



El futuro digital es de todos

Gobierno de Cundinamarca MiNTIC

### Mapa de Riesgos de Seguridad de la Información



El futuro digital es de todos

Gobierno de Cundinamarca 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 Telefono: 001 8979300 Celular 311264878				
----------------------	--	--	--	--	--	--	-------------------	--	---	--	--	--	--

IDENTIFICACION DEL RIESGO			ANÁLISIS DEL RIESGO INHERENTE						IDENTIFICACION DE CONTROLES			RESGO 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	Página Web Institucional	1	Confidencialidad Integridad Disponibilidad	Desconocimiento de la Ley de Transparencia y el acceso TIC de la estructura general de la redación que en su caso se debe publicar por parte de los funcionarios y contratistas.	Profesional Universitario	Fallas humanas	Falta de capacitación	BAJA	MODERADO: Afecta de la imagen, de la credibilidad y de la confianza.	ALTA	ACEPTAR EL RIESGO: No se adopta ninguna medida que afecte la probabilidad e impacto del riesgo.	Solicitar constantemente a los productores de la información que se actualice a página Web Interno	* Profesional TIC * Secretario y * Director de Desarrollo Operativo 2	25%	55%	ALTO	Revisar mensualmente la matriz de la estructura general de la redación y actualizar información en caso de cambios de funciones y constantes.	Matriz de ITA y del respectivo Control AS1.1	Cumplimiento de requisitos legales y contractuales	Revisión mensual matriz ITA	Profesional Universitario TIC	1.01.2023	31/12.2023	No Reservas / No Reservas solicitadas
Información y datos de la entidad	Correas Electrónicas	2	Confidencialidad Integridad Disponibilidad	Recepción de Archivos Maliciosos, espías, Phishing, Publicidad espionaje (Spies), intercepto de información y datos.	Profesional Universitario	Fallas humanas	Desconocimiento de los protocolos de seguridad y privacidad de la información	BAJA	MODERADO: Afecta de la imagen, de la credibilidad y de la confianza.	ALTA	ACEPTAR EL RIESGO: No se adopta ninguna medida que afecte la probabilidad e impacto del riesgo.	Solicitar constantemente a los usuarios la apertura y contenidos del correo electrónico	* Profesional TIC * Secretario y * Director de Desarrollo Operativo 2	30%	55%	ALTO	Revisar y mantener los correos activos con el proveedor.	Mantener las copias de respaldo de los correos electrónicos	Mantener los correos activos e iniciar el acceso autorizado a internet y servidores	Revisión mensual de correos	Profesional Universitario TIC	1.01.2023	31/12.2023	No Reservas / No Reservas solicitadas
Información y datos de la entidad	Servidor de Archivos	3	Confidencialidad Integridad Disponibilidad	Abuso de los derechos de almacenamiento	Profesional Universitario	Fallas humanas	Asesoría de copia de respaldo o backup de la información	MODERADO: Se afecta a todo el proceso	MODERADO: Afecta a todo el proceso	MODERADA	REDUCIR EL RIESGO: Se adopta medidas para reducir la probabilidad e impacto del riesgo e impactos por la generalización de la implementación de controles	Realizar Backup del servidor en físico y en la nube	Profesional TIC	30%	35%	MEDIO	Revisar el servidor de archivos, realizando mantenimiento preventivo y optimización de recursos	Mantener el servidor de archivos con el sistema de respaldo de información	Asesorar al acceso de los usuarios autorizados a realizar el acceso autorizado a internet y servidores	Realizar mantenimiento del servidor mensual	Profesional Universitario TIC	1.01.2023	31/12.2023	No mantenimientos / No mantenimientos programados
Información y datos de la entidad	Software Abstracto	4	Confidencialidad Integridad Disponibilidad	Error de uso por parte de los funcionarios	Profesional Universitario	Perdida de información	Configuración incorrecta de parámetros	MODERADO: Se afecta a todo el proceso	MODERADO: Afecta a todo el proceso	MODERADA	REDUCIR EL RIESGO: Se adopta medidas para reducir la probabilidad e impacto del riesgo e impactos por la generalización de la implementación de controles	Verificar la actividad de los servidores de Abstracto y en los equipos instalados	Profesional TIC	30%	30%	MEDIO	Mantener actualizados los recursos en los equipos, realizar backup preventivo en el servidor de Abstracto	Mantener actualizado el sistema de Abstracto	Los equipos deben estar actualizados o programados para reducir el riesgo debido a amenazas o ataques del entorno	Revisión semanal de servidor de Abstracto	Profesional Universitario TIC	1.01.2023	31/12.2023	No Reservas / No Reservas solicitadas
