

**Formato de Requerimientos técnicos de referencia para la contratación de bienes y servicios**

|  |  |
| --- | --- |
| **Instancia encargada del levantamiento de requerimientos** | **Subdirección de estándares y arquitectura** |
| **Justificación de la necesidad** | Para apoyar la implementación de la política de Gobierno digital en Colombia es muy importante contar con una herramienta que permita centralizar la información de la gestión en seguridad y privacidad que realizan las Entidades, teniendo en cuenta los siguientes aspectos: El proyecto para el reporte de la gestión de seguridad de la información y riesgos de seguridad digital, está enmarcado dentro la política de Gobierno Digital, la cual genera un enfoque en donde no sólo el Estado sino también los diferentes actores de la sociedad son fundamentales para un desarrollo integral del Gobierno Digital en Colombia y en donde las necesidades y problemáticas del contexto determinan el uso de la tecnología y la forma como ésta puede aportar en la generación de valor público. Promoviendo el uso y aprovechamiento de las tecnologías de la información y las comunicaciones para consolidar un Estado y ciudadanos competitivos, proactivos, e innovadores, que generen valor público en un entorno de confianza digital.Este es el fin último del uso de la tecnología en la relación del Estado y el ciudadano. El valor público se relaciona con el desarrollo social, la gobernanza, la garantía de derechos, la satisfacción de necesidades y la prestación de servicios de calidad. No sólo es hacer uso de las tecnologías, sino cómo las tecnologías ayudan a resolver problemas reales. Valor público también es lograr que el Estado llegue a donde no llega el mercado, y posibilitar la creación de nuevos mercados. Por otro lado, la confianza digital es la principal característica del entorno en donde se relaciona el Estado con los ciudadanos y los demás actores del ecosistema digital. Este entorno debe ser sencillo, corresponsable, previsible y seguro. Debe permitir un diálogo permanente entre los actores del ecosistema y proporcionar medios digitales ágiles, sencillos y útiles para el ciudadano.Para la implementación de la Política de Gobierno Digital, se han definido varios elementos que brindan orientaciones generales y específicas que deben ser acogidas por las entidades, a fin de alcanzar los propósitos de la política. Dentro de los cuales encontramos los tres habilitadores transversales Arquitectura, Seguridad y privacidad y Servicios Ciudadanos Digitales, que son elementos de base que permiten el desarrollo de los componentes de la política. A través de seguridad y privacidad se busca preservar la confidencialidad, integridad y disponibilidad de los activos de información de las entidades del Estado, garantizando su buen uso y la privacidad de los datos, a través de un Modelo de Seguridad y Privacidad de la Información. Razón por la cual es de vital importancia contar con la herramienta mencionada. |
| **Objetivo general del requerimiento técnico** | Adquirir una solución tecnológica que ya se encuentre en el mercado, a través de la cual las Entidades públicas realicen la gestión de seguridad de la información de acuerdo con las fases de la implementación del modelo de seguridad y privacidad de la información del componente habilitador de seguridad y privacidad de la política de gobierno digital. |
| **Alcance del requerimiento**  | Adquirir una solución tecnológica a través de la cual las entidades públicas realicen la gestión de seguridad de la información reporten el avance de acuerdo con las fases de la implementación del modelo de seguridad y privacidad de la información – **MSPI**, del componente habilitante de seguridad y privacidad de la política de gobierno digital... Para lograr una apropiada gestión en lo que refiere a la apropiación del Modelo de Seguridad y Privacidad de la Información, que nos permita analizar el estado actual de las Entidades en materia de seguridad y privacidad, identificando y construyendo estrategias que nos permitan ayudar a fortalecer las Entidades que se encuentren más a trazadas en la implementación del **MSPI**. |
| **Aspectos no incluidos en el requerimiento** | N/A  |
| **Productos, entregables y resultados esperados** | Se deberá realizar un proceso de identificación de requerimientos que permitan completar los requerimientos propuestos para el sistema centralizado (Saas) de gestión de seguridad de la información que permita el reporte de la gestión de seguridad de la información y seguridad digital, para las entidades públicas de acuerdo a la normatividad vigente, generando los reportes de la implementación del avance del Modelo de Seguridad y Privacidad de la Información (**MSPI**), tanto del orden Nacional como Territorial.Requerimientos técnicos **NO FUNCIONALES** identificados para el desarrollo del sistema:* El servicio deberá ser basado en WEB, escalable que permita integrar entidades del orden nacional y territorial.
