MINISTERIO DE AMBIENTE Y DESARROLLO SOSTENIBLE	MATRIZ DE REQUISITOS DE NORMAS VS PROCESOS	MADSIG Sistema Integrado de Gestión
	Proceso: Administración del Sistema Integrado de Gestion	
Versión 2	Vigencia: 3/11/2016	Código: G-E-SIG-01

REQUISITO NORMA SEGURIDAD DE LA INFORMACION ISO 27001:2006	1-Gestión integrada del portafolio de planes, programas y proyectos.	2-Administración del Sistema Integrado de Gestión	3-Gestión de Información y Comunicaciones	4-Negociacion Internacional, Recursos de	5-Formulación, seguimiento y evaluación de Políticas Públicas	6- Instrumentación ambiental	7-Gestión del Desarrollo sostenible	8- Atención al ciudadano	9- Gestión Administrativa	10- Gestión Financiera	11- Gestión Documental	12-Administración del Talento	13- Gestión Jurídica	14- Contratación	15- Soporte técnico de TIC	16- Gestión Disciplinaria	17- Evaluación independiente
	Oficina Asesora de Planeación, Despacho Ministro	Oficina Asesora de Planeación, Despacho Ministro	Oficina de Tecnologías de la Información y la Comunicación, Despacho	Oficina Asuntos Internacionales, Despacho	Despacho Vicemin , Of. negocios verdes y sostenibles, Dir. Ord Amb. Territ y coord. SINA, Dir. Bosques, biodiversidad y serv ecosistémicos.			Grupo de Atención al ciudadano	Subdirección administrativa y financiera	Subdirección administrativa y financiera	Grupo de Gestión Documental	Secretaria general	Oficina asesora jurídica	Secretaria general	Oficina de Tecnologías de la Información y	Secretaria general	Oficina de control interno
4. SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACION	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
4.1 Requisitos generales	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
4.2 Establecimiento y Gestión del SGSI		x	x														
4.2.1 Establecimiento del SGSI (P)		x	x														
a. Alcance y límites		x	x														
b. Política		x	x														
c. Enfoque organizacional para valoración del riesgo		x	x														
d. Identificar los riesgos		x	x														
e. Analizar y evaluar los riesgos		x	x														
f. Opciones para el tratamiento de los riesgos		x	x														
g. Objetivos de control y controles para el tratamiento de los riesgos		x	x														
h. Aprobación de la Dirección sobre los riesgos residuales propuestos		x	x														
i. Autorización de la Dirección para implementar el SGSI		x	x														
j. Elaborar declaración de aplicabilidad		x	x														
4.2.2 Implementación y operación del SGSI (H)		x	x														
a. Formular plan para el tratamiento de riesgos		x	x														
a. Implementar plan para el tratamiento de riesgos		x	x														
c. Implementar controles seleccionados		x	x														
d. Definir cómo medir la eficacia de los controles		x	x														
e. Implementar programas de formación y de toma de conciencia		x	x									x					
f. Gestionar la operación del SGSI		x	x														
g. Gestionar los recursos del SGSI	x	x	x							x							
h. Implementar procedimientos y otros controles para detectar y dar respuesta oportuna a los incidentes de seguridad		x	x												x		
4.2.3 Seguimiento y revisión del SGSI (V)		x	x												x		x
a. Ejecutar procedimientos de seguimiento y revisión y otros controles, para: -Detectar errores en resultado del procesamiento _Identificar incidentes e intentos de violación de s.i. - Que la Dir. Determine si las actividades de seguridad se están ejecutando de forma esperada - Ayudar a detectar eventos de seguridad e impedir incidentes -Determinar si las acciones tomadas xa problemas de violación de s.i. fueron eficaces		x	x												x		x
b. Emprender revisiones regulares de la eficacia del SGSI		x	x												x		x
c. Medir la eficacia de los controles		x	x												x		x
d. Revisar las valoraciones de los riesgos ante cambios en la org, tecnología, negocio		x	x												x		x
e. Realizar auditorías internas del SGSI a intervalos planificados		x	x												x		x
f. Revisión por la Dirección del SGSI		x	x												x		x
g. Actualizar los planes de seguridad según conclusiones de las actividades de seguimiento y revisión		x	x												x		x
h. Registrar acciones y eventos que podrían tener impacto en la eficacia o desempeño del SGSI		x	x												x		x
4.2.4 Mantenimiento y mejora del SGSI (A)																	
a. Implementar las mejoras identificadas en el SGSI	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
b. Emprender acciones correctivas y preventivas	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
c. Comunicar las acciones y mejoras a las partes interesadas	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
d. Asegurar que las mejoras logran los objetivos previstos	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
