



SEGURTASUN SAILA

Administrazio eta Zerbitzuen Sailordetza
Telekomunikazioak eta Sistema Informatikoak
Kudeatzeko Zuzendaritza

DEPARTAMENTO DE SEGURIDAD

Vice consejería de Administración y Servicios
Dirección de Gestión de Telecomunicaciones y
Sistemas Informáticos

PLIEGO DE PRESCRIPCIONES TÉCNICAS

EVOLUCIÓN Y SOPORTE RED ENBOR SAREA

ÍNDICE

1. ANTECEDENTES Y OBJETO	1
1.1. OBJETO.....	1
2. ALCANCE DEL CONTRATO	2
2.1. ÁMBITO DE RESPONSABILIDAD	4
2.2. ÁMBITO GEOGRÁFICO	5
2.3. GESTIÓN DEL SERVICIO Y CONTROL DE CALIDAD	5
3. SERVICIOS REQUERIDOS	6
3.1. EVOLUCIÓN DE DIMETRA IP A DIMETRA XCORE	6
3.1.1 Trabajos previos	6
3.1.2 Alimentación	6
3.1.3 Trabajos de instalación.....	7
3.1.4 Trabajos de puesta en marcha	7
3.1.5 Arquitectura objetivo	7
3.2. SOPORTE TÉCNICO DE 2º NIVEL	9
3.2.1 Descripción de los servicios de soporte técnico	10
3.2.2 Definiciones del nivel de prioridad y tiempos de respuesta.....	11
3.3. INFORMES DE RENDIMIENTO	13
3.4. PARCHES DE SEGURIDAD	14
3.5. ACTUALIZACIÓN DEL SISTEMA	14
3.6. INTEROPERABILIDAD SISTEMA DIMETRA XCORE CON SISTEMAS BANDA ANCHA	16
3.7. AUDITORÍA Y EVALUACIÓN DE RIESGOS CIBERNÉTICOS	17
3.8. EXPANSIÓN DEL SERVIDOR DCS.....	17
3.9. EXPANSIÓN DEL GRABADOR	18
4. EJECUCIÓN DEL CONTRATO	19
4.1. SUPERVISIÓN DE LA ACTUACIÓN DE LA EMPRESA ADJUDICATARIA.....	19
4.1.1 Responsable de la empresa	19
4.2. PLANIFICACIÓN Y ORGANIZACIÓN DEL SERVICIO.....	19
4.2.1 Inicio del servicio.....	19
4.2.2 Registro y control de actividades.....	19
4.3. NORMATIVAS Y SEGURIDAD	20
5. ANEXO I - INTEROPERABILIDAD CON APLICATIVOS DEL DSGV.....	21
6. ANEXO II - NORMAS DE SEGURIDAD RELATIVAS A LOS SISTEMAS DE INFORMACIÓN	22
6.1. NORMAS BÁSICAS	22
6.2. ACCESO Y PROTECCIÓN DE DATOS	22
6.3. PROPIEDAD INTELECTUAL	23

1. ANTECEDENTES Y OBJETO

El Departamento de Seguridad del Gobierno Vasco (en adelante DSGV) dispone de una red de radiocomunicaciones móviles, *Red ENBOR Sarea*, mediante la cual da servicio a la Policía Autónoma Vasca y otras agencias del Sistema Vasco de Seguridad y Emergencia Pública. Esta red presta todos los servicios de comunicación recogidos en el estándar TETRA: comunicaciones de voz de misión crítica, comunicaciones de datos de baja velocidad, envío y recepción de datos cortos, etc. Además, presta otros servicios de gran valor para las agencias usuarias, tales como grabación de comunicaciones, posicionamiento de flotas, gestión de estados o consulta de datos pertinentes para la operativa de las diversas unidades.

El despliegue de la *Red ENBOR Sarea* se realizó a finales de los años 90 con un número de estaciones bases reducido, entorno a las 30, y se ha ido añadiendo progresivamente nuevas estaciones base para ampliar la cobertura de la red. Actualmente se cuenta con 130 emplazamientos con estaciones base diseminadas por toda la orografía de la Comunidad Autónoma de Euskadi (CAE), extensores de cobertura para túneles de carretera, infraestructuras de metro y edificios singulares. En el año 2014 se renovaron los centros de conmutación de la red y en el año 2015 las estaciones base de los emplazamientos.

La red da servicio a más de 14.000 usuarios finales de las distintas agencias que componen el ámbito de la Seguridad y Emergencias de la CAE. Diseñada con redundancia geográfica del centro de conmutación, actualmente la *Red ENBOR Sarea* dispone de la tecnología DIMETRA IP Scalable D8.1, del fabricante MOTOROLA. Tecnología obsoleta, fuera del soporte oficial del fabricante y finalizada la última prórroga del expediente que se tiene adjudicado para el soporte de 2º nivel de la infraestructura de conmutación.

En el Plan Estratégico de las Tecnologías de la Información y Comunicaciones para la Seguridad Pública de Euskadi para el período comprendido entre los años 2021 y 2024, PETICSEG 21-24, se identifica la necesidad de la evolución tecnológica de la *Red ENBOR Sarea* dentro de su mapa de ruta.

1.1. Objeto

El objeto del presente expediente es la contratación de los servicios necesarios para la evolución tecnológica de la infraestructura de conmutación de red (incluidos los suministros necesarios) y el soporte de 2º nivel de la propia infraestructura.

En este Pliego de Prescripciones Técnicas (PPT) se define el alcance, así como las características generales y particulares y condiciones de ejecución a las que deben ajustarse los servicios para la evolución y soporte solicitados.

2. ALCANCE DEL CONTRATO

La oferta deberá incluir todos los servicios de ingeniería, de garantía de calidad y de soporte necesarios, así como materiales y equipos, para asegurar la correcta ejecución de la evolución tecnológica y correcto funcionamiento posterior de la red.

A modo de referencia, se recogen los principales servicios que el contratista deberá incluir:

Ingeniería

- Análisis de la infraestructura actual, incluyendo ingeniería de emplazamientos.
- Diseño de la solución, con especial atención a la interconexión e integración de los equipos, los sistemas y servicios existentes en la *Red Oficial de Comunicaciones de Seguridad y en las plataformas y aplicaciones del DSGVO*.
- Logística.
- Pre configuración del sistema.
- Plan de migración de los servicios actuales que garantice una mínima interrupción de los servicios prestados a la hora de realizar la evolución.

El proveedor será responsable de que el nuevo sistema sea completamente funcional.

Gestión de proyecto

- Plan global del proyecto con todas las fases y tareas necesarias.
- Recursos y mecanismos de seguimiento y supervisión del proyecto.
- Definición de medidas medioambientales y de prevención de riesgos laborales de aplicación.

