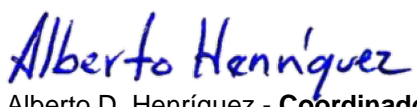
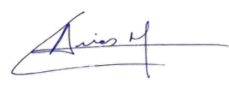
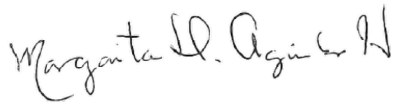


**GERENCIA DE CONTROL DE LA GESTIÓN  
CONDICIONES ESPECIALES  
Servicio de Recurso en Sitio para  
Ciberseguridad y Seguridad de la Información**

|  |                |   |                       |
|--|----------------|---|-----------------------|
|  |                |   |                       |
| <b>Fecha</b>   | <b>Rev. 00</b> | <b>Modificación</b>                                     | <b>Solicitado por</b> |
| <b>Servicio de Recurso en Sitio para<br/>Ciberseguridad y Seguridad de la Información</b>  |                |   |                       |
| <b>Preparado por:</b><br><br>Alberto D. Henríquez - <b>Coordinador de Seguridad de la Información</b> |                |   |                       |
| <br>Edwin O. Arias M. - <b>Coordinador de Riesgos</b>   |                |   |                       |
| <b>Aprobado por:</b><br><br>Margarita Aguilar H. - <b>Gerente de Control de la Gestión</b>          |                | <b>Fecha de Elaboración:</b><br><br>10 de enero de 2024 |                       |

## TABLA DE CONTENIDO

|     |  |          |
|-----|--|----------|
| 1.  | <b>Objetivo .....</b>  | <b>3</b> |
| 2.  | <b>Alcance.....</b>  | <b>3</b> |
| 3.  | <b>Requisitos vinculados a la empresa y su personal .....</b>  | <b>5</b> |
| 4.  | <b>Seguridad para Acceso a las Soluciones del Cliente.....</b> | <b>6</b> |
| 5.  | <b>Gestión del Servicio.....</b>                               | <b>6</b> |
| 6.  | <b>Penalizaciones: .....</b>                                   | <b>7</b> |
| 7.  | <b>Finalización del Servicio.....</b>                          | <b>8</b> |
| 8.  | <b>Valores Agregados .....</b>                                 | <b>8</b> |
| 9.  | <b>Términos de Pago.....</b>                                   | <b>8</b> |
| 10. | <b>Puntaje Habilitador Técnico .....</b>                       | <b>8</b> |
| 11. | <b>Criterios de Evaluación .....</b>                           | <b>9</b> |

## 1. Objetivo

El objeto del presente documento es definir las Condiciones Especiales para la contratación de servicios especializados de un recurso en sitio para Ciberseguridad y Seguridad de la Información.

## 2. Alcance

2.1 ENSA requiere contratar el servicio de un recurso en sitio responsable de atender lo siguiente:

- a) Relacionamiento con el Centro de Operaciones de Seguridad (SOC).
- b) Participación a requerimiento en los principales proyectos que requieren una representación en esta materia.
- c) Asesoría y participación a requerimiento ante la gestión de incidentes de naturaleza significativa.
- d) Generación de reportes producto del ejercicio de controles periódicos según se detalla a continuación, sin limitar cambios o adiciones que sean necesarias por cambios o actualizaciones en las aplicaciones que se presenten durante la vigencia del contrato:

