ANEXO A1

SOLUCIÓN PARA LA GESTIÓN DE RIESGOS DE SEGURIDAD DE TI

I. Software de Gestión de riesgos de seguridad de TI

Se requiere para el ambiente de producción y de manera opcional 2 ambientes no productivos.

- **Componente Gestión de Cumplimiento Normativo y Corporativo**

1. Debe estar licenciada para 07 (siete) usuarios por un periodo de mil noventa y cinco (1095) días calendario. Para la interacción de encuestas, planees de recolección de datos, entre otros; deberá permitir un mínimo de 2500 usuarios.
2. Todos los componentes necesarios a fin de cumplir con los requerimientos técnicos deben ser provistos como parte de la solución.
3. Debe proveer toda la infraestructura de software requerido para la implementación de la solución requerida.
4. Permitir la gestión de riesgos derivado del incumplimiento regulatorio.
5. Disponer de metodologías precargadas de incumplimiento regulatorio.
6. Permitir la gestión del conjunto de normativas que apliquen a la compañía.
7. Disponer de catálogos precargados de normativas como COBIT, ISO27001, NIST y CIS controls. Para el caso de CIS controls el cual podrá estar desarrollado y configurado por el proveedor, debiendo este contar un estándar de calidad y seguridad que deberá ser presentado en el plan de trabajo y sin ningún costo adicional.
8. Permitir gestionar hasta 36 normativas diferentes cargando sus requisitos para llevar un seguimiento.
9. Permitir el envío de encuestas a un mínimo de 2500 usuarios para la recolección de todos los datos referentes a las normativas gestionadas y sus requisitos.
10. Disponer de históricos del avance de adecuación a las normativas.
11. Disponer de gráficos e informes del estado de situación de cada normativa.
12. Disponer de evidencias que permitan relacionar los requisitos normativos con los documentos del MEF.
13. Permitir la categorización, evaluación y análisis de los Bancos de Datos del MEF
14. Permitir la gestión de riesgos de protección de datos, para la evaluación de los Bancos de Datos.
15. Disponer de metodologías precargadas de protección de datos.
16. Disponer de catálogos precargados de la Ley y Reglamento de Protección de Datos del Perú (Ley 29733)
17. Permitir el envío de encuestas a un mínimo de 2500 usuarios para la recolección de todos los datos referentes a la protección de datos. (Bancos de Datos, Riesgos, Controles, Evidencias)
18. Permitir la gestión de los derechos ARCO con workflows y alertas como mínimo a 2500 usuarios propietarios de datos.
19. Disponer de históricos del avance de adecuación a la Ley 29733.
20. Disponer de gráficos e informes del estado de situación de la Ley 29733
21. Disponer de evidencias que permitan relacionar los requisitos normativos con los documentos del MEF.
22. El modelo de implementación deberá ser “Onprimise”.

- **Componente Gestión de riesgo de seguridad de TI**

1. Debe estar licenciada por un periodo de mil noventa y cinco (1095) días calendario y licenciado para 07 (siete) usuarios.
2. Todos los componentes necesarios a fin de cumplir con los requerimientos técnicos deben ser provistos como parte de la solución.
3. Debe proveer toda la infraestructura de software requerido para la implementación de la solución requerida.
4. Debe permitir la conexión simultánea de usuarios.
5. Debe disponer de un manual de usuario del software en español.
6. Debe soportar la gestión de riesgos, gestión de seguridad de la información, gestión de la protección de datos personales según la Ley 29733 de Perú y gestión del cumplimiento corporativo; permitiendo la integración de todos estos en un solo entorno.
7. En función del tipo de usuario se podrán crear y gestionar otros usuarios, o gestionar perfiles a medida.
8. Permitir la configuración de notificaciones, a través de las cuales el usuario recibirá por correo electrónico información necesaria para el desarrollo de actividades pendientes.
9. Permitir la gestión desde una sola herramienta y que las diversas funcionalidades estén integradas entre los distintos módulos. Entre las herramientas y plataformas incluidas para la integración cabe destacar: organigrama, procesos, productos, servicios, controles, etc.
10. Permitir definir los servicios y productos implicados en el alcance. Los servicios y productos que se definan pasarán a formar parte del sistema y permitirán categorizar y tipificar todo el sistema.
11. Permitir la definición de los procesos de negocio.
12. Permitir establecer dependencias entre los diferentes procesos de negocio (Macroprocesos, procesos, subprocesos, etc.).
13. Permitir establecer dependencias entre los servicios y los procesos.
14. Permitir establecer dependencias entre los procesos y los elementos del inventario (como mínimo activos, procesos y procedimientos).
15. Permitir la definición de la estructura organizativa del cliente, es decir, los departamentos, áreas, gerencias, etc. en los que se estructura la organización.
16. Permitir utilizar los elementos definidos en la estructura organizativa para asociar servicios, procesos, empleados, etc. a una estructura concreta.
17. Permite la realización de hasta 7 análisis de riesgos diferentes (como mínimo operacional, cumplimiento, salud, trabajo, auditoria)
18. Permitir la configuración de hasta 7 metodologías diferentes para la evaluación de los riesgos.
19. Permitir la definición de diferentes dimensiones, tanto cualitativas como cuantitativas, con diferentes niveles por cada dimensión.
20. Permitir metodologías cuantitativas y cualitativas.
21. Permitir realizar la identificación de riesgos asociados a la gestión de riesgos. Cada uno de estos con sus propias características y campos. Permitiendo: a. Realizar la evaluación de riesgos a nivel inherente y a nivel residual, u otros factores. y b. Asociar controles a los riesgos analizados para obtener el riesgo residual de manera manual o automática y condicionada a ponderaciones y otros factores parametrizables.
22. Actualización automática de los riesgos al modificar la valoración de los controles asociados
23. Permitir la configuración de una metodología para la evaluación de controles.

24. Permitir la definición de niveles por cada dimensión definida en la evaluación de controles.
25. Permitir la evaluación de los riesgos considerando el resultado de la evaluación de los controles.
26. Permitir asociar controles a los riesgos analizados para obtener el riesgo residual.
27. Permitir la posibilidad de realizar diferentes Planes de Tratamiento de Riesgos para los riesgos que se vayan a tratar, así como su seguimiento.
28. Permitir realizar un seguimiento del grado de avance de implantación de los controles definidos, reportados y registrados por los usuarios responsables.
29. Permitir la configuración de dimensiones y de metodologías para la evaluación de controles.
30. Permitir registrar todos los controles y medidas que el MEF tiene implantado.
31. Permitir el análisis de la eficacia de todos los controles registrados en esta opción, en función de la metodología definida para ello.
32. Permitir asociar los controles a las amenazas/riesgos de forma que se pueda reflejar qué controles están relacionados con qué amenazas.
33. Permitir el cálculo del riesgo residual en función de los controles implantados y su eficacia.
34. Permitir la generación de históricos para comparar la evolución del análisis y gestión de riesgos a lo largo del tiempo.
35. Permitir mediante el análisis de riesgos evaluar las amenazas que afectan a cada uno de los procesos y activos.
36. Permitir la categorización de los riesgos y definir taxonomías y tipologías de ellos.
37. Dispone de catálogos de amenazas, vulnerabilidades y controles predefinidos.
38. Permite la definición de KRIs de riesgos y la relación de amenazas con incidencias y vulnerabilidades.
39. Permitir obtener resultados de riesgos en función de los Servicios, Procesos, Departamentos, Tipologías de riesgos.
40. Permitir definir y adjuntar evidencias de los controles.
41. Permitir la definición de modelos de encuestas para levantar y revisar de manera periódica la información referente a Riesgos, Controles, Planes de Acción, Evidencias.
42. Permitir el envío de encuestas como mínimo a 2500 usuarios y con la posibilidad de definir workflows de revisión y aprobación.
43. Permite realizar la proyección y simulación de los riesgos en base a diferentes criterios.
44. Permite la gestión de proveedores, y los riesgos y controles derivados de estos.
45. Permitir la configuración de campos para implementar la identificación, valoración y clasificación de los activos de información, considerando:
46. Permitir la definición de los niveles de confidencialidad, integridad y disponibilidad, entre otras dimensiones, haciendo uso de un cuestionario creado para ello, así como cualquier otra característica de los activos.
47. Permitir el cálculo del nivel de criticidad del activo de información.
48. Permitir la configuración de las categorías de elementos (servicios, procesos, personal, software, etc.) que se consideran en el inventario.
49. Permitir la configuración de dimensiones cualitativas y cuantitativas para clasificar y valorar el elemento del inventario.
50. Permitir calcular la importancia de cada activo en función de la valoración realizada en las dimensiones definidas.
51. Disponer de un módulo de dependencias que permite asociar los elementos del inventario a los diferentes productos, servicios y procesos de negocio definidos, así como asociar los elementos entre sí.

52. Permitir la definición de modelos de encuestas para levantar información sobre la identificación, clasificación y definición de criticidad de cada activo de información.
53. Permite definir y documentar los Planes de Capacidad, Planes de Disponibilidad, Planes de Continuidad.
54. Permite definir la estrategia de capacitación y formación de los empleados, seguimiento de cursos.
55. Permitir la gestión de eventos, vulnerabilidades, incidencias y problemas, a través de la utilización de estados y categorías, asociación a servicios, almacenamiento de evidencias, etc.
56. Permitir asignarlos a uno o varios empleados del MEF, de forma que la herramienta avisa mediante correo electrónico de la asignación. Permite definir Workflows de gestión automatizados.
57. Permitir realizar el seguimiento de cada evento, incidencia y problema, registrando toda la información asociada
58. Permitir consultar y proponer modificaciones del análisis de riesgos ante la ocurrencia de la eventos e incidencia.
59. Permitir reevaluar los riesgos de forma automática a partir de la ocurrencia de eventos e incidencia.
60. Permitir asociar KRIs a riesgos, de acuerdo a criterios definidos.
61. Permitir asociar KPIs a activos, de acuerdo a criterios definidos.
62. Permitir establecer diversas características para los KRIs y KPIs, tales como métricas, responsables, fórmula de cálculo, etc.
63. Permitir realizar el seguimiento de KRIs y KPIs a ser reportados por los usuarios responsables.
64. Disponer de reportes genéricos que permiten visualizar la información relevante.
65. Disponer de interfaz para diseño de reportes a requerimientos del usuario.
66. Permitir la creación de informes personalizados sobre la información de la plataforma
67. Permitir visualizar de manera gráfica los resultados obtenidos tras la realización de los análisis de riesgos a través de un listado de riesgos, mapa de calor, gráfica de burbujas, gráficas de dispersión entre otros.

- **Componente Gestión de Auditoria**

1. Debe estar licenciada por un periodo de mil noventa y cinco (1095) días calendario y licenciado para 07 (siete) usuarios.
2. Todos los componentes necesarios a fin de cumplir con los requerimientos técnicos deben ser provistos como parte de la solución.
3. Debe proveer toda la infraestructura de software requerido para la implementación de la solución requerida.
4. Permitir la configuración y parametrización de metodologías de Auditoría
5. Permitir configurar la metodología de auditoría para la evaluación de los Servicios, Procesos y Activos de la organización de acuerdo a la normativa actual.
6. Permitir configurar la metodología de auditoría para la evaluación de los Riesgos de acuerdo a la normativa actual.
7. Permitir configurar la metodología de auditoría para la evaluación de los Controles de acuerdo a la normativa actual.
8. Permite automatizar la obtención de resultados de las metodologías de Auditoría de acuerdo a la normativa actual.
9. Permitir la planificación anual de auditorías
10. Permitir la planificación detallada de cada trabajo de auditoría
11. Permitir la definición de roles y equipos de trabajo de auditoría

12. Permitir la ejecución de auditorías con la información actualizada de las áreas de riesgos
13. Permitir la evaluación, análisis y adjuntado de información referente a los trabajos de auditoría
14. Permitir el adjuntado, workflows de revisión, alertas y seguimiento de Papeles de Trabajo
15. Permitir consulta y revisión de evidencias de auditoría
16. Permitir consulta y revisión de las evidencias de controles
17. Permitir descarga de información sobre la ejecución de auditorías
18. Permitir generación del informe de auditoría
19. Disponer de un panel con los tiempos de auditoría, por trabajos, por auditor, por servicios.
20. Dispone de alertas y recordatorios para los auditores.
21. Permitir la creación de 5 usuarios específicos auditores
22. Permitir el perfilado de usuarios para la definición de los roles de auditoría.