· Número de acceso a aplicaciones, sistemas de información y equipos de cómputo vs accesos anormales y no documentados. · Vulnerabilidades detectadas vs vulnerabilidades establecidas. · Accesos autorizados a la dependencia vs total de accesos a la dependencia
R-61 Destrucción de equipos	4	5	Realizar la verificación y monitoreo de la autonomía de las UPS de la alcaldía municipal de Chía, procedimiento para el registro de eventos o logs de los servidores, sistemas de información, aplicaciones y equipos de cómputo. Diseñar y aplicar un plan de protección física contra desastres naturales, ataques maliciosos o accidentes y un lineamiento sobre la seguridad física en las instalaciones, oficinas y recintos de cada sede de la alcaldía municipal de chía.	4	5	1. Realizar la verificación y monitoreo de la autonomía de las UPS de la alcaldía municipal de Chía. 2. Procedimiento para el registro de eventos o logs de los servidores, sistemas de información, aplicaciones y equipos de cómputo. 3. Diseñar y aplicar un plan de protección física contra desastres naturales, ataques maliciosos o accidentes y un lineamiento sobre la seguridad física en las instalaciones, oficinas y recintos de cada sede de la alcaldía municipal de chía.	Oficina de las tecnologías de la información y comunicaciones. Jefe, director o secretario de cada dependencia o secretaria.	· Número de ups vs ups monitoreadas. · Cambios y eventos registrados vs total de cambios y eventos
R-62 Acceso no autorizado	3	4	Diseñar e implementar una política de control de acceso donde se documenten los procesos de acceso seguro a aplicaciones, permisos en red, logs de acceso y modificación de usuarios y contraseñas en el directorio activo; además un procedimiento para el acceso y privilegios de usuarios; y procedimiento para la revisión de los derechos de acceso de usuarios.	3	4	1. Diseñar e implementar una política de control de acceso donde se documenten los procesos de acceso seguro a aplicaciones, permisos en red, logs de acceso y modificación de usuarios y contraseñas en el directorio activo; además un procedimiento para el acceso y privilegios de usuarios; y procedimiento para la revisión de los derechos de acceso de usuarios.	Oficina de las tecnologías de la información y comunicaciones	· Número de acceso a aplicaciones, sistemas de información y equipos de cómputo vs accesos anormales y no documentados. · Permisos y roles de usuarios vs permisos y roles de usuarios inscritos
R-63 No disponibilidad de la información fallas de medio de transmisión	3	5	Procedimiento para la gestión de capacidad de los sistemas. Realizar la verificación y monitoreo de la autonomía de las UPS de la alcaldía municipal de Chía	3	5	1. Elaborar e implementar procedimiento para la gestión de capacidad de los sistemas. Realizar la verificación y monitoreo de la autonomía de las UPS de la alcaldía municipal de Chía	Oficina de las tecnologías de la información y comunicaciones Obras públicas	· Número de ups vs ups monitoreadas
R-64 Daño físico	3	5	Procedimiento para la gestión de capacidad de los sistemas. Realizar la verificación y monitoreo de la autonomía de las UPS de la alcaldía municipal de Chía. Lineamiento para la ubicación y protección de equipos de cómputo y servidores. Establecer una política de control de acceso físico a las instalaciones	3	5	1. Elaborar e implementar procedimiento para la gestión de capacidad de los sistemas. Realizar la verificación y monitoreo de la autonomía de las UPS de la alcaldía municipal de Chía. Implementar lineamiento para la ubicación y protección de equipos de cómputo y servidores. 2. Establecer una política de control de acceso físico a las instalaciones	Oficina de las tecnologías de la información y comunicaciones	· Número de ups vs ups monitoreadas · Equipos de cómputo y servidores ubicados según su criticidad vs total de equipos y servidores de la alcaldía municipal de Chía. · Accesos autorizados a la dependencia vs total de accesos a la dependencia