Gestión de la seguridad

- Supervisión de los trabajos de instalación y del resto de tareas objeto del pliego.
- Redacción y gestión de plan de seguridad aplicable y coordinación de actividades empresariales.
- Especificación de normas y estándares que cumplen los equipos.

Pruebas de aceptación

- Pruebas de aceptación en fábrica (FAT), con pruebas consensuadas y documento de aceptación.
- Pruebas de la calidad de los materiales suministrados, de la instalación realizada.
- Pruebas de aceptación y del funcionamiento del conjunto del sistema en cliente, con pruebas consensuadas y documento de aceptación.

Soporte de 2º nivel de la infraestructura

- Elaboración de los procedimientos generales de mantenimiento preventivo y correctivo de los equipos.
- Compromiso de facilitar información de las revisiones o mejoras futuras en los sistemas suministrados.

- Compromiso del fabricante que deberá garantizar la no obsolescencia de la tecnología seleccionada, emitiendo un certificado que garantice la disponibilidad del producto durante al menos 10 años desde el momento de su puesta en marcha. Durante este tiempo, deberán estar disponibles los componentes, módulos y equipos seleccionados, o en su defecto componentes compatibles con iguales o mejores características, sin necesidad de modificar los ya instalados.

Formación

El objeto de esta formación es la capacitación técnica del personal del DSGV en el sistema, para la realización de las pruebas de aceptación de equipos y del sistema, y una vez implantado el sistema, para la realización de las tareas de operación, gestión y mantenimiento general.

El curso de formación se impartirá en cualquiera de las dos lenguas oficiales de la CAE en las dependencias que el Gobierno Vasco determine, y se apoyará en documentación técnica y manuales adecuados. El entrenamiento del personal debe contemplar como mínimo los siguientes aspectos:

- Un curso introductorio sobre las características y funcionalidades básicas de la nueva infraestructura en general y de los equipos en particular.
- Cursos de formación del personal de gestión de infraestructura del DSGV.
- Cursos de formación del personal de mantenimiento del DSGV.

Documentación

La documentación técnica a entregar tras la finalización de los trabajos de instalación deberá estar en cualquiera de las dos lenguas oficiales de la CAE e incluir como mínimo los siguientes datos:

1. *Proyecto técnico* descriptivo del sistema, donde se incluya la ingeniería de diseño del sistema global, con detalle de la integración de todo el equipamiento con el resto de los sistemas.
2. *Manuales técnicos de los equipos*, que contendrán la siguiente información:
 - Descripción general de los equipos, indicando dimensiones, peso, características mecánicas, de composición, de montaje, de consumo y disipación, instalación y conexionado.
 - Descripción de los elementos que los componen, con los esquemáticos completos y descripción de la interacción entre los diversos bloques.
 - Relación de los componentes de los distintos equipos con indicación de los datos necesarios para posteriores peticiones de repuestos.
 - Texto de explotación, con los procedimientos a seguir para la realización de los pertinentes ajustes, revisiones y mantenimiento de los equipos. Se incluirán normas precisas de mantenimiento, interpretación de errores más frecuentes y método de resolución. Se dará la relación de averías más frecuentes y normas para su reparación.
3. *Protocolos de pruebas, con los resultados de las pruebas realizadas.*

Esta documentación es extensiva a todas las pruebas realizadas: aceptación en fábrica, en maqueta previa a la instalación; y para el conjunto de la infraestructura ya instalada en cliente, incluido sistema de gestión.

4. *Manuales de instrucciones* del equipamiento.
5. *Cartografías de instalación*. Un documento por cada instalación realizada donde se incluirán:
 - Disposición relativa, plano en planta de los equipos, planos de cableado y esquemas de conexiones entre los diferentes equipos.
 - Además de los esquemas eléctricos propiamente dichos, se proporcionarán fotografías y planos con la identificación y la situación de los elementos del equipo, para su rápida y precisa localización. También se incluirán fotografías del aspecto exterior del mismo.
 - Inventario de los equipos, con la información y formato que determine el DSGV.
 - Tipo y características de los cables empleados, longitud de éstos, identificativos asignados.
 - Licencias de software: número de serie, clave de activación, nombre del usuario, número de usuarios autorizados, código de autorización, etc.
 - Configuración actualizada de los parámetros.

En todo caso, la oferta deberá incluir detalle de todos los entregables de documentación técnica que se generen en el proyecto.

2.1. **Ámbito de responsabilidad**

El ámbito de actuación de los servicios se extiende a los sistemas que se integrarán en la nueva infraestructura y su posterior soporte, generándose una serie de responsabilidades, por parte de la empresa adjudicataria, entre las que se encuentran:

- Disponibilidad 24x7, 365 días al año, para responder a incidentes y solicitudes del DSGV sobre la infraestructura.
- Coordinación con proveedores externos acordados para resolución de incidentes y problemas técnicos.
- Publicar actualizaciones de seguridad periódicas probadas y verificadas.
- Completar una actualización global de la infraestructura durante el periodo de vigencia del contrato.
- Entrega de documentación actualizada por cambios o actualizaciones.
- Realizar estudios anteriores a cualquier modificación que pueda afectar a los servicios y pruebas de aceptación para comprobar su correcto funcionamiento.

2.2. Ámbito geográfico

El ámbito de cobertura del servicio será la CAE. Los trabajos se realizarán principalmente en las dependencias del DSGV en Erandio y Gasteiz, pudiéndose realizar trabajos en cualquiera de los edificios o emplazamientos en los que disponga el DSGV de equipos relacionados con el objeto del expediente, si así se requiere.

2.3. Gestión del servicio y Control de calidad

El adjudicatario será responsable del control para la correcta ejecución de todos los trabajos consecuencia del objeto del contrato, siempre de acuerdo a los requisitos y pautas establecidos por los técnicos del DSGV.

Los principales trabajos de gestión y control que el contratista deberá incluir son:

Gestión de los trabajos:

- Seguimiento del avance en la ejecución de tareas, elaboración de los informes y documentaciones solicitadas y mantenimiento de reuniones periódicas para informar del avance de las mismas y resolución de problemas que puedan acontecer.

Control de la calidad:

- Supervisión del cumplimiento de los trabajos solicitados.
- Realización de informes sobre el nivel de cumplimiento de los trabajos realizados para garantizar la calidad de los mismos.

La información proporcionada se corresponderá como mínimo con los parámetros de interés que se fijen para el DSGV.

3. SERVICIOS REQUERIDOS

3.1. Evolución de DIMETRA IP a DIMETRA XCORE

El objetivo del servicio requerido es la evolución de los centros de conmutación de la red y los subsistemas relacionados a la versión 9.2, denominada comercialmente XCORE.

