



MINISTERIO DE AMBIENTE Y DESARROLLO SOSTENIBLE

Política de seguridad de la información para desarrollo de proyectos

PROCESO
Gestión Estratégica de
Tecnologías de la Información
Versión 1
23/12/2022



MINISTERIO DE AMBIENTE Y DESARROLLO SOSTENIBLE	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN PARA DESARROLLO DE PROYECTOS	 Sistema Integrado de Gestión
	Proceso: Gestión Estratégica de Tecnologías de la Información	
Versión: 1	Vigencia: 23/12/2022	Código: DS-E-GET-26

TABLA DE CONTENIDO

1. OBJETIVO	3
2. ALCANCE	3
3. REQUERIMIENTOS	3
3.1 Etapa precontractual	3
3.2 Etapa Contractual	4
3.3 Etapa Post contractual	5
4. LINEAMIENTOS	5
4.1. Proyectos definidos en la entidad	5
4.2. Proyectos en fase de desarrollo	5

Sistema Integrado de Gestión

MINISTERIO DE AMBIENTE Y DESARROLLO SOSTENIBLE	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN PARA DESARROLLO DE PROYECTOS	 Sistema Integrado de Gestión
	Proceso: Gestión Estratégica de Tecnologías de la Información	
Versión: 1	Vigencia: 23/12/2022	Código: DS-E-GET-26

1. OBJETIVO

Establecer los lineamientos y mecanismos de control por parte del MINISTERIO a través de buenas prácticas de seguridad de la información en el desarrollo de proyectos de TI.


2. ALCANCE

La presente política aplica para todos los proyectos de TI que se realicen en la entidad, los cuales se regirán por los lineamientos de Seguridad de la Información aquí definidos. El uso de los activos de información, siempre que sea necesario serán bajo la supervisión y en cumplimiento de las políticas de seguridad de la información establecidas para este fin.

3. REQUERIMIENTOS

3.1 Etapa precontractual

- Durante la Etapa Precontractual, desde la construcción de los estudios previos, el área solicitante de la contratación, debe identificar los riesgos asociados a seguridad de la información. Como parte de la estimación de los riesgos del proceso de contratación se deberá evaluar y valorar el riesgo inherente, sus controles y el riesgo residual resultante calificando, probabilidad de ocurrencia estimada, su impacto, la determinación de la parte que debe asumirlas, el tratamiento que se les debe dar para eliminarlos o mitigarlos y las características del monitoreo más adecuado para administrarlos.
- El supervisor debe identificar si el objeto del contrato, requiere del acceso de terceros a la información reservada o clasificada de la entidad, datos sensibles, sistemas de información y/o áreas seguras de la entidad; de ser así, se deben determinar los requisitos mínimos de seguridad y los controles necesarios por parte del funcionario y/o contratista que esté desarrollando el proyecto para ejecutar dicho contrato.
- Asegurar la inclusión de la cláusula de confidencialidad, protección de datos, intercambio de información, derechos de propiedad intelectual, las políticas de seguridad y privacidad de la información y derechos de autor. Generar un modelo base para los acuerdos de niveles de servicios en la suscripción y perfeccionamiento del contrato que se celebre entre el MINISTERIO y aquellos contratistas que tendrán acceso a la información reservada o clasificada de la Entidad.

MINISTERIO DE AMBIENTE Y DESARROLLO SOSTENIBLE	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN PARA DESARROLLO DE PROYECTOS	
	Proceso: Gestión Estratégica de Tecnologías de la Información	
Versión: 1	Vigencia: 23/12/2022	Código: DS-E-GET-26


- El supervisor debe socializar con contratistas las políticas, procedimiento y demás documentos asociados a la seguridad de la información y ciberseguridad del MINISTERIO
- Para la contratación de servicios o componentes de la infraestructura de TI y/o áreas seguras, se debe exigir a los contratistas la presentación de los planes de contingencia que aseguren la disponibilidad de la información, suministrada y procesada entre las partes.