R-65-No disponibilidad de los servicios de los servidores	3	5	Procedimiento para la gestión de capacidad de los sistemas. Procedimientos para la gestión de acceso de los usuarios. Política de control de acceso físico a las instalaciones	3	5	1. Procedimiento para la gestión de capacidad de los sistemas. 2. Elaborar e implementar procedimiento para la gestión de acceso de los usuarios, donde se establezca el registro y cancelación de usuarios, la asignación de los permisos o roles para el ingreso a las aplicaciones o sistemas de información y la revisión de los derechos de acceso, perfiles y roles de los usuarios en las aplicaciones o sistemas de información. 3. Establecer una política de control de acceso físico a las instalaciones	Oficina de las tecnologías de la información y comunicaciones	· Número de acceso a aplicaciones, sistemas de información y equipos de cómputo vs accesos anormales y no documentados. · Permisos y roles de usuarios vs permisos y roles de usuarios inscritos · Accesos autorizados a la dependencia vs total de accesos a la dependencia

R-66 Permisos de roles mal gestionados	3	4	Procedimiento para el control de cambios en los procesos, instalaciones de las aplicaciones y sistemas de información. Procedimientos para la gestión de acceso de los usuarios.	3	4	1. Elaborar e implementar procedimiento para el control de cambios en los procesos, instalaciones de las aplicaciones y sistemas de información. 2. Elaborar e implementar procedimiento para la gestión de acceso de los usuarios, donde se establezca el registro y cancelación de usuarios, la asignación de los permisos o roles para el ingreso a las aplicaciones o sistemas de información y la revisión de los derechos de acceso, perfiles y roles de los usuarios en las aplicaciones o sistemas de información.	Oficina de las tecnologías de la información y comunicaciones	· Cambios y eventos registrados vs total de cambios y eventos. · Número de acceso a aplicaciones, sistemas de información y equipos de cómputo vs accesos anormales y no documentados. · Permisos y roles de usuarios vs permisos y roles de usuarios inscritos
R-67 Robo de información	4	5	Acuerdos de transferencia segura de información entre las entidades externas y la alcaldía municipal de Chía, además, de acuerdos de confidencialidad y no divulgación de información. Procedimientos para la gestión de acceso de los usuarios.	4	5	1. Implementar Acuerdos de transferencia segura de información entre las entidades externas y la alcaldía municipal de Chía, además, de acuerdos de confidencialidad y no divulgación de información. Elaborar e implementar procedimiento para la gestión de acceso de los usuarios, donde se establezca el registro y cancelación de usuarios, la asignación de los permisos o roles para el ingreso a las aplicaciones o sistemas de información y la revisión de los derechos de acceso, perfiles y roles de los usuarios en las aplicaciones o sistemas de información.	Oficina de las tecnologías de la información y comunicaciones el jefe de cada dependencia	· Acuerdos de transferencias firmados vs total entidades y personas con las que se realiza transferencia de información. · Número de acceso a aplicaciones, sistemas de información y equipos de cómputo vs accesos anormales y no documentados. · Permisos y roles de usuarios vs permisos y roles de usuarios inscritos

MAPA DE RIESGO								
PROCESO: Comunicación Estratégica								
OBJETIVO DEL PROCESO: Formular y desarrollar una estrategia que dimensione los diferentes componentes del proceso comunicativo y supere el alcance de socialización y de mantenimiento de una imagen institucional favorable de la entidad en la opinión pública.								