| Entregable | Reportes   | Frecuencia |
|------------|--|------------|
| 1          | Informe de Vulnerabilidades TI y ADMS (TO)                 | Mensual    |
| 2          | Reporte de Escaneos programados estaciones de trabajo      | Bimensual  |
| 3          | Equipos Sin antivirus                                      | Trimestral |
| 4          | Equipos sin cifrado  | Trimestral |
| 5          | Informe de indicadores                                     | Mensual    |
| 6          | Informe de revisión usuarios y roles maximo                | Semestral  |
| 7          | Informe de revisión usuarios y roles infoweb               | Semestral  |
| 8          | Informe de revisión usuarios y roles sistema de lectura WM | Semestral  |
| 9          | Informe de revisión usuarios y roles sap erp / IS-U        | Semestral  |
| 10         | Informe de revisión usuarios y roles sap crm               | Semestral  |
| 11         | Informe de revisión usuarios y roles sap po                | Semestral  |
| 12         | Informe de revisión usuarios y roles ADMS                  | Semestral  |
| 13         | Informe de revisión usuarios y roles GIS                   | Semestral  |
| 14         | Informe de revisión usuarios y roles VPN (Locales)         | Semestral  |
| 15         | Informe de revisión usuarios y roles VPN (AD-Internos)     | Semestral  |
| 16         | Informe de revisión usuarios y roles VPN (AD-Externos)     | Semestral  |
| 17         | Informe de revisión usuarios y roles AD TI                 | Semestral  |
| 18         | Informe de revisión usuarios y roles prepago               | Semestral  |
| 19         | Informe de revisión usuarios y roles ACH                   | Semestral  |
| 20         | Informe de parámetros maximo                               | Anual      |
| 21         | Informe de parámetros infoweb                              | Anual      |
| 22         | Informe de parámetros sistema de lectura WM                | Anual      |
| 23         | Informe de parámetros sap erp / IS-U                       | Anual      |
| 24         | Informe de parámetros sap crm                              | Anual      |
| 25         | Informe de parámetros sap po (antes PI)                    | Anual      |
| 26         | Informe de parámetros ADMS                                 | Anual      |

| Entregable | Reportes  | Frecuencia |
|------------|---|------------|
| 27         | Informe de parámetros GIS                                 | Anual      |
| 28         | Informe de parámetros VPN (local)                         | Anual      |
| 29         | Informe de parámetros Prepago                             | Anual      |
| 30         | Informe de parámetros AD TI                               | Anual      |
| 31         | Informe de revisión accesos físicos                       | Semestral  |
| 32         | Informe de revisión cuentas default maximo                | Anual      |
| 33         | Informe de revisión cuentas default infoweb               | Anual      |
| 34         | Informe de revisión cuentas default sistema de lectura WM | Anual      |
| 35         | Informe de revisión cuentas default sap erp / IS-U        | Anual      |
| 36         | Informe de revisión cuentas default sap crm               | Anual      |
| 37         | Informe de revisión cuentas default sap po                | Anual      |
| 38         | Informe de revisión cuentas default ADMS                  | Anual      |
| 39         | Informe de revisión cuentas default GIS                   | Anual      |
| 40         | Informe de revisión cuentas default VPN                   | Anual      |
| 41         | Informe de revisión cuentas default prepago               | Anual      |
| 42         | Informe de revisión de Niveles de Autorización en SAP     | Anual      |
| 43         | Informe de revisión de Niveles de Autorización No SAP     | Anual      |
| 44         | Informe de monitoreo accesos DEBUG                        | Quincenal  |
| 45         | Informe de monitoreo accesos SAP ALL/SAP_NEW              | Quincenal  |

- 2.2 El servicio deberá entregar durante los primeros cinco (5) días hábiles de cada mes, un informe sobre el servicio ofrecido el mes anterior, disponibilidad, casos pendientes e incidentes presentados en el periodo.
- 2.3 El servicio deberá contemplar el proceso de escalamiento hacia el área de TI/TO o hacia los proveedores y/o fabricantes de las soluciones dependiendo de la situación coordinada con el SOC.
- 2.4 El servicio deberá mantener un inventario actualizado de las herramientas de seguridad con las que cuenta ENSA e indicar anticipadamente cuándo corresponde realizar actualizaciones.
- 2.5 Los requisitos de habilitación que las empresas que participen de esta licitación deberán cumplir son:
- 2.5.1 Solicitar los detalles de los tipos de soluciones de seguridad, fabricante, tecnologías, cantidad de consolas, tipo de ambiente, previa a la firma de un acuerdo de confidencialidad de la información que deberán remitir al representante de ENSA que los contacte para tal fin.
- 2.5.2 El proveedor oferente no debe ofrecer servicios a las áreas de Tecnología Informática o Tecnología Operativa de ENSA relacionados con Seguridad de la Información o Ciberseguridad.
- 2.5.3 Lo anterior para mantener el modelo de Control Interno bajo COSO, en donde Seguridad de la Información pertenece a una gerencia distinta a TI (Tecnología Informática) o TO por ser parte de lo que se denomina “Segunda Línea de Defensa”. Debe entregar una nota o carta informando que cumple con ese requisito.