En ningún momento la calidad de los servicios que presta el Departamento de Seguridad pueden verse degradados después de la instalación del nuevo sistema Dimetra Xcore.

En el caso de necesidad de suministros para la evolución objeto del presente expediente se realizará en las instalaciones del DSGV a las que vaya destinado el material, principalmente en las instalaciones de Erandio y Vitoria-Gasteiz. La empresa adjudicataria correrá con los gastos del transporte del suministro a cada una de las ubicaciones, responsabilizándose de los posibles daños que pudieran producirse. El DSGV proveerá la infraestructura asociada para la instalación: sistemas de alimentación, cuartos técnicos, etc. La titularidad de los equipos anteriormente mencionados será del Departamento de Seguridad desde el momento de la instalación en las dependencias del mismo.

La empresa adjudicataria será la responsable de la correcta instalación y del buen funcionamiento, de acuerdo a las normas y recomendaciones de los organismos competentes aplicables y a los requerimientos específicos del presente pliego. Asimismo, deberá asegurar la correcta integración de sus equipos con los actualmente instalados.

Los trabajos de instalación, retirada y adaptación del equipamiento se realizarán con mínima interferencia sobre los servicios de telecomunicaciones activos, previa coordinación con la persona responsable por parte del DSGV y minimizando los cortes y afecciones a servicios en la migración a los nuevos equipos.

Tras las tareas de instalación se procederá a la limpieza de los locales, dejando estos como mínimo en las mismas condiciones de limpieza en las que se encontraron.

3.1.1 Trabajos previos

De forma previa al comienzo de los trabajos de suministro e instalación, la empresa adjudicataria deberá realizar trabajos de ingeniería correspondientes a cada una de las ubicaciones consideradas en el presente expediente.

Es obligatoria la realización de un replanteo previo de todas las instalaciones a realizar en los centros, en los que se tendrán en cuenta: adecuaciones requeridas para ubicar los nuevos equipos, definición de áreas y armarios para la instalación de los equipos, comprobación de suministros de energía, cumplimiento de condiciones de seguridad, etc.

Los suministros e instalaciones se realizarán según lo indicado en el presente pliego de prescripciones técnicas y en el replanteo previo.

3.1.2 Alimentación

Como norma general, la empresa adjudicataria deberá respetar el tipo de energía eléctrica existente en el centro y suministrar, en caso de ser necesario, los sistemas de alimentación y protección eléctrica que se requieran para asegurar una adecuada alimentación de los equipos.

Siempre que sea posible, el suministro energético de los equipos se realizará a través de los cuadros de alimentación de uso exclusivo para sistemas de comunicaciones existentes en las

ubicaciones. Se adecuará la instalación eléctrica a los nuevos equipos con el suministro e instalación de las protecciones eléctricas requeridas en los bastidores destinados a albergar los nuevos equipos. Todo el cableado de alimentación deberá ser convenientemente rotulado y etiquetado.

La alimentación de referencia será la de 230VAC.

3.1.3 Trabajos de instalación

Los equipos se instalarán de acuerdo al replanteo que se realice para cada instalación. De manera general, la instalación de los equipos se realizará respetando las siguientes normas:

- Todos los equipos deberán estar convenientemente identificados en el armario donde vayan alojados.
- Todos los equipos y bastidores deberán estar conectados a tierra. Se dotará a cada equipo de la adecuada estructura para sujeción de los bastidores.
- Se desinstalará y retirará los equipos sustituidos, además de aquellos que queden en desuso a causa del proyecto, de acuerdo con las instrucciones de la persona responsable por parte del DSGV.
- Los cables de interconexión y latiguillos incluidos en el suministro deberán ser los adecuados a los protocolos e interfaces de los equipos a conectar y vendrán provistos de los conectores adecuados.

3.1.4 Trabajos de puesta en marcha

Todos los equipos ofertados deberán ser correctamente configurados de acuerdo con los objetivos del proyecto y acorde con la arquitectura de red actual y prevista.

El contrato incluye la puesta en marcha de la nueva infraestructura de conmutación, así como la continuidad en el funcionamiento de los subsistemas y aplicaciones asociados a la operativa de dicha infraestructura (terminales de radio móvil, estaciones base y puestos de operador de despacho TETRAKOM), quedando excluidos los sistemas, equipos y aplicaciones externos al sistema Dimetra Xcore.

No obstante, la empresa adjudicataria deberá comprometerse a la colaboración máxima posible con el responsable del DSGV para la continuidad de la interoperabilidad de los aplicativos propietarios del DSGV con el sistema DIMETRA XCORE, con las mismas funcionalidades que con la versión DIMETRA 8.1.

Para ello, el DSGV facilitará toda la información requerida por la empresa adjudicataria para poder colaborar con las soluciones que el DSGV necesite realizar por sus propios medios para la continuidad de las funcionalidades definidas y anexadas al presente documento.

3.1.5 Arquitectura objetivo

El sistema TETRA de la *Red ENBOR Sarea* del DSGV está basado en dos zonas redundadas geográficamente operando actualmente bajo la versión DIMETRA IP Scalable D8.1 y que contienen los siguientes elementos y subsistemas:

- Primary Zone Server (ZC, UIS, CSMS - zone1) – Servidores de comunicaciones del sistema

- Secondary Zone Server (ZC, UIS) – Servidores de comunicaciones del sistema redundantes
- Primary Management Server (ZDS, UEM, ATR, ZSS, CADI, UCS - zone1, EAuC - zone1, SSS - zone1) – Servidores de gestión del sistema
- Secondary Management Server (ZDS, UEM, ATR, ZSS, CADI, UCS - zone1, EAuC - zone1) – Servidores de gestión del sistema redundantes
- Primary Data Server (Packet Data, Short Data - zone 1) y GGSN - zone 1 – Servidores de datos del sistema
- Secondary Data Server (Packet Data, Short Data - zone 1) y GGSN - zone 1 – Servidores de datos del sistema redundantes
- MTIG IP (zone 1) – Sistema de interconexión con la red telefónica departamental
- Equipamiento de red (Firewalls, routers, switches) configurado ad-hoc para los Servicios de voz y datos específicos del DSGV
- NTS redundante (zone 1) – Servidor de tiempos para sincronización del sistema
- Subsistema de grabación basado en la solución NICE logger – Nice Inform Lite
- Subsistema DCS (Dispatch Console System) – proporciona servicio a las consolas de despacho
- CCGW - zone 1 – Equipo para interconexión con redes externas
- TRACES - zone 2 – Análisis en tiempo real de cobertura – enlace ascendente todas estaciones base (100 por zona)
- Clientes de gestión de red (NMTs) locales. Se configurará la red para que se pueda acceder a cualquier elemento de networking tanto de la infraestructura Xcore como de los subsistemas (como el subsistema DCS) desde cualquier NMT.
- Salas de control remotas con consolas MCC7500/MCC7500C y cliente de gestión de red (NMTs).