4.3 Requisitos de documentación																	
4.3.1 Generalidades	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
4.3.2 Control de documentos	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
4.3.3 Control de los registros	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
5. RESPONSABILIDAD DE LA DIRECCIÓN	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
5.1 Compromiso de la dirección	x	x			x	x	x										x
5.2 GESTIÓN DE LOS RECURSOS																	
5.2.1 Provisión de recursos	x	x	x	x						x		x		x	x		
5.2.2 Formación, toma de conciencia y competencia.												x					
6. AUDITORIAS INTERNAS DEL SGSI	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
7. REVISION DEL SGSI POR LA DIRECCION		x	x														
7.1 Generalidades		x	x														x
7.2 Información para la revisión		x	x														x
7.3 Resultados de la revisión		x	x														x
8. MEJORA DEL SGSI	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
8.1 Mejora continua	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
8.2 Acción correctiva	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
8.3 Acción preventiva	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
ANEXO A. OBJETIVOS DE CONTROL Y CONTROLES																	
5 POLITICA DE SEGURIDAD																	
5.1 Política de s.i.																	
5.1.1. Documento de la poítica		x	x														
5.1.2. Revisión de la poítica de s.i.		x	x														
6 ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACION		x	x														
6.1 Organización interna		x	x														
6.1.1 Compromiso de la Dir con la s.i.		x	x														
6.1.2 Coordinación de la s.i.		x	x														
6.1.3 Asignación de responsabilidades para la s.i.		x	x														
6.1.4 Proceso de autorización para los serv. de procesamiento de inf		x	x														
6.1.5 Acuerdos sobre confidencialidad		x	x									x					
6.1.6 Contacto con las autoridades		x	x														
6.1.7 Contacto con grupos de interés especiales		x	x														
6.1.8 Revisión independiente de s.i.		x	x														
6.2 Partes externas		x	x														
6.2.1 Identificar riesgos relacionados con partes ext		x	x														

REQUISITO NORMA SEGURIDAD DE LA INFORMACION ISO 27001:2006	1-Gestión integrada del portafolio de planes, programas y proyectos.	2-Administración del Sistema Integrado de Gestión	3-Gestión de Información y Comunicaciones	4-Negociación Internacional, Recursos de	5-Formulación, seguimiento y evaluación de Políticas Públicas	6- Instrumentación ambiental	7-Gestión del Desarrollo sostenible	8- Atención al ciudadano	9- Gestión Administrativa	10- Gestión Financiera	11- Gestión Documental	12-Administración del Talento	13- Gestión Jurídica	14- Contratación	15- Soporte técnico de TIC	16- Gestión Disciplinaria	17- Evaluación independiente
6.2.2 Seguridad cuando se trata de clientes		x	x														
6.2.3 Seguridad en los acuerdos con terceras partes		x	x														
7 GESTION DE ACTIVOS		x	x														
7.1 Responsabilidad por los activos		x	x												x		
7.1.1 Inventario de activos		x	x												x		
7.1.2 "Propiedad" de los activos		x	x												x		
Uso aceptable de los activos		x	x												x		
7.2 Clasificación de la información		x	x												x		
7.2.1 Directrices de clasificación		x	x												x		
7.2.2 Etiquetado y manejo de información		x	x												x		
8 SEGURIDAD DE LOS RECURSOS HUMANOS		x	x									x			x		
8.1 Antes de la contratación laboral		x	x									x			x		
8.1.1 Roles y responsabilidades		x	x									x			x		
8.1.2 Selección		x	x									x			x		
8.1.3 Términos y condiciones laborales		x	x									x			x		
8.2 Durante la vigencia de la contratación laboral		x	x									x			x		
8.2.1 Responabilidades de la dirección		x	x									x			x		
8.2.2 Educación, formación y concientización sobre la s.i.		x	x									x			x		
8.2.3 Proceso disciplinario		x	x									x			x	x	
8.3 Terminación o cambio de la contratación laboral		x	x									x			x		
8.3.1 Responsabilidades en la terminación		x	x									x			x		
8.3.2 Devolución de activos		x	x									x			x		
8.3.3 Retiro de los derechos de acceso		x	x									x			x		
9 SEGURIDAD FISICA Y DEL ENTORNO		x	x						x						x		
9.1 Areas seguras		x	x						x						x		
9.1.1 Perímetro de seguridad física		x	x						x						x		
9.1.2 Controles de acceso físico		x	x						x						x		
9.1.3 Seguridad de oficinas, recintos e instalaciones		x	x						x						x		
9.1.4 Protección contra amenazas externas y ambientales		x	x						x						x		
9.1.5 Trabajo en áreas seguras		x	x						x						x		
9.1.6 Areas de carga, despacho y acceso público		x	x						x						x		
9.2 Seguridad de los equipos		x	x						x						x		
