

GIPUZKOAKO UR KONTSORTZIOA – GIPUZKOAKO URAK

PLIEGO DE PRESCRIPCIONES TÉCNICAS PARA LA CONTRATACIÓN DEL SERVICIO DE GESTIÓN Y MONITORIZACIÓN, TANTO A NIVEL DE DISPOSITIVO COMO A NIVEL DE CIBERSEGURIDAD, DE LA INFRAESTRUCTURA DE SEGURIDAD AMPLIADA (FIREWALLS, SWITCHES, NAC, GESTIÓN CENTRALIZADA Y DNS)

Integración de la nueva infraestructura de seguridad perimetral, conmutación, NAC, gestión centralizada y analítica con el servicio SOC existente

1.- OBJETO DEL CONTRATO

El presente documento tiene por objeto describir las especificaciones que han de regir la contratación, en modo servicio, de la gestión y monitorización —tanto a nivel de dispositivo como a nivel de ciberseguridad— de la infraestructura de seguridad de GIPUZKOAKO URAK, ampliando el alcance del servicio SOC actual para incorporar la nueva infraestructura de seguridad perimetral, conmutación, gestión centralizada, analítica de seguridad y control de acceso a red recientemente desplegada.

Este pliego sustituye y amplía al pliego técnico del servicio SOC vigente, manteniendo su filosofía, niveles de servicio (SLA) y requisitos de plataforma, y extendiéndolos a los equipos de nueva instalación, así como a las fuentes adicionales necesarias para garantizar una monitorización completa de la organización (incluidos los servidores DNS).

Durante la duración del contrato podrán producirse modificaciones para atender nuevas necesidades, según lo estipulado en el punto 24 de la Carátula del Pliego de Cláusulas Administrativas Particulares.

2.- ALCANCE Y EQUIPOS INCLUIDOS EN EL SERVICIO

El servicio cubre la infraestructura de seguridad existente y la de nueva instalación. El siguiente inventario relaciona la totalidad de los equipos objeto del servicio:

Ubicación	Equipo / Plataforma	Cantidad
1 Sede Central	Firewall Palo Alto PA-820 en HA activo pasivo (2)	2
Euskaltel (Cloud)	Firewall Fortinet (alcance parcial)	1
27 plantas (ETAP/EDAR)	NGFW/SD-WAN FortiGate 70G en HA activo pasivo (2 por planta)	54
13 oficinas remotas	NGFW/SD-WAN FortiGate 70G en HA activo pasivo (2 por oficina)	26
44 Switch	Switch de acceso gestionable (42 × S124FN de 24 puertos y 2 × S148FN de 48 puertos)	44
Centro de proceso	Plataforma de gestión centralizada (Manager – FortiManager)	1
Centro de proceso	Sistema de registro y analítica de seguridad	1



Ubicación	Equipo / Plataforma	Cantidad
	(SGCES – FortiAnalyzer)	
Centro de proceso	Plataforma NAC / control de acceso a red (FortiNAC)	1
Sede Central	Servidores DNS	2

Total de firewalls bajo servicio: 82 (2 Palo Alto existente + 80 NGFW FortiGate 70G de nueva instalación). **Total de switches:** 44 (42 × S124FN y 2 × S148FN). **Plataformas centralizadas:** Manager, SGCES y NAC (FortiManager, FortiAnalyzer y FortiNAC). **Servidores DNS:** 2.

Aclaración sobre la alta disponibilidad (HA): los 82 firewalls corresponden a **41 clústeres lógicos** en configuración de alta disponibilidad activo-pasivo: 1 clúster Palo Alto PA-820 en la Sede Central, 27 clústeres en las plantas ETAP/EDAR y 13 clústeres en las oficinas remotas. A efectos del servicio, la monitorización y gestión se realizará sobre la **totalidad de los equipos físicos (82)**, supervisando de forma individual cada miembro del clúster y el estado de sincronización HA, de modo que una avería, pérdida de sincronismo o indisponibilidad del nodo pasivo genere la correspondiente alerta y actuación aunque el servicio no se vea interrumpido. Los cambios de configuración y políticas se aplicarán a nivel de clúster, garantizando la coherencia entre ambos miembros.

