Herramienta para Cumplimiento y Gestión de Riesgos

Consulta Pública

AGESIC

Torre Ejecutiva Sur
Liniers 1324 - Piso 4
Montevideo - Uruguay
gub.uy/agesic

Contenido

1. Antecedentes

Agesic crea en 2016 su primera versión del Marco de Ciberseguridad de Uruguay (MCU), teniendo como principal objetivo generar confianza en el uso de la tecnología, unificar todos los recursos existentes en materia de ciberseguridad, y sustentar la evolución del gobierno digital de Uruguay. Asimismo, busca promover una visión integral y multi-sectorial de la ciberseguridad, apostando a la mejora continua de la seguridad de la información y a contribuir a la definición de planes de acción. Su implementación se basó en Core del Cybersecurity Framework (CSF) v1.1 (ISO/IEC 27001:2013, COBIT 5 y NIST 800-53 rev.4, entre otras), además contó con el trabajo de especialistas en seguridad de la información, consultoras internacionales y la academia.

A la fecha ha sido utilizado para el diagnóstico y evaluación de los ministerios de la administración central, gobiernos departamentales, instituciones de salud e instituciones financieras.

Dicho Marco presenta una serie de requisitos que incluyen buenas prácticas sobre gobernanza de la seguridad, gestión de riesgos, control de acceso, seguridad de las operaciones, gestión de incidentes y continuidad del negocio asociados a las distintas subcategorías del Marco de Ciberseguridad (CSF) del Instituto de Nacional de Estándares y Tecnologías (NIST, por sus siglas en inglés); además, incluye perfil de organización y un modelo de madurez con el que las organizaciones podrán definir las líneas de acción para mejorar su ciberseguridad. Dichos requisitos tienen adecuaciones para organismos de la Administración Central de Uruguay y para instituciones de salud.

El MCU propone un conjunto de 68 requisitos generados a partir de los controles ISO/IEC 27001 y la normativa uruguaya vinculada a ciberseguridad.

La ciberseguridad está alineada con los objetivos y estrategias de la organización. Cualquier organización pública o privada podrá usar el documento como herramienta de autoconocimiento y mejora de sus niveles de seguridad. A la fecha no es de adopción obligatoria, aunque se prevé a corto plazo su obligatoriedad para algunos sectores críticos.

Sobre esta base es que actualmente Agesic está interesada en conocer las distintas herramientas que permitan llevar el cumplimiento y gestión de riesgos, que existen en el mundo.

2. Objetivo

El objetivo de la implementación de esta herramienta es realizar el relevamiento, seguimiento y gestión del cumplimiento del MCU, así como gestionar los riesgos de seguridad de la información que tienen las organizaciones dentro del alcance de la implementación.

Agesic es rector en materia de seguridad de la información y ciberseguridad a nivel de Gobierno; en este sentido, se ha diseñado un modelo federado de gobernanza, donde cada organización tiene una total independencia de gestión, desarrollo e inversión, pero reporta a Agesic, mediante las auditorías de ciberseguridad y demás mecanismos, los informes de resultado tanto de cumplimiento de requisitos como de modelo de madurez. Con la consolidación de estos resultados, Agesic logra identificar los principales riesgos por sector, por áreas de interés, etc.; que permiten la implementación de diversas iniciativas con el fin de mejorar los niveles de ciberseguridad del Gobierno.

La herramienta que se desea adquirir cumplirá un rol de facilitación en el modelo de gobernanza descrito anteriormente. Por tanto, deberá cubrir la función de cumplimiento (compliance) así como la de gestión de riesgos (risk management).

Algunos de los beneficios que se esperan de la solución/herramienta son:

- Permitir hacer el relevamiento y gestión de la madurez y cumplimiento del MCU de forma centralizada.
- Permitir hacer el relevamiento de riesgos de las organizaciones vinculadas al alcance de implementación y gestionar los mismos de manera centralizada.
- Contar con una metodología replicable que permita el análisis de la evolución tanto del cumplimiento como de los riesgos identificados en las organizaciones.
- Facilitar la emisión de reportes, medición de indicadores y cuadros de mando; que posibilite el monitoreo y mejora continua.
- Automatizar el proceso de auditoría.
- Centralizar evidencias.
- Realizar la gestión de documentos basado en controles SoA (Declaración de Aplicabilidad).
- Permitir la integración con sistemas de gestión Marco de Ciberseguridad AGESIC, ISO 27.000, ISO 31.000, ISO 20.000, ISO 9.001.
- Disponer de mecanismos de encuestas centralizadas y programables.

3. Requerimientos de la solución

Se busca una solución que cuente con mecanismos para el seguimiento del cumplimiento en base a estándares de seguridad (en particular el MCU) y la gestión de riesgos. Se espera que la solución cuente con ambos módulos.

La solución propuesta podrá ser implementada in-situ (on premises) en formato llave en mano, donde la empresa proveedora se encargue de suministrar la instalación e implementación del producto ofrecido; así como la documentación y entrenamiento necesario para los futuros administradores de la misma.

El proveedor deberá contemplar y especificar todos los requerimientos técnicos necesarios para el funcionamiento óptimo de las soluciones (sistema operativo, base de datos, licencias, hardware/máquinas virtuales, networking). Contemplar la posibilidad de una instalación en alta disponibilidad. El proveedor será el responsable de la instalación, configuración e implementación de la solución en Agesic. Contemplando todos los requerimientos y licenciamiento de la solución.

Si la solución cuenta con modalidad en la nube pública, especificar cuáles son los mecanismos de resguardo de la información y en particular cuales son las alternativas de cifrado de la información y las comunicaciones.

Se deberá incluir la capacitación para la administración y gestión de la solución; el equipo de Agesic deberá ser capaz de formar a terceros en el uso de la misma. Disponibilizar un curso en línea autogestionado para formación a terceras partes en el uso de la herramienta.

Se deberá especificar, cuál es la forma de venta de la solución (licenciamiento, modular, etc.), costos a grandes rasgos de las distintas opciones de licenciamiento, así como también los costos futuros que pueda tener (mantenimiento); contemplando todas las vigencias pertinentes y sus actualizaciones.

Se deberá especificar tiempo esperado de entrega una vez solicitado el producto.

Especificar integraciones disponibles con otros sistemas, por ejemplos, SIEM (por ejemplo QRadar), BI, ticketing, etc. Incluir los formatos de intercambio disponibles.

A continuación, se listan los principales requerimientos funcionales que se espera que la solución contemple.

Características deseables para **ambos módulos**:

- Multiempresa y multitenant para que cada organización pueda (eventualmente) gestionar su propio cumplimiento/riesgo.
- Idioma español en interfaces, así como en las ayudas y manuales de uso.

- Envío/recepción de cuestionarios para poder realizar relevamiento a diferentes entidades.
- Permitir el reporte de cada organización a la organización “consolidadora”.
- Contar con distintas visualizaciones, reportes, y posibilidad de personalizar los informes.
- Consolidación de resultados en empresas y en Agesic (centralizador).
- Soporte/capacitación en horario local.
- Manuales actualizados para técnicos y usuarios.
- Personalización de parámetros.
- Gestor documental.
- Cuadro de mando personalizable y/o sugerido.
- Información actualizada en tiempo real para todos.
- Manejo de roles y responsabilidades.
- Visualización de cambios de un ciclo de revisión al siguiente.
- Sistema de alertas.
- Manejo de métricas e indicadores centralizados.
- Configuración flexible

Características deseables para el **módulo cumplimiento**:

- Estándares como ISO 27001, CSF del NIST, MCU.
- Declaración de aplicabilidad (SOA) por “empresa”.
- Permitir realizar auditoria de sistemas de gestión integrados.
- Auditoria orientada a compliance.
- Auditoria orientada a riesgo.
- Auditoria multiempresa.
- Workflow de Auditoría.
- Coordinación de equipos de auditoria.

Características deseables para el **módulo de riesgos**:

- Gestión de riesgos (manejo de tipología de riesgos)
- Identificación de riesgos.
- Evaluación de riesgo.
- Análisis de riesgo.
- Estándares como ISO 31000, marco NIST de riesgos, ISO 27005, etc.
- Catálogos de amenazas, vulnerabilidades, activos, controles, etc.
- Retorno de inversión.
- Análisis de sensibilidad y escenarios.
- Que permita establecer propietarios de riesgos, u otra acción para garantizar una responsabilidad y una rendición de cuenta clara.
- Que permita categorizar los riesgos, con múltiples categorías personalizables para facilitar la generación de informes, la agrupación y el filtrado de registros.
- Comprender y visualizar las interdependencias de los riesgos.

- Desarrollar planes para mitigar riesgos en función de su criticidad o prioridad.
- Corrección, revisión y aprobaciones asociadas.

4. Alcance de la consulta pública

La presente Consulta Pública tiene como alcance exclusivo la recolección de información referente a las distintas herramientas que permitan llevar el cumplimiento y gestión de riesgos, que existen en el mundo.

Agesic no asume al realizarla compromiso de ningún tipo a los efectos de elegir, contratar o implementar producto ni servicio alguno.

La realización de la presente consulta no implica que, si en el futuro se realiza efectivamente la implementación de esta plataforma, se hará obligatoriamente seleccionando una solución de las presentadas en este proceso.

Tampoco implica que los participantes del mismo tendrán privilegios o preferencias en futuros llamados.

Los proveedores que se presenten a esta Consulta Pública, por el solo hecho de hacerlo, dejan en claro que entienden este alcance y lo aceptan como satisfactorio.

5. Procedimiento

El procedimiento de la Consulta Pública será el siguiente:

- Los interesados deberán manifestar su interés enviando un correo electrónico a adquisiciones@agesic.gub.uy hasta el **jueves 26 de noviembre de 2020, a las 12:00 hs.**
  El correo debe incluir los datos de la empresa, persona de contacto y un resumen de los antecedentes de la empresa en este rubro.

- Los interesados podrán realizar preguntas únicamente por correo electrónico a adquisiciones@agesic.gub.uy hasta el **martes 24 de noviembre de 2020, a las 12:00 hs.**
  AGESIC responderá a las consultas formuladas y publicará dichas respuestas en el sitio web de la Agencia Reguladora de Compras Estatales (ARCE).

- Los interesados deberán subir las presentaciones obligatoriamente en el sitio web de la ARCE hasta el **jueves 26 de noviembre de 2020, a las 12:00 hs.** La Consulta

Pública se encuentra publicada en Compras Estatales en el Inciso 2 – Unidad Ejecutora 10, **Solicitud de Información N° 0002/2020.**
Los interesados deberán subir únicamente al sitio web las presentaciones que van a realizar el día dispuesto por la agenda que definirá AGESIC. No se requiere ingresar al mencionado sitio un precio general de la solución presentada.

6. Presentaciones

Las sesiones serán virtuales (via MS Teams o Zoom) y serán grabadas.

Para cada empresa interesada, Agesic propondrá la fecha y hora para la presentación, que tendrá una duración máxima de 120 (ciento veinte) minutos.

Los interesados podrán solicitar a Agesic una fecha y hora diferentes a la propuesta.

La presentación será virtual y deberán participar hasta 4 (cuatro) personas por empresa, 2 (dos) de los cuales serán los encargados de realizar / responder eventuales preguntas técnicas del equipo presente (perfil técnico).

El contenido de la presentación se deberá ajustar al siguiente esquema:

Experiencia de la empresa y en particular en la implementación de soluciones de Cumplimiento y Gestión de Riesgos	Máximo 10 (diez) minutos
Describir el alcance de la solución, características y beneficios comenzando por cumplimiento. Demo.	Máximo 50 (cincuenta) minutos
Describir cómo se implementa y los requerimientos de tiempo y equipamiento.	Máximo 20 (veinte) minutos
Sugerir una estrategia de implementación de la solución y adopción de la misma por parte del interesado.	Máximo 10 (diez) minutos
Se deberá brindar una estimación de esfuerzo en horas (fecha de finalización) para la implementación y despliegue de la solución.	Máximo 20 (veinte) minutos
Se deberá indicar costos de administración, mantenimiento y actualización de la solución.	
Se deberá indicar costos y forma de licenciamientos y necesidades para la solución.	
Preguntas	Máximo 10 (diez) minutos

A todas las presentaciones podrán asistir representantes de las áreas sustantivas de Agesic, técnicos especialistas en diversas temáticas y asesores.

Toda información que se entregue o se pretenda entregar que NO esté relacionada con la consulta pública, se descartará o rechazará en el acto.

Agesic no emitirá ningún juicio de valor sobre ninguna propuesta en particular; tampoco se puntuará técnicamente, ni generará ningún ranking, resumen o informe para los interesados.

Los resultados obtenidos luego del análisis de las presentaciones realizadas serán de uso exclusivo de Agesic y tendrán carácter confidencial.

La presentación deberá ser en idioma español, o contar con un traductor por parte de la empresa.

7. Información Confidencial

En caso de que los oferentes presentaren información considerada confidencial, al amparo de lo dispuesto en el artículo 10 literal I) de la Ley N° 18.381 de Acceso a la Información Pública de 17 de octubre de 2008 y del art. 65 del TOCAF, la misma deberá ser ingresada indicando expresamente tal carácter.

8. Aceptación

Por el solo hecho de presentarse al presente llamado se entenderá que el interesado conoce y acepta sin reservas los términos y condiciones establecidos en el presente documento.