RIESGO	**CALIFICACIÓN**		**CONTROLES**	**NUEVA CALIFICACIÓN**		**ACCIONES**	**RESPONSABLE**	**INDICADORES**
	PROBABILIDAD	**IMPACTO**		**PROBABILIDAD**	**IMPACTO**			
R-07 Robo de información del computador del funcionario	3	4	Procedimientos para la gestión de acceso de los usuarios.	3	4	1. Elaborar e implementar procedimiento para la gestión de acceso de los usuarios, donde se establezca el registro y cancelación de usuarios, la asignación de los permisos o roles para el ingreso a las aplicaciones o sistemas de información y la revisión de los derechos de acceso, perfiles y roles de los usuarios en las aplicaciones o sistemas de información.	Oficina de las tecnologías de la información y comunicaciones	· Permisos y roles de usuarios vs permisos y roles de usuarios inscritos. · Accesos autorizados a la dependencia vs total de accesos a la dependencia
R-08 Alteración de la información del computador del funcionario	4	5	Procedimientos para la gestión de acceso de los usuarios. Lineamiento para la gestión de contraseñas.	4	5	1. Elaborar e implementar procedimiento para la gestión de acceso de los usuarios, donde se establezca el registro y cancelación de usuarios, la asignación de los permisos o roles para el ingreso a las aplicaciones o sistemas de información y la revisión de los derechos de acceso, perfiles y roles de los usuarios en las aplicaciones o sistemas de información. 2. Elaborar e implementar lineamiento para la gestión de contraseñas dentro de las aplicaciones, sistemas de información y equipos de cómputo, donde se exija la robustez de las contraseñas y se controle el cambio periódico de las contraseñas.	Oficina de las tecnologías de la información y comunicaciones	· Permisos y roles de usuarios vs permisos y roles de usuarios inscritos. · Accesos autorizados a la dependencia vs total de accesos a la dependencia. · Contraseñas actualizadas vs contraseñas genéricas
R-09 Alteración de la información	4	4	Procedimientos para la gestión de acceso de los usuarios. Lineamiento para la gestión de contraseñas.	4	4	1. Elaborar e implementar procedimiento para la gestión de acceso de los usuarios, donde se establezca el registro y cancelación de usuarios, la asignación de los permisos o roles para el ingreso a las aplicaciones o sistemas de información y la revisión de los derechos de acceso, perfiles y roles de los usuarios en las aplicaciones o sistemas de información. 2. Elaborar e implementar lineamiento para la gestión de contraseñas dentro de las aplicaciones, sistemas de información y equipos de cómputo, donde se exija la robustez de las contraseñas y se controle el cambio periódico de las contraseñas.	Oficina de las tecnologías de la información y comunicaciones	· Permisos y roles de usuarios vs permisos y roles de usuarios inscritos. · Contraseñas actualizadas vs contraseñas genéricas
R-10 Alteración de la información por manipulación	2	5	Procedimientos para la gestión de acceso de los usuarios.	2	5	1. Elaborar e implementar procedimiento para la gestión de acceso de los usuarios, donde se establezca el registro y cancelación de usuarios, la asignación de los permisos o roles para el ingreso a las aplicaciones o sistemas de información y la revisión de los derechos de acceso, perfiles y roles de los usuarios en las aplicaciones o sistemas de información.	Oficina de las tecnologías de la información y comunicaciones	· Permisos y roles de usuarios vs permisos y roles de usuarios inscritos. · Accesos autorizados a la dependencia vs total de accesos a la dependencia

R-11 Alteración de la información del escritorio del funcionario	2	5	Procedimientos para la gestión de acceso de los usuarios. Lineamiento para la gestión de contraseñas. Establecer una política de control de acceso físico a las instalaciones	2	5	1. Elaborar e implementar procedimiento para la gestión de acceso de los usuarios, donde se establezca el registro y cancelación de usuarios, la asignación de los permisos o roles para el ingreso a las aplicaciones o sistemas de información y la revisión de los derechos de acceso, perfiles y roles de los usuarios en las aplicaciones o sistemas de información. 2. Elaborar e implementar lineamiento para la gestión de contraseñas dentro de las aplicaciones, sistemas de información y equipos de cómputo, donde se exija la robustez de las contraseñas y se controle el cambio periódico de las contraseñas. 3. Establecer una política de control de acceso físico a las instalaciones	Oficina de las tecnologías de la información y comunicaciones	· Permisos y roles de usuarios vs permisos y roles de usuarios inscritos. · Accesos autorizados a la dependencia vs total de accesos a la dependencia · Contraseñas actualizadas vs contraseñas genéricas

MAPA DE RIESGO								
PROCESO: Gestión de Contratación								
OBJETIVO DEL PROCESO: Organizar, coordinar, controlar y ejecutar los procesos, procedimientos y actividades propias de las etapas precontractuales, contractuales y postcontractuales que se adelante en la Alcaldía para la adquisición de los bienes y servicios requeridos para el desarrollo y cumplimiento de la misión y operación de la entidad, a través de la celebración de contratos y/o convenios, acorde con el procedimiento previsto en la Ley 80 de 1993, Ley 1150 de 2007 y sus decretos reglamentarios y hacer el seguimiento a la ejecución de los mismos.								