Información y datos de la entidad	Personal Personal	5	Confidencialidad Integridad Disponibilidad	Angustia entrada de los derechos de acceso	Profesional Universitario	Perdida de información	Configuración incorrecta de parámetros	BAJO	BAJO: Se afectan que realizar acciones de procedimientos del proceso	MODERADA	ACEPTAR EL RIESGO: No se adopta ninguna medida que afecte la probabilidad e 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 los funcionamiento y control	Hacer pruebas de acceso en distintos equipos	Prevenir la pérdida, daño, robo o compromiso de activos, y la interrupción de los operativos de la organización	Realizar pruebas de acceso en equipos de la organización	Profesional Universitario TIC	1.01.2023	31/12.2023	No de políticas actualizadas / No de políticas efectivas
Recursos de información y aplicaciones de software	SINRA	6	Confidencialidad Integridad Disponibilidad	Mal funcionamiento del software, Corrupción de datos.	Profesional Universitario	Perdida de información	No tener de copia de respaldo o backup de la información	POSIBLE El evento puede ocurrir en algún momento	MODERADO: Se afecta a todo el proceso	MODERADA	REDUCIR EL RIESGO: Se adopta medidas para reducir la probabilidad e impacto del riesgo e impactos por la generalización de la implementación de controles	Realizar backup de los bases de datos del programa SINRA, mínimo 15 veces	Profesional TIC	5%	60%	MEDIO	Revisar y verificar las copias de seguridad según procedimientos establecidos	Realizar 20 copias de seguridad según procedimientos establecidos	Asesorar de qué la seguridad de la información está diseñada e implementada de acuerdo a los estándares de la información	Realizar copia en el servidor y en la nube según procedimientos	Profesional Universitario TIC	1.01.2023	31/12.2023	No de copias mensuales / No de copias programadas
Recursos de información y aplicaciones de software	FORM CODE	7	Confidencialidad Integridad Disponibilidad	Mal funcionamiento del software, Corrupción de datos.	Profesional Universitario	Perdida de información	No tener de copia de respaldo o backup de la información	POSIBLE El evento puede ocurrir en algún momento	BAJO: Se afectan que realizar acciones de procedimientos del proceso	MODERADA	REDUCIR EL RIESGO: Se adopta medidas para reducir la probabilidad e impacto del riesgo e impactos por la generalización de la implementación de controles	Realizar backup por la noche 50 días anteriores de la base de datos	Profesional TIC	5%	40%	MEDIO	Revisar y verificar las copias de seguridad según procedimientos establecidos	Mantener 10 copias de seguridad en la nube	Asesorar de qué la seguridad de la información está diseñada e implementada de acuerdo a los estándares de la información	Realizar copia en el servidor y en la nube según procedimientos	Profesional Universitario TIC	1.01.2023	31/12.2023	No de copias mensuales / No de copias programadas
Recursos de información y aplicaciones de software	Aplicativos de las entidades de control	8	Confidencialidad Integridad Disponibilidad	Mal funcionamiento del software, no de internet y del Firewall	Profesional Universitario	Perdida de información	Asesoría de respaldo de información y actualización, como la actualización de usuarios	BAJO	BAJO: Se afectan que realizar acciones de procedimientos del proceso	MODERADA	REDUCIR EL RIESGO: Se adopta medidas para reducir la probabilidad e impacto del riesgo e impactos por la generalización de la implementación de controles	Revisar aplicaciones y puntos que vitorear para su actividad	Profesional TIC	5%	30%	BAJO	Verificar el estado del internet, las actualizaciones de los equipos y el antivirus.	Revisar la instalación de los aplicativos, manteniendo los equipos actualizados, AS1.2	Mantener la seguridad de la información mediante control de acceso de la organización y con cualquier actividad externa	Revisión de equipos, actualizaciones y el antivirus	Profesional Universitario TIC	1.01.2023	31/12.2023	No de mantenimientos preventivos/ No mantenimientos solicitados
Recursos de información y aplicaciones de software	Aplicativos de portales bancarios	9	Confidencialidad Integridad Disponibilidad	Mal funcionamiento del software, no de internet y del Firewall	Profesional Universitario	Perdida de información	Asesoría de respaldo de información y actualización, como la actualización de usuarios	BAJO	BAJO: Se afectan que realizar acciones de procedimientos del proceso	MODERADA	REDUCIR EL RIESGO: Se adopta medidas para reducir la probabilidad e impacto del riesgo e impactos por la generalización de la implementación de controles	Revisar aplicaciones y puntos que vitorear para su actividad	Profesional TIC Funcionario Desarrollo	5%	40%	BAJO	Verificar el estado del internet, las actualizaciones de los equipos y el antivirus.	Control AS1 A11.1	Prevenir la pérdida, daño, robo o compromiso de activos, y la interrupción de los operativos de la organización	Revisión de equipos, actualizaciones y el antivirus, revisión de recomendaciones de los operativos de la organización	Profesional Universitario TIC	1.01.2023	31/12.2023	No de mantenimientos preventivos/ No mantenimientos solicitados