Las licencias asociadas a los diferentes servicios de voz, datos y gestión de la red de que dispone el sistema actual DIPS 8.1 son las siguientes:

Funcionalidad	Activo	Licencias Z1	Licencias Z2	Total Licencias
Digital Operation	Sí	Activo	Activo	
Radio Control Manager Capability	Sí	Activo	Activo	
Dynamic Regrouping Capability	Sí	Activo	Activo	
Security Partitioning Capability	Sí	Activo	Activo	
Computer Aided Dispatch Interface	Sí	Activo	Activo	
Zone Watch Capability	Sí	Activo	Activo	
Radio Control Manager Users	Sí	Activo	Activo	
Dynamic Regrouping Users	Sí	Activo	Activo	
Status Message User	Sí	Activo	Activo	
Air Traffic Information Access	Sí	Activo	Activo	
System ATIA Packages	Sí	Activo	Activo	
Security Partitioning	Sí	Activo	Activo	
ZoneWatch Users	Sí	Activo	Activo	
Affiliation Display Users	Sí	Activo	Activo	
Dynamic Shared Service	Sí	Activo	Activo	

Computer Aided Dispatch Interface	Sí	Activo	Activo	
UEM Server NBI API	Sí	Activo	Activo	
UEM ClusterWide NBI	Sí	Activo	Activo	
1000 Radio User	Sí	Activo	Activo	16
Radio Control Manager Users	Sí	5	5	10
ZoneWatch Users	Sí	3	3	6
Dynamic Reports Users	Sí	3	3	6
Affiliation Display Users	Sí	3	3	6
Computer Aided Dispatch Interface	Sí	1	1	2
4 Sites	Sí	25	25	50
Zone Configuration Management Users	Sí	3	3	6
Historical Reports Users	Sí	3	3	6
Vortex Voice Logging Group Call	Sí	6	0	6
Vortex Voice Logging Private Call	Sí	6	0	6
10 TELEPHONE INTERCON CALLS	Sí	6	0	6
Ethernet Site Link	Sí	100	100	200
1 Console	Sí	5	0	5
1 Dispatch Communications Server Platform	Sí	5	5	10
1 Dispatch Communications Server Application	Sí	45	45	90

La funcionalidad de todos los servicios proporcionados por esta infraestructura, así como el número de licencias asociadas a sus diferentes servicios deberá, como mínimo, mantenerse al actualizar el sistema DIPS 8.1 a la nueva versión, pudiendo no obstante incorporarse nuevos servicios adicionales que puedan coexistir con los actualmente existentes y/o un aumento de las licencias de uso de los mismos.

El sistema del DSGV, una vez migrado a la arquitectura DIMETRA X Core, continuará basado en dos zonas redundadas geográficamente operando bajo la versión D9.2.

A su vez, los identificativos de personas usuarias (con sus correspondientes claves) del sistema y de los diferentes subsistemas (NICE, TETRAKOM y demás subsistemas) deberán ser migrados al nuevo XCORE sin que se produzca perjuicio para las personas usuarias finales ni para las personas administradoras del mismo y sin necesidad de volver a generar usuarios ni claves en ellos. Se ejecutará una carga masiva de Identificativo/clave.

3.2. Soporte técnico de 2º nivel

Se solicita grupo de soporte técnico para brindar un servicio de asistencia mediante consultas telefónicas ante problemas técnicos que requieran un alto nivel de conocimiento y capacidad de resolución de problemas específicos de la red DIMETRA.

Este soporte técnico remoto se ejecutará en las dependencias de la empresa adjudicataria, mediante un equipo de personas con perfil de ingeniería de soporte técnico especializadas

en el diagnóstico y la resolución rápida de problemas operativos y de rendimiento de la infraestructura.

También se solicita un grupo de soporte de operaciones en campo, que posea un conocimiento específico del sistema del DSGV, lo que agrega la capacidad adicional para la investigación y resolución de los problemas. El DSGV, a través de la persona responsable del contrato, podrá solicitar la presencia de una persona o varias del grupo en sus instalaciones para realizar tareas de mantenimiento tales como:

- Instalación de un parche de software
- Configuración avanzada de un elemento de red o un servidor
- Toma compleja de logs.

3.2.1 Descripción de los servicios de soporte técnico

El objetivo principal de los grupos de soporte (de asistencia remota y de operaciones en campo) deberá ser la resolución de problemas del DSGV y el cumplimiento de solicitudes de servicio en la infraestructura actualmente admitida del fabricante. Este equipo de personas especialistas altamente calificadas, conocedores y experimentadas deberá estar disponible para el DSGV como parte integral del proceso de soporte y resolución de problemas técnicos.

Los grupos de soporte que brinden soporte remoto al cliente y deberán trabajar con, entre otros, herramientas de diagnóstico de fallos, redes de simulación y motores de búsqueda de bases de datos de fallos.

Es posible que las personas del grupo de soporte remoto necesiten conectarse de forma remota y acceder a elementos de todo el sistema y de subconjuntos del sistema. El permiso para dicho acceso remoto no se denegará injustificadamente. La interpretación en línea de estos elementos por parte de los ingenieros especialistas se utilizará únicamente para analizar fallos y ejecutar programas de optimización del sistema.

Después de un incidente informado, donde se proporciona acceso remoto, el grupo de soporte restaurará la funcionalidad del sistema.

Si no se puede establecer o entregar una conexión remota, el DSGV proporcionará registros del sistema, definidos por el grupo de soporte, para permitir que el grupo técnico del soporte ayude con una solución para la rehabilitación in situ.

Las llamadas que requieran restauración de incidentes o solicitudes de servicio se registrarán en el sistema de gestión de relaciones con el cliente (CRM) de la empresa adjudicataria. Esto ayuda a garantizar que los problemas técnicos se prioricen, actualicen, rastreen y escalen según sea necesario. Se asignan el nivel de prioridad de acuerdo con las Definiciones de Nivel de Prioridad indicado en este pliego.

La empresa adjudicataria seguirá el progreso de cada caso desde la captura inicial hasta la resolución. La empresa adjudicataria asesorará e informará al DSGV sobre el progreso del caso y las tareas que requieran mayor investigación y asistencia de los recursos técnicos del DSGV.