9.2.1 Ubicación y protección de los equipos		x	x						x						x		
9.2.2 Servicios de suministro		x	x						x						x		
9.2.3 Seguridad del cableado		x	x						x						x		
9.2.4 Mtto de los equipos		x	x						x						x		
9.2.5 Seguridad de los equipos fuera de las instalaciones		x	x						x						x		
9.2.6 Seguridad en la reutilización o eliminación de los equipos		x	x						x						x		
9.2.7 Retiro de activos		x	x						x						x		
10 GESTION DE COMUNICACIONES Y OPERACIONES		x	x														
10.1 Procedimientos operacionales y responsabilidades		x	x														
10.1.1 Documentos de los procedimientos de operación		x	x														
10.1.2 Gestión del cambio		x	x														
10.1.3 Distribución de funciones		x	x														
10.1.4 Separación de la sinstalaciones de desarrollo, ensayo y operación		x	x														
10.2 Gestión de la prestación del servicio por terceras partes		x	x														
10.2.1 Prestación del servicio		x	x														
10.2.2 Monitoreo y revisión de los servicios por terceras partes		x	x														
10.2.3 Gestión de los cambios en los servicios por terceras partes		x	x														
10.3 Planificación y aceptación del sistema		x	x														
10.3.1 Gestión de la capacidad		x	x														
10.3.2 Aceptación del sistema		x	x														
10.4 Protección contra códigos maliciosos y móviles		x	x														
10.4.1 Controles contra códigos maliciosos		x	x														
10.4.2 Controles contra códigos móviles		x	x														
10.5 Respaldo		x	x														
10.5.1 Respaldo de la información		x	x														
10.6 Gestión de la seguridad de las redes		x	x														
10.6.1 Controles de las redes		x	x														
10.6.2 Seguridad de los servicios de red		x	x														
10.7 Manejo de los medios		x	x														
10.7.1 Gestión de los medios removibles		x	x														
10.7.2 Eliminación de los medios		x	x														
10.7.3 Procedimientos para el manejo de la información		x	x														
10.7.4 Seguridad de la documentación del sistema		x	x														
10.8 Intercambio de la información		x	x														
10.8.1 Políticas y procedimientos para el intercambio de inf		x	x														
10.8.2 Acuerdos para el intercambio		x	x														
10.8.3 Medios físicos en tránsito		x	x														
10.8.4 Mensajería electrónica		x	x														
10.8.5 Sistemas de inf del negocio		x	x														
10.9 Servicios de comercio electrónico		x	x														
10.9.1 Comercio electrónico		x	x														
10.9.2 Transacciones en línea		x	x														
10.9.3 Información disponible al público		x	x														
10.10 Monitoreo		x	x														
10.10.1 Registro de auditorías		x	x														
10.10.2 Monitoreo del uso del sistema		x	x														
10.10.3 Protección de la inf de registro		x	x														
10.10.4 Registros del admor y del operador		x	x														
10.10.5 Registro de fallas		x	x														
10.10.6 Sincronización de relojes		x	x														
11 CONTROL DE ACCESO		x	x														
11.1 Requisito del negocio para el control de acceso		x	x														
11.1.1 Política de control de acceso		x	x														
11.2 Gestión del acceso de usuarios		x	x														
11.2.1 Registro de usuarios		x	x														
11.2.2 Gestión de privilegios		x	x														
11.2.3 Gestión de contraseñas para usuarios		x	x														
11.2.4 Revisión de los derechos de acceso de usuarios		x	x														
11.3 Responsabilidad de los usuarios		x	x														
11.3.1 Uso de contraseñas		x	x														
11.3.2 Equipo de usuario desatendido		x	x														
11.3.3 Política de escritorio despejado y de pantalla despejada		x	x														
11.4 Control de acceso a las redes		x	x														
11.4.1 Política de uso de los servicios de red		x	x														
11.4.2 Autenticación de usuarios para conexiones externas		x	x														
11.4.3 Identificación de los equipos en las redes		x	x														
11.4.4 Protección de los puertos de configuración y diagnóstico remoto		x	x														
11.4.5 Separación en las redes		x	x														
11.4.6 Control de conexión a las redes		x	x														

REQUISITO NORMA SEGURIDAD DE LA INFORMACION ISO 27001:2006	1-Gestión integrada del portafolio de planes, programas y proyectos.	2-Administración del Sistema Integrado de Gestión	3-Gestión de Información y Comunicaciones	4-Negociación Internacional, Recursos de	5-Formulación, seguimiento y evaluación de Políticas Públicas	6- Instrumentación ambiental	7-Gestión del Desarrollo sostenible	8- Atención al ciudadano	9- Gestión Administrativa	10- Gestión Financiera	11- Gestión Documental	12-Administración del Talento	13- Gestión Jurídica	14- Contratación	15- Soporte técnico de TIC	16- Gestión Disciplinaria	17- Evaluación independiente