Recursos de información y aplicaciones de software	Aplicativos varios	10	Confidencialidad Integridad Disponibilidad	Mal funcionamiento del software, no de internet y del Firewall	Profesional Universitario	Perdida de información	Asesoría de respaldo de información y actualización, como la actualización de usuarios	BAJO	BAJO: Se afectan que realizar acciones de procedimientos del proceso	MODERADA	REDUCIR EL RIESGO: Se adopta medidas para reducir la probabilidad e impacto del riesgo e impactos por la generalización de la implementación de controles	Revisar aplicaciones y puntos que vitorear para su actividad	Profesional TIC Funcionario Desarrollo	5%	25%	BAJO	Verificar el estado del internet, las actualizaciones de los equipos y el antivirus.	Control AS1 A11.1	Prevenir la pérdida, daño, robo o compromiso de activos, y la interrupción de los operativos de la organización	Revisión de equipos, actualizaciones y el antivirus	Profesional Universitario TIC	1.01.2023	31/12.2023	No de mantenimientos preventivos/ No mantenimientos solicitados
Recursos de Tecnología de Información-Redes	Servidores	11	Confidencialidad Integridad Disponibilidad	Fallas tecnológicas	Profesional Universitario	Perdida de información	Asesoría de respaldo de información y actualización, como la actualización de usuarios	POSIBLE El evento puede ocurrir en algún momento	MODERADO: Se afecta a todo el proceso	MODERADA	ACEPTAR EL RIESGO: No se adopta ninguna medida que afecte la probabilidad e impacto del riesgo.	Revisar mensualmente el caso de los servidores.	Profesional TIC	30%	30%	BAJO	Verificar el estado de los equipos, realizar mantenimiento preventivo, revisar antivirus y actualizaciones de seguridad	Control AS1 A11.1	Prevenir la pérdida, daño, robo o compromiso de activos, y la interrupción de los operativos de la organización	Revisión de equipos, actualizaciones y el antivirus	Profesional Universitario TIC	1.01.2023	31/12.2023	No de mantenimientos preventivos/ No mantenimientos solicitados
Recursos de Tecnología de Información-Redes	Equipos de Computo Funcionarios	12	Confidencialidad Integridad Disponibilidad	Mantenimiento preventivo/actualización fallas de los medios de almacenamiento	Profesional Universitario	Perdida de información	Mantenimiento preventivo/actualización fallas de los medios de almacenamiento	POSIBLE El evento puede ocurrir en algún momento	MODERADO: Se afecta a todo el proceso	MODERADA	REDUCIR EL RIESGO: Se adopta medidas para reducir la probabilidad e impacto del riesgo e impactos por la generalización de la implementación de controles	Revisar y realizar los mantenimientos respectivos	Profesional TIC	30%	25%	BAJO	Verificar el estado del internet, las actualizaciones de los equipos y el antivirus.	Control AS1 A11.1	Prevenir la pérdida, daño, robo o compromiso de activos, y la interrupción de los operativos de la organización	Revisión de equipos, actualizaciones y el antivirus	Profesional Universitario TIC	1.01.2023	31/12.2023	No de mantenimientos preventivos/ No mantenimientos solicitados
Recursos de Tecnología de Información-Redes	Equipos de Computo Públicos	13	Confidencialidad Integridad Disponibilidad	Fallas tecnológicas	Profesional Universitario	Destrucción de equipos o de medios	Asesoría de respaldo de información y actualización, como la actualización de usuarios	POSIBLE El evento puede ocurrir en algún momento	MODERADO: Se afecta a todo el proceso	MODERADA	REDUCIR EL RIESGO: Se adopta medidas para reducir la probabilidad e impacto del riesgo e impactos por la generalización de la implementación de controles	Revisar y realizar los mantenimientos respectivos	Profesional TIC	30%	15%	BAJO	Verificar el estado del internet, las actualizaciones de los equipos y el antivirus.	Control AS1 A11.1	Prevenir la pérdida, daño, robo o compromiso de activos, y la interrupción de los operativos de la organización	Revisión de equipos, actualizaciones y el antivirus	Profesional Universitario TIC	1.01.2023	31/12.2023	No de mantenimientos preventivos/ No mantenimientos solicitados
