MINISTERIO DE AMBIENTE Y DESARROLLO SOSTENIBLE	PLAN DE TRATAMIENTO DE RIESGO	MADSIG Sistema Integrado de Gestión
	Proceso: Gestión de servicios de información y soporte tecnologíco	
Versión: 5	**Vigencia:** 20/10/2022	**Código:** DS-A-GTI-01

N°	Riesgos encontrados	Vulnerabilidades	Tratamiento	Control	Actividad - Control	Responsable	Referencia anexo A	Fecha Máxima de implementación	Estado	Observaciones
1	Daño o Averia en los equipos	No se han implementado políticas de ubicación de equipos de cómputo.	Mitigar	CNTRL001	Documentar, aprobar e implementar Políticas sobre el buen uso de los activos de información.	Gestión de TICs y GTI	A.5.1.1, A.8.1.3	24 de Agosto de 2014	Cerrado	Manual V3
		No se han implementado polticas para evitar el consumo de liquidos y alimentos en los equipos.								
		No hay planes de mantenimiento.		CNTRL007	Documentar, implementar y registrar plan de mantenimiento a los servidores y equipos de cómputo.		A.11.2.4	24 de Agosto de 2014	Cerrado	Procedimiento de mantimiento aprobado grupo sistemas
		Equipos de seguridad ambiental insuficientes.		CNTRL016	Implementar controles ambietales en el Datacenter		A.11.1.4	10 de Diciembre de 2014	Cerrado	Se realizan arreglos al DC
		Falta de mantenimiento en la malla de puesta a Tierra.		CNTRL028	Establecer plan de mantenimiento a la malla de tierra.		A.11.2.4	10 Diciembre de 2014	Cerrado	Se cambian UPSs
2	No disponibilidad de los sistemas de Información.	Datacenter compartido	Mitigar	CNTRL002	Realizar separación de los servidores del Ministerio con los de ANLA.	Gestión de TICs y GTI	A.11.1.2, A.11.1.5	12 Mayo de 2014	Cerrado	Centro de Datos independientes para cada área desde 2014
		No se cuenta con plan de continuidad de negocio para el ministerio	Mitigar	CNTRL020	Diseñar, Documentar, aprobar y probar el Plan de Continuidad de Negocio del Ministerio de Ambiente y Desarrollo Sostenible	Gestión de TICs y GTI	A.17	25 Octubre de 2014	Cerrado	Acuerdo Interadminsitrativo IDEAM
		No se tiene definido un procedimiento de respuesta a eventos e incidentes de seguridad	Mitigar	CNTRL014	Documentar e implementar procedimiento de eventos e incidentes de Seguridad de la Información en el MADS	Gestión de TICs y GTI	A.16	25 de Octubre de 2013	Cerrado	Procedimiento implementado y en ejecución
		Control de la temperatura inadecuado	Mitigar	CNTRL017	Implementar control de temperatura en el Data Center.	Gestión de TICs y GTI	A.11.1.4	18 de Febrero de 2014	Cerrado	Se realiza mantenimeinto y ajustes al sistema de aire acondicionado
		Dependencia del mismo tablero electríco y acometida electríco.	Aceptar	NA	NA	NA	NA	NA	Cerrado	
		Dependencia de una UPS para toda la infraestructura de telecomucaciones.	Mitigar	CNTRL022	Adquirir, configurar, probar e implementar UPS alterna que soporte la infraestructura tecnológica del Ministerio.	Gestión de TICs y GTI	A.11.2.2	10 de Diciembre de 2014	Cerrado	Ejecutado
		No se tiene control de acceso a los centro de cableado.	Mitigar	CNTRL023	Implementar controles de accesos a los centros de cableado.	Gestión de TICs y GTI	A.11.1.2, A.11.1.5	18 de Febrero de 2014	Cerrado	Se iaseguran puertas bajo llave, se asigna control a vigilancia y se deja registro en bitacoras
		No se tieneservidores de contingencia para lograr alta disponibilidad en los servidores críticos.	Mitigar	CNTRL024	Adquirir, configurar, probar e implementar servidores de contingencia para los servidores críticos.	Gestión de TICs y GTI	A.17.2	10 Diciembre de 2014	Cerrado	Servidor de correo único servicio crítico, se implementa con actualización exchange 2015
		Centro de computo con flujo y corriente de aire	Mitigar	CNTRL025	Sellamiento hermético del datacenter	Gestión de TICs y GTI	A.11.1.4	14 Enero de 2015	Cerrado	Se realiza en mantenimiento de datacenter