3.2.2 Definiciones del nivel de prioridad y tiempos de respuesta

Las siguientes definiciones se utilizarán para determinar los tiempos de respuesta máximos:

PRIORIDAD	DEFINICIÓN DEL INCIDENTE
P1 CRÍTICO	Núcleo: fallo del servidor central o del vínculo principal. No hay servidor o enlace redundante disponible. Sitios: más del 10 % de los sitios de RF caídos. Consolas: Más del 40 % de las posiciones de la consola de un sitio están inoperativos. DCS: Más del 40 % de los DCS de un sitio están inactivos (no brindan servicio al 40 % de los clientes de DCS). MTIG: Servidor virtual o error de enlace IP. No hay servidor o enlace redundante disponible. Canales convencionales: Puertas de enlace de canales convencionales (CCGW) inactivas sin puertas de enlace redundantes disponibles. Funciones de seguridad: la seguridad no funciona o está degradada. Por ejemplo, ataques DDoS en los firewalls, el servidor de administración antivirus no está disponible, los firewalls no están disponibles sin servidores o firewalls redundantes, o Crypter no está disponible.
P2 ALTO	Núcleo servidor central o fallos de enlace. Servidor redundante o enlace disponible. Sitios: hasta el 10 % de los sitios de RF inactivos. Consolas: Entre el 20 % y el 40 % de las posiciones de la consola de un sitio están hacia abajo. DCS: entre el 20 % y el 40 % de los DCS de un sitio están inactivos (no brindan servicio a entre el 20 % y el 40 % de los clientes de DCS). MTIG: Servidor virtual o error de enlace IP. Servidor redundante o enlace disponible. Canales Convencionales: Hasta 50% de CCGWs caídos. Puertas de enlace redundantes disponibles. Funciones de seguridad: cortafuegos, uno o más clientes antivirus no disponibles, servidor RSA no disponible o servidor AuC no disponible. Firewalls o servidores redundantes disponibles. Elementos de red: el router o el switch del emplazamiento están desactivados. No hay ningún elemento de red redundante disponible. Edge Gateway: pérdida de un sitio de Edge Gateway NICE Voice Logging: servidor de registro, AIS, servidor de información o servidor de copia de seguridad inactivos. No hay servidor redundante disponible

P3 MEDIO	Consolas: Hasta el 20 % de las posiciones de la consola de un sitio están inactivas. DCS: Hasta el 20 % de los clientes DCS de un sitio están inactivos (no brindan servicio hasta al 20 % de los clientes DCS). Canales Convencionales: Canal único caído. Puerta de enlace redundante disponible. Elementos de red: el router o el switch de un emplazamiento están inactivos. Elemento de red redundante disponible. NICE Voice Logging : servidor de registro, AIS, servidor de información o servidor de copia de seguridad inactivo. Servidor redundante disponible NTS : pérdida de NTS, pérdida de GPS en un MSO o sitio de estación base.
P4 BAJO	Solicitud de información: Análisis de la causa raíz de un fallo recuperada, asistencia con el mantenimiento planificado o de rutina, actualizaciones de un sistema, fallos cosméticos o fallos intermitentes que ocurren con poca frecuencia y que afectan los servicios principales.

Los tiempos de respuesta son los siguientes:

PRIORIDAD DEL INCIDENTE	TIEMPO DE RESPUESTA DEL INCIDENTE
CRÍTICO P1	Respuesta las 24 horas del día, los 7 días de la semana, hasta la restauración del servicio. El recurso técnico reconocerá el incidente y responderá dentro de los 30 minutos posteriores al registro del incidente en CCSD.
P2 ALTA	Respuesta las 24 horas del día, los 7 días de la semana, hasta la restauración del servicio. El recurso técnico reconocerá el incidente y responderá dentro de 1 hora del incidente de registro de CCSD.
MEDIO P3	Respuesta durante el horario comercial normal hasta la restauración del servicio. El recurso técnico reconocerá el incidente y responderá dentro de las 4 horas posteriores al registro del incidente en CCSD.

BAJO P4	Respuesta durante el horario comercial normal. La empresa adjudicataria reconocerá y responderá dentro de los 7 días hábiles.
----------------	--

Si se requieren visitas in situ de emergencia para resolver problemas técnicos que no se pueden resolver remotamente, la empresa adjudicataria enviará un miembro del grupo de soporte a la mayor brevedad posible.

Para incidentes no críticos, problemas o consultas se determinarán formas de contacto, preferiblemente dirección de email y/o teléfono, para que se dirijan al personal del soporte de trabajos en campo.

3.3. Informes de rendimiento

Es responsabilidad de la empresa adjudicataria la recopilación y conservación de toda la información necesaria para la generación de los informes de rendimiento detallados más adelante en este apartado.

Los servicios solicitados para la generación de informes de rendimiento engloban los suministros e instalaciones de aplicativos, en caso de ser necesarios, para la generación de los mismos, que cuentan por parte de la empresa adjudicataria.

Con carácter trimestral, la empresa adjudicataria analizará los datos recabados y generará los informes en formato digital. Se programará una reunión, telemática o presencial, lo más pronto posible para que se expongan las conclusiones del informe generado, siempre con la finalidad de recomendar mejoras del uso del equipamiento.

DATOS DEL INFORME:

La siguiente lista resume las secciones del informe estándar de gestión de rendimiento:

- Resumen del informe
- Resumen de rendimiento y utilización de zona (descripción general y análisis de tendencias)
- Estadísticas de zona de las 5 horas pico más importantes
- Resumen de estadísticas de a nivel de zona (sitios por llamada, llamadas de zona, PTT de zona, zona ocupada y rechazo de zona)
- Utilización de zona
- Resumen de estadísticas a nivel de emplazamiento RF (llamadas, ocupados y rechazos)
- Resumen de disponibilidad (tiempo de inactividad del sitio y tiempo de inactividad del radio base)
- Apéndice A: lista de sitios monitoreados
- Apéndice B: Disponibilidad. Desglose detallado de eventos (tiempo de inactividad del sitio, tiempo de inactividad de la radio base, tiempo de inactividad de los componentes del sitio, tiempo de inactividad de los componentes de la radio base y tiempo de inactividad de los grupos de dispositivos).

3.4. Parches de seguridad

Se solicita un servicio de actualización de seguridad que proporcione actualizaciones de seguridad probadas previamente, para minimizar el riesgo cibernético y los impactos generados sobre el rendimiento del software. Estas actualizaciones de seguridad deberán contener parches de seguridad del sistema operativo y definiciones de antivirus cuya compatibilidad y estabilidad con los sistemas DIMETRA se han validado exhaustivamente en los laboratorios de la empresa adjudicataria.

El DSGV descargará e instalará estas actualizaciones de seguridad.

En caso de necesidad se podrá acordar con la empresa adjudicataria que las actualizaciones de seguridad de los sistemas operativos sean realizadas por el grupo de soporte de campo, siempre que se requiera con una antelación acordada.

