Mapa de Riesgos de Seguridad de la Información

Nombre de la Entidad	ALCALDIA MUNICIPAL DE LA MESA - CUNDINAMARCA	Datos de contacto	Nombre: CARLOS HUMBERTO CASTRO GIRALDO Email: sistemas@lamesa-cundinamarca.gov.co Teléfono:

IDENTIFICACIÓN DEL RIESGO								ANÁLISIS DEL RIESGO INHERENTE			IDENTIFICACIÓN DE CONTROLES			RIESGO RESIDUAL			MANEJO DEL RIESGO RESIDUAL - Plan de Tratamiento de Riesgos							
Tipo de Activo de Información	Activo de Información	Nro.	Propiedad que afecta el Riesgo	Descripción del Riesgo	Responsable de determinar la materialización del riesgo	Amenazas	Vulnerabilidades	Probabilidad	Impacto	Zona de Riesgo	Opciones de manejo del riesgo	Descripción del control	Responsable de ejecutar el control	Probabilidad	Impacto	Zona de Riesgo Residual	Opciones de manejo del riesgo	Controles	Objetivo del Control	Actividad	Responsable de Ejecutar el control	Periodo / Fecha inicio	Periodo / Fecha fin	Propuesta/Descripción del indicador
Información y datos de la entidad:	Pagina Web Institucional	1	Confidencialidad Integridad Disponibilidad	Desconocimiento de la Ley de Transparencia y la matriz ITA de la procuraduría general de la nación de que es que lo que se debe publicar por parte de los funcionarios y contratistas	Profesional Universitario	Fallas humanas	Retraso en la entrega de información por parte del personal	CASI SEGURO, Más de 1 vez al año, Se espera que el evento ocurra en la mayoría de las circunstancias.	MAYOR Afectación de la imagen, de la credibilidad y de la confianza, investigaciones	ALTA Confidencialidad 2 Imagen 4 Legal 3 Operativo 2	ACEPTAR EL RIESGO: No se adopta ninguna medida que afecte la probabilidad o el impacto del riesgo.	Solicitar constantemente a los productores de la información para ser subidos a la pagina Web	* Profesional TIC * Secretarios y Directores de Despacho * Director de Control Interno	25%	55%	ALTO	Revisar mensualmente la matriz de la contraloria general de la nación y solicitar información a cada uno de los funcionarios y contatistas	Matriz de ITA con el respectivo url Control A18,1	Cumplimiento de requisitos legales y contractuales	Revision mensual matriz ITA	Profesional Universitario TIC	1/01/2024	31/12/2024	No Revisones / No Revisones estipuladas
Información y datos de la entidad:	Correo Electronico	2	Confidencialidad Integridad Disponibilidad	Recepción de Archivos Malicioso, ataques Phishing, Publicidad engañosa (Spam), Búsqueda de información y datos	Profesional Universitario	Fallas humanas	Desconocimiento o no aplicación de las politicas de seguridad y privacidad de la información	CASI SEGURO, Más de 1 vez al año, Se espera que el evento ocurra en la mayoría de las circunstancias.	MAYOR Afectación de la imagen, de la credibilidad y de la confianza, investigaciones	ALTA Confidencialidad 4 Imagen 2 Legal 3 Operativo 2	ACEPTAR EL RIESGO: No se adopta ninguna medida que afecte la probabilidad o el impacto del riesgo.	Solicitar constantemente a los usuarios la apertura y contestación del correo electronico	* Profesional TIC * Secretarios y Directores de Despacho * Director de Control Interno	30%	55%	ALTO	Revisar y mantener los correos activos con el proveedor	Mantener los correos activos e inactivos, su espacio y opciones de seguridad Control A9,2 / A9,4	Asegurar el acceso de los usuarios autorizados y evitar el acceso no autorizado a sistemas y servicios	Revisión mensual de correos	Profesional Universitario TIC	1/01/2024	31/12/2024	No Revisones / No Revisones estipuladas