* Compatibilidad como mínimo para los siguientes navegadores (Internet Explorer, Firefox, Chrome y Safari).
* El sistema de información deberá estar soportado en un servicio en la nube Saas, por un (14) meses.
* Los tiempos de respuesta relacionados con formularios de manejo de información como: adición, modificación, eliminación, consulta de registros, autenticación, emisión de avisos y confirmaciones por parte del usuario, no deberán superar los 25 segundos de ser posible para la carga de información.
* La concurrencia puede ser entre 1 y 2800 entidades, teniendo en cuenta que por entidad solo habrá un usuario y password, para la carga de información.
* Realizar pruebas de estrés de la solución con el objetivo de comprobar y certificar las capacidades reales del sistema, presentando un informe del estado y las capacidades del sistema, el número de usuarios es escalable y dependerá del número de entidades que se integren paulatinamente al sistema, para realizar su gestión de seguridad.
* No debe requerir de la instalación de ningún software del lado del usuario para su funcionamiento, debe accederse solo a través del navegador web.
* El sistema permitirá una gestión de observaciones o hallazgos, para la corrección de ítems según criticidad relacionados con el resultado del análisis, permitiendo una gestión y seguimiento de la implementación de las medidas correctoras identificadas. Estas tareas y su programación, prioridad, etc. lo verán el **MINTIC** y la entidad.
* La transferencia de conocimiento relacionada con la administración y funcionalidades del sistema deber ser como mínimo de 120 horas insitu, con talleres prácticos, de la siguiente manera: 40 en capacitación de la herramienta para la vigencia 2019, y 80 horas en el 2020, sobre actualizaciones o uso de la herramienta que permitan reforzar os conocimientos, sobre el manejo de la herramienta de reporte de **MSPI**.
* Se debe entregar manual de usuario y una guía práctica de administrador y usuario.
* Toda la interfaz, los menús, y opciones para el uso de las funcionalidades del sistema y la documentación de manuales técnicos, de administración y de usuarios deben estar en idioma español.
* El sistema debe ser multi tenant, es decir que a través de en una sola instancia de la aplicación se deben poder aprovisionar por separado el acceso a los datos y al uso del sistema a diversas entidades.
* Crear y administrar usuarios y así poder asignar funcionalidades, con diferentes niveles de accesos de edición, eliminación, administración, gestión de información y de consulta de reportes.
* Definir los procesos de cada entidad que estarán en el alcance de la gestión, así como los usuarios autorizados para acceder a la información de cada proceso.
* Administrar las notificaciones de las tareas y acciones que realizan los usuarios en el sistema vía e-mail o en la interfaz del aplicativo. Estas notificaciones no deben venir por defecto, sino que deben poder ser administradas decidiendo cuales se quieren habilitar o crear y con qué frecuencia se desean obtener.
* Configuración del servicio de correo electrónico a través del cual el sistema enviará información y notificaciones.
* El sistema debe permitir que el usuario, a través de su interfaz, lleve a cabo la carga de las normas o estándares que requiera cada entidad para hacer referencia a los marcos referencia normas o controles. La carga de una nueva norma no deberá tener costos para **MINTIC** y los administradores del sistema designados por **MINTIC** deberían poder modificar o cargar, ellos mismos sin intervención del fabricante, nuevas normas, estándares o leyes.
* El sistema debe permitir que el usuario administrador del sistema pueda ingresar y observar los registros de auditoría relacionados con los accesos al sistema y las acciones críticas realizadas por los usuarios de las entidades.