2.1 Licencias y servicios de seguridad incluidos en la monitorización

Las licencias de seguridad activas en cada plataforma forman parte del alcance de monitorización:

- Firewall Palo Alto PA-820: Threat Prevention, WildFire, DNS Security y URL Filtering.
- NGFW de plantas (27 sedes ETAP/EDAR): paquete de seguridad con IPS, control de aplicaciones, antivirus y seguridad OT/ICS (firmas de vulnerabilidades industriales y DPI de protocolos Modbus/TCP, S7, EtherNet/IP (CIP), DNP3, OPC UA y Profinet).
- NGFW de oficinas (13 sedes): IPS, control de aplicaciones, antivirus y protección frente a amenazas avanzadas.
- Firewall Fortinet de Euskaltel: queda fuera de la monitorización, actualización e inyección de IOCs. Sobre él únicamente se realizarán cambios cuando sea necesario añadir alguna regla derivada de una actuación en el Palo Alto PA-820 o en los NGFW, y se prestará asistencia ante problemas e incidencias.

3.- FUENTES DE MONITORIZACIÓN

Con el fin de garantizar una monitorización completa de la organización, el adjudicatario deberá dar de alta en la plataforma de monitorización/SIEM la totalidad de las fuentes de eventos relevantes. Como mínimo se integrarán las siguientes fuentes, incorporando expresamente los dos servidores DNS:

Nº	Fuente	Recolección	Eventos / datos a monitorizar
1	Firewall PA-820 (Central)	Syslog / API	Amenazas, malware, vulnerabilidades, tráfico de aplicaciones, URL Filtering, DNS Security y



Nº	Fuente	Recolección	Eventos / datos a monitorizar
			veredictos WildFire.
2	NGFW de plantas (54 equipos / 27 sedes OT)	Syslog / CEF (vía SGCES)	Amenazas, IPS, control de aplicaciones, antivirus, inspección profunda de protocolos industriales, eventos de segmentación TI/OT, descubrimiento pasivo de activos OT (PLC, HMI, RTU) y estado de la HA.
3	NGFW de oficinas (26 equipos / 13 sedes)	Syslog / CEF (vía SGCES)	Amenazas, IPS, control de aplicaciones, antivirus, tráfico VPN/SD-WAN y estado de la HA.
4	Switches de acceso (44)	Syslog / SNMP	Eventos de puerto, autenticación 802.1X y MAC-Auth Bypass, cambios de topología STP, anomalías MAC, ACL por VLAN/puerto y estado de enlaces agregados (LACP).
5	Plataforma de gestión centralizada (Manager – FortiManager)	Syslog / API REST	Accesos de administradores, cambios de configuración y de políticas, despliegue de plantillas/firmware, versionado/rollback y registros de auditoría (RBAC).
6	Sistema de registro y analítica (SGCES – FortiAnalyzer)	Syslog / API REST	Eventos correlados, alertas, estado de ingesta y salud de la plataforma. Actúa además como concentrador de logs de los 80 NGFW para su reenvío al SIEM del SOC.
7	Plataforma NAC / control de acceso a red (FortiNAC)	Syslog / API / webhook	Autenticaciones (EAP-TLS/PEAP, MAB), perfilado y descubrimiento de endpoints, asignación dinámica de VLAN/microsegmentación, cuarentenas, altas BYOD/invitado y revocaciones.
8	Servidores DNS (2 máquinas)	Syslog / consultas DNS	Consultas y respuestas DNS, resolución de dominios maliciosos o relacionados con APT/campañas de malware, detección de DNS tunneling/exfiltración, dominios de baja reputación (DGA) y errores de resolución. Se monitorizarán de forma independiente las dos máquinas, en alta disponibilidad.
9	Firewall Fortinet de Euskaltel	Bajo demanda	Sin monitorización continua. Asistencia ante problemas e incidencias y cambios de reglas derivados de actuaciones en los firewalls bajo servicio.

Particularidad del servidor DNS: en el reporte de incidencias relacionadas con el servidor DNS se proporcionará la dirección IP del equipo solicitante (origen de la consulta), no la del propio servidor DNS, para permitir la identificación efectiva del equipo afectado.

El adjudicatario completará el alta con cualquier otra fuente que resulte necesaria para una monitorización completa (p. ej. controladores de dominio, servidores de tiempo, plataformas de autenticación o cualquier sistema corporativo que aporte contexto al análisis de incidentes), previa coordinación con GIPUZKOAKO URAK.



4.- SERVICIOS A CONTRATAR

4.1 Servicio de monitorización de la infraestructura de seguridad (24x7)

Los servicios de monitorización, gestión y alerta temprana en 24x7 incluirán la monitorización, gestión y alerta de cualquier incidente de seguridad que se identifique sobre las fuentes anteriores, estableciendo unos niveles de alerta en coordinación con GIPUZKOAKO URAK y un asesoramiento en 10x5 sobre el incidente detectado, de forma que se mitigue de la manera más efectiva y en el menor tiempo posible acorde a los SLA establecidos. En el reporte de incidencias se requiere especificar la dirección IP del equipo afectado (y, en el caso del DNS, la del equipo solicitante).