Para mayor claridad se ilustra el modelo de Controles Internos existente en la estructura administrativa de ENSA:



2.6 El servicio será prestado durante cuarenta y ocho (48) meses con una disponibilidad 8x6, lunes a sábado de 8 a 5:00 p.m.

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

#### 3.1 Empresa:

La empresa oferente debe contar con aquellas certificaciones, autorizaciones y permisos vigentes para la prestación de los servicios solicitados, como mínimo durante los 48 meses durante los cuales prestará el servicio.

En este sentido, se validará la experiencia mínima del Oferente, en los servicios relacionados al objeto de esta licitación mediante un mínimo de dos (2) 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.
- Duración del Contrato.
- Evaluación general de la calidad del servicio soporte recibido.
- Valoración en cuanto al tiempo de respuesta y cumplimiento de ANS.
- Confirmación de la calidad y continuidad del servicio considerando si se presentaron reclamos, interrupciones, penalizaciones u otras circunstancias especiales.

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 de que no contenga la información requerida la carta de referencia no será considerada como válida.

### 3.2 **Personal:**

3.2.1 El Oferente debe presentar Hoja de vida en español.

3.2.2 El Oferente debe presentar las Certificaciones y/o diplomas de cursos en donde se pueda evidenciar el conocimiento del personal técnico en las herramientas de Ciberseguridad. Las certificaciones deben ser en las herramientas de fabricante a las que ENSA posee (según lo entregado en el punto 2.5.1) o su equivalente al tipo de herramienta que ENSA posee. En caso de no contar con las certificaciones debe indicarse en la Hoja de Vida de cada personal la experiencia en el manejo de cada una de las herramientas y el detalle de referencia que permita validar dicha experiencia y el manejo de la misma.

3.2.3 El Oferente debe presentar dos (2) referencias de clientes en donde se indique los trabajos realizados por el **recurso en sitio** asignado. La carta debe ser emitida en papel membrete de la empresa que emite la referencia, indicando el personal que ofreció el servicio. Se aceptarán cartas de servicios prestados en el extranjero. Los proyectos deben haber sido ejecutados durante los últimos cinco (5) años.

3.2.4 Deberá contar con una experiencia mínima de tres (3) años en posiciones similares. Detallar el periodo (inicio y fin) de ejecución de las posiciones.

3.2.5 El personal en sitio deberá contar en todo momento con un gafete que lo identifique. El mismo debe contar con una foto, nombre completo y cargo legible.

3.2.6 El personal oferente debe cumplir con el código de vestimenta ENSA.

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

El Oferente deberá cumplir con las siguientes especificaciones:

4.1 Asignar un equipo portátil y un celular para la realización de las tareas asignadas en ENSA.

4.2 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.

4.3 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.

### 5. **Gestión del Servicio**

5.1 El servicio debe iniciar a partir de la fecha indicada en el Contrato en la Cláusula - DURACIÓN DEL CONTRATO.

5.2 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.

- 5.3 El proveedor y el personal asignado a la prestación del servicio deberán firmar acuerdo de confidencialidad de la información.
- 5.4 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.
- 5.5 Instruir a su personal, que bajo ninguna circunstancia está autorizado para compartir las contraseñas de acceso a las soluciones que ENSA le suministró.
- 5.6 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.
- 5.7 En caso de que ENSA identifique que el personal asignado al servicio 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.
- 5.8 Mantener los servicios contratados con ENSA, aún en los casos en que se presenten renunciaciones, incapacidades que deriven en ausencias del personal u otras de naturaleza similar.
- 5.9 El servicio será prestado de manera presencial, sin embargo, por situación del país como protestas o situaciones inseguras, se podrá previa comunicación con ENSA aceptar cambios temporales a remoto.
- 5.10 ENSA realizará cada año evaluación de desempeño, con el propósito de mantener la calidad de servicio.