Información y datos de la entidad:	Servidor de Archivos	3	Confidencialidad Integridad Disponibilidad	Abuso de los derechos de almacenamiento	Profesional Universitario	Fallas humanas	Ausencia de copias de respaldo o backups de la información	CASI SEGURO, Más de 1 vez al año, Se espera que el evento ocurra en la mayoría de las circunstancias.	MODERADO: Se afecta a todo el proceso	MODERADA Confidencialidad 3 Imagen 1 Legal 1 Operativo 2	REDUCIR EL RIESGO: Se adoptan medidas para reducir la probabilidad o el impacto del riesgo,o ambos; por lo general conlleva a la implementación de controles	Realizar Backup del servidor en fisico cada 6 meses	Profesional TIC	30%	35%	MEDIO	Mantener el servidor de archivo, realizando mantenimiento preventivo y eliminando archivos no institucionales	Mantener el servidor de archivos con el mantenimiento preventivo, actualizaciones y antivirusControl A9,2	Asegurar el acceso de los usuarios autorizados y evitar el acceso no autorizado a sistemas y servicios	Realizar mantenimiento del servidor mensual, borrado de temporales, actualizacion de parches de seguridad, antivirus	Profesional Universitario TIC	1/01/2024	31/12/2024	No mantenimientos / No mateniimientos programados
Información y datos de la entidad:	Software Antivirus	4	Confidencialidad Integridad Disponibilidad	Error de Uso por parte de los funcionarios	Profesional Universitario	Perdida de Información	Configuración incorrecta de parámetros	CASI SEGURO, Más de 1 vez al año, Se espera que el evento ocurra en la mayoría de las circunstancias.	MODERADO: Se afecta a todo el proceso	MODERADA Confidencialidad 2 Imagen 1 Legal 2 Operativo 2	REDUCIR EL RIESGO: Se adoptan medidas para reducir la probabilidad o el impacto del riesgo,o ambos; por lo general conlleva a la implementación de controles	Verificar la actividad en el servidor de Antivirus y en los equipos instalados	Profesional TIC	20%	30%	MEDIO	Mantener establecido fechas de vencimiento en los equipos, revisar las alertas que presenta en el servidor de antivirus	Mantener actualizado el antivirus. Control A9,2	Los equipos deben estar ubicados o protegidos para reducir el riesgo debido a amenazas o peligros del entorno	Revision semanal de servidor de antivirus	Profesional Universitario TIC	1/01/2024	31/12/2024	No Revisones / No Revisones estipuladas
Información y datos de la entidad:	Firewall Perimetral	5	Confidencialidad Integridad Disponibilidad	Asignación errada de los derechos de acceso	Profesional Universitario	Perdida de Información	Configuración incorrecta de parámetros	RARO El evento puede ocurrir solo en circunstancias excepcionales	MINOR: Se tendrían que realizar ajustes en los procedimientos del proceso	ALTA Confidencialidad 4 Imagen 3 Legal 3 Operativo 3	ACEPTAR EL RIESGO: No se adopta ninguna medida que afecte la probabilidad o el impacto del riesgo.	Verificar permisos y accesos de los equipos que conforman la red	Profesional TIC	5%	65%	MEDIO	Revisar y entrar cada mes al firewall para establecer su funcionamiento y control	Hacer pruebas de accesos en distintos equipos Control A11,2,3	Prevenir la perdida, daño, robo o compromiso de activos, y la interrupción de las operaciones de la organización	Realizar pruebas de acceso en equipos de la red	Profesional Universitario TIC	1/01/2024	31/12/2024	No de politicas actualizadas / No de politicas efectivas
Sistemas de información y aplicaciones de Software	SINFA	6	Confidencialidad Integridad Disponibilidad	Mal funcionamiento del software, Corrupción de datos	Profesional Universitario	Perdida de Información	En términos de tiempo utilización de datos errados en los programas de aplicación, Ausencia de copias de respaldo o backups de la información	POSIBLE: El evento podría ocurrir en algún momento	MODERADO: Se afecta a todo el proceso	MODERADA Confidencialidad 3 Imagen 3 Legal 3 Operativo 3	REDUCIR EL RIESGO: Se adoptan medidas para reducir la probabilidad o el impacto del riesgo,o ambos; por lo general conlleva a la implementación de controles	Realizar backup de las bases de datos del programa SINFA minimo 15 al mes	Profesional TIC	15%	60%	MEDIO	Realizar y verificar las copias de seguridad segun procedimiento establecido	Realizar 15 copias de seguridad segun porcedimiento establecido Control A14,2	Asegurar de que la seguridad de la información está diseñada e implementada dentro del ciclo de vida de desarrollo de los sistemas de información	Realizar copia en el servidor y en la nube, según procedimiento	Profesional Universitario TIC	1/01/2024	31/12/2024	No de copias mensuales / No de copias programadas