Las tareas mínimas que deberá incluir el servicio son las siguientes:

- Monitorización de eventos de seguridad en 24x7 de todas las incidencias de seguridad ocurridas en GIPUZKOAKO URAK a nivel de firewalls, switches, NAC, plataformas de gestión/analítica y servidores DNS.
- Monitorización diaria del tráfico de red, revisando que no se hayan producido ni se produzcan incidentes de seguridad. Se monitorizarán al menos los siguientes ítems:
 - Amenazas
 - Aplicaciones no permitidas
 - Vulnerabilidades
 - Comportamientos extraños
 - Consumos excesivos
 - Eventos en entornos OT/ICS: tráfico anómalo en protocolos industriales y detección de activos no autorizados en redes de plantas ETAP/EDAR.
 - Eventos de acceso a red (NAC): autenticaciones fallidas, endpoints no conformes y cuarentenas.
 - Eventos DNS: resolución de dominios maliciosos, DNS tunneling y consultas anómalas.
- Recogida de información de las fuentes para la detección y análisis de posibles incidentes de seguridad.
- Inyección diaria de IoC (Indicadores de Compromiso) en los firewalls bajo servicio para mejorar la seguridad de GIPUZKOAKO URAK.
- Informes mensuales del estado de los incidentes de seguridad ocurridos y presentación de un resumen y de los planes de mejora cada 3 meses. Se valorará la calidad de los informes.
- Asistencia ante problemas e incidencias con el Fortinet de Euskaltel.

4.2 Servicio de gestión y operación rutinaria (8x5)

Se realizarán las tareas de gestión planificada y operación rutinaria necesarias para el mantenimiento de la plataforma ya definida, en horario 8x5 y bajo control de cambios. Quedan incluidas:

- Modificación de reglas y políticas de seguridad en los firewalls bajo servicio.



- Modificación de perfiles de acceso.
- Actualización y parches de configuración / políticas de seguridad (firmas, IPS, perfiles) de carácter programado, sin perjuicio del mantenimiento de hardware y firmware cubierto por el contrato de suministro a 5 años de los equipos.
- Asistencia en la gestión de las VLAN existentes y, eventualmente, en la creación de nuevas (incluidas las modificaciones necesarias en los switches), respetando el esquema de 5 VLAN por sede (datos, voz, gestión, invitados y OT).
- Gestión operativa de las políticas de control de acceso en la plataforma NAC y de las plantillas de despliegue en el Manager, en coordinación con GIPUZKOAKO URAK.

Las actuaciones de contención y resolución que no admitan demora se atenderán bajo el servicio de respuesta a incidentes en 24x7 descrito en el apartado 4.3, con independencia del horario en que se produzcan.

4.2.1 Soporte para sustitución física de equipamiento (RMA)

El adjudicatario deberá realizar hasta un máximo de 160 horas anuales de intervención con desplazamiento incluido a las distintas sedes de Gipuzkoako Urak para la sustitución física de switches o firewalls que presenten averías (gestión de RMA).

A diferencia del resto del servicio de gestión, estas intervenciones tendrán un carácter de pago por uso:

- Facturación: Se facturarán de forma independiente a la cuota fija mensual, aplicando el precio unitario por hora establecido por el licitador en su oferta económica.
- Condición de cobro: Solo se podrán facturar las horas correspondientes a intervenciones efectivamente realizadas y validadas por Gipuzkoako Urak.
- Alcance: El precio por hora deberá incluir todos los gastos de desplazamiento y la mano de obra necesaria para la sustitución y verificación del nuevo equipo.

Las **160 horas de intervención constituyen un máximo anual, no un mínimo**

garantizado: podrán consumirse en su totalidad, parcialmente o no consumirse, sin que GIPUZKOAKO URAK contraiga obligación de pago alguna por las horas no consumidas. Únicamente se abonarán, al precio unitario ofertado, las horas efectivamente ejecutadas y validadas.

