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

Tipo de Activo de Información	Proceso	Activo de Información	Nro.	Dueño del activo	Propiedad que afecta el Riesgo	Causa	Descripción del Riesgo	Responsable de determinar la materialización del riesgo	Amenazas	Vulnerabilidades
Información y datos de la entidad:	Todos los Procesos	**Pagina Web Institucional**	1	Todos los directores y jefes de despacho	**Confidencialdad Integridad Disponibilidad**	Desconocimiento de la Ley de Transparencia y la matriz ITA de la procuraduria general de la nación de que es que lo que se debe publicar por parte de los funcionarios y contratistas	Posibilidad que no se cumplacon la Ley de Transparencia y la matriz ITA de la procuraduria general de la nación respecto a la publicación de la informacion en la pagina Web	Profesional Universitario	Fallas humanas	Retraso en la entrega de información por parte del personal
Información y datos de la entidad:	Todos los Procesos	**Correo Electronico**	2	Todos los directores y jefes de despacho	**Confidencialdad Integridad Disponibilidad**	Desconocimiento y reconocimiento por parte de los funcionarios sobre los controles en la recepcion de correos que contienen archivos maliciosos, taques Phishing, Publicidad engañosa (Spam), Búsqueda de información y datos	Posibilidad que los funcionarios de la Administracón Municipal abran correos con Archivos Maliciosos, ataques Phishing, Publicidad engañosa (Spam), Búsqueda de información y datos	Profesional Universitario	Fallas humanas	Desconocimiento o no aplicación de las políticas de seguridad y privacidad de la información
Información y datos de la entidad:	Todos los Procesos	**Servidor de Archivos**	3	Todos los directores y jefes de despacho	**Confidencialdad Integridad Disponibilidad**	Abuso de los derechos de almacenamiento por parte de los funcionarios y contratistas	Posibilidad de perdida de la información por el abuso de los derechos de almacenamiento por parte de los funcionarios y contratistas	Profesional Universitario	Fallas humanas	Ausencia de copias de respaldo o backups de la información
Información y datos de la entidad:	Todos los Procesos	**Software Antvirus**	4	Todos los directores y jefes de despacho	**Confidencialdad Integridad Disponibilidad**	Error de Uso por parte de los funcionarios y desconocimientmo de las alertas de seguridad	Posibilidad de que se presenten infecciones en el equipo de computo por omision a los protocolos de seguridad y las alertas del antivirus	Profesional Universitario	Perdida de Información	Configuración incorrecta de parámetros
Información y datos de la entidad:	Todos los Procesos	**Firewall Perimetral**	5	Direccion de Planeacion	**Confidencialdad Integridad Disponibilidad**	Desconocimiento en la aplicación de los controles del Fireword	Posibilidd de Asignación errada de los derechos de acceso a paginas Web que ponga en riesgo la seguridad de la información	Profesional Universitario	Perdida de Información	Configuración incorrecta de parámetros
Sistemas de información y aplicaciones de Software	Gestion de Desarrollo Urbano, Gestion de Talento Humano, Gestion Financiera, Gestion logistica y abastecimiento	**SINFA**	6	Secretario de Hacienda	**Confidencialdad Integridad Disponibilidad**	Desconocimietno por parte de los funcionarios de reporte a tiempo de incidencias de Seguridad de la información	Posibilidad de que se genere errores en el funcionamiento del software SINFA por parte de los funcionarios por uso indebido del programay produzca 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
Sistemas de información y aplicaciones de Software	Todos los Procesos	**PQRS CODE**	7	Secretario de Gobierno	**Confidencialdad Integridad Disponibilidad**	Desconocimietno por parte de los funcionarios de reporte a tiempo de incidencias de Seguridad de la información	Posibilidad de que se genere errores en el funcionamiento del software PQRS por parte de los funcionarios por uso indebido del programay produzca corrupción de datos	Profesional Universitario	Perdida de Información	Ausencia de copias de respaldo o backups de la información