Sistemas de información y aplicaciones de Software	PQRS CODE	7	Confidencialidad Integridad Disponibilidad	Mal funcionamiento del software, Corrupción de datos	Profesional Universitario	Perdida de Información	Ausencia de copias de respaldo o backups de la información	RARO El evento puede ocurrir solo en circunstancias excepcionales	MINOR: Se tendrían que realizar ajustes en los procedimientos del proceso	BAJA Confidencialidad 2 Imagen 2 Legal 2 Operativo 2	COMPARTIR EL RIESGO: Se reduce la probabilidad o el impacto del riesgo transfiriendo acompartiendo una parte de este	Tener el backup por lo menos 10 dias anteriores de la base de datos	Profesional TIC	5%	40%	MEDIO	Realizar y verificar las copias de seguridad segun procedimiento establecido	mantener 10 copias de seguridad en la nube. Control A14,2	Asegurar de que la seguridad de la información está diseñada e implementada dentro del ciclo de vida de desarrollo de los sistemas de información	Realizar copia en el servidor y en la nube, según procedimiento	Profesional Universitario TIC	1/01/2024	31/12/2024	No de copias mensuales / No de copias programadas
Sistemas de información y aplicaciones de Software	Aplicativos de las entidades de control	8	Confidencialidad Integridad Disponibilidad	Mal funcionamiento del software, red de internet y del Firewall	Profesional Universitario	Perdida de Información	Ausencia de mecanismos de identificación y autenticación, como la autenticación de usuario	RARO El evento puede ocurrir solo en circunstancias excepcionales	MINOR: Se tendrían que realizar ajustes en los procedimientos del proceso	BAJA Confidencialidad 1 Imagen 1 Legal 2 Operativo 2	COMPARTIR EL RIESGO: Se reduce la probabilidad o el impacto del riesgo transfiriendo acompartiendo una parte de este	Revisar aplicaciones y puertos que utiliza para su actividad	Profesional TIC	5%	30%	BAJO	Verificar el estado del internet, las actualizaciones de los equipos y el antivirus	Revisar la instalacion de los aplicativos, manteniendo los equipos actualizados, A13,2	Mantener la seguridad de la información transferida dentro de una organización y con cualquier entidad externa	Revisión de equipos, actualizaciones y el antivirus	Profesional Universitario TIC	1/01/2024	31/12/2024	No de mantenimientos preventivos/ No mantenimiento solicitados
Sistemas de información y aplicaciones de Software	Aplicativos de portales bancarios	9	Confidencialidad Integridad Disponibilidad	Mal funcionamiento del software, red de internet y del Firewall	Profesional Universitario	Perdida de Información	Ausencia de mecanismos de identificación y autenticación, como la autenticación de usuario	RARO El evento puede ocurrir solo en circunstancias excepcionales	MINOR: Se tendrían que realizar ajustes en los procedimientos del proceso	MODERADA Confidencialidad 1 Imagen 3 Legal 3 Operativo 1	REDUCIR EL RIESGO: Se adoptan medidas para reducir la probabilidad o el impacto del riesgo,o ambos; por lo general conlleva a la implementación de controles	Revisar aplicaciones y puertos que utiliza para su actividad, atender las recomendaciones de los portales	Profesional TIC Tesorero General Funcionario Encargado	5%	40%	BAJO	Verificar el estado del internet, las actualizaciones de los equipos y el antivirus. Junto con los controles de cada uno de los portales	Controles A11 A11,1	Prevenir la perdida, daño, robo o compromiso de activos, y la interrupción de las operaciones de la organización	Revisión de equipos, actualizaciones y el antivirus, revisión de recomendaciones portales y equipos especiales en el firewall	Profesional Universitario TIC	1/01/2024	31/12/2024	No de mantenimientos preventivos/ No mantenimiento solicitados