4.3 Servicio de respuesta y contención ante incidentes (24x7)

Con independencia de la gestión rutinaria en 8x5, el adjudicatario dispondrá de capacidad de respuesta y contención en modo 24x7x365, alineada con la monitorización y con los tiempos de resolución comprometidos en los SLA (apartado 7), de forma que un incidente crítico detectado fuera del horario laboral pueda contenerse dentro de plazo. Este servicio incluye:

- Aplicación de la solución y de las medidas de contención ante incidentes de seguridad (bloqueo de tráfico, aislamiento de VLAN/segmentos, deshabilitación de cuentas o puertos, cuarentena de endpoints vía NAC), en cualquier momento del día.



- Inyección urgente de IoC (Indicadores de Compromiso) en los firewalls bajo servicio cuando la criticidad del incidente lo requiera.
- Solución de cualquier incidencia que pudiera surgir en el firewall Palo Alto (PA-820) y en los NGFW de nueva instalación que afecte a la disponibilidad o seguridad del servicio.
- Contención específica en entornos OT/ICS de las plantas ETAP/EDAR, dado su carácter de infraestructura crítica en operación continua.
- Escalado y coordinación con GIPUZKOAKO URAK durante la gestión del incidente hasta su cierre, y registro de las actuaciones para el informe posterior.

Todas las acciones de contención y mitigación de incidentes de prioridad **Crítica o Alta** (según la clasificación del apartado 7) se prestarán en modo 24x7x365 y estarán **incluidas en la cuota fija del servicio, sin coste adicional, sin horas facturables ni recargos por franja horaria**, con independencia del momento en que se produzca el incidente. El licitador no podrá condicionar la ejecución de estas medidas a facturación variable alguna.

4.4 Asesoramiento de un CISO

Servicio de asesoramiento de la figura de CISO para la elaboración de planes de acción y mejoras relacionados con la ciberseguridad. Dada la ampliación del alcance (entornos OT/ICS en plantas ETAP/EDAR, NAC y nuevas sedes), se establece una bolsa máxima de 200 horas anuales de asesoramiento, a consumir bajo demanda de GIPUZKOAKO URAK. Estas horas podrán consumirse en su totalidad, parcialmente o no consumirse, sin mínimo garantizado: se facturarán exclusivamente las horas efectivamente consumidas y validadas, al precio unitario (euros/hora) establecido por el licitador en su oferta económica.

La figura del CISO tiene como objetivo principal gestionar la adecuación, implantación, monitorización y mejora de los controles de seguridad, así como de las obligaciones y riesgos asociados. El contratista debe disponer de un equipo multidisciplinar en materia de ciberseguridad que garantice en cada momento los conocimientos y la experiencia necesarios. Sus principales funciones serán:

- Asesoría especializada y centralizada de ciberseguridad, en especial en la elaboración del Plan de Ciberseguridad.
- Consultoría y cumplimiento normativo (PCI DSS, ENS, etc.).
- **Asesoramiento para la adaptación y el cumplimiento de la Directiva (UE) 2022/2555 (NIS2)**, de obligado cumplimiento para GIPUZKOAKO URAK como operador de servicios esenciales del sector del agua. Dado que se está a la espera de su transposición al ordenamiento jurídico español, el servicio incluirá la preparación anticipada a dicha transposición: análisis de aplicabilidad y categorización de la entidad, medidas de gestión de riesgos de ciberseguridad, obligaciones de notificación de incidentes a la autoridad competente, requisitos de gobernanza y responsabilidad de la dirección, y plan de adecuación con su seguimiento.
- Consultoría de infraestructura técnica IT/OT y asesoramiento experto en



ciberseguridad IT/OT.

- Cumplimiento de la legislación vigente, normas sectoriales y contratos.
- Visión experta, multidisciplinar e independiente.
- Participación experta en la estrategia de la organización u otros comités internos.
- Diseño y definición de arquitecturas de ciberseguridad.
- Asesoramiento en adaptación a normativas y estándares (ISO 27000, ISA99/IEC 62443, etc.).
- Redacción de políticas, procedimientos y procesos de ciberseguridad.
- Formación.

