
 El futuro digital es de todos Gobierno de Colombia MiNTIC		Mapa de Riesgos de Seguridad de la Información		 El futuro digital es de todos Gobierno de Colombia MiNTIC	
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:	1.8973000 Celular 311264678

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 al 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	Página Web Institucional	1	Confidencialidad Integridad Disponibilidad	Descapacitamiento de la Ley de Transparencia y el acceso TIC de la información general de la nación de que se que se que se debe publicar por parte de los funcionarios y contristas	Profesional Universitario	Falsa humana	Exceso 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 Atención de la imagen, de la confiabilidad y de la confianza, Investigaciones	ALTA Confidencialidad 3 Impacto 4 Logro 5 Operativo 2	ACCIÓN EL RIESGO: No se adopta ninguna medida que afecte la probabilidad o el impacto del riesgo.	Seleccionar compromisos a los proveedores de la información para ser revisados a página web	Profesional TIC Funcionario y Promotor de Desarrollo Ejecutor de Control Interno	25%	55%	ALTO	Revisar mensualmente la matriz de la confiabilidad general de la nación y publicar información a cada uno de los funcionarios y contristas	Revisión de ITA, con el respectivo rol Control A15.1	Completación de requisitos legales y contractuales	Revisión mensual matriz ITA	Profesional Universitario TC	1/05/2023	31/12/2023	No Revisión / No Revisión estipulada
Información y datos de la entidad	Correo Electronico	2	Confidencialidad Integridad Disponibilidad	Invasión de Archivo Maliciosos, ataques Phishing, Publicación espionaje (Espies), Malware de información y datos	Profesional Universitario	Falsa humana	Descapacitamiento o no actualización de las políticas 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 Atención de la imagen, de la confiabilidad y de la confianza, Investigaciones	ALTA Confidencialidad 4 Impacto 2 Logro 5 Operativo 2	ACCIÓN EL RIESGO: No se adopta ninguna medida que afecte la probabilidad o el impacto del riesgo.	Seleccionar compromisos a los usuarios de correo electrónico y controlados del correo electrónico	Profesional TIC Funcionario y Promotor de Desarrollo Ejecutor de Control Interno	30%	55%	ALTO	Revisar y mantener los correos activos con el proveedor	Mantener los correos activos e Backups, en espacio y políticas de seguridad Control A5.2 / A5.6	Assegurar el acceso de los usuarios autorizados y evitar el acceso no autorizado a sistemas y servicios.	Revisión mensual de correos	Profesional Universitario TC	1/05/2023	31/12/2023	No Revisión / No Revisión estipulada
Información y datos de la entidad	Servidor de Archivos	3	Confidencialidad Integridad Disponibilidad	Abuso de los derechos de almacenamiento	Profesional Universitario	Pérdida de información	Asesinato de copias de respaldo a backup 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 Impacto 1 Logro 5 Operativo 2	REDUCIR EL RIESGO: Se adoptan medidas para reducir la probabilidad o el impacto del riesgo, transfiriendo compromisos a una parte de este	Realizar Backup del servidor en físico cada 4 meses	Profesional TIC	30%	35%	MEDIO	Mantener el servidor de archivos, realizando mantenimientos preventivos y actualizaciones de software	Mantener el servidor de archivos con el mantenimiento preventivo, actualizaciones y antivirusControl A5.2	Assegurar el acceso de los usuarios autorizados y evitar el acceso no autorizado a sistemas y servicios	Realizar mantenimiento del servidor cada semana, borrado de temporales, actualización de parches de seguridad, antivirus	Profesional Universitario TC	1/05/2023	31/12/2023	No mantenimientos / No mantenimientos programados
Información y datos de la entidad	Software Antivirus	4	Confidencialidad Integridad Disponibilidad	Error de Use por parte de los funcionarios	Profesional Universitario	Pérdida 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 3 Impacto 1 Logro 5 Operativo 2	REDUCIR EL RIESGO: Se adoptan medidas para reducir la probabilidad o el impacto del riesgo, transfiriendo compromisos a una parte de este	Verificar la actividad en el servidor de Antivirus y en los equipos instalados	Profesional TIC	20%	30%	MEDIO	Mantener establecidos fechas de vencimiento en los equipos, revisar los alertas que presente en el servidor de antivirus	Mantener actualizado el antivirus. Control A5.3	Los equipos deben estar protegidos o protegidos para reducir el riesgo debido a amenazas o malware del sistema	Revisión mensual de servidor de antivirus	Profesional Universitario TC	1/05/2023	31/12/2023	No revisiones / No de revisiones programadas