## 6. Penalizaciones:

| Descripción de la Acción   | Penalización  |
|--|---|
| Incumplimiento en la prestación del servicio contratado que <b>NO</b> genere ninguna pérdida de información o disponibilidad de los servicios o sistemas de ENSA | \$100.00 por no atención incurrida hasta un máximo del 10% del valor mensual del contrato.  |
| Incumplimiento en la prestación del servicio contratado que <b>SI</b> genere pérdida de información o indisponibilidad de los servicios o sistemas de ENSA       | <p>\$100.00 por no atención incurrida hasta un máximo del 10% del valor mensual del contrato. Más los costos que se deriven de recuperar, reconstruir o generar nuevamente la información.</p> <p>Más los salarios del personal que no pueda laborar y los costos de recuperación que se deriven de no haber identificado la incidencia de manera oportuna.</p> |

## **7. Finalización del Servicio**

- 7.1 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.
- 7.2 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.
- 7.3 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.
- 7.4 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.
- 7.5 El Oferente debe indicar como parte de la propuesta el tiempo máximo que requiere para realizar esta etapa de cierre o finalización del contrato.

## **8. Valores Agregados**

Se considera (n) valor (es) agregado (s) en el servicio, como:

- ✓ Alineación a NIST.
- ✓ Poseer certificación CERT.
- ✓ Alineación a ISO 27001.
- ✓ Contar con BCP/DRP.
- ✓ Ser partner oficial de las soluciones que utiliza ENSA.
- ✓ Contar con personal certificado en Ethical Hackers, CISSP, PMO, ISO 27001, CISA, CISM, CRISC.
- ✓ Capacitado en seguridad de Office 365.
- ✓ Experiencia de la empresa en redes OT.

## **9. Términos de Pago**

- 9.1 Los pagos que tenga que hacer ENSA por los servicios efectivamente prestados y recibidos a satisfacción, se realizarán mensualmente dentro de los treinta (30) días calendarios siguientes a la aceptación del servicio y fecha de recepción de la factura correspondiente. Ejemplo: El mes de enero se facturará a finales de dicho mes y será pagado el mes siguiente.
- 9.2 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 7. Finalización del Servicio.

## **10. 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.



## 11. Criterios de Evaluación

El Oferente, deberá entregar como parte de su oferta el **cuadro o matriz de cumplimiento** en donde se identifique la aceptación del requisito, la explicación detallada y en qué sección de la propuesta (página y numeración) 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 de la tabla de contenido establecidos en este documento de Condiciones Especiales. En caso de no cumplir con este requisito el factor no identificado, no será evaluado, dando como resultado el menor valor de la calificación (0%).

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

| No. Requisito | Factor   | Información para la Evaluación   |
|---------------|--|--|
| 2.            | Alcance  | Inclusión en la propuesta del conocimiento y compromiso de cumplimiento con el Alcance del servicio requerido por ENSA (numerales 2.1 al 2.4 y 2.6).   |
| 3.1           | Requisitos vinculados a la empresa                 | Certificaciones, autorizaciones y permisos para la prestación de los servicios solicitados.<br><br>Mínimo de dos (2) cartas o certificación de un cliente que haya recibido este servicio y en la que se detalle como mínimo lo indicado en el numeral 3.1.  |
| 3.2           | Requisitos vinculados al personal                  | Hoja de Vida en español del profesional asignado para prestar los servicios que incluya el detalle de experiencia mínima de tres años que se está solicitando (numerales 3.2.1 y 3.2.4).<br><br>Certificaciones y/o diplomas de cursos en donde se pueda evidenciar el conocimiento del personal técnico en las herramientas de Ciberseguridad de uso en ENSA o su equivalente (numeral 3.2.2).<br><br>Dos (2) referencias de clientes en donde se indique los trabajos realizados por el recurso en sitio asignado (numeral 3.2.3). |
| 4.            | Seguridad para acceso a las soluciones del cliente | 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.<br><br>Método de verificación propuesto para asegurar al cliente que las mismas se mantendrán actualizadas durante la prestación del servicio.   |

| No.<br>Requisito | Factor                           | Información para la Evaluación   |
|------------------|----------------------------------|--|
|                  |                                  | <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>  |
| 5.               | <b>Gestión del Servicio</b>      | <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 5.1, 5.2, 5.3 y 5.4 de la presente especificación técnica.</p> <p>Expresión de compromiso formal incluida en la propuesta con relación a lo especificado en 5.7 y 5.8.</p> |
| 7.               | <b>Finalización del servicio</b> | <p>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 7.1 a 7.5.</p>  |
| 8.               | <b>Valores agregados</b>         | <p>Se evaluará la Inclusión en la propuesta de valores agregados según se detallan en el numeral 8.</p>  |