MINISTERIO DE AMBIENTE Y DESARROLLO SOSTENIBLE	PLAN DE TRATAMIENTO DE RIESGOS Proceso : Gestion de Tecnologias y Soporte de Informacion	MADSIG
Version 1	Vigencia :08/01/2016	Codigo: DS-A-GTI-01

FECHA DE REVISION: 06/01/2016

N°	Riesgos encontrados	Vulnerabilidades	Tratamiento	Control	Actividad	Responsable	Recursos Adicionales	Referencia anexo A	Fecha Máxima de	Observaciones
1	Daño o Averia en los equipos	No se han implementado politicas de ubicación de equipos de cómputo. No se han implementado politicas para evitar el consumo de liquidos y alimentos en los equipos.	Mitigar	CNTRL001	Documentar, aprobar e implementar Políticas sobre el buen uso de los activos de información.	Gestión de TICs	120000000 (contrato fase II)	A.5.1.1, A.8.1.3	24 de Agosto de 2014	
		No hay planes de mantenimiento.		CNTRL007	Documentar, implementar y registrar plan de mantenimiento a los servidores y equipos de cómputo.		Contrato fase II SGSI Documentación Contrato ETB ejecución	A.11.2.4	24 de Agosto de 2014	
		Equipos de seguridad ambiental insuficientes.		CNTRL016	Implementar controles ambietales en el Datacenter		50000000 (Licitación Centro de D	A.11.1.4	10 de Diciembre de 2014	
		Falta de mantenimiento en la malla de puesta a Tierra.		CNTRL028	Establecer plan de mantenimiento a la malla de tierra.		Licitación UPS	A.11.2.4	10 Diciembre de 2014	
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	N/A	A.11.1.2, A.11.1.5	12 Mayo de 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	Contrato fase II SGSI Planeación Contrato ETB Datacenter alterno Ejecución	A.17	25 Octubre de 2014	
		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	Contrato fase II SGSI Documentación Contrato ETB ejecución	A.16	25 de Octubre de 2013	
		Control de la temperatura inadecuado	Mitigar	CNTRL017	Implementar control de temperatura en el Data Center.	Gestión de TICs	50000000 (Licitación Centro de Datos)	A.11.1.4	18 de Febrero de 2014	
		Dependencia del mismo tablero electrico y acometida electrico.	Aceptar	NA	NA	NA	NA	NA	NA	
		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	Contrato UPS	A.11.2.2	10 de Diciembre de 2014	
		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	Caja Menor	A.11.1.2, A.11.1.5	18 de Febrero de 2014	
		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	Contratación ETB BCP	A.17.2	10 Diciembre de 2014	
		Centro de computo con flujo y corriente de aire	Mitigar	CNTRL025	Sellamiento hermético del datacenter	Gestión de TICs	NA	A.11.1.4	14 Enero de 2015	
		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	Caja Menor	A.11.2.3	18 de Marzo de 2014	
		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	Licitación UPS	A.11.1.4	10 Diciembre de 2014	
		Acceso Directo a administración de impresoras	Mitigar	CNTRL035	Corregir la configuración por defecto y configurar contraseña de acceso	Gestión de TICs	NA	A.9.4.3	20 Enero de 2014	
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	NA (Incluir en presupuesto año próximo)	A.12.3	NA	
		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	NA	A.5.1.1, A.9.4.3	12 Septiembre de 2014	
		Documentación sin la protección adecuada		CNTRL009	Asegurar la correcta ubicación de la documentación física de las historias laborales.	Gestión de TICs	NA	A.11.1.3	25 de Octubre de 2013	
		No se ha implementado un procedimiento de Backups para equipos		CNTRL003	Documentar e implementar políticas o procedimientos de copias de resplado a equipos de cómputo críticos.	Gestión de TICs	NA	A.12.3	13 de Agosto de 2013	
		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	NA	A.16		
		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	NA (Incluir en presupuesto año próximo)	A.12.3		
5	Fuga de información	No se han implementado politicas 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	NA	5.3, A.9.2	jun-15	
		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	NA	A.13.2.1, A.13.2.2	jun-15	
		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	NA	A.5.1.1, A.9.4.3	jun-15	
		Documentación sin la confidencialidad adecuada		CNTRL010	Establecer ubicación adecuada de las historias laborales.	Gestión de Talento Humano	NA	A.11.1.3	jun-15	
		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	NA	A.16	jun-15	
		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	NA	A.13.2.4	jun-15	
		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	NA	A.9.2.3	jun-15	
		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	NA	A.11.2.9	jun-15	
		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	NA	A.13.1.2	jun-15	
		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	NA	A.13.11, A.13.1.2	jun-15	
		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	NA	A.13.1.2	jun-15	
6	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	NA	A.5.1.1, A.9.4.3		
7	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.	Gestión de Talento Humano	NA	A.7.2.2	jun-15	A mitad de año y finales todos los años
8	Suspensión del servicio	No hay personal de respaldo para cargos críticos	Mitigar	CNTRL012	Documentación de los procesos.	Gestión de Mejora Continua	NA	A.12.1.1		
9	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	NA	A.11.2.7	jun-15	
		No se cuenta con el uso de HTTPS en Aranda	Aceptar	CNTRL034	NA	Gestión de TICs	NA	NA	jun-15	
		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 características técnicas lo permiten	Gestión de TICs	NA	A.12.6.1	jun-15	
10	Denegación de Servicio	Servicio de un solo ISP	Aceptar	CNTRL013	NA	NA	NA	NA	NA	
11		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	NA	A.12.6.1	jun-15	
12	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	NA	A.13.2.3	jun-15	