Información y datos de la entidad	Firewall Perimetral	5	Confidencialidad Integridad Disponibilidad	Asignación errada de los derechos de acceso	Profesional Universitario	Pérdida de información	Configuración incorrecta de parámetros	MODERADO: Se afecta a todo el proceso	MODERADO: Se tendrían que realizar ajustes en los procedimientos del proceso.	MODERADA Confidencialidad 4 Impacto 1 Logro 5 Operativo 2	ACCIÓN 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	3%	65%	MEDIO	Revisar y actualizar cada mes el firewall para mantenerlo en funcionamiento y control	Realizar pruebas de acceso de dispositivos Control A13.2	Prevenir la pérdida, 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 TC	1/05/2023	31/12/2023	No de políticas actualizadas / No de políticas actualizadas
Sistemas de Información y aplicaciones de Software	SIRFA	6	Confidencialidad Integridad Disponibilidad	No funcionamiento del software, Corrupción de datos	Profesional Universitario	Pérdida de información	Exceso de tiempo de ejecución de datos erróneos en los programas de aplicación, Asesinato de copias de respaldo a backup de la información	MODERADO: El evento podría ocurrir en algún momento	MODERADO: Se tendrían que realizar ajustes en los procedimientos del proceso	MODERADA Confidencialidad 3 Impacto 3 Logro 5 Operativo 3	REDUCIR EL RIESGO: Se adoptan medidas para reducir la probabilidad o el impacto del riesgo, transfiriendo compromisos a una parte de este	Realizar backup de los bases de datos del programa SIRFA mínimo 15 al mes	Profesional TIC	15%	60%	MEDIO	Realizar y verificar las copias de seguridad según procedimientos establecidos	Realizar 15 copias de seguridad según procedimientos establecidos Control A12.3	Assegurar de que la seguridad de la información está clasificada e implementada dentro del ciclo de vida de desarrollo de los sistemas de información.	Realizar copia en el servidor y en la nube, según procedimientos	Profesional Universitario TC	1/05/2023	31/12/2023	No de copias mantenidas / No de copias programadas
Sistemas de Información y aplicaciones de Software	PDQS CODE	7	Confidencialidad Integridad Disponibilidad	No funcionamiento del software, Corrupción de datos	Profesional Universitario	Pérdida de información	Asesinato de copias de respaldo a backup de la información	MODERADO: El evento podría ocurrir solo en circunstancias excepcionales	MODERADO: Se tendrían que realizar ajustes en los procedimientos del proceso.	BAA Confidencialidad 2 Impacto 2 Logro 5 Operativo 2	COMPARTIR EL RIESGO: Se reduce la probabilidad o el impacto del riesgo transfiriendo compromisos a una parte de este	Tener el backup por lo menos 20 días anteriores de la base de datos	Profesional TIC	3%	40%	MEDIO	Realizar y verificar las copias de seguridad según procedimientos establecidos	Mantener 20 copias de seguridad de los datos Control A12.2	Assegurar de que la seguridad de la información está clasificada e implementada dentro del ciclo de vida de desarrollo de los sistemas de información.	Realizar copia en el servidor y en la nube, según procedimientos	Profesional Universitario TC	1/05/2023	31/12/2023	No de copias mantenidas / No de copias programadas
Sistemas de Información y aplicaciones de Software	Aplicativos de las entidades de Control	8	Confidencialidad Integridad Disponibilidad	No funcionamiento del software, rol de internet y del Firewall	Profesional Universitario	Pérdida de información	Asesinato de documentos de identificación y autenticación como la actualización de usuarios	MODERADO: El evento podría ocurrir solo en circunstancias excepcionales	MODERADO: Se tendrían que realizar ajustes en los procedimientos del proceso.	BAA Confidencialidad 1 Impacto 1 Logro 5 Operativo 2	COMPARTIR EL RIESGO: Se reduce la probabilidad o el impacto del riesgo transfiriendo compromisos a una parte de este	Realizar actualizaciones y pruebas con rolles para su actividad	Profesional TIC	3%	30%	BAJO	Verificar el estado del internet, las actualizaciones de los equipos y el antivirus	Mantener la seguridad de la información transfiriendo dentro de una organización y con realizar entidad externa	Revisión de equipos, actualizaciones y el antivirus	Profesional Universitario TC	1/05/2023	31/12/2023	No de mantenimientos preventivos/ No mantenimientos actualizados	