Sistemas de información y aplicaciones de Software	Aplicativos varios	10	Confidencialidad Integridad Disponibilidad	Mal funcionamiento del software, red de internet y del Firewall	Profesional Universitario	Perdida de Información	Ausencia de mecanismos de identificación y autenticación, como la autenticación de usuario	RARO El evento puede ocurrir solo en circunstancias excepcionales	MINOR: Se tendrían que realizar ajustes en los procedimientos del proceso	BAJA Confidencialidad 2 Imagen 1 Legal 1 Operativo 1	COMPARTIR EL RIESGO: Se reduce la probabilidad o el impacto del riesgo transfiriendo acompartiendo una parte de este	Revisar aplicaciones y puertos que utiliza para su actividad	Profesional TIC Funcionario Encargado	5%	25%	BAJO	Verificar el estado del internet, las actualizaciones de los equipos y el antivirus. Realizar plan de mantenimiento	Controles A11 A11,1	Prevenir la perdida, daño, robo o compromiso de activos, y la interrupción de las operaciones de la organización.	Revisión de equipos, actualizaciones y el antivirus	Profesional Universitario TIC	1/01/2024	31/12/2024	No de mantenimientos preventivos/ No mantenimiento solicitados
Dispositivos de Tecnologías de Información-Hardware:	Servidores	11	Confidencialidad Integridad Disponibilidad	Fallas tecnologicas	Profesional Universitario	Perdida de Información	Ausencia de mecanismos de identificación y autenticación, como la autenticación de usuario	POSIBLE: El evento podría ocurrir en algún momento	MODERADO: Se afecta a todo el proceso	MODERADA Confidencialidad 1 Imagen 1 Legal 1 Operativo 2	ACEPTAR EL RIESGO: No se adopta ninguna medida que afecte la probabilidad o el impacto del riesgo.	Revisar mensualmente el uso de los servidores	Profesional TIC	10%	30%	BAJO	Verificar el estado de los equipos, realizar mantenimiento preventivo, revisar antivirus y actualizaciones de seguridad	Controles A11 A11,1	Prevenir la perdida, daño, robo o compromiso de activos, y la interrupción de las operaciones de la organización	Revisión de equipos, actualizaciones y el antivirus	Profesional Universitario TIC	1/01/2024	31/12/2024	No de mantenimientos preventivos/ No mantenimiento solicitados
Dispositivos de Tecnologías de Información-Hardware:	Equipos de Computo funcionarios	12	Confidencialidad Integridad Disponibilidad	Fallas tecnologicas	Profesional Universitario	Perdida de Información	Mantenimiento insuficiente/instalación fallida de los medios de almacenamiento	POSIBLE: El evento podría ocurrir en algún momento	MODERADO: Se afecta a todo el proceso	MODERADA Confidencialidad 1 Imagen 1 Legal 1 Operativo 2	REDUCIR EL RIESGO: Se adoptan medidas para reducir la probabilidad o el impacto del riesgo,o ambos; por lo general conlleva a la implementación de controles	Revisar y realizar los mantenimientos respectivos	Profesional TIC	10%	25%	BAJO	Verificar el estado del internet, las actualizaciones de los equipos y el antivirus. Realizar plan de mantenimiento	Controles A11 A11,1	Prevenir la perdida, daño, robo o compromiso de activos, y la interrupción de las operaciones de la organización.	Revisión de equipos, actualizaciones y el antivirus	Profesional Universitario TIC	1/01/2024	31/12/2024	No de mantenimientos preventivos/ No mantenimiento solicitados
Dispositivos de Tecnologías de Información-Hardware:	Equipos de Computo Publicos	13	Confidencialidad Integridad Disponibilidad	Fallas tecnologicas	Profesional Universitario	Destrucción de equipos o de medios	Ausencia de esquemas de reemplazo periódico	POSIBLE: El evento podría ocurrir en algún momento	MODERADO: Se afecta a todo el proceso	BAJA Confidencialidad 0 Imagen 1 Legal 1 Operativo 1	EVITAR EL RIESGO: Se abandonan las actividades que dan lugar al riesgo, es decir, no iniciar o no continuar con la actividad que lo provoca.	Revisar y realizar los mantenimientos respectivos	Profesional TIC	10%	15%	BAJO	Verificar el estado del internet, las actualizaciones de los equipos y el antivirus. Realizar plan de mantenimiento	Controles A11 A11,1	Prevenir la perdida, daño, robo o compromiso de activos, y la interrupción de las operaciones de la organización	Revisión de equipos, actualizaciones y el antivirus	Profesional Universitario TIC	1/01/2024	31/12/2024	No de mantenimientos preventivos/ No mantenimiento solicitados