		No se cuenta con protección física en algunos segmentos del cableado estructurado que comunica el centro de cómputo con los diferentes pisos de la entidad.	Mitigar	CNTRL026	Diseñar y aprobar plan de mejoramiento del cableado estructurado que comunica del datacenter a los diferentes pisos de la entidad.	Gestión de TICs y GTI	A.11.2.3	18 de Marzo de 2014	Cerrado	
		No se monitorean los controles ambientales (Tableros, UPS, Aire Acondicionado)	Mitigar	CNTRL027	Establecer monitoreo de controles ambientales y de UPS para alertar en caso de eventos e incidentes físicos.	Gestión de TICs y GTI	A.11.1.4	10 Diciembre de 2014	Cerrado	ejecutado, se adquiere herramienta de monitoreo
		Acceso Directo a administración de impresoras	MItigar	CNTRL035	Corregir la configuración por defecto y configurar contraseña de acceso	Gestión de TICs y GTI	A.9.4.3	20 Enero de 2014	Cerrado	corregido
3	Perdida de la información	No se cuenta con copias de resplado externas.	Aceptar	CNTRL003	Documentar e implementar políticas o procedimientos de copias de resplado en custodia externa.	Gestión de TICs y GTI	A.12.3	NA	Cerrado	
		No se exige el uso de contraseñas seguras para los accesos a los sistemas de información.	Mitigar	CNTRL006	Documentar e implementar políticas de uso de contraseñas seguras para el acceso a los sistemas de información.	Gestión de TICs y GTI	A.5.1.1, A.9.4.3	12 Septiembre de 2014	Cerrado	Implementado, política en manual, sensibilización a equipo técnico
		Documentación sin la protección adecuada		CNTRL009	Asegurar la correcta ubicación de la documentación física de las historias laborales.	Gestión de TICs y GTI	A.11.1.3	25 de Octubre de 2013	Cerrado	Se implementa archivo
		No se ha implementado un procedimiento de Backups para equipos		CNTRL003	Documentar e implementar políticas o procedimientos de copias de resplado a equipós de cómputo críticos.	Gestión de TICs y GTI	A.12.3	25 Abril de 2014	Cerrado	Back a equipos bajo solicitud
		No se tiene definido un procedimiento de respuesta a eventos e incidentes de seguridad		CNTRL014	Documentar e implementar procedimiento de eventos e incidentes de Seguridad de la Información en el MADS.	Gestión de TICs y GTI	A.16	25 Abril de 2014	Cerrado	Ejecutado
		No hay lugar de almacenamiento seguro para la información de resplado	Aceptar	CNTRL003	Documentar e implementar políticas o procedimientos de copias de resplado en custodia externa.	Gestión de TICs y GTI	A.12.3	Febrero de 2016	Cerrado	Incluir en mejjoramiento BCP

4	Fuga de información	No se han implementado políticas o procedimientos para la asignación y reintegro de privilegios.	Mitigar	CNTRL004	Documentar, aprobar e implementar Políticas o procedimientos para la asignación, verificación y eliminación de los privilegios de los usuarios a los sistemas de información críticos.	Gestión de Talento Humano	5.3, A.9.2	25 Marzo de 2015	Cerrado	Revisión completa (JohnCruz)
		No se cuenta con políticas de transporte de información en medios magnéticos.		CNTRL005	Establecer políticas para el transporte de medios de información cifrados.	Gestión de TICs y GTI	A.13.2.1, A.13.2.2	25 Abril de 2014	Cerrado	Política en Manual, procedimiento de clasificación, manejo y etiquetado (Verificar nuevos riesgos)
		No se exige el uso de contraseñas seguras para los accesos a los sistemas de información		CNTRL006	Documentar e implementar políticas de uso de contraseñas seguras para el acceso a los sistemas de información.	Gestión de TICs y GTI	A.5.1.1, A.9.4.3	25 Marzo de 2015	Cerrado	Manual , cambios en AD
		Documentación sin la confidencialidad adecuada		CNTRL010	Establecer ubicación adecuada de las historías laborales.	Gestión de Talento Humano	A.11.1.3	25 de Octubre de 2013	Cerrado	Realizado con archivador