Sistemas de Información y aplicaciones de Software	Aplicativos de portales bancarios	9	Confidencialidad Integridad Disponibilidad	No funcionamiento del software, rol de internet y del Firewall	Profesional Universitario	Pérdida de información	Asesinato de documentos de identificación y autenticación como la actualización de usuarios	MODERADO: El evento podría ocurrir solo en circunstancias excepcionales	MODERADO: Se tendrían que realizar ajustes en los procedimientos del proceso.	MODERADA Confidencialidad 1 Impacto 1 Logro 5 Operativo 2	REDUCIR EL RIESGO: Se adoptan medidas para reducir la probabilidad o el impacto del riesgo, transfiriendo compromisos a una parte de este	Realizar aplicaciones y pruebas con rolles para su actividad, atender las recomendaciones de los portales	Profesional TIC Funcionario de Desarrollo	3%	40%	BAJO	Verificar el estado del internet, las actualizaciones de los equipos y el antivirus. Realizar plan de mantenimiento	Control A11 A11.1	Prevenir la pérdida, daño, robo o compromiso de activos, y la interrupción de las operaciones de la organización.	Realizar de equipos, actualizaciones y el antivirus, revisión de recomendaciones parches y equipos instalados en el Firewall	Profesional Universitario TC	1/05/2023	31/12/2023	No de mantenimientos preventivos/ No mantenimientos actualizados
Sistemas de Información y aplicaciones de Software	Aplicativos varios	10	Confidencialidad Integridad Disponibilidad	No funcionamiento del software, rol de internet y del Firewall	Profesional Universitario	Pérdida de información	Asesinato de documentos de identificación y autenticación como la actualización de usuarios	MODERADO: El evento podría ocurrir solo en circunstancias excepcionales	MODERADO: Se tendrían que realizar ajustes en los procedimientos del proceso.	BAA Confidencialidad 2 Impacto 1 Logro 5 Operativo 2	COMPARTIR EL RIESGO: Se reduce la probabilidad o el impacto del riesgo transfiriendo compromisos a una parte de este	Realizar aplicaciones y pruebas con rolles para su actividad	Profesional TIC Funcionario de Desarrollo	3%	25%	BAJO	Verificar el estado del internet, las actualizaciones de los equipos y el antivirus. Realizar plan de mantenimiento	Control A11 A11.1	Prevenir la pérdida, daño, robo o compromiso de activos, y la interrupción de las operaciones de la organización.	Revisión de equipos, actualizaciones y el antivirus	Profesional Universitario TC	1/05/2023	31/12/2023	No de mantenimientos preventivos/ No mantenimientos actualizados
Dispositivos de Tecnología de Información- Hardware	Servidores	11	Confidencialidad Integridad Disponibilidad	Fallas tecnológicas	Profesional Universitario	Pérdida de información	Malfuncionamiento/actualización fallida de los medios de almacenamiento	MODERADO: El evento podría ocurrir en algún momento	MODERADO: Se tendrían que realizar ajustes en los procedimientos del proceso	MODERADA Confidencialidad 1 Impacto 1 Logro 5 Operativo 2	ACCIÓN 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 mantenimientos preventivos, realizar auditorías y actualizaciones de seguridad	Control A11 A11.1	Prevenir la pérdida, daño, robo o compromiso de activos, y la interrupción de las operaciones de la organización.	Revisión de equipos, actualizaciones y el antivirus	Profesional Universitario TC	1/05/2023	31/12/2023	No de mantenimientos preventivos/ No mantenimientos actualizados
Dispositivos de Tecnología de Información- Hardware	Equipos de Computo Funcionarios	12	Confidencialidad Integridad Disponibilidad	Fallas tecnológicas	Profesional Universitario	Pérdida de información	Malfuncionamiento/actualización fallida de los medios de almacenamiento	MODERADO: El evento podría ocurrir en algún momento	MODERADO: Se tendrían que realizar ajustes en los procedimientos del proceso.	MODERADA Confidencialidad 1 Impacto 1 Logro 5 Operativo 2	REDUCIR EL RIESGO: Se adoptan medidas para reducir la probabilidad o el impacto del riesgo, transfiriendo compromisos a una parte de este	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	Control A11 A11.1	Prevenir la pérdida, daño, robo o compromiso de activos, y la interrupción de las operaciones de la organización.	Revisión de equipos, actualizaciones y el antivirus	Profesional Universitario TC	1/05/2023	31/12/2023	No de mantenimientos preventivos/ No mantenimientos actualizados