La cadencia de la publicación de actualizaciones por parte de la empresa adjudicataria deberá ser en los tiempos reflejados en la siguiente tabla:

SOFTWARE	CADENCIA
Archivos de definición de ESET Antivirus	Semanal
Microsoft Windows	Mensual
Microsoft Windows de terceros (Adobe Reader)	Mensual
Red Hat Linux (RHEL)	Trimestralmente

La empresa adjudicataria:

- Publicará actualizaciones de seguridad probadas y verificadas en un sitio web seguro
- Publicará la documentación para la instalación, los cambios de configuración recomendados, cualquier problema identificado e instrucciones de corrección para cada versión de actualización de seguridad
- Enviará notificaciones por correo electrónico cuando las actualizaciones de seguridad estén disponibles para descargar desde el sitio web seguro.

Es responsabilidad del DSGV:

- Analizar las recomendaciones e instrucciones para la instalación de los parches de seguridad y a su implantación, cuando sea necesario para continuar con el servicio.
- Cumplir con los términos de los acuerdos de licencia aplicables entre el DSGV y los propietarios de los derechos de autor del software que no sean de la empresa adjudicataria.

3.5. Actualización del sistema

Cuando se vaya a finalizar el contrato, en su último año de ejecución, se procederá, por parte de la empresa adjudicataria, a la actualización del sistema a la última versión oficial del sistema DIMETRA, con la finalidad de mejorar la funcionalidad, la seguridad y el funcionamiento del sistema con respecto a las versiones anteriores.

Como parte de la actualización se realizará la actualización de la versión inicial del software del sistema y cualquier actualización posterior llevará el software y el hardware del sistema del DSGV (incluidos los repuestos críticos del cliente) a la versión de envío más reciente.

El software del sistema DIMETRA cubre los siguientes productos:

- Estaciones base
- Controladores de sitio
- Routers
- Switches
- Servidores
- Soluciones de consolas de despacho
- Edge Gateways
- Terminales de gestión (NMT)
- Productos de administración de fallos de red
- Dispositivos de seguridad de red; cortafuegos, sensores de detección de intrusos
- Equipo de registro - AIS
- NICE Logging Solutions
- Software Aries
- Aplicación Tetrakom (90 licencias).

Los siguientes componentes de hardware, si los proporcionó originalmente la empresa adjudicataria, son elegibles para el reemplazo completo del producto cuando sea necesario según la actualización de la versión del software del sistema:

- Servidores
- Ordenadores
- Routers
- Switches LAN
- Consolas de despacho
- Componentes de Estaciones base MTS que puedan requerir reemplazo por obsolescencia.
- Logging Equipment - AIS
- NICE Logging Solutions.

Las actualizaciones del sistema DIMETRA incluyen el reemplazo del hardware de terceros proporcionado por la empresa adjudicataria, cuando el hardware especificado ya no está certificado por la versión de software del sistema en la versión de envío actual. El hardware se reemplazará para mantener las funciones y funciones existentes en el momento de la actualización del sistema.

La empresa adjudicataria proporcionará los servicios de implementación necesarios para actualizar el sistema a una versión futura con un nivel de funcionalidad equivalente y proporcionará el diseño de software y los recursos técnicos necesarios para completar las actualizaciones de la versión del software del sistema.

La empresa adjudicataria deberá:

- Obtener y revisar los datos de auditoría del sistema de infraestructura según sea necesario.

- Identificar el equipo del sistema adicional necesario para implementar una versión del sistema, si corresponde.
- Completar un plan de actualización que defina la versión del sistema, los requisitos del equipo, el plan de instalación y el impacto para los usuarios del sistema.
- Informar sobre el impacto probable en los usuarios del sistema durante la implementación de la actualización de campo real.
- Realizar un plan de instalación/calendario de impacto.
- Entregar de documentación de la nueva versión del sistema (Releases Notes).
- Certificar que se hayan completado las copias de seguridad del sistema correspondientes.
- Certificar que se haya reemplazado todo el hardware obligatorio.
- Realizar la prueba de aceptación de implementación posterior a la actualización.

Para dar por finalizado este servicio se deberá contar con la aprobación de la finalización de la actualización del software del sistema por parte de la persona responsable del DSGV.

3.6. Interoperabilidad sistema DIMETRA XCORE con sistemas banda ancha

Se solicita un servicio que permita el intercambio de información, voz, datos y vídeo entre redes, aplicaciones y las distintas agencias que intervienen en el seguridad y emergencia dependientes del DSGV. Este interfaz/plataforma deberá ser único y seguro.

Las capacidades del servicio deberán ser como mínimo:

- Llamada de grupo: Los grupos de conversación y los participantes asignados son creados y administrados por la herramienta de administración de la plataforma de interoperabilidad.
- Llamada privada individual: llamadas privadas entre dos usuarios. Un usuario selecciona a la persona a la que desea llamar de una lista de contactos disponible dentro de la aplicación y puede comunicarse con solo presionar un botón.
- Mensajes de texto: envío y recepción de mensajes de texto grupales con otros usuarios en un grupo de conversación.
- Uso compartido multimedia: compartición de imágenes o videos desde la galería o directamente desde la cámara. Los usuarios pueden compartir con otros usuarios o un grupo, y pueden ver los videos y fotos recibidos, reproducirlos o guardarlos en su dispositivo.
- Ubicación: muestra la ubicación de los miembros del grupo en un mapa.
- Mensaje de voz pregrabado o grabar y enviar: permite grabar un mensaje que los usuarios pueden enviar a un grupo o a un contacto. Los usuarios pueden reproducir los mensajes de voz en cualquier momento.
- Historial persistente en el cliente: historial de mensajes de texto y eventos de PTT para llamadas grupales o privadas, incluso si cierran sesión y vuelven a iniciar sesión. Los eventos que ocurren mientras los usuarios están desconectados se enviarán al cliente para su captura.
- PTT desde la pantalla de bloqueo: los usuarios pueden pulsar PTT desde la pantalla de bloqueo de un dispositivo sin tener que desbloquear el dispositivo o pasar por la aplicación.

- Integraciones de auriculares: se pueden usar auriculares con cable o Bluetooth para responder con manos libres en cualquier situación.

La solución propuesta deberá ofrecer la funcionalidad “Push to Talk over Cellular” integrada con la red de comunicaciones móviles digitales (TETRA). Así mismo, deberá incluir todos los dispositivos necesarios para la interconexión a “nivel de Core” de la red y los datos deberán estar protegidos extremo a extremo.

Los usuarios podrán estar vinculados tanto a una red de banda ancha comercial como privada.

3.7. Auditoría y evaluación de riesgos cibernéticos

El Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información, en su artículo 16 dice que: “Los Operadores de Servicios Esenciales y los Proveedores de Servicios Digitales deberán adoptar medidas técnicas y de organización, adecuadas y proporcionadas, para gestionar los riesgos que se planteen para la seguridad de las redes y sistemas de información utilizados en la prestación de los servicios sujetos a este real decreto-ley”.