**NOTA 1:** Los tiempos de respuesta anteriores deberán ser validados en un ambiente de pruebas generado por el proveedor y que, a su vez, permitan definir los requerimientos finales a nivel de infraestructura para el ambiente de producción del servicio, para garantizar este tiempo sin embargo el proveedor puede realizar un ajuste al tiempo, contando con la infraestructura tecnológica con la que se cuenta actualmente.**NOTA 2:** Los tiempos de respuesta relacionados con cargues masivos de información podrán varias según el tamaño de los archivos y el ancho de banda disponible.* El rendimiento deberá ser acorde con los tiempos de respuesta y la cantidad de usuarios que deberá proyectarse, por lo que el diseño de los componentes deberá ser eficiente, siendo necesaria la aplicación de las mejores prácticas para diseño y construcción del sistema de información.
* La solución deberá parametrizarse para usuarios concurrentes como mínimo 1 hasta 2800 de entidades públicas, con la posibilidad de ser escalable a futuro, para todas las entidades del orden nacional y territorial.

**REQUERIMIENTOS FUNCIONALES:**Para el sistema centralizado de seguridad de la información se han identificado los siguientes requerimientos técnicos FUNCIONALES el sistema deberá contar como mínimo con los siguientes módulos/funciones:* Sistema centralizado para el reporte de la gestión del cumplimiento del Modelo de Seguridad y Privacidad de la Información **(MSPI):**
* Es un sistema de reporte de avance de la implementación del **MSPI**, no requiere la carga de evidencias, debe contar un campo en donde permita indicar la ubicación de las evidencias.
* Debe estar basado en ISO 27001, y en este los usuarios deben poder acceder online y gestionar el nivel de cumplimiento de su **MSPI**, permitiendo visualizar el resultado, de tal forma que se centralice la información permitiendo realizar análisis del avance de cada entidad.
* Adicionar y administrar las normas, estándares o leyes sobre las cuales se quiere medir el cumplimiento normativo de marcos de referencia de arquitectura, gestión de TIC, gobierno, continuidad o seguridad de la información u otros, sin que represente costos adicionales para **MINTIC** ante nueva normatividad que se requiera incluir.
* Definir los ciclos de tiempo sobre los cuales se va a realizar la medición del cumplimiento de acuerdo con lo establecido por cada entidad alineado con MECI.
* Calificar el nivel de cumplimiento de un control o requisito, navegando por objetivo de control ó área de cumplimiento y subárea ó domino.
* Permitir que los usuarios justifiquen la calificación de cumplimiento con observaciones y recomendaciones, y que adicionen los enlaces la ubicación de las evidencias, sin tener que cargarlas en el sistema.
* El sistema indique automáticamente cuáles controles o requisitos normativos están asociados a los activos y riesgos registrados en el sistema y muestre la información de esos activos y riesgos que tienen asociado el control o requisito y el estado en el cual se encuentra el mismo.
* Guardar los registros de información de quien realizó las calificaciones de cumplimiento y cuando se realizaron o actualizaron (trazabilidad).
* Permitir que cada requisito o control sea calificado a través de niveles de cumplimiento que pueden ser configurados para cada norma o estándar, definiendo los porcentajes de cumplimiento asociados a cada nivel. Esto con el fin de poder calificar cada requisito o control y obtener el promedio de cumplimiento.
* El sistema debe permitir excluir controles o dominios para que la calificación global de cumplimiento no se vea afectada (se deben justificar con la declaración de aplicabilidad).
* El sistema debe permitir observar gráficamente al menos dos ciclos de cumplimiento para comparar y ver el avance o diferencia en la brecha de cumplimiento en el tiempo de una norma o estándar.
* Obtener los reportes de datos y gráficos de la gestión de cumplimiento en cuanto:
	+ Niveles de cumplimiento por control, objetivo de control y área/dominio.
	+ Reporte de radar gráfico de cumplimiento por área/dominio.
	+ Reportes de gráficos de barra de cumplimiento de área/dominio.
	+ Reportes de gráficos de barra de cumplimiento de objetivos de control.
	+ Exportar los resultados de la gestión de cumplimiento a Excel.
* El sistema debe permitir consolidar y verificar reportes que permitan analizar avances por sector, por tipo de entidad entre otros filtros, con base a la hoja de vida de registro de las entidades.
* El sistema debe tener una interfaz amigable y sencilla con el Usuario.