		No se tiene definido un procedimiento de respuesta a eventos e incidentes de seguridad		CNTRL014	Documentar e implementar procedimiento de eventos e incidentes de Seguridad de la Información en el MADS.	Gestión de TICs y GTI	A.16	25 Abril de 2014	Cerrado	Ejecutado
		No se cuenta con acuerdos de confidencialidad con los funcionarios		CNTRL015	Establecer política para que todos los funcionarios y contratistas del MADS tengan Acuerdos de Confidencialidad o No Divulgación de Información Confidencial.	Gestión de Talento Humano	A.13.2.4	Ver Plan de mejoramiento NC auditoria de certificación	Cerrado	Manual de contratación
		No se cuenta con registros de los privilegios asignados a los funcionarios y contratistas		CNTRL018	Establecer políticas o procedimientos para asignación de privilegios a los funcionarios y contratistas del MADS.	Gestión de Talento Humano	A.9.2.3	25 Marzo de 2015	Cerrado	Verificación (JohnCruz)
		No se cuenta con bloqueos automáticos o políticas de bloqueo manual para la pantalla		CNTRL019	Establecer y aprobar política de bloqueo automático de pantalla tras inactividad del equipo. Política de bloqueo manual al abandonar el puesto de trabajo.	Gestión de TICs y GTI	A.11.2.9	25 Abril de 2014	Cerrado	AD
		No se cuenta con control de acceso a FTP externos	Mitigar	CNTRL029	Establecer y aprobar una política que impida la conexión con FTP externos.	Gestión de TICs y GTI	A.13.1.2	23 Mayo de 2014	Cerrado	Implementación FortiWeb
		Configuración por defecto de servicios	Mitigar	CNTRL032	Una vez realizado el análisis de vulnerabilidades y el ethical hacking configurar con niveles de seguridad adecuados las aplicaciones y servicios que se encuentren configurados por defecto	Gestión de TICs y GTI	A.13.11, A.13.1.2	01-dic-2014	Cerrado	Primeras pruebas realizadas, primer hardening)
		Nivel de cifrado medio o bajo para Terminal Services	Mitigar	CNTRL033	Migrar a aplicaciones de administración con nivel de cifrado seguro como SSH	Gestión de TICs y GTI	A.13.1.2	27-mar-2015	Cerrado	Compra de certifiacdos a certicamara (Ssitemas y TICs)
5	Modificación de la Información	No se exige el uso de contraseñas seguras para los accesos a los sistemas de información	Mitigar	CNTRL006	Documentar e implementar políticas de uso de contraseñas seguras para el acceso a los sistemas de información.	Gestión de TICs y GTI	A.5.1.1, A.9.4.3	12 Septiembre de 2014	Cerrado	Ejecutado
6	Demandas por incumplimiento de normas	Falta formación en aspectos legales, contractuales y regulatorios de la seguridad de la información	Mitigar	CNTRL008	Establecer Plan de formación en temas legales y de protección de la información con Talento Humano.	Gestión de Talento Humano	A.7.2.2	Constante	Cerrado	Se han realizado talleres, sensibilizaciones inducciones y etiquetado de información
7	Suspensión del servicio	No hay personal de respaldo para cargos críticos	Mitigar	CNTRL012	Documentación de los procesos.	Gestión de Mejora Continua	A.12.1.1	Constante	Cerrado	Varias áreas
8	Pérdida de la confidencialidad de información	No hay control sobre la información en los equipos reutilizados	Mitigar	CNTRL011	Documentar e implementar procedimientos o políticas para garantizar la confidencialidad en los equipos de cómputo a reutilizar.	Gestión de TICs y GTI	A.11.2.7	15-dic-15	Cerrado	Verificar equipos en piso -2
		No se cuenta con el uso de HTTPS en Aranda	Aceptar	CNTRL034	NA	Gestión de TICs y GTI	NA	NA	Cerrado	
		No se tiene actualizados parches de seguridad	Mitigar	CNTRL036	Verificar la versión del software instalado en los servidores, verificar la versión actual en la que se encuentra el software en cada servidor actualizar y/o parchar si las caracteristicas técnicas lo permiten	Gestión de TICs y GTI	A.12.6.1	15-dic-15	Cerrado	Actualización plataforma Vm
