
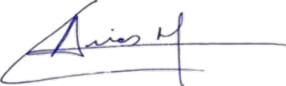


**GERENCIA DE CONTROL DE LA GESTIÓN  
CONDICIONES ESPECIALES  
IMPLEMENTACIÓN DE LA HERRAMIENTA  
SAP Cloud Identity Access Governance**

<b>Fecha</b>	<b>Rev. 00</b>	<b>Modificación</b>	<b>Solicitado por</b>
<b>IMPLEMENTACIÓN</b> <b>SAP Cloud Identity Access Governance</b>			
<b>Preparado por:</b>  Sandra Mojica – <b>Coordinador de Gestión Integral de Riesgos</b>  Edwin Arias – <b>Coordinador de Procesos y Controles Internos</b>			
<b>Aprobado por:</b>  Margarita Aguilar H. - <b>Gerente de Control de la Gestión</b>		<b>Fecha de Elaboración:</b>  14 de julio de 2023	

## TABLA DE CONTENIDO

<b>1. Objetivo.....</b>	<b>3</b>
<b>2. Alcance .....</b>	<b>3</b>
<b>3. Requisitos vinculados a la empresa y su personal .....</b>	<b>3</b>
<b>4. Requisitos Vinculados a la Implementación de SAP Cloud Identity Access Governance .</b>	<b>4</b>
4.1 Arquitectura, Integración y Configuración.....	4
4.2 Validación del Set de Reglas considerando los roles .....	6
4.3 Capacitación.....	6
<b>5. Experiencia del Proveedor Oferente.....</b>	<b>7</b>
<b>6. Metodologías y Planificación .....</b>	<b>7</b>
<b>7. Seguridad para acceso a las soluciones del cliente.....</b>	<b>8</b>
<b>8. Gestión del Servicio .....</b>	<b>8</b>
<b>9. Generación de Reportes .....</b>	<b>9</b>
<b>10. Finalización del Servicio .....</b>	<b>9</b>
<b>11. Valores Agregados .....</b>	<b>9</b>
<b>12. Términos de Pago.....</b>	<b>10</b>
<b>13. Puntaje Habilitador Técnico .....</b>	<b>10</b>
<b>14. Penalización .....</b>	<b>10</b>
<b>15. Criterios de Evaluación.....</b>	<b>11</b>

## **1. Objetivo**

El objeto del presente documento es definir las Condiciones Especiales para la contratación de servicios especializados de implementación de la solución de SAP Cloud Identity Access Governance.

## **2. Alcance**

**2.1** ENSA requiere contratar el servicio de implementación de la solución de SAP Cloud Identity Access Governance integrado con las herramientas con las que actualmente cuenta.

- 2.1.1 SAP ERP / I-SU
- 2.1.2 SAP CRM
- 2.1.3 SAP Success Factor
- 2.1.4 IBM Máximo
- 2.1.5 ADMS

**2.2** Servicio de validación de set reglas considerando los roles para los sistemas:

- 2.2.1 SAP ERP / I-SU
- 2.2.2 SAP CRM
- 2.2.3 SAP Success Factor

**2.3** Las empresas que participen de esta licitación deberán solicitar los detalles de las versiones de las soluciones y otros, previa a la firma de un acuerdo de confidencialidad que deberán remitir al representante de ENSA que los contacte para tal fin.

## **3. Requisitos vinculados a la empresa y su personal**

### **3.1 Empresa:**

La empresa proponente debe contar con aquellas certificaciones, autorizaciones y permisos del fabricante para la prestación de los servicios solicitados. Los cuales deben ser certificados mediante una carta o certificación emitida por el fabricante en el cual conste:

- 3.1.1 Nivel de Partner vigente a la fecha de la presentación de la documentación.
- 3.1.2 Competencias o especializaciones del oferente vigentes a la fecha de la presentación de la documentación.

### **3.2 Personal:**

- 3.2.1 El Oferente debe presentar una Declaración formal listando el equipo técnico mínimo del que dispondrá para la ejecución del contrato.
- 3.2.2 El Oferente debe demostrar que el personal asignado al proyecto cuenta con certificaciones técnicas SAP GRC.