RIESGO	**CALIFICACIÓN**		**CONTROLES**	**NUEVA CALIFICACIÓN**		**ACCIONES**	**RESPONSABLE**	**INDICADORES**
	PROBABILIDAD	**IMPACTO**		**PROBABILIDAD**	**IMPACTO**			
R-03 Alteración de copias de seguridad	4	3	Procedimientos para la gestión de acceso de los usuarios. Implementar política de escritorio y pantalla limpia, lineamiento para asegurar el bloqueo de pantallas de equipo de cómputo desatendidos. Política de control de acceso.	4	3	1. Procedimientos para la gestión de acceso de los usuarios. 2. Implementar política de escritorio y pantalla limpia, lineamiento para asegurar el bloqueo de pantallas de equipo de cómputo desatendidos. 3. Política de control de acceso. 4. Establecer una política de control de acceso físico a las instalaciones	Oficina de las tecnologías de la información y comunicaciones. Jefe, director o secretario de cada dependencia o secretaria.	· Número de equipos bloqueados, pantallas y escritorios limpios vs número de equipos de la alcaldia municipal de Chía. · Número de acceso a aplicaciones, sistemas de información y equipos de cómputo vs accesos anormales · Perfiles y permisos asignados nuevos vs perfiles y permisos de usuarios · Accesos autorizados a la dependencia vs total de accesos a la dependencia
R-21 Fuga de información	3	4	Implementar política de escritorio y pantalla limpia, lineamiento para asegurar el bloqueo de pantallas de equipo de cómputo desatendidos.	3	4	1. Implementar política de escritorio y pantalla limpia, lineamiento para asegurar el bloqueo de pantallas de equipo de cómputo desatendidos.	Oficina de las tecnologías de la información y comunicaciones Jefe, director o secretario de cada dependencia o secretaria.	· Número de equipos bloqueados, pantallas y escritorios limpios vs número de equipos de la alcaldia municipal de Chía.
R-22 Manipulación de la información	3	4	Implementar política de escritorio y pantalla limpia, lineamiento para asegurar el bloqueo de pantallas de equipo de cómputo desatendidos. Política de control de acceso.	3	4	1.Implementar política de escritorio y pantalla limpia, implementar lineamiento para asegurar el bloqueo de pantallas de equipo de cómputo desatendidos. 2.Diseñar e implementar una política de control de acceso donde se documenten los procesos de acceso seguro a aplicaciones, permisos en red, logs de acceso y modificación de usuarios y contraseñas en el directorio activo; además un procedimiento para el acceso y privilegios de usuarios.	Oficina de las tecnologías de la información y comunicaciones Jefe, director o secretario de cada dependencia o secretaria.	· Número de equipos bloqueados, pantallas y escritorios limpios vs número de equipos de la alcaldia municipal de Chía.
R-34 Compromiso de la información del equipo de cómputo	2	5	Procedimientos establecidos para la actualización y mantenimiento de los equipos de cómputo. Establecer una política de control de acceso físico a las instalaciones	1	4	1. Procedimiento establecido para la actualización y mantenimiento de los equipos de cómputo. 2. Establecer una política de control de acceso físico a las instalaciones	Oficina de las tecnologías de la información y comunicaciones Jefe, director o secretario de cada dependencia o secretaria.	· Número de mantenimientos realizados vs Número de mantenimientos programados

MAPA DE RIESGO								
PROCESO: Gestión de Atención a la Ciudadanía								
OBJETIVO DEL PROCESO: Garantizar la calidad de la atención, la oportunidad y capacidad de respuesta a la ciudadanía mediante la definición e implementación de políticas de servicio, protocolos de atención, la estructuración de canales de atención y un modelo de servicio a la comunidad para satisfacer de manera efectiva la demanda de servicios y trámites en el municipio.								