Sistemas de información y aplicaciones de Software	Gestion estrategica, Gestion de darriollo urbano, Gestion de Educacion, Gestion de la Salud, Gestion Desarrollo social, Gestion DesarrolloEconomico, Gestion para la seguridad, Gestion de Talento humano, Gestion Financiera, Gestion de logistica, Gestion juridica y contratación, Gestion TIC, Gestion integral de control interno	**Aplicativos de las entidades de control**	8	Todos los directores y jefes de despacho	**Confidencialdad Integridad Disponibilidad**	Cargue incorrecto de informacion a los aplicativos de las entidades control por parte de los funcionarios designados Fallas en el suminsitro de energia electrica	Posibilidad que se genere errores en el cargue de información por mal funcionamiento de las plataformas, caida de servicio de Intenet y fallas electricas	Profesional Universitario	Perdida de Información	Ausencia de mecanismo de identificación y autenticación, como la autenticación de usuario
Sistemas de información y aplicaciones de Software	Gestion Financiera	**Aplicativos de portales bancarios**	9	Secretario de hacienda y tesoreria	**Confidencialdad Integridad Disponibilidad**	Cargue incorrecto de informacion a los aplicativos bancarios por parte de los funcionarios designados Fallas en el suminsitro de energia electrica	Posibilidad que se genere errores en el cargue de información por mal funcionamiento de las plataformas bancarias, caida de servicio de Intenet y fallas electricas	Profesional Universitario	Perdida de Información	Ausencia de mecanismo de identificación y autenticación, como la autenticación de usuario
Sistemas de información y aplicaciones de Software	Gestion estrategica, Gestion de darriollo urbano, Gestion de Educacion, Gestion de la Salud, Gestion Desarrollo social, Gestion DesarrolloEconomico, Gestion para la seguridad, Gestion de Talento humano, Gestion Financiera, Gestion de logistica, Gestion juridica y contratación, Gestion TIC, Gestion integral de control interno	**Aplicativos varios**	10	Todos los directores y jefes de despacho	**Confidencialdad Integridad Disponibilidad**	Cargue incorrecto de informacion a los aplicativos varios por parte de los funcionarios designados Fallas en el suminsitro de energia electrica	Posibilidad que se genere errores en el cargue de información por mal funcionamiento de las plataformas varias, caida de servicio de Intenet y fallas electricas	Profesional Universitario	Perdida de Información	Ausencia de mecanismo de identificación y autenticación, como la autenticación de usuario
Dispositivos de Tecnologías de información-Hardware:	Todos los Procesos	**Servidores**	11	Direccion de Planeacion	**Confidencialdad Integridad Disponibilidad**	Falta de aplicación de las politicas de mantenimiento de los equipos de computo	Posibilidad de que se presenten Fallas tecnologicas por falta de mantenimietno de los servidores	Profesional Universitario	Perdida de Información	Ausencia de mecanismo de identificación y autenticación, como la autenticación de usuario
Dispositivos de Tecnologías de información-Hardware:	Todos los Procesos	**Equipos de Computo funcionarios**	12	Todos los directores y jefes de despacho	**Confidencialdad Integridad Disponibilidad**	Falta de aplicación de las politicas de mantenimiento de los equipos de computo	Posibilidad de que se presenten Fallas tecnologicas por falta de mantenimietno de los equipos de computo	Profesional Universitario	Perdida de Información	Mantenimiento insuficiente/instalación fallida de los medios de almacenamiento
Dispositivos de Tecnologías de información-Hardware:	Gestion de Educacion, Gestion de para la cultura y la juventuid	**Equipos de Computo Publicos**	13	Secretario de Educacion, cultura y juventud	**Confidencialdad Integridad Disponibilidad**	Falta de aplicación de las politicas de mantenimiento de los equipos de computo	Posibilidad de que se presenten Fallas tecnologicas por falta de mantenimietno de los equipos de computo publicos	Profesional Universitario	Destrucción de equipos o de medios	Ausencia de esquemas de reemplazo periódico
Soporte para almacenamiento de información:	Todos los Procesos	**Nube Google Drive**	14	Todos los directores y jefes de despacho	**Confidencialdad Integridad Disponibilidad**	Desconocimiento por parte de los funcionarios del uso adecuado de almacenamiento de la información en la nube	Posiblidad que se presente fallas tecnologicas en el proceso de almacenamiento de información por uso indebido de la nube google drive y duplicidad de la información	Profesional Universitario	Perdida de Información	Ausencia de mecanismo de identificación y autenticación, como la autenticación de usuario