11.4.7 Control de enrutamiento en la red		x	x														
11.5 Control de acceso al sistema operativo		x	x														
11.5.1 Procedimientos de ingreso seguro		x	x														
11.5.2 Identificación y autenticación de usuarios		x	x														
11.5.3 Sistema de gestión de contraseñas		x	x														
11.5.4 Uso de las utilidades del sistema		x	x														
11.5.5 Tiempo de inactividad de la sesión		x	x														
11.5.6 Limitación del tiempo de conexión		x	x														
11.6 Control de acceso a las aplicaciones y a la información		x	x														
11.6.1 Restricción de acceso ala informeción		x	x														
11.6.2 Aislamiento de sistemas sensibles		x	x														
11.7 Computación móvil y trabajo remoto		x	x														
11.7.1 Computación y comunicaciones móviles		x	x														
11.7.2 Trabajo remoto		x	x														
12 ADQUISICION, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACION		x	x														
12.1 Requisitos de seguridad de los sist. de información		x	x														
12.1.1 Análisis y especificación de los requisitos de seguridad		x	x														
12.2 Procesamiento correcto en las aplicaciones		x	x														
12.2.1 Validación de los datos de entrada		x	x														
12.2.2 Control de procesamiento interno		x	x														
12.2.3 Integridad del mensaje		x	x														
12.2.4 Validación de los datos de salida		x	x														
12.3 Controles criptográficos		x	x														
12.3.1 Política sobre el uso de Controles criptográficos		x	x														
12.3.2 Gestión de llaves		x	x														
12.4 Seguridad de los archivos del sistema		x	x														
12.4.1 Control del software operativo		x	x														
12.4.2 Protección de los datos de prueba del sistema		x	x														
12.4.3 Control de acceso al código fuente de los programas		x	x														
12.5 Seguridad en los procesos de desarrollo y soporte		x	x														
12.5.1 Procedimientos de control de cambios		x	x														
12.5.2 Revisión técnica de las aplicaciones después de los cambios en el sistema operativo		x	x														
12.5.3 Restricciones en los cambios a los paquetes de software		x	x														
12.5.4 Fuga de información		x	x														
12.5.5 Desarrollo de software contratado externamente		x	x														
12.6 Gestión de la vulnerabilidad técnica		x	x														
12.6.1 Control de vulnerabilidades técnicas		x	x														
13 GESTION DE LOS INCIDENTES DE LA SEGURIDAD DE LA INFORMACION		x	x														
13.1 Reporte sobre los eventos y las debilidades de la s.i.		x	x														
13.1.1 Reporte sobre los eventos de s.i.		x	x														
13.1.2 Reporte sobre las debilidades de la seguridad		x	x														
13.2 Gestión de los incidentes y las mejoras en la s.i.		x	x														
13.2.1 Responabilidades y procedimientos		x	x														
13.2.2 Aprendizaje debido a los incidentes de s.i.		x	x														
13.2.3 Recolección de evidencia		x	x														
14 GESTION DE LA CONTINUIDAD DEL NEGOCIO		x	x						x								
14.1 Aspectos de la s.i., de la gestión de la continuidad del negocio		x	x						x								
14.1.1 Inclusión de la s.i. en el proceso de gestión de la continuidad del negocio		x	x						x								
14.1.2 Continuidad del negocio y evaluación de riesgos		x	x						x								
14.1.3 Dllo e implementación de planes de continuidad que incluyen la s.i.		x	x						x								
14.1.4 Estructura para la planificación de la continuidad del negocio		x	x						x								
14.1.5 Pruebas, mtto y reevlaución de los planes de continuidad del negocio		x	x														
15 CUMPLIMIENTO		x	x														
15.1 Cumplimiento de los requisitos legales		x	x														
15.1.1 Identificación de la legislación aplicable		x	x														
15.1.2 Derechos de propiedad intelectual (DPI)		x	x														
15.1.3 Protección de los registros de la organización		x	x														
15.1.4 Protección de los datos y privacidad de la información personal		x	x														
15.1.5 Prevención del uso inadecuado de los servicios de procesamiento de inf		x	x														
15.1.6 Reglamento de los controles criptográficos		x	x														
15.2 Cumplimiento de las políticas y las normas de seguridad y cumplimiento técnico		x	x														
15.2.1 Cumplimiento con las políticas y nromas de seguridad		x	x														
15.2.2 Verificación del cumplimiento técnico		x	x														
15.3 Consideraciones de la auditoría de los sistemas de información		x	x														
15.3.1 Controles de auditoría de los sistemas de inf		x	x														
15.3.2 Protección de las herramientas de auditoría de los sistemas de inf		x	x														