Dispositivos de Tecnología de Información- Hardware	Equipos de Computo Publicos	13	Confidencialidad Integridad Disponibilidad	Fallas tecnológicas	Profesional Universitario	Destrucción de equipos o de medios	Asesinato de equipos de respaldo a backup de la información	MODERADO: El evento podría ocurrir en algún momento	MODERADO: Se tendrían que realizar ajustes en los procedimientos del proceso	MODERADA Confidencialidad 0 Impacto 1 Logro 5 Operativo 2	EVITAR EL RIESGO: Se abandonan las actividades que dan lugar al riesgo, no destruyéndolo ni transfiriendo compromisos a una parte de este	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	Control A11 A11.2	Prevenir la pérdida, daño, robo o compromiso de activos, y la interrupción de las operaciones de la organización.	Revisión de equipos, actualizaciones y el antivirus	Profesional Universitario TC	1/05/2023	31/12/2023	No de mantenimientos preventivos/ No mantenimientos actualizados
Soporte para almacenamiento de información:	Nube Google Drive	14	Confidencialidad Integridad Disponibilidad	Fallas tecnológicas	Profesional Universitario	Pérdida de información	Asesinato de documentos de identificación y autenticación como la actualización de usuarios	MODERADO: El evento podría ocurrir solo en circunstancias excepcionales	MODERADO: Se tendrían que realizar ajustes en los procedimientos del proceso.	BAA Confidencialidad 2 Impacto 1 Logro 5 Operativo 2	COMPARTIR EL RIESGO: Se reduce la probabilidad o el impacto del riesgo transfiriendo compromisos a una parte de este	Mantener activo la nube y borrar los mantenimientos respectivos	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 servicios	Revisión de políticas de copia de seguridad y a la nube de Google Drive	Profesional Universitario TC	1/05/2023	31/12/2023	No de copias mantenidas / No de copias programadas
Servicio:	Internet	15	Confidencialidad Integridad Disponibilidad	Fallas tecnológicas, Falso del equipo de telecomunicaciones, soporte técnico por parte del proveedor de mantenimiento	Profesional Universitario	Punto débil de falla	Asesinato de equipos para respaldar el proceso	MODERADO: El evento podría ocurrir en algún momento	MODERADO: Se tendrían que realizar ajustes en los procedimientos del proceso.	MODERADA Confidencialidad 0 Impacto 2 Logro 5 Operativo 2	EVITAR EL RIESGO: Se abandonan las actividades que dan lugar al riesgo, no destruyéndolo ni transfiriendo compromisos a una parte de este	Revisión diaria, realizar conectividad diagnóstica	Profesional TIC	20%	30%	BAJO	Verificar el internet diariamente el tener actividades y mantener constante comunicación con el proveedor	Control A15.2	Mantener el nivel acordado de seguridad de la información y de protección del servicio en línea con los usuarios con los proveedores.	Revisar la velocidad de bajada, la velocidad de subida, la latencia y tracer y ping constantemente	Profesional Universitario TC	1/05/2023	31/12/2023	Hora de caída sin internet / Tiempo largo del internet
Servicio:	Telefonos IP	16	Confidencialidad Integridad Disponibilidad	Fallas tecnológicas, Falso del equipo de telecomunicaciones, soporte técnico por parte del proveedor de mantenimiento	Profesional Universitario	Punto débil de falla	Interrupción de comunicación de voz	MODERADO: El evento podría ocurrir en algún momento	MODERADO: Se tendrían que realizar ajustes en los procedimientos del proceso.	MODERADA Confidencialidad 2 Impacto 1 Logro 5 Operativo 2	COMPARTIR EL RIESGO: Se reduce la probabilidad o el impacto del riesgo transfiriendo compromisos a una parte de este	Revisión de conectividad diaria	Profesional TIC	20%	25%	BAJO	Verificar diariamente el nivel de actividad y mantener constante comunicación con el proveedor	Control A15.2	Mantener el nivel acordado de seguridad de la información y de protección del servicio en línea con los usuarios con los proveedores.	Revisión de cambio e interoperación de los telefonos IP	Profesional Universitario TC	1/05/2023	31/12/2023	Incidente con los telefonos IP / Actividad en horas de los telefonos
Servicio:	Camara de Seguridad	17	Confidencialidad Integridad Disponibilidad	Fallas tecnológicas, Pérdida del suministro de energía	Profesional Universitario	Punto débil de falla	Asesinato de una cámara electrónica	MODERADO: El evento podría ocurrir solo en circunstancias excepcionales	MODERADO: Se tendrían que realizar ajustes en los procedimientos del proceso.	MODERADA Confidencialidad 0 Impacto 1 Logro 5 Operativo 2	COMPARTIR EL RIESGO: Se reduce la probabilidad o el impacto del riesgo transfiriendo compromisos a una parte de este	Revisión de conectividad diaria	Profesional TIC	5%	15%	BAJO	Verificar el funcionamiento de las cámaras de seguridad diariamente	Control A13.1	Assegurar la protección de la información de la cámara, y sus mantenimientos de procesamiento de información de soporte.	Realizar copia de las cámaras y estado de las mismas automáticamente	Profesional Universitario TC	1/05/2023	31/12/2023	No de cámaras activas / No cámaras en uso