Soporte para almacenamiento de información:	Nube Google Drive	14	Confidencialidad Integridad Disponibilidad	Fallas tecnologicas	Profesional Universitario	Perdida de Información	Ausencia de mecanismos de identificación y autenticación, como la autenticación de usuario	RARO El evento puede ocurrir solo en circunstancias excepcionales	MINOR: Se tendrían que realizar ajustes en los procedimientos del proceso	BAJA Confidencialidad 2 Imagen 1 Legal 1 Operativo 1	COMPARTIR EL RIESGO: Se reduce la probabilidad o el impacto del riesgo transfiriendo acompartiendo una parte de este	Mantener activa la nube y borrar los archivos segun procedimiento	Profesional TIC	10%	30%	BAJO	Verificar el estado del internet, las actualizaciones de los equipos y el antivirus. Realizar plan de mantenimiento	Control A17,1	Evitar el acceso no autorizado a sistemas y aplicaciones	Revisión de politicas de copia de seguridad y a la nube de google Drive	Profesional Universitario TIC	1/01/2024	31/12/2024	No de copias mensuales / No de copias programadas
Servicios:	Internet	15	Confidencialidad Integridad Disponibilidad	Fallas tecnologicas, Falla del equipo de telecomunicaciones, soporte tardio por parte del proveedor de restablecimiento	Profesional Universitario	Punto único de falla	Ausencia de segundo canal de internet para respaldar el primero	POSIBLE: El evento podría ocurrir en algún momento	MAYOR: Se presentarían intermitencias o dificultades en la operación del proceso	MODERADA Confidencialidad 0 Imagen 2 Legal 0 Operativo 0	COMPARTIR EL RIESGO: Se reduce la probabilidad o el impacto del riesgo transfiriendo acompartiendo una parte de este	Revisión diaria, evaluar conectividad diariamente	Profesional TIC	20%	30%	BAJO	Verificar el internet diariamente al iniciar actividades y mantener constante comunicación con el proveedor	Control A15,2	Mantener el nivel acordado de seguridad de la información y de prestación del servicio en línea con los acuerdos con los proveedores	Revisar la velocidad de bajada, la velocidad de subida, la latencia y tracer y ping semanalmente	Profesional Universitario TIC	1/01/2024	31/12/2024	Hora de caidas sin internet / tiempo arriba del internet
Servicios	Camara de Seguridad	16	Confidencialidad Integridad Disponibilidad	Fallas tecnologicas, Pérdida del suministro de energía	Profesional Universitario	Punto único de falla	Ausencia de una planta electrica	RARO El evento puede ocurrir solo en circunstancias excepcionales	MINOR: Se tendrían que realizar ajustes en los procedimientos del proceso	BAJA Confidencialidad 0 Imagen 1 Legal 2 Operativo 0	COMPARTIR EL RIESGO: Se reduce la probabilidad o el impacto del riesgo transfiriendo acompartiendo una parte de este	Revisión de conectividad diaria	Profesional TIC	5%	15%	BAJO	Verificar el funcionamiento de las camaras de seguridad diariamente	Control A15,3	Asegurar la protección de la información en las redes, y sus instalaciones de procesamiento de información de soporte	Revisar copias de las camaras y estado de las mismas semanalmente	Profesional Universitario TIC	1/01/2024	31/12/2024	No de camaras activas / No camaras en uso
Dispositivos de Tecnologías de Información-Hardware:	NUBE PRIVADA NAS	17	Confidencialidad Integridad Disponibilidad	Asignación errada de los derechos de acceso	Profesional Universitario	Perdida de Información	Configuración incorrecta de parámetros	RARO El evento puede ocurrir solo en circunstancias excepcionales	MINOR: Se tendrían que realizar ajustes en los procedimientos del proceso	ALTA Confidencialidad 4 Imagen 3 Legal 3 Operativo 3	ACEPTAR EL RIESGO: No se adopta ninguna medida que afecte la probabilidad o el impacto del riesgo.	Verificar permisos y accesos de los equipos de la NAS	Profesional TIC	5%	65%	MEDIO	Revisar y entrar cada mes la NAS para establecer su funcionamiento y control	Hacer pruebas de accesos en distintos equipos Control A11,2,3	Prevenir la perdida, daño, robo o compromiso de activos, y la interrupción de las operaciones de la organización	Realizar pruebas de acceso a la NAS de la red	Profesional Universitario TIC	1/01/2024	31/12/2024	No de politicas actualizadas / No de politicas efectivas