La *Red ENBOR Sarea* es servicio esencial para las comunicaciones críticas en el ámbito de la Seguridad y Emergencia de la CAE. Por ello, se solicita un servicio de auditoría ante los riesgos cibernéticos que sufre la red de comunicaciones críticas del DSGV.

Mediante una evaluación de riesgos cibernéticos se pretende tener una imagen actualizada de las políticas de seguridad que se ejecutan actualmente en el DSGV para la *Red ENBOR Sarea*, la idoneidad de las mismas, definir los riesgos a los que está expuesta la red y poder tener unas pautas de mejora para minimizar los riesgos existentes.

Para ello se solicita:

- Revisión de configuraciones de los equipos de red
- Análisis de configuraciones de autenticación y registro de logs.
- Identificación de brechas de seguridad.
- Propuesta de mejoras

Este servicio se verá culminado con un informe al final de la evaluación en el que se reflejarán las incidencias detectadas durante la evaluación y las propuestas para minimizar los riesgos.

Durante la ejecución del contrato se contempla la realización de dos evaluaciones de riesgos cibernéticos. Una a mitad de ejecución y otra al final.

3.8. Expansión del servidor DCS

Se solicita un servicio para expandir a la máxima capacidad los servidores DCS del DSGV. Estos servidores dan servicio a las consolas de despacho TETRA de los puestos comunicaciones avanzados que permiten tareas de comunicación y coordinación de las

comunicaciones mucho más complejas que las que se pueden realizar con los terminales radio de un usuario final.

Las características funcionales de los usuarios de consolas del DSGV requieren que estos puestos se usen de manera concurrente con otras aplicaciones de coordinación y gestión de incidencias, por lo que deben ejecutarse desde puestos de usuario departamentales. Por ello el DSGV dispone de un subsistema de consolas basado en el producto de Motorola DCS (Dispatch Console System), que proporciona funciones avanzadas de acceso a las comunicaciones de la red TETRA a través de APIs.

La infraestructura actual del servicio DCS consta de dos ecosistemas, cada uno de los cuales cuenta con capacidad para hasta 50 puestos de operador simultáneos, lo que proporciona un máximo de 100 puestos de operador de comunicaciones avanzado concurrentes, aunque actualmente hay disponibles 90 licencias de uso.

3.9. Expansión del grabador

Parte de la gran cantidad de grupos de comunicaciones críticas de la *Red ENBOR Sarea* se graban y posteriormente se pueden gestionar con el subsistema de grabación. La escucha de grabaciones y administración de usuarios y auditorías de acceso a las mismas se realizan desde equipos departamentales que tengan acceso http a las Inform replay stations y credenciales de acceso a la aplicación Inform Lite.

El subsistema de grabación contempla varios tipos de dimensionamiento. Por un lado, el número total de grupos de llamada y usuarios individuales que pueden ser grabados a través de cada AIS. Por otro lado, el número de llamadas concurrentes que puede grabar cada logger. Por último, el número de usuarios de Inform Lite que pueden estar utilizando la reconstrucción de comunicaciones de manera simultánea.

Número total actual de licencias de uso de grupos de llamada e individuales por AIS:

AIS	Total Grupos llamada	Total individuales
AIS 1 (Erandio)	256	3000
AIS 2 (Gasteiz)	256	3000

Número de grabaciones concurrentes por logger:

Logger	Licencias contratadas	Licencias soportadas
Logger 1 (Erandio)	30	120
Logger 2 (Gasteiz)	30	120

Licencias uso Inform Lite:

Replay Station	Usuarios simultáneos
Erandio	5
Gasteiz	5

Se solicita un servicio de expanda la capacidad del subsistema de grabación.

4. EJECUCIÓN DEL CONTRATO

La empresa adjudicataria será responsable del correcto desarrollo de los trabajos y proyectos relacionados, de acuerdo a los requerimientos del presente pliego.

4.1. Supervisión de la actuación de la empresa adjudicataria.

La actuación de la empresa adjudicataria será supervisada por una persona del DSGV responsable del contrato, a su vez la empresa adjudicataria designará un responsable de contrato de la empresa.

La persona responsable de la empresa adjudicataria y la del DSGV mantendrán reuniones periódicas para revisar la situación y desarrollo de los servicios.

La empresa adjudicataria deberá proporcionar la información requerida por el DSGV para conocer la situación y desarrollo de las actividades solicitadas.

Las discrepancias sobre el desarrollo de los servicios serán resueltas al nivel más elevado de representación

El incumplimiento por parte de la empresa adjudicataria de lo establecido en el presente Pliego de Prescripciones Técnicas y cuando dicho incumplimiento sea reiterativo o se refiera a órdenes que le hayan sido impartidas por escrito y advirtiéndole que son esenciales para el buen fin del contrato, se considerará causa de resolución del mismo.

4.1.1 Responsable de la empresa

La empresa adjudicataria designará un responsable que se encargará de la relación profesional entre la empresa adjudicataria y el DSGV, y de supervisar el correcto desarrollo del contrato.

Dicha figura se encargará también de comunicar al personal que vaya a prestar servicios para el DSGV, las Normas generales de Seguridad y Salud para contratas y subcontratas, así como de certificar que dicho personal ha recibido y conoce dicho documento y que se compromete a cumplir y a hacer cumplir a su personal la normativa de seguridad y salud vigente durante el tiempo de ejecución del contrato.

4.2. Planificación y organización del servicio

4.2.1 Inicio del servicio

Como primera actividad asociada al contrato se establecerá una reunión de “lanzamiento del servicio” entre la empresa adjudicataria y el DSGV, en el cual se identificarán los interlocutores de ambas partes.

En esta reunión además se definirán el resto de condiciones que afectan a la ejecución del servicio, si existiesen, y se establecerán los procedimientos de trabajo a ejecutar, en base a la propuesta presentada, que deberán ser aprobados por el DSGV.

4.2.2 Registro y control de actividades

Los trabajos se realizarán con el alcance y objetivos que determine el personal del DSGV.

Como parte del contrato, la empresa adjudicataria estará obligado a dar total cumplimiento a las condiciones que al efecto de seguimiento y control de actividades establezca el DSGV u organismos por él designados.

Así mismo, la empresa adjudicataria se compromete a rellenar convenientemente los registros que a efectos de control de presencia disponga el DSGV en sus instalaciones.

4.3. Normativas y seguridad

Normas técnicas

La empresa adjudicataria estará obligado a conocer las normativas técnicas vigentes y de uso común en los sistemas informáticos y de telecomunicaciones, necesarias para la correcta ejecución de las tareas que les sean solicitadas.