RIESGO	**CALIFICACIÓN**		**CONTROLES**	**NUEVA CALIFICACIÓN**		**ACCIONES**	**RESPONSABLE**	**INDICADORES**
	PROBABILIDAD	**IMPACTO**		**PROBABILIDAD**	**IMPACTO**			
R-14 Manipulación indebida de la información	4	5	Implementar política de escritorio y pantalla limpia, lineamiento para asegurar el bloqueo de pantallas de equipo de cómputo desatendidos.	4	5	1. Implementar política de escritorio y pantalla limpia, lineamiento para asegurar el bloqueo de pantallas de equipo de cómputo desatendidos.	Oficina de las tecnologías de la información y comunicaciones Jefe, director o secretario de cada dependencia o secretaria.	· Número de equipos bloqueados, pantallas y escritorios limpios vs número de equipos de la alcaldia municipal de Chía.

MAPA DE RIESGO								
PROCESO:Gestión del Riesgo y Atención de Desastres								
OBJETIVO DEL PROCESO: Garantizar la protección de personas y colectividades de los efectos negativos de desastres de origen natural o antrópico, mediante la generación de políticas, estrategias y normas que promuevan capacidades orientadas a identificar, analizar, prevenir y mitigar riesgos para enfrentar y manejar eventos de desastre.								
RIESGO	**CALIFICACIÓN**		**CONTROLES**	**NUEVA CALIFICACIÓN**		**ACCIONES**	**RESPONSABLE**	**INDICADORES**
	PROBABILIDAD	**IMPACTO**		**PROBABILIDAD**	**IMPACTO**			
R-01 Divulgación de información	4	5	Procedimientos establecidos para la actualización y mantenimiento de los equipos de cómputo. Política de control de acceso. Establecer una política de control de acceso físico a las instalaciones	4	5	1. Procedimiento establecido para la actualización y mantenimiento de los equipos de cómputo. 2. Diseñar e implementar una política de control de acceso donde se documenten los procesos de acceso seguro a aplicaciones, permisos en red, logs de acceso, modificación de usuarios y contraseñas en el directorio activo; además un procedimiento para el acceso y privilegios de usuarios. 3. Establecer una política de control de acceso físico a las instalaciones	Oficina de las tecnologías de la información y comunicaciones. Jefe, director o secretario de cada dependencia o secretaria.	· Número de mantenimientos realizados vs Número de mantenimientos programados · Número de acceso a aplicaciones, sistemas de información y equipos de cómputo vs accesos anormales. · Accesos autorizados a la dependencia vs total de accesos a la dependencia
R-16 Pérdida de información	3	4	Procedimientos para la gestión de acceso de los usuarios. Implementar política de escritorio y pantalla limpia, lineamiento para asegurar el bloqueo de pantallas de equipo de cómputo desatendidos. Política de control de acceso físico a las instalaciones	3	4	1. Elaborar e implementar procedimiento para la gestión de acceso de los usuarios, donde se establezca el registro y cancelación de usuarios, la asignación de los permisos o roles para el ingreso a las aplicaciones o sistemas de información y la revisión de los derechos de acceso, perfiles y roles de los usuarios en las aplicaciones o sistemas de información. 2. Implementar política de escritorio y pantalla limpia, lineamiento para asegurar el bloqueo de pantallas de equipo de cómputo desatendidos. 3. Establecer una política de control de acceso físico a las instalaciones	Oficina de las tecnologías de la información y comunicaciones Jefe, director o secretario de cada dependencia o secretaria.	· Permisos y roles de usuarios vs permisos y roles de usuarios inscritos. · Accesos autorizados a la dependencia vs total de accesos a la dependencia
R-17 Pérdida de información de escritorio de funcionario	4	5	Implementar política de escritorio y pantalla limpia, lineamiento para asegurar el bloqueo de pantallas de equipo de cómputo desatendidos. Política de control de acceso físico a las instalaciones	4	5	1. Implementar política de escritorio y pantalla limpia, implementar lineamiento para asegurar el bloqueo de pantallas de equipo de cómputo desatendidos. 2. Establecer una política de control de acceso físico a las instalaciones	Oficina de las tecnologías de la información y comunicaciones. Jefe, director o secretario de cada dependencia o secretaria.	· Número de equipos bloqueados, pantallas y escritorios limpios vs número de equipos de la alcaldia municipal de Chía. · Accesos autorizados a la dependencia vs total de accesos a la dependencia
R-18 Pérdida de información de equipo de cómputo	3	4	Política para realizar copias de seguridad o respaldo de la información almacenada en los servidores de la alcaldia municipal de Chía.	3	4	1. Elaborar e Implementar política para realizar copias de seguridad o respaldo de la información almacenada en los servidores de la alcaldía municipal de Chía.	Oficina de las tecnologías de la información y comunicaciones	· Copias de seguridad realizadas vs copias de seguridad programadas

MAPA DE RIESGO								
PROCESO: Gestión de Gobierno y Seguridad								
OBJETIVO DEL PROCESO: Mejorar los niveles de seguridad, participación y convivencia ciudadana, y el control del espacio público, mediante estrategias y acciones de promoción de la cultura de la legalidad, control, defensa, protección, recuperación y prevención para el fortalecimiento institucional, con el fin de garantizar las libertades civiles, la convivencia y el disfrute de la comunidad.								