Reporte para mantenimiento de información	Hoja Google Drive	14	Confidencialidad Integridad Disponibilidad	Fallas tecnológicas	Profesional Universitario	Perdida de información	Asesoría de respaldo de información y actualización, como la actualización de usuarios	BAJO	BAJO: Se afectan que realizar acciones de procedimientos del proceso	MODERADA	REDUCIR EL RIESGO: Se adopta medidas para reducir la probabilidad e impacto del riesgo e impactos por la generalización de la implementación de controles	Revisar y actualizar los archivos según procedimientos	Profesional TIC	30%	30%	BAJO	Verificar el estado del internet, las actualizaciones de los equipos y el antivirus.	Control A17.1	Evitar el acceso no autorizado a sistemas y aplicaciones	Revisión de políticas de copia de seguridad y aplicaciones	Profesional Universitario TIC	1.01.2023	31/12.2023	No de copias mensuales / No de copias programadas
Redes	Internet	15	Confidencialidad Integridad Disponibilidad	Fallas tecnológicas, Falta del equipo de telecomunicaciones, soporte técnico por parte del proveedor de mantenimiento	Profesional Universitario	Punto único de falla	Asesoría de respaldo de información y actualización, como la actualización de usuarios	POSIBLE El evento puede ocurrir en algún momento	MODERADO: Se afectan que realizar acciones de procedimientos del proceso	MODERADA	REDUCIR EL RIESGO: Se adopta medidas para reducir la probabilidad e impacto del riesgo e impactos por la generalización de la implementación de controles	Revisar datos, evaluar conectividad de servicios	Profesional TIC	20%	30%	BAJO	Verificar el internet diariamente a través actividades / mantener constante comunicación con el proveedor	Control AS1.2	Mantener el nivel acordado de seguridad de la información y prevención del fraude de línea con los acuerdos con los proveedores	Revisión de la velocidad de banda, la velocidad de subida, la latencia y otros ping constantemente	Profesional Universitario TIC	1.01.2023	31/12.2023	Horas de caídas en internet / Tiempo arriba del internet
Redes	Telefonía IP	16	Confidencialidad Integridad Disponibilidad	Fallas tecnológicas, Falta del equipo de telecomunicaciones, soporte técnico por parte del proveedor de mantenimiento	Profesional Universitario	Punto único de falla	Líneas de comunicación sin protección	POSIBLE El evento puede ocurrir en algún momento	MODERADO: Se afecta a todo el proceso	MODERADA	REDUCIR EL RIESGO: Se adopta medidas para reducir la probabilidad e impacto del riesgo e impactos por la generalización de la implementación de controles	Revisión de conectividad diaria	Profesional TIC	20%	25%	BAJO	Verificar diariamente e iniciar actividades y mantener canales de comunicación con el proveedor	Control AS1.3	Mantener el nivel acordado de seguridad de la información y prevención del fraude de línea con los acuerdos con los proveedores	Revisión de estado de infraestructura de los telefonos IP	Profesional Universitario TIC	1.01.2023	31/12.2023	Incidentes con los telefonos IP / Actividad en horas de los telefonos
Redes	Cameras de Seguridad	17	Confidencialidad Integridad Disponibilidad	Fallas tecnológicas, Falta del equipo de telecomunicaciones, soporte técnico por parte del proveedor de mantenimiento	Profesional Universitario	Punto único de falla	Asesoría de respaldo de información y actualización, como la actualización de usuarios	POSIBLE El evento puede ocurrir en algún momento	MODERADO: Se afectan que realizar acciones de procedimientos del proceso	MODERADA	REDUCIR EL RIESGO: Se adopta medidas para reducir la probabilidad e impacto del riesgo e impactos por la generalización de la implementación de controles	Revisión de conectividad diaria	Profesional TIC	5%	15%	BAJO	Verificar el funcionamiento de las cámaras de seguridad de la información	Control AS1.3	Revisar copias de las cámaras e iniciar de las mismas mantenimiento	Revisión de las cámaras e iniciar de las mismas mantenimiento	Profesional Universitario TIC	1.01.2023	31/12.2023	No de cámaras activas / No de cámaras en uso
Recursos de Tecnología de Información-Redes	BASE PRIVADA NAS	18	Confidencialidad Integridad Disponibilidad	Angustia entrada de los derechos de acceso	Profesional Universitario	Perdida de información	Configuración incorrecta de parámetros	BAJO	BAJO: Se afectan que realizar acciones de procedimientos del proceso	MODERADA	REDUCIR EL RIESGO: Se adopta medidas para reducir la probabilidad e impacto del riesgo.	Verificar permisos y accesos de los equipos de la NAS	Profesional TIC	5%	65%	MEDIO	Revisar y entrar cada mes a la NAS para establecer los funcionamiento y control	Hacer pruebas de acceso en distintos equipos	Prevenir la pérdida, daño, robo o compromiso de activos, y la interrupción de los operativos de la organización	Realizar pruebas de acceso a NAS de los operativos de la organización	Profesional Universitario TIC	1.01.2023	31/12.2023	No de políticas actualizadas / No de políticas efectivas