Asimismo, elaborará sus estudios técnicos e informes de acuerdo con dichas normativas técnicas, la legislación aplicable y los requerimientos específicos solicitados por el DSGV en cada caso, asegurando su cumplimiento.

Normas de seguridad relativas a los sistemas de información

La empresa adjudicataria se compromete a cumplir las normas respecto a los sistemas de información del DSGV recogidas en el anexo del presente documento: “Normas de seguridad relativas a los sistemas de información”.

5. ANEXO I - INTEROPERABILIDAD CON APLICATIVOS DEL DSGV

La infraestructura TETRA actualmente en servicio en el DSGV dispone de una serie de interfaces software (APIs) para que los sistemas informáticos departamentales puedan acceder a los servicios de voz y datos de la red TETRA e incorporar sus funcionalidades en los sistemas de información propios.

En la actualidad el DSGV está utilizando algunos de estos interfaces para incorporar servicios de la red TETRA en los sistemas de gestión de recursos e incidencias en tiempo real del departamento, por lo que es necesario que, tras la actualización de la infraestructura, el nuevo entorno siga proporcionando las mismas opciones de integración de manera que se pueda mantener la continuidad de los servicios actualmente prestados.

Además, en la medida de lo posible, los interfaces de la nueva versión deberán mantener compatibilidad con las de la versión anterior, de manera que el cambio en las aplicaciones del DSGV sea mínimo. En caso de no ser posible mantener esta compatibilidad, la empresa adjudicataria deberá proporcionar toda la documentación necesaria para que el DSGV pueda conocer en detalle los cambios en los interfaces de manera previa a la actualización de la infraestructura y adecuar sus aplicaciones a dichos cambios.

Así mismo, se proporcionarán al DSGV los elementos software o hardware necesarios para que el DSGV pueda probar estos nuevos interfaces en un entorno real de trabajo, así como toda la ayuda técnica necesaria por parte de la empresa adjudicataria para la correcta puesta en funcionamiento de las aplicaciones integradas en el nuevo sistema

A continuación, se describen los interfaces (APIs) actualmente en uso y cuya funcionalidad deberá mantenerse en la nueva versión de la infraestructura:

- Protocolos asociados al servicio de datos cortos: Se accede a este servicio desde aplicaciones departamentales utilizando la implementación del mismo en la infraestructura Motorola DIPS 8.1 (protocolos SDS y SDTS).
- Información de tráfico en tiempo real ATIA: El DSGV utiliza la información recibida de la red a través del interfaz B-ATIA (Backwards compatible ATIA), que proporciona un flujo de datos de formato fijo.
- Integración asociada a la interfaz CADI: El DSGV utiliza las funcionalidades de este interfaz para realizar funciones como la asignación dinámica de grupos de llamada o inhabilitar y habilitar terminales.

Otros interfaces:

- Packet Data: Aunque actualmente no se utiliza en el DSGV, se ha verificado su funcionamiento para transmisión de datos de capacidad limitada y como sistema portador para el envío de datos de posicionamiento GPS como alternativa al servicio de datos cortos.
- UCS API: API de acceso incorpora nuevas funcionalidades. No utilizada de momento en DSGV, aunque se requiere que la funcionalidad siga estando disponible.

6. ANEXO II - NORMAS DE SEGURIDAD RELATIVAS A LOS SISTEMAS DE INFORMACIÓN

6.1. Normas básicas

La empresa adjudicataria se compromete a cumplir la política de Seguridad de la Información del DSGV y todas las normativas y procedimientos aplicables en el contexto del servicio. La empresa adjudicataria y el personal a su cargo están obligadas a guardar secreto y absoluta confidencialidad respecto de la información que les sea confiada en virtud del servicio prestado, así como seguir las siguientes normas de comportamiento respecto a los sistemas de información del DSGV:

- No introducir software informático ajeno al DSGV.
- No difundir ni publicar los sistemas de seguridad existentes o previstos.
- No revelar la información obtenida de los sistemas de información del Departamento de Seguridad, ni la documentación que se le suministre o la que pudiera tener acceso en el desempeño de sus funciones, con independencia del soporte en que se encuentre contenida.
- Acceder únicamente a la información necesaria para el desempeño de las funciones encomendadas.

La empresa adjudicataria deberá adoptar las medidas de índole técnica y organizativa necesarias que garanticen la seguridad de la información y eviten su alteración, pérdida, sustracción, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que estén expuestos, ya provengan de la acción humana o del medio físico o natural. Además, la empresa adjudicataria adquirirá los siguientes compromisos, que a continuación se describen en cuanto a materia de seguridad se refiere:

- Los equipos conectados a la Intranet del Departamento de Seguridad no podrán conectarse a ningún sistema informático o de telecomunicaciones ajeno al DSGV.
- Los equipos o sistemas que por su actividad requieran conexión a servicios externos al DSGV deberán estar aislados, es decir, separados física y lógicamente de la red informática del DSGV.
- Está expresamente prohibida la instalación de módems (o similar) en equipos (PCs, Servidores, etc.) conectados a la red del DSGV.

6.2. Acceso y protección de datos

La empresa adjudicataria quedará expresamente obligado a mantener absoluta confidencialidad y reserva sobre cualquier dato que pudiera conocer con ocasión del cumplimiento del contrato, especialmente los de carácter personal, que no podrá copiar o utilizar con fin distinto al que figura en este Pliego de Prescripciones Técnicas, ni tampoco ceder a otros ni siquiera a efectos de conservación.

A estos efectos, deberán establecerse las máximas cautelas en el acceso a los datos. Cualquier infracción en este sentido será calificada como grave y será causa de resolución del contrato, sin perjuicio de las responsabilidades penales, o de otro tipo, en que se pueda incurrir.

La empresa adjudicataria se compromete a garantizar y mantener el nivel de seguridad que corresponda en cada caso.

6.3. Propiedad intelectual

Los derechos de propiedad intelectual relacionados con el trabajo realizado pertenecerán al DSGV. Cualquier producto o subproducto derivado del mismo no podrá ser utilizado para otros fines fuera del ámbito que le corresponda, sin el permiso expreso por escrito del DSGV.

Asimismo, todos los entregables que deban facilitarse al DSGV (salvo las ofertas previas) únicamente deberán llevar como logotipo o señas de identidad el escudo del Gobierno Vasco o logotipos aceptados por el propio DSGV.

La empresa adjudicataria se verá también obligada a guardar las normas vigentes sobre, Copyright, propiedad intelectual y documentación clasificada o de difusión restringida que, por necesidades del contrato, se vea obligado a manejar.

Erandio, a la fecha de la firma electrónica



Fdo.: Miguel Álvarez Ramírez
Jefe Sección TETRA
Área de Comunicaciones - DGTSI