RIESGO	**CALIFICACIÓN**		**CONTROLES**	**NUEVA CALIFICACIÓN**		**ACCIONES**	**RESPONSABLE**	**INDICADORES**
	PROBABILIDAD	**IMPACTO**		**PROBABILIDAD**	**IMPACTO**			
R-01 Divulgación de información	4	5	Procedimientos establecidos para la actualización y mantenimiento de los equipos de cómputo. Política de control de acceso. Establecer una política de control de acceso físico a las instalaciones	4	5	1. Procedimiento establecido para la actualización y mantenimiento de los equipos de cómputo. 2. Diseñar e implementar una política de control de acceso donde se documenten los procesos de acceso seguro a aplicaciones, permisos en red, logs de acceso, modificación de usuarios y contraseñas en el directorio activo; además un procedimiento para el acceso y privilegios de usuarios. 3. Establecer una política de control de acceso físico a las instalaciones	Oficina de las tecnologías de la información y comunicaciones. Jefe, director o secretario de cada dependencia o secretaria.	· Número de mantenimientos realizados vs Número de mantenimientos programados · Número de acceso a aplicaciones, sistemas de información y equipos de cómputo vs accesos anormales. · Accesos autorizados a la dependencia vs total de accesos a la dependencia
R-02 Manipulación de información	2	3	Procedimientos establecidos para la actualización y mantenimiento de los equipos de cómputo. Política de control de acceso.	2	3	1. Procedimiento establecido para la actualización y mantenimiento de los equipos de cómputo. 2. Diseñar e implementar una política de control de acceso donde se documenten los procesos de acceso seguro a aplicaciones, permisos en red, logs de acceso y modificación de usuarios y contraseñas en el directorio activo; además un procedimiento para el acceso y privilegios de usuarios.	Oficina de las tecnologías de la información y comunicaciones	· Número de mantenimientos realizados vs Número de mantenimientos programados · Número de acceso a aplicaciones, sistemas de información y equipos de cómputo vs accesos anormales y no documentados.
R-18 Pérdida de información de equipo de cómputo	3	4	Política para realizar copias de seguridad o respaldo de la información almacenada en los servidores de la alcaldia municipal de Chía.	3	4	1. Elaborar e Implementar política para realizar copias de seguridad o respaldo de la información almacenada en los servidores de la alcaldía municipal de Chía.	Oficina de las tecnologías de la información y comunicaciones	· Copias de seguridad realizadas vs copias de seguridad programadas
R-19 Fuga de información	3	3	Procedimientos establecidos para la actualización y mantenimiento de los equipos de cómputo.	3	3	1. Procedimiento establecido para la actualización y mantenimiento de los equipos de cómputo. 2. Diseñar e implementar una política de control de acceso donde se documenten los procesos de acceso seguro a aplicaciones, permisos en red, logs de acceso y modificación de usuarios y contraseñas en el directorio activo; además un procedimiento para el acceso y privilegios de usuarios.	Oficina de las tecnologías de la información y comunicaciones	· Número de mantenimientos realizados vs Número de mantenimientos programados · Número de acceso a aplicaciones, sistemas de información y equipos de cómputo vs accesos anormales y no documentados.

MAPA DE RIESGO								
PROCESO: Gestión del Medio Ambiente								
OBJETIVO DEL PROCESO: Desarrollar en el municipio y de acuerdo a sus competencias, las políticas y regulaciones ambientales de recuperación, conservación, protección, ordenamiento, manejo, uso y aprovechamiento de los recursos naturales renovables y del medio ambiente para asegurar el desarrollo sostenible.								
RIESGO	**CALIFICACIÓN**		**CONTROLES**	**NUEVA CALIFICACIÓN**		**ACCIONES**	**RESPONSABLE**	**INDICADORES**
	PROBABILIDAD	**IMPACTO**		**PROBABILIDAD**	**IMPACTO**			
R-04 Compromiso de la información	4	5	Lineamiento para la gestión de contraseñas.	4	5	Diseñar e implementar lineamiento para la gestión de contraseñas dentro de las aplicaciones, sistemas de información y equipos de cómputo, donde se exija la robustez de las contraseñas y se controle el cambio periódico de las contraseñas.	Oficina de las tecnologías de la información y comunicaciones	Contraseñas actualizadas vs contraseñas genéricas
R-05 Robo de información de equipos de cómputo	2	4	Lineamiento para la gestión de contraseñas. Implementar política de escritorio y pantalla limpia, lineamiento para asegurar el bloqueo de pantallas de equipo de cómputo desatendidos. Política de control de acceso físico a las instalaciones	2	4	1.Diseñar e implementar lineamiento para la gestión de contraseñas dentro de las aplicaciones, sistemas de información y equipos de cómputo, donde se exija la robustez de las contraseñas y se controle el cambio periódico de las contraseñas. 2. implementar política de escritorio y pantalla limpia, lineamiento para asegurar el bloqueo de pantallas de equipo de cómputo desatendidos. 3.Establecer una política de control de acceso físico a las instalaciones	Oficina de las tecnologías de la información y comunicaciones Jefe, director o secretario de cada dependencia o secretaria.	· Contraseñas actualizadas vs contraseñas genéricas. · Número de equipos bloqueados, pantallas y escritorios limpios vs número de equipos de la alcaldia municipal de Chía. · Accesos autorizados a la dependencia vs total de accesos a la dependencia
R-06 Robo de información del escritorio del funcionario	3	4	Lineamiento para la gestión de contraseñas. Política de control de acceso físico a las instalaciones	3	4	1. Implementar lineamiento para la gestión de contraseñas dentro de las aplicaciones, sistemas de información y equipos de cómputo, donde se exija la robustez de las contraseñas y se controle el cambio periódico de las contraseñas. 2. Establecer una política de control de acceso físico a las instalaciones	Oficina de las tecnologías de la información y comunicaciones	· Contraseñas actualizadas vs contraseñas genéricas · Accesos autorizados a la dependencia vs accesos no autorizados.

MAPA DE RIESGO								
PROCESO: Gestión de Movilidad								
OBJETIVO DEL PROCESO: Garantizar la circulación de los diferentes actores Mediante la aplicación de mecanismos de planeación y control de tránsito y transporte que permitan la movilidad de forma cómoda, segura, ágil y oportuna en el Municipio de Chía.								
RIESGO	**CALIFICACIÓN**		**CONTROLES**	**NUEVA CALIFICACIÓN**		**ACCIONES**	**RESPONSABLE**	**INDICADORES**
	PROBABILIDAD	**IMPACTO**		**PROBABILIDAD**	**IMPACTO**			
R-20 Destrucción de la información	3	3	Lineamiento para la gestión de contraseñas. Implementar política de escritorio y pantalla limpia, lineamiento para asegurar el bloqueo de pantallas de equipo de cómputo desatendidos.	3	3	1. Implementar lineamiento para la gestión de contraseñas dentro de las aplicaciones, sistemas de información y equipos de cómputo, donde se exija la robustez de las contraseñas y se controle el cambio periódico de las contraseñas. 2. Implementar política de escritorio y pantalla limpia, lineamiento para asegurar el bloqueo de pantallas de equipo de cómputo desatendidos.	Oficina de las tecnologías de la información y comunicaciones Jefe, director o secretario de cada dependencia o secretaria.	· Contraseñas actualizadas vs contraseñas genéricas. · Número de equipos bloqueados, pantallas y escritorios limpios vs número de equipos de la alcaldia municipal de Chía.