La Oficina de Tecnologías de la información y la Secretaría General para la Prevención del Fraude deben:

- Establecer las condiciones de comunicación segura, cifrado y transmisión de información desde y hacia los terceros, prestadores de servicios e implementar controles de cifrado y asegurar la transferencia de la información entre las partes de ser requerida.
- Establecer las condiciones de conexión adecuada para los equipos de cómputo y dispositivos móviles de los terceros en la red de datos de Minambiente.
- Gestionar los riesgos relacionados con terceras partes que tengan acceso a los sistemas de información y la plataforma tecnológica de Minambiente.
- Verificar el cumplimiento de los controles de software base instalado y de licenciamiento de software y hacer extensivos los controles existentes en la red a equipos de cómputo de terceras partes cuando los contratistas o prestadores de servicios que por necesidades o por acuerdos contractuales de la operación, incorporen equipos de cómputo a la red corporativa

3.2 Etapa Contractual

- El supervisor del contrato debe monitorear el acceso a la información y a los recursos de almacenamiento o procesamiento de la misma, la gestión de incidentes de seguridad de la información, continuidad del negocio y acordar el canal para su debido reporte.
- El supervisor del contrato debe contemplar procesos de auditoría a contratistas cuyo objetivo sea validar el cumplimiento de los requisitos de seguridad de la información definidos y consignarlos en los informes de supervisión presentados.
- Toda gestión del contratista que represente una modificación, mantenimiento, revisión al servicio de tecnología de la información, comunicaciones o equipos de suministros, debe pasar por el Procedimiento gestión de cambios antes de su ejecución.

MINISTERIO DE AMBIENTE Y DESARROLLO SOSTENIBLE	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN PARA DESARROLLO DE PROYECTOS	 Sistema Integrado de Gestión
	Proceso: Gestión Estratégica de Tecnologías de la Información	
Versión: 1	Vigencia: 23/12/2022	Código: DS-E-GET-26

3.3 Etapa Post contractual

- Durante la Etapa Post Contractual, el supervisor del contrato debe monitorear y hacer seguimiento a los controles pactados para asegurar la confidencialidad, integridad y disponibilidad de la información, frente a los riesgos previamente identificados.
- El supervisor del contrato debe validar que los controles de seguridad de la información definidos al terminar el contrato se realicen de forma adecuada y con los protocolos y procedimientos adecuados tales como procesos de entrega y destrucción de la información que pertenezcan a Minambiente.

4. LINEAMIENTOS

4.1. Proyectos definidos en la entidad


Toda iniciativa de proyecto aprobada en el Ministerio en su etapa de definición deberá cumplir con el siguiente punto de control:

1. Verificar que los objetivos de Seguridad de la información se incluyan en los objetivos del proyecto
2. Identificación de riesgos de Seguridad de la información en el proyecto.

4.2. Proyectos en fase de desarrollo

Los proyectos que se estén desarrollando deberán cumplir con los siguientes puntos de control:

1. Verificar el cumplimiento de los objetivos de Seguridad de la información en el desarrollo del proyecto.
2. Identificar, evaluar y valorar nuevos riesgos de Seguridad de la información en el proyecto a nivel de ejecución
3. Establecer un Mapa de Riesgos de Seguridad de la Información
4. Validar la implementación de los controles definidos para mitigar los riesgos de Seguridad de la Información.
5. Verificar la gestión de control de cambios efectuada en el desarrollo del proceso
6. Verificar que las pruebas realizadas estén enmarcadas dentro de las políticas de seguridad de la información.
7. Validar las pruebas de aceptación de criterios definidos en el proyecto
8. Verificar que los cambios propuestos por los usuarios y otros interesados, se hayan efectuado cumpliendo lineamientos de Seguridad de la Información y respetando sus políticas.

MINISTERIO DE AMBIENTE Y DESARROLLO SOSTENIBLE	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN PARA DESARROLLO DE PROYECTOS	 MAD SIG Sistema Integrado de Gestión
	Proceso: Gestión Estratégica de Tecnologías de la Información	
Versión: 1	Vigencia: 23/12/2022	Código: DS-E-GET-26

9. Revisión de controles y procedimientos de integridad para garantizar que no sean comprometidos los activos de Información.

En caso de que el proyecto involucre desarrollo de sistemas, aplicaciones y otros artefactos de sistemas de información, se debe:

1. Validar el cumplimiento de los lineamientos para desarrollo seguro en caso de que se considere tercerización de este.
 - a. Acuerdos de licencias, propiedad de códigos y derechos de contenidos (Derechos de propiedad intelectual)
 - b. Requerimientos contractuales respecto de la calidad del código, garantías, metodología y codificación segura.

4.3. Proyectos en fase de finalización

En esta etapa del proyecto se valida el cumplimiento de los lineamientos de Seguridad de la Información, aplicados en las etapas anteriores por parte del líder del proyecto junto con el usuario final emitiendo así el concepto favorable por parte del equipo de seguridad de la información mediante una acta o informe de cumplimiento.