* Gestión de Observaciones/Hallazgos:
	+ Realizar el registro de toda la información de los hallazgos producto de las revisiones del **MINTIC**, clasificarlos y definir fechas acordadas de cierre.
	+ Permitir que la entidad describa el análisis de causas, causa raíz y consecuencias posibles de los hallazgos.
	+ Definir y hacer seguimiento a las acciones para el cierre de los hallazgos y no conformidades y definir su estado. Permitiendo recibir notificaciones de las fechas de cumplimiento de estas acciones.
	+ Registrar los resultados y lecciones aprendidas del tratamiento de los hallazgos.
	+ Obtener de manera automatizada y oportuna reportes gráficos acerca de:
		- * Estado de los hallazgos.
			* Tipos de hallazgos.
			* Causas de los hallazgos.
			* Generar reportes aplicando diferentes criterios de filtrado y selección de información de los hallazgos a través de un generador dinámico de reportes.
			* Exportar los reportes de datos a Excel.
* **Módulo de Login/autenticación/creación de usuarios:**
* Los usuarios deben poder acceder al sistema con su usuario y contraseña, y contar con doble o más factores de autenticación, con el fin de garantizar la confidencialidad, integridad y disponibilidad de la información almacenada en este, de igual manera permitirá la recuperación de su contraseña, mediante mecanismos de verificación.
* Para el registro por primera vez la entidad debe enviar una solicitud previa para crear el usuario.
* Hoja de vida de la entidad, se deberán pedir datos mínimos obligatorios para el registro e identificación de la entidad como: Deberá contar con un módulo parametrizable, con mínimo los siguientes datos: Entidad, tipo de entidad, sector al que pertenece, responsable o delegado del reporte de información, datos de contacto, que permita enviarle alertas o mensajes MSN, correo electrónico a alertas a través del sistema, entre otras.
* Las entidades deben poder ingresar por primera vez y realizar su registro en la plataforma, validando que únicamente existan máximo dos usuarios por entidad (realizando la debida verificación a través de la cuenta de correo electrónico institucional que haga el registro, es decir, dominios gov.co).
* **Módulo de bienvenida al usuario (home):**
	+ Que le permita ver un perfil básico de la entidad que está accediendo, donde se puedan configurar/actualizar datos como: responsable del reporte de la información, datos de contacto, adicionalmente en esta sección debe tener todos los menús de opciones disponibles para las entidades de los diferentes módulos.
* **Módulo de administración principal:**
	+ **MINTIC** debe poder realizar la gestión general de los usuarios (creación, restauración de accesos, asignación de roles entre otras funciones).
	+ Registrar la entidad, tipo de entidad, responsable o delegado del reporte de información, datos de contacto entre otros que se definan para este formulario.
* **Análisis de Tipo Técnico/Seguimiento:**
	+ Deben poderse consultar informes de tipo técnico como los siguientes:
		- Qué entidades reportaron durante la fecha de corte.
		- Quienes incumplieron con el reporte.
		- Quienes nunca han reportado.
		- Quienes actualizaron información entre otros tipos de consulta.
	+ Este módulo de análisis de información debe tener una vista global que permita identificar información importante.
	+ Tablero de control que permita identificar niveles de criticidad a nivel nacional, territorial o sectorial.
	+ Muestra de reportes con base al método específico de Balanced Scorcard con muestra de resultado de perspectivas, objetivos estratégicos e indicadores través de semáforos.

**REQUERIMIENTOS DE SEGURIDAD DE LA INFORMACIÓN:**El software o **Saas**, deberá cumplir con los siguientes requerimientos técnicos en seguridad de la información:* Análisis de gestión de capacidades de la infraestructura tecnológica necesaria y adecuada para el funcionamiento del sistema de información (si solo se entrega el software).
* Relacionado al servicio de reporte, deberá diseñarse con el objetivo de que se prevengan los ataques enunciados por la metodología OWASP.
* Deberán emplearse algoritmos de cifrado y de comprobación de integridad para las bases de datos, sin emplear configuraciones por defecto.
* Deberá diseñarse el servicio con la premisa de preservar la confidencialidad, integridad y disponibilidad del servicio y los datos alojados en el mismo.