- 3.2.3 El personal asignado al contrato debe haber participado por lo menos en una implementación de Solución de SAP Cloud Identity Access Governance.
- 3.2.4 El personal asignado al servicio de Validación del Set de Reglas considerando los roles, deberá contar con por lo menos dos referencias comprobadas donde se haya realizado la validación del set de reglas y la construcción de los roles.

#### **4. Requisitos Vinculados a la Implementación de SAP Cloud Identity Access Governance**

##### **4.1 Arquitectura, Integración y Configuración**

- 4.1.1 El oferente deberá proponer a ENSA el diseño de la arquitectura de la solución considerando la integración con las soluciones locales (On Premise) o en la nube que formaran parte del alcance de integración como son:
  - a. SAP ERP / I-SU
  - b. SAP CRM
  - c. SAP Success Factor
  - d. IBM Máximo
  - e. ADMS
- 4.1.2 El oferente deberá considerar que el SAP Cloud Identity Access Governance deberá ser implementado en dos ambientes: Calidad y Productivo.
- 4.1.3 El oferente deberá realizar el aprovisionamiento de la herramienta SAP Cloud Identity Access Governance y deberá como parte del servicio recomendar y configurar el esquema de roles y perfiles en la herramienta, manteniendo una adecuada Segregación de Funciones.
- 4.1.4 El oferente se encargará de realizar todas las actividades de instalación (últimas versiones disponibles) y configuraciones requeridas para lograr la integración con los sistemas definidos en el numeral 4.1.1. La instalación y configuración se realizará para cada sistema indicado en el numeral 4.1.1 en los ambientes desarrollo, calidad y productivo (disponibles). Ejemplo: SAP ERP la integración se realizará con los mandantes de Desarrollo, Calidad y Producción.
- 4.1.5 El oferente debe considerar que de ser necesario la aplicación de Notas en los sistemas SAP On Premise, dichas actividades deben ser consideradas como parte del alcance de integración y deben ser consideradas en el cronograma de trabajo, bajo la responsabilidad de El oferente. Las actividades deberán ser realizadas por personal idóneo.
- 4.1.6 En los casos que la integración no se realice directamente sobre los sistemas, sino que se realice a través del LDAP o Active Directory, el oferente deberá definir cuál sería la arquitectura recomendada que permita realizar las pruebas sin afectar los ambientes productivos de ENSA y de ser requerido alguna instalación y/o configuración debe estar considerado en el cronograma y ser considerado como parte del alcance de integración bajo la responsabilidad de El oferente.
- 4.1.7 El oferente deberá especificar a ENSA e incluir en la propuesta los requerimientos de infraestructura requerida para la instalación de los conectores de acuerdo con las características recomendadas por el fabricante.
- 4.1.8 El oferente deberá activar y/o configurar el set de reglas estándar de segregación de funciones con las que cuenta la solución, para las herramientas de SAP ERP/I-

SU y SAP Success Factor. Para SAP CRM debe configurar las reglas de roles y/o transacciones técnicas usadas por los ABAP y Basis.

- 4.1.9 El oferente deberá considerar, la configuración del set de reglas para los sistemas No SAP (IBM Maximo y ADMS). El mínimo de reglas a configurar será de 10 reglas.
- 4.1.10 El proyecto contempla la activación de todos los módulos que componen la solución con excepción de aquellas funcionalidades que involucran el aprovisionamiento directo sobre la solución integrada.
- 4.1.11 El oferente deberá habilitar los módulos y configuraciones requeridas en la solución para permitir realizar simulaciones o identificación de riesgos previos a la asignación de permisos.
- 4.1.12 El oferente deberá definir un flujo de trabajo soportado por la herramienta que permita que los usuarios definidos como líderes funcionales y Seguridad de la Información puedan revisar los roles asignados a su personal y que en la herramienta quede documentada su decisión de aprobación o sugerencia de corrección.
- 4.1.13 El oferente deberá proponer y explicar detalladamente, una opción que permita validar roles y/o usuarios que no han sido utilizados en un periodo de tiempo por Altas, Bajas y Cambios y emitir un informe o una alerta para su corrección.  
Ejemplos:
  - Roles que no han sido utilizados.
  - Usuarios que nunca han ingresado al sistema o tiene la contraseña inicial expirada.
  - Usuarios que tienen más de 90 días que no ingresan al ambiente.
  - Usuarios que están vencidos o bloqueados y que tienen autorizaciones asignadas.
- 4.1.14 En los casos que las reglas estándar de SAP no lo contemplen se deberán crear el set de reglas que permitan identificar como críticos los roles que contienen objetos y autorizaciones como por ejemplo las siguientes:

**Objeto Crítico**

S\_DATASET \*  
S\_BTCH\_JOB \*  
P\_ORGIN \*  
S\_USER\_GRP \*  
S\_USER\_PRO \*  
S\_USER\_AGR \*  
S\_USER\_AUT \*  
S\_TRANSPRT \*  
S\_BTCH\_ADM \*  
S\_DEVELOP \*  
S\_USER\_SYS \*  
S\_TABU\_DIS \*  
S\_ADMI\_FCD \*  
S\_TABU\_CLI \*  
S\_RFC \*  
S\_PROGRAM \*  
SAP\_ALL

SAP\_NEW.  
SAP\_DEBUG

- 4.1.15 El sistema debe permitir guardar las decisiones que en función de los procesos se hayan tomado y deben poderse consultar en el tiempo.
- 4.1.16 Entregables para el numeral 4.1:
  - a. Roles y perfiles de la Solución SAP Cloud Identity Access Governance.
  - b. Documentación detallada de las integraciones.
  - c. Documentación de reglas establecidas para cada solución.
  - d. Reporte de riesgos identificados.
  - e. Diseño de los procesos que serán habilitados en la solución.

## **4.2 Validación del Set de Reglas Considerando los Roles**

Este servicio será realizado como un servicio de estabilización de la solución.

- 4.2.1 El oferente luego de cumplida la etapa de integración y de generar el primer análisis de riesgos deberá proponer a ENSA la construcción de nuevos roles para la solución SAP ERP/I-SU, SAP CRM y SAP Success Factor para lo cual deberá cumplir con las siguientes actividades:
  - a. Analizar el uso transaccional de los usuarios.
  - b. Generar propuesta de retiro de roles, transacciones, actividades, objetos de autorización.
  - c. Generar propuesta de roles nuevos.
  - d. Alinear permisos con cargos dentro de la compañía.
  - e. Generar plan de pruebas.
  - f. Realizar pruebas.
- 4.2.2 Documentación y capacitación.

Se deberá entregar:

  - a. Nomenclatura recomendada de roles.
  - b. Matriz de cambios (roles nuevos vs roles antiguos).
  - c. Matriz de asignación de roles nuevos.
  - d. Matrices de SoD (roles y usuarios).
  - e. Matrices de Accesos Críticos (roles y usuarios).

## **4.3 Capacitación**

- 4.3.1 El oferente deberá realizar un Workshop detallado de no menos de 40 horas durante la primera semana luego de firmado el contrato, con el objetivo que el personal de ENSA cuente con todo el conocimiento y criterio para aprobar el diseño a implementar de la solución SAP Cloud Identity Access Governance.
- 4.3.2 El oferente deberá realizar una capacitación detallada y certificada del uso de la solución al personal de ENSA. La capacitación debe considerar los temas relacionados con la configuración, parametrización, conectividad, administración y reportería de la solución una vez finalizada la implementación e integración.
- 4.3.3 El oferente deberá realizar una capacitación detallada y certificada de la metodología y mejores prácticas para el cumplimiento de la Validación de Set de Reglas Considerando los Roles.

#### 4.3.4 Entregables:

- a. Material de capacitación.
- b. Manuales de usuario final del objeto del contrato (Técnicos y Funcionales).

### 5. Experiencia del Proveedor Oferente

5.1 La empresa deberá demostrar su buena experiencia y calidad del servicio prestado para lo cual debe hacer una relación de los trabajos de igual naturaleza a los que constituyen el objeto de esta licitación, como mínimo durante los últimos tres años.