Servicios:	Todos los Procesos	**Internet**	15	Todos los directores y jefes de despacho	**Confidencialdad Integridad Disponibilidad**	Falta de aplicaion de los ANS (acuerdos nativos de servicio) con el proveedor de internet	Posibilidad que se presete fallas tecnologicas, Falla del equipo de telecomunicaciones, soporte tardio por parte del proveedor de restablecimiento del servicio	Profesional Universitario	Punto único de falla	Ausencia de segundo canal de internet para respaldar el primero
Servicios	Gestion para la Seguridad, Gestion TIC	**Camara de Seguridad**	16	Direcion de planeacion	**Confidencialdad Integridad Disponibilidad**	Falta de aplicación dela politica de tratamientode datos personales Falla electrica	Posibilidad de el sistema de CCTV no cumpla con su funcioonabilidad por falta de implementacion de la politica de protecion y tratamiento de datos personales, Pérdida del suministro de energía	Profesional Universitario	Punto único de falla	Falta de implementacion de la politica de tratamiento de datos personales Ausencia de una planta electrica
Dispositivos de Tecnologías de información-Hardware:	Todos los Procesos	**NUBE PRIVADA NAS**	17	Direccion de Planeacion	**Confidencialdad Integridad Disponibilidad**	Falta de aplicación de las politicas de mantenimiento de los equipos de computo	Posibilidad de que se presenten Fallas tecnologicas por falta de mantenimietno de los servidor NAS	Profesional Universitario	Perdida de Información	Configuración incorrecta de parámetros
Servicios	Todos los Procesos	UPS	18	Direccion de Planeacion	**Integridad disponibilidad**	Fallas en el suminsitro de energia electrica	Posibilidad que se genere errores en el cargue de información por mal funcionamiento de las plataformas bancarias, caida de servicio de Intenet y fallas electricas	Profesional Universitario	Perdida de Información	Mantenimiento insuficiente/saño en las baterias

ANÁLISIS DEL RIESGO INHERENTE / IDENTIFICACIÓN DE CONTROLES / RIESGO RESIDUAL

Nro.	Probabilidad (inherente)	Impacto (inherente)	Zona de Riesgo	Opciones de manejo del riesgo	Descripción del control	Responsable de ejecutar el control	Probabilidad (residual)	Impacto (residual)	Zona de Riesgo Residual
1	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
2	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
3	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
4	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
5	RARO El evento puede ocurrir solo en circunstancias excepcionales	MENOR: Se tendrían que realizar ajustes en los procedimientos del proceso	ALTA Confidencialidad 4 Imagen 3 Legal 3 Operativo 2	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
6	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
7	RARO El evento puede ocurrir solo en circunstancias excepcionales	MENOR: 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 ocompartiendo una parte de este	Tener el backup por lo menos 10 días anteriores de la base de datos	Profesional TIC	5%	40%	MEDIO
8	RARO El evento puede ocurrir solo en circunstancias excepcionales	MENOR: 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 ocompartiendo una parte de este	Revisar aplicaciones y puertos que utiliza para su actividad	Profesional TIC	5%	30%	BAJO
9	RARO El evento puede ocurrir solo en circunstancias excepcionales	MENOR: 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
10	RARO El evento puede ocurrir solo en circunstancias excepcionales	MENOR: 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 ocompartiendo una parte de este	Revisar aplicaciones y puertos que utiliza para su actividad	Profesional TIC Funcionario Encargado	5%	25%	BAJO
11	POSIBLE: El evento podría ocurrir en algún momento	MODERADO: Se afecta a todo el proceso	MODERADA Confidencialidad 1 Imagen 1 Legal 1 Operativo 3	ACEPTAR EL RIESGO: No se adopta ninguna medida que afecte la probabilidad o el impacto del riesgo.	Revisar mensualmete el uso de los servidores	Profesional TIC	10%	30%	BAJO
12	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
13	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
14	RARO El evento puede ocurrir solo en circunstancias excepcionales	MENOR: Se tendrían que realizar ajustes en los procedimientos del proceso	BAJA Confidencialidad 2 Imagen 1 Legal 1 Operativo 2	COMPARTIR EL RIESGO: Se reduce la probabilidad o el impacto del riesgo transfiriendo ocompartiendo una parte de este	Mantener activa la nube y borrar los archivos según procedimiento	Profesional TIC	10%	30%	BAJO