* Implementación de RBAC (Rol Based Access Control), es decir, que el desarrollo permita la creación de roles con permisos, para controlar los privilegios que cada usuario puede tener dentro del servicio de reporte, los roles se definirán durante el desarrollo del proyecto, teniendo en cuenta la arquitectura de seguridad AAA (Authorization, Authentication & Accounting).
* Implementación de Logs, donde cada transacción quede debidamente registrada en el sistema, como mínimo deberán registrarse las siguientes acciones:
	+ Accesos/login a la plataforma.
	+ Cada vez que los usuarios/entidades realicen una modificación o cargue de información a la plataforma.
* Implementar WAF en el servicio, con la respectiva documentación para su instalación, actualización y mantenimiento.
* Implementar sistemas anti-robot para el acceso al servicio web.
* El servicio deberá ofrecerse en **HTTPS**, con el debido certificado **TLS v 1.2** validado con entidad certificadora, que demuestre que es un sitio legítimo de **MINTIC**.
* Acceso y administración a través de una red.
* Actividades gestionadas desde ubicaciones centrales.
* La distribución de la aplicación es más cercana al modelo uno-a-muchos (una instancia con múltiples usuarios) que al modelo uno-a-uno, incluyendo arquitectura, precios, colaboración, y administración.

Actualizaciones centralizadas, lo cual elimina la necesidad de descargar parches por parte de los usuarios finales.**NOTA:** No deberán emplearse algoritmos de cifrado o de hash cuyo estado sea “histórico” o que tengan proyección de obsolescencia próxima.Módulo de gestión del conocimiento que me permita consolidad las lecciones aprendidas. |
| **Criterios de aceptación de los productos** | * Deberá entregarse parametrizado y configurado de acuerdo con los parámetros mencionados anteriormente.
* Las licencias del software deben ser a tres (14 meses) años.
* Soporte técnico durante el tiempo de prestación del servicio.
* El oferente deberá brindar soporte telefónico y remoto cinco días (5) x ocho (8) horas con un tiempo de respuesta no mayor a ocho (8) horas, durante el tiempo de prestación del servicio.
* La proyección de costos para las vigencias 2021 y 2022, que permitan establecer cuál sería el valor por vigencia en caso de continuar con la renovación del servicio.
* El oferente deberá suministrar datos de contacto para soporte y el paso a paso de cómo generar un caso (procedimiento).
* El oferente deberá ofrecer capacitación mínima para diez (10) funcionarios del Ministerio TIC, la cual será certificada por el fabricante, acerca del manejo, instalación y administración de las herramientas con un tiempo no inferior a ocho (120) horas; la capacitación deberá ser dictada por un profesional certificado por el proveedor de la herramienta de este tipo, en donde la prestación y oportunidad de los servicios conexos será de responsabilidad exclusiva del oferente favorecido.
* El oferente deberá suministrar los manuales en formato digital, así como la documentación necesaria para la configuración e instalación de la herramienta en idioma español.
* La herramienta deberá contar con actualizaciones tanto de software como de firmas durante el tiempo de prestación del servicio, a partir de la recepción, instalación y entrega a satisfacción de los bienes
* Al finalizar el servicio el contratista se compromete a entregar la información en dispositivos de almacenamiento con cadena de custodia, una vez terminado el contrato deberá realizar el proceso de borrado seguro de la información que se almacene en su infraestructura, referente a este proyecto, y permitirá ser auditado por el CSIRT de Gobierno y/o CCP y/o ColCERT, en el proceso de borrado de la información.
 |
| **Otros requerimientos técnicos** | N/A  |
| **Obligaciones técnicas específicas que deberá cumplir el contratista** | 1. Cumplir el objeto del contrato, ejecutando y entregando los productos de acuerdo con los criterios de calidad exigibles y las especificaciones técnicas, que hacen parte del pliego de condiciones, con sujeción a los precios ofertados en la propuesta económica y dentro del plazo establecido.
2. Ejercer la dirección y el control propio de todas las actividades encomendadas, en forma oportuna y dentro del término establecido, con el fin de obtener la correcta realización del objeto contractual.
3. Responder, sin perjuicio de la respectiva garantía, por el cumplimiento y calidad de los servicios prestados, por el término previsto en el presente contrato.
4. Salvaguardar la información confidencial que obtenga o conozca en el desarrollo de sus actividades salvo requerimiento expreso de Autoridad competente. Toda la información y/o documentos que se produzcan en desarrollo del presente contrato serán de uso exclusivo del **MINTIC**, obligándose desde ya al CONTRATISTA a no utilizarlos para fines distintos a los previstos en este contrato, ni a divulgar la información que se le suministre ni los resultados de su trabajo conservando la confidencialidad de estos, de conformidad con la Ley, so pena de las acciones civiles, administrativas o penales a que haya lugar.
5. Entregar al supervisor del contrato, el informe sobre las actividades ejecutadas, los informes que se soliciten sobre cualquier aspecto y/o resultados obtenidos en cada actividad encomendada cuando así se requiera.
6. Atender los requerimientos, instrucciones y/o recomendaciones que durante el desarrollo del contrato le imparta el **MINTIC** a través del supervisor de este, para una correcta ejecución y cumplimiento de sus obligaciones.
7. Reportar, de manera inmediata al supervisor del contrato la ocurrencia de cualquier novedad o anomalía durante la ejecución del contrato.
8. No acceder a peticiones o amenazas de quienes actúen por fuera de la Ley, con el fin de obligarlo hacer u omitir algún acto o hecho, debiendo informar inmediatamente al **MINTIC** a través del funcionario responsable de la supervisión y control de ejecución, acerca de la ocurrencia de tales peticiones o amenazas, y a las demás autoridades competentes para que se adopten las medidas y correctivos que fueren necesarios.
9. Acreditar, en las oportunidades que así se requiera, de conformidad con lo establecido en el inciso segundo del artículo 41 de Ley 80 de 1993 –adicionado mediante el artículo 23 de la Ley 1150 de 2007–, que se encuentra al día en el pago de aportes parafiscales relativos al Sistema de Seguridad Social Integral, así como los propios al Servicio Nacional de Aprendizaje - SENA, Instituto Colombiano de Bienestar Familiar – ICBF y las cajas de compensación familiar cuando haya lugar, para el personal de la oficina que presta el apoyo a la ejecución de las actividades, como de todo el personal vinculado directamente a la ejecución del contrato, este último cuando corresponda.
10. Indemnizar y/o asumir todo daño que se cause a terceros, a bienes propios o de terceros, o al personal contratado para la ejecución del contrato, por causa o con ocasión del desarrollo de este.
11. Responder por el pago de los tributos que se causen o llegaren a causarse por la celebración, ejecución y liquidación del contrato.
 |
| **Obligaciones técnicas específicas que deberá cumplir ACAC para la ejecución del contrato** | 1. Pagar el valor del presente contrato, en la forma, fechas y bajo las condiciones señaladas más adelante.
2. Verificar la afiliación y pago de aportes que EL CONTRATISTA debe efectuar al Sistema de Seguridad Social y ARL como independiente.
3. Vigilar la debida y oportuna ejecución del contrato y el cumplimiento de todas las obligaciones contractuales a cargo de EL CONTRATISTA.
4. Garantías de seriedad de la oferta.
 |
| **Duración del Contrato:** | **Hasta 14 meses** |
| **Valor estimado del contrato:** | **SETECIENTOS CATORCE MILLONES DE PESOS $714.000.000** |
| **Documentos Anexos:** | * Manual de usuario
* Datasheet
* Documentos requeridos por ACAC para realizar la contratación.
 |
| **Observaciones:** | N/A  |
|
| **Valor agradado** |

|  |  |
| --- | --- |
| **CRITERIO DE CALIFICACIÓN** | **PUNTAJE** |
| Curso de interpretación - ISO 31000 - gestión del riesgo, para diez (10) funcionarios del **MINTIC,** más certificación. | 2 |
| Modulo para el reporte de riesgos del Modelo de Seguridad y Privacidad de la Información del **MSPI** | 4 |
| Modulo para auditoria del Modelo de Seguridad y Privacidad de la Información del **MSPI** | 4 |
| **TOTAL** | **10** |

 |