9	Denegación de Servicio	Back Up de canal de internet sin doble anillo de fibra optica	Aceptar	CNTRL013	NA	NA	NA	NA	Cerrado	
		Configuración por defecto de servicios	Evitar	CNTRL034	Una vez realizado el análisis de vulnerabilidades y el ethical hacking configurar con niveles de seguridad adecuados las aplicaciones y servicios que se encuentren configurados por defecto	Gestión de TICs y GTI	A.12.6.1	15-dic-15	Cerrado	
10	Suplantación de Identidad	No se tiene bloqueado el servicio mail RELAY	Evitar	CNTRL031	Apagar el servicio en el servidor de correo Xchange, si el servicio es necesario para el funcionamiento adecuado del buzon de correo cerrar el puerto 25 del servidor que permite la conexión externa.	Gestión de TICs y GTI	A.13.2.3	15-dic-15	Cerrado	Actualización Exchange 15 Dic de 2015
11	Pérdida de Gobierno de Información	EL nivel de cifrado y la herramienta usada no permititía la recuperación de la inforamción.	Mitigar		Se maneja sobre cerrado con contraseña, pendiente mejorar herramienta	GTI	A.13.2.1, A.13.2.2	15-dic-15	Cerrado	Vera crypt

12	Fuga de información	Gestión de medios removibles	Mitigar		Licenciamiento Kaspersky no permite una gestión integral de los medios removibles se evaluará módulo DLP en fortiSanbox	Gestión de TICs y GTI	A.10.7.1	01-dic-18	Abierto	
		Uso de dispositivos móviles BYOD	Mitigar		Se deben establecer políticas para el uso de dispositivos personales, establecer controles y restricciones sobre la red, ejercer control de licencias disponibles para correos móviles y Backup al firmar salida.	Gestión de TICs y GTI	A5.1.1	01-dic-18	Abierto	Se implementan los controles necesarios. Pendiente revisión políticas BYOD
		Deficiencias en borrado seguro por Volumen de equipos	Mitigar		Capacitación Mesa de Ayuda,documentación procedimiento, llevar control sobre la aplicación del mismo	Gestión de TICs y GTI	A.9.2.6, A.10.7.2	01-dic-17	Cerrado	Se documenta procedimiento, mesa de ayuda lleva a cabo procedimientos de borrado seguro, se tiene acuerdo a través del Sistema de Gestión Ambiental para cuándo se dan de baja equipos
		Deficiencia en el monitoreo de información	Mitigar		Adquirir SIEM para monitoreo de eventos tanto dentro de la red como en el perimetro permitiendo la correlación y análisis para respuesta a incidentes	GTI	-	01-dic-17	Cerrado	Se implementienta SIEM en la red, el cuál se encuentra en proceso de constante afinamiento.
13	Pérdida de la Disponibilidad de la información	Deficiencias en la definición de requisitos y pruebas de Coninuidad de negocio	Mitigar		Se proyecta mejora de los referente a continuidad de negocio gestionando la ctualización, mejora y prueba de acuerdo a la norma ISO 22301, se proyecta prueba para Nov de 2017	GTI	.	01-dic-17	Abierto	Se realiza proceso de contratación. Es necesario realizar pruebas sobre la continuidad del mismo.
14	No disponibilidad de los sistemas de Información.	Desactualización en parches, tecnología y pérdida de soporte	Mitigar		Se debe programar actualización periodica en el software que soporta los sistemas de información	GTI	-	01-dic-18	Abierto	Se deben actualizar todas las platadormas de los sistemas de información del Minsiterio. Durante 2017 se actualziaron plataformas de seguridad perimetral.
15	Pérdida de Gobierno de Información	Pérdida del control, acceso y confidencialidad de la información del MADS en sistemas de información de terceros tales como SIGDMA	Mitigar		Establecer controles y políticas para el sistema de información	Gestuón de TICs y GTI	-	01-dic-18	Abierto	Se cuenta con acta de confidealizdad, se requiere plan de migración y controles para exportar información