15	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 4	COMPARTIR EL RIESGO: Se reduce la probabilidad o el impacto del riesgo transfiriendo ocompartiendo una parte de este	Revisión diaria, evaluar conectividad diariamente	Profesional TIC	20%	30%	BAJO
16	RARO El evento puede ocurrir solo en circunstancias excepcionales	MENOR: 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 ocompartiendo una parte de este	Revisión de conectividad diaria	Profesional TIC	5%	15%	BAJO
17	RARO El evento puede ocurrir solo en circunstancias excepcionales	MENOR: 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
18	POSIBLE: El evento podría ocurrir en algún momento	MAYOR Afectación de la imagen, de la credibilidad y de la confianza	MODERADA Confidencialidad 0 Imagen 2 Legal 0 Operativo 4	ACEPTAR EL RIESGO: No se adopta ninguna medida que afecte la probabilidad o el impacto del riesgo.	Revisar y realizar los mantenimientos respectivos	Profesional TIC	25%	70%	MEDIO

MANEJO DEL RIESGO RESIDUAL - Plan de Tratamiento de Riesgos

Nro.	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
1	Revisar trimestral 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 trimestral matriz ITA	Profesional Universitario TIC	1/01/2025	31/12/2025	No Revisones / No Revisones estipuladas
2	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	1/01/2025	31/12/2025	No Revisones / No Revisones estipuladas
3	Revisar el servidor de archivo, realizando mantenimiento preventivo y eliminando archivos no institucionales	Mantener el servidor de archivos con el mantenimiento preventivo, actualizaciones y antivirus Control 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	1/01/2025	31/12/2025	No mantenimientos / No matenimientos programados
4	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	Resvision semanal de servidor de antivirus	Profesional Universitario TIC	1/01/2025	31/12/2025	No Revisones / No Revisones estipuladas
5	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	1/01/2025	31/12/2025	No de politicas actualizadas / No de politicas efectivas
6	Realizar y verificar las copias de seguridad según procedimiento establecido	Realizar 15 copias de seguridad según porcedimiento establecido Control A14,2	Asegurar de que la seguridad de la información esté 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	1/01/2025	31/12/2025	No de copias mensulaes / No de copias programadas
7	Realizar y verificar las copias de seguridad según procedimiento establecido	mantener 10 copias de seguridad en la nube. Control A14,2	Asegurar de que la seguridad de la información esté 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	1/01/2025	31/12/2025	No de copias mensulaes / No de copias programadas
8	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	1/01/2025	31/12/2025	No de mantenimientos preventivos/ No mantenimiento solicitados
9	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 espciales en el firewall	Profesional Universitario TIC	1/01/2025	31/12/2025	No de mantenimientos preventivos/ No mantenimiento solicitados
10	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	1/01/2025	31/12/2025	No de mantenimientos preventivos/ No mantenimiento solicitados
11	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	1/01/2025	31/12/2025	No de mantenimientos preventivos/ No mantenimiento solicitados
12	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	1/01/2025	31/12/2025	No de mantenimientos preventivos/ No mantenimiento solicitados
13	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	1/01/2025	31/12/2025	No de mantenimientos preventivos/ No mantenimiento solicitados
14	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	1/01/2025	31/12/2025	No de copias mensulaes / No de copias programadas
15	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	1/01/2025	31/12/2025	Hora de caidas sin internet / tiempo arriba del internet
16	Verifiar 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	1/01/2025	31/12/2025	No de camaras activas / No camaras en uso
17	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	1/01/2025	31/12/2025	No de politicas actualizadas / No de politicas efectivas
18	Verifiar el funcionamiento de la UPS para establecer su funcionamiento y control	Control A, 11, 2	Prevenir daño de los equipos de computo	Realizar pruebas de funcionamiento al inicio de la jornada	Profesional Universitario TIC	1/01/2025	31/12/2025	Pruebas de fucnionamiento / dias de trabajo diario