5.- REQUISITOS DE LA PLATAFORMA DE MONITORIZACIÓN (SIEM)

Con el fin de obtener sinergias con los servicios previstos a futuro, la solución SIEM deberá cumplir los siguientes requisitos:

- Producto incluido con certificación ENS ALTA en el Catálogo de Productos de Seguridad de las Tecnologías de la Información y la Comunicación (CCN-STIC 105), como producto cualificado en la familia de Sistemas de Gestión de Eventos de Seguridad (SIEM).
- Plataforma interoperable con los servicios y herramientas del CCN-CERT y con la Red Nacional de SOC que resulten aplicables, mediante estándares, formatos, protocolos, API o conectores documentados. La pertenencia al conjunto de herramientas comunes del CCN-CERT no será un requisito obligatorio.
- Diseñada para la monitorización tanto de entornos IT como de entornos OT y redes ICS (Sistemas de Control Industrial), requisito imprescindible dado el despliegue en las plantas ETAP/EDAR.
- Capacidad de ingesta ilimitada: la plataforma y el servicio deberán admitir la ingesta de la totalidad de los eventos y logs generados por todas las fuentes definidas en el apartado 3, sin límite de eventos por segundo (EPS), de volumen diario ni de número de fuentes, y sin coste adicional alguno en función del volumen ingerido. No se admitirán ofertas que condicionen el servicio a un tope de EPS, de GB/día o de activos monitorizados inferior a las necesidades reales de GIPUZKOAKO URAK, ni que prevean sobrecostes por exceso de ingesta.

Volumetría orientativa del servicio actual: a título exclusivamente informativo y sin que constituya límite alguno a la ingesta exigida, los informes mensuales del servicio SOC vigente reflejan que la monitorización actualmente en explotación —esencialmente el firewall Palo Alto PA-820 y los servidores DNS ya integrados— genera un volumen del orden de 30 millones de logs diarios (superior a 900 millones de eventos mensuales), con una media aproximada de 350-400 eventos por segundo (EPS). El firewall Palo Alto, de forma individual, aporta del orden de 85-120 EPS de media, con picos de hasta 150 EPS.



La incorporación al servicio de la nueva infraestructura desplegada (80 NGFW FortiGate 70G, 44 switches gestionables y las plataformas FortiManager, FortiAnalyzer y FortiNAC) incrementará de forma muy significativa el volumen de eventos y logs a ingerir, sin que sea posible cuantificar a priori la magnitud de dicho incremento. Por este motivo, la plataforma y el servicio deberán garantizar en todo caso la ingesta ilimitada establecida en este apartado, sin tope de EPS, de volumen diario ni de número de fuentes, y sin sobre coste alguno en función del volumen ingerido.

El SGCES (FortiAnalyzer) de nueva instalación actuará como sistema de recopilación y analítica de logs de los 80 NGFW (ambos miembros de cada clúster HA: el nodo activo aporta los logs de tráfico y amenazas y el nodo pasivo los eventos de sistema y de estado HA) y reenviará los eventos al SIEM del SOC mediante Syslog/CEF (UDP/TCP/TLS) y/o API REST, garantizando la trazabilidad extremo a extremo.

6.- CONDICIONES

- El adjudicatario deberá garantizar la transferencia del servicio sin interrupción del mismo a la finalización del contrato, de forma que GIPUZKOAKO URAK pueda explotar a través de otros grupos de trabajo los servicios, tecnologías y configuraciones adoptadas en cuanto se produzca el fin de la presente contratación.
- El adjudicatario deberá contar con certificación ENS Nivel Alto (Esquema Nacional de Seguridad).
- El SOC se deberá prestar bajo un modelo 24x7x365, localizado en territorio de la Unión Europea. En caso necesario, la solución se albergará en un DataCenter en la Unión Europea para asegurar el cumplimiento de la legislación vigente.

Para la operación y administración de todos los dispositivos y herramientas, el adjudicatario utilizará canales de comunicaciones cifrados y sistemas de autenticación robusta, con tres niveles de seguridad:

- Acceso VPN sobre IPSEC o SSL.
- Una vez conectados mediante VPN, acceso por SSH a los dispositivos con un usuario nominal para cada técnico.
- Una vez conectados al dispositivo vía SSH, autenticación con credenciales de administrador para la ejecución de actividades privilegiadas y registros de auditoría de las mismas.
- La prestación de los servicios objeto del pliego conllevará el cumplimiento de una serie de niveles de servicio (SLA). En la propuesta, el licitador deberá especificar los valores a los que se compromete en relación con los mismos.
- La respuesta y contención de incidentes de prioridad Crítica o Alta en modo 24x7 (apartado 4.3) **está incluida en la cuota fija del servicio y no generará facturación adicional de ningún tipo** (horas de dedicación, recargos por franja horaria o



conceptos análogos).

6.1 Inicio de la facturación y continuidad del pago durante la transición

El abono del servicio queda condicionado a su puesta en marcha efectiva. En ningún caso se iniciará el pago al adjudicatario antes de que el servicio esté implantado y plenamente operativo, según las reglas siguientes:

- El pago del servicio comenzará