5.2 En este sentido, se validará la experiencia mínima del Oferente, en los servicios de implementación de soluciones de Gobierno, Riesgo y Cumplimiento de SAP. La misma debe ser acreditada por el Oferente mediante un mínimo de tres cartas o certificación de un cliente que haya recibido este servicio y en la que se detalle como mínimo lo siguiente:

- Nombre o tipo de servicio recibido.
- DD/MM/AAAA de inicio del servicio recibido.
- DD/MM/AAAA de finalización del servicio recibido.
- Confirmación de la calidad y continuidad del servicio considerando si se presentaron reclamos, interrupciones, penalizaciones u otras circunstancias especiales.

Una de las cartas debe ser de una implementación de SAP Cloud Identity Access Governance.

La misma será calificada a través del formulario de **Referencia Externa** de clientes que tenga o haya tenido el Oferente; aunque no será excluyente el tipo de formato que se utilice para presentar esta información, siempre y cuando se detalle claramente los puntos arriba listados, en caso que no contenga la información requerida la carta de referencia no será considerada como válida.

### 6. Metodologías y Planificación

6.1 Los Oferentes deberán presentar un cronograma como parte de la propuesta. En los que deben quedar claramente identificadas las fechas en las que se cumplirán los hitos que a continuación se detallan, el orden enumerado debe mantenerse, esto no limita que El Oferente pueda realizar tareas de manera simultánea para acortar los tiempos sin afectar la calidad.:

1. Aprovisionamiento SAP Cloud Identity Access Governance.
2. Integración SAP ERP / I-SU y activación de set de reglas estándar.
3. Integración SAP CRM y activación de set de reglas técnicas (ABAP y Basis).
4. Integración SAP Success Factor y activación de set de reglas estándar.
5. Integración IBM Máximo y creación de set de reglas.
6. Integración ADMS y creación de set de reglas.
7. Validación del Set de Reglas considerando los roles SAP ERP / I-SU
8. Validación del Set de Reglas considerando los roles SAP CRM
9. Validación del Set de Reglas considerando los roles SAP Success Factor

- 6.2 En este sentido, el Oferente debe explicar en su propuesta de manera detallada la forma en la que abordará cada uno de los hitos establecidos en el numeral anterior. (Metodología, recursos, y otros)
- 6.3 La empresa proponente debe demostrar que opera con una metodología alineada con marcos y estándares de referencia como por ejemplo serían: ITIL, ISO 27001, NIST, CERT, NERC-CIP, prácticas del SANS Institute, SAP y otras con las que pudiera contar.
- 6.4 El detalle debe permitir medir que sus metodologías y planificación van a llevar a ENSA a lograr recibir los servicios dentro de los tiempos especificados y con la calidad requerida.
- 6.5 El proyecto tendrá una duración máxima de ocho (8) meses.
- 6.6 Los hitos 6.1.1 y 6.1.2 deberán ser finalizados con fecha límite al 11 de diciembre de 2023.

## **7. Seguridad para Acceso a las Soluciones del Cliente**

7.1 El Oferente deberá cumplir con las siguientes especificaciones:

- 7.1.1 Contar con una aplicación o software que permita la protección de ataque por código malicioso, tipo antivirus/antimalware en cada uno de los equipos utilizados para ofrecer el servicio. El cual deberá mantenerse actualizado y vigente de acuerdo con lo que recomienda el fabricante de la aplicación.
- 7.1.2 Deberá proporcionar a ENSA, la constancia de la fecha de expiración de los softwares de seguridad y durante la prestación del servicio, el software de seguridad debe contar con licencias vigentes.
- 7.1.3 Mantener una comunicación segura con ENSA mediante un VPN el cual será configurado de acuerdo con las especificaciones técnicas definidas por ENSA.

## **8. Gestión del Servicio**

- 8.1 El servicio debe iniciar a partir de la fecha indicada en el Contrato en la Cláusula - DURACIÓN DEL CONTRATO.
- 8.2 Por lo sensitivo que resulta para ENSA el proceso se prefiere el servicio sin subcontratación; de existir esta figura el Oferente debe detallarlo como parte de la propuesta y de presentarse posteriormente durante la vigencia del contrato debe someterse a la revisión y aprobación de ENSA.
- 8.3 El Oferente recibirá por parte de ENSA un entendimiento inicial en las soluciones y políticas, y será responsabilidad de El Oferente mantener en todo momento a sus técnicos en conocimiento actualizado de las soluciones y políticas de ENSA.
- 8.4 Instruir a su personal, que bajo ninguna circunstancia está autorizado para compartir las contraseñas de acceso a las soluciones que ENSA le suministró.
- 8.5 Reportar de forma inmediata los cambios de personal asignado a ENSA a los que se les haya otorgado acceso, ya sean salidas, incapacidades y cambios de funciones que demanden cambios o eliminación de los accesos otorgados como parte de la prestación del servicio.
- 8.6 En caso de que ENSA identifique que el personal asignado al proyecto no tiene los conocimientos y experiencia requerida podrá solicitar a costo del Oferente el reemplazo de este en un lapso no mayor de cinco (5) días laborables. El personal de reemplazo



deberá cumplir con el perfil solicitado en el numeral 3.2 y se deberá entregar a ENSA toda la información requerida para la validación y aprobación correspondiente.

- 8.7 Mantener los niveles de servicio y tiempos acordados con ENSA, aún en los casos en que se presenten renunciaciones, incapacidades que deriven en ausencias del personal u otras de naturaleza similar.
- 8.8 El Oferente será responsable de ejecutar el respaldo de las configuraciones realizadas como parte del proyecto y solicitar de manera formal los respaldos requeridos en los sistemas de ENSA.

## **9. Generación de Reportes**

- 9.1 El oferente deberá habilitar todos los reportes estándar de la solución y deberá contar con reportes y plantillas modificables de categorías como las siguientes:
  - Listado de reglas.
  - Listado de riesgos identificados.
- 9.2 El oferente deberá capacitar al personal de ENSA en la construcción de reportes avanzados.
- 9.3 El oferente deberá explicar al personal de ENSA como se ejecuta la funcionalidad de exportación de los reportes a formatos:
  - Excel con datos y detalle
  - CSV
  - PDF
- 9.4 No obstante, Igualmente incluirá ejemplos de cuadros de mando con métricas e indicadores de la Gestión de Gobierno de Identidades.

## **10. Finalización del Servicio**

- 10.1 Esta fase se deberá realizar cuando se determine la finalización del servicio, ya sea por cumplimiento del plazo inicial establecido para el contrato, o por la resolución del contrato instada por alguna de las partes con base en el incumplimiento contractual.
- 10.2 Antes de la finalización del contrato, el Oferente del servicio queda comprometido a facilitar el retorno de toda la documentación (informes, procedimientos y otros) generada a lo largo del contrato y de todos los registros de actividad del servicio y configuraciones almacenados en medios digitales.
- 10.3 El Oferente del servicio queda igualmente comprometido con destruir toda esta información una vez haya sido transferida a ENSA lo que corresponda y entregar evidencias de estas acciones realizadas.
- 10.4 Antes de la finalización del contrato, el Oferente del servicio queda comprometido a coordinar el cambio de contraseñas y demás accesos que le hayan sido asignados como parte del servicio. Esto incluye y sin limitaciones gestionar el cambio de contraseñas de los ambientes de la herramienta SAP Cloud Identity Access Governance para que ENSA tenga el control único de la herramienta.
- 10.5 El Oferente debe indicar como parte de la propuesta el tiempo máximo que requiere para realizar esta etapa de cierre o finalización del contrato.

## **11. Valores Agregados**

- 11.1 El oferente debe indicar los valores agregados que ofrece como parte de los servicios de Implementación de la Herramienta SAP Cloud Identity Access Governance los cuales pueden corresponder a servicios adicionales, capacitaciones, etc.

## 12. Términos de Pago

- 12.1 El Oferente deberá emitir una sola factura por el monto total y los pagos que tenga que hacer ENSA por los servicios efectivamente prestados, se realizarán 30 días después de haber recibido a satisfacción el cumplimiento de cada hito correspondiente según lo indicado en el numeral 6.1.
- 12.2 Para poder realizar el último pago y ejecutar el Acta de Cierre de Cuentas, el Oferente debe asegurar la confidencialidad, eliminando la información de ENSA, mediante el cumplimiento de la etapa de Finalización del Servicio.

## 13. Puntaje Habilitador Técnico

Considerando la especialización del servicio se establece que la evaluación técnica corresponda al 90% de toda la evaluación de la propuesta del servicio.

## 14. Penalización

Se aplicará por atrasos en la fecha límite establecidas para cada hito como se detalla a continuación:

Hito	Fecha límite	Penalización
Aprovisionamiento SAP Cloud Identity Access Governance.	11 de diciembre de 2023	15% del monto del hito
Integración SAP ERP / I-SU y activación de set de reglas estándar.	11 de diciembre de 2023	15% del monto del hito
Integración SAP CRM y activación de set de reglas técnicas (ABAB y Basis).	Fecha establecida en cronograma aprobado por ENSA.	10% del monto del hito
Integración SAP Success Factor y activación de set de reglas estándar.	Fecha establecida en cronograma aprobado por ENSA.	10% del monto del hito
Integración IBM Máximo y creación de set de reglas.	Fecha establecida en cronograma aprobado por ENSA.	10% del monto del hito
Integración ADMS y creación de set de reglas.	Fecha establecida en cronograma aprobado por ENSA.	10% del monto del hito
Validación del Set de Reglas considerando los roles SAP ERP / I-SU	Fecha establecida en cronograma aprobado por ENSA.	10% del monto del hito
Validación del Set de Reglas considerando los roles SAP CRM	Fecha establecida en cronograma aprobado por ENSA.	10% del monto del hito

Hito	Fecha límite	Penalización
Validación del Set de Reglas considerando los roles SAP Success Factor	Fecha establecida en cronograma aprobado por ENSA.	10% del monto del hito

## 15. Criterios de Evaluación

El Oferente, deberá entregar un cuadro de cumplimiento en donde indique su aceptación del requisito, la explicación detallada y en qué sección de la propuesta o a través de qué documento (referenciar en el cuadro el anexo o nombre del documento), cumple con todos los requerimientos de ENSA los cuales deben mantener la misma numeración del requerimiento de ENSA establecidos en este documento de Condiciones Especiales. En caso de no cumplir con este requisito el punto no será evaluado.

En este sentido, los criterios y mecanismos de evaluación son los siguientes:

No. Requisito	Factor	Información para la Evaluación
3.1	<b>Requisitos vinculados a la empresa</b>	<p>Certificaciones, Permisos, Autorizaciones relacionadas con el servicio que sean presentadas.</p> <p>Carta o certificación emitida por el fabricante donde conste el nivel de Partner autorizado de SAP.</p> <p>Carta o certificación emitida por el fabricante donde conste las competencias o especializaciones vigentes a la fecha de la presentación de la propuesta.</p> <p>Explicaciones, procedimientos y otros detalles que se adjunten en la propuesta como apoyo de las certificaciones.</p>
3.2	<b>Requisitos vinculados al personal</b>	<p>Listado completo y con información adecuada (experiencia, formación académica, premios o reconocimientos recibidos según su nivel de responsabilidad, referencias de empresas servidas por el mismo, etc.) para valorar el personal asignado al servicio de ENSA.</p> <p>Estructura de atención y detalles de responsabilidades.</p> <p>Certificaciones de cada persona listada y que guarden relación con SAP Gobierno, Riesgo y Cumplimiento.</p> <p>Carta de referencia o correo de contacto donde conste el proyecto ejecutado por el personal que</p>

No. Requisito	Factor	Información para la Evaluación
		<p>participará en la implementación, en donde conste que ha realizado por lo menos una implementación de SAP Cloud Identity Access Governance.</p> <p>Carta de referencia o correo de contacto donde conste el proyecto ejecutado por el personal que participará en la Validación de Set de Reglas Considerando los Roles.</p>
<b>4</b>	<b>Requisitos Vinculados a la implementación e Integración</b>	
<b>4.1</b>	<b>Arquitectura, Integración y Configuración</b>	<p>Descripción de la Arquitectura (numeral 4.1.1).</p> <p>Descripción detallada de los requisitos y método de integración que permita medir o validar el cumplimiento de El oferente para su puesta en producción de la solución (numerales 4.1.2 a 4.1.7).</p> <p>Descripción detallada de los requisitos y método de configuración que permita medir o validar el cumplimiento de El oferente para su puesta en producción de la solución (numerales 4.1.8 a 4.1.15).</p> <p>Descripción detallada de los entregables mínimos requeridos que permita validar el cumplimiento de documentación formal a ser entregada por el oferente (numeral 4.1.16).</p>
<b>4.2</b>	<b>Validación del Set de Reglas Considerando los Roles</b>	<p>Descripción detallada de los requisitos y método de trabajo que permita medir o validar el compromiso de El oferente para la ejecución de las actividades requeridas.</p> <p>Listado de entregables enumerando el contenido de cada documento.</p>
<b>4.3</b>	<b>Capacitación</b>	<p>Listado de las capacitaciones ofrecidas por Oferente en donde se enumeren los temas a ser tratados en cada capacitación, duración de las capacitaciones, cantidad de personas que por parte de ENSA pueden participar en la cada una de las capacitaciones.</p>
<b>5</b>	<b>Experiencia del Proveedor Oferente</b>	<p>Cantidad y contenido de las cartas de referencia de calidad y experiencia en el servicio requerido por ENSA.</p>

No. Requisito	Factor	Información para la Evaluación
		<p>Nivel y relación de la autoridad que firma la carta de referencia con el conocimiento técnico del servicio que se está recomendando.</p>
6.	<p><b>Metodologías y Planificación</b></p>	<p>Estructura, responsabilidades, etapas de planeación y tiempos para el proyecto o etapa de implementación del servicio.</p> <p>Planeación, métodos de comunicación, métodos de seguimiento y otros que se usarán durante la prestación del servicio.</p>
7.	<p><b>Seguridad para acceso a las soluciones del cliente</b></p>	<p>Constancia gráfica de la protección de ataque por código malicioso, tipo antivirus/antimalware en cada uno de los equipos utilizados para ofrecer el servicio con visualización de la fecha de expiración de dichas soluciones.</p> <p>Método de verificación propuesto para asegurar al cliente que las mismas se mantendrán actualizadas durante la prestación del servicio.</p> <p>Método de verificación propuesto para asegurar al cliente que mantendrá durante la prestación del servicio una comunicación segura con ENSA mediante un VPN el cual será configurado de acuerdo con las especificaciones técnicas definidas por ENSA.</p> <p>Indicación y detalles del sistema de recepción de correos que utilizará garantizando la correcta comunicación con ENSA.</p>
8.	<p><b>Gestión del Servicio</b></p>	<p>Descripción del mecanismo de formalización y concienciación que aplican para cumplir con las medidas de seguridad que su personal debe tener con los accesos brindados por el cliente a sus soluciones.</p> <p>Descripción de la metodología y responsable de la comunicación inmediata de las rotaciones del personal.</p> <p>Método y responsable de las acciones de seguimiento descritas en el 8.5 de la presente especificación técnica.</p>

No. Requisito	Factor	Información para la Evaluación
		Expresión de compromiso formal incluida en la propuesta con relación a lo especificado en 8.6 y 8.7.
9.	<b>Generación de Reportes</b>	<p>Presentación del método y responsabilidades para cumplir con la habilitación de los informes con los que cuenta la aplicación.</p> <p>Duración y detalle de la capacitación que será impartida al personal de ENSA en la construcción de los informes avanzados.</p>
10.	<b>Finalización del servicio</b>	Se evaluará la Inclusión en la propuesta de una carta formal de compromiso de la forma de cumplir con los controles de finalización del contrato tal como se presentan en 10.1 a 10.7
11.	<b>Valores agregados</b>	Se evaluará la Inclusión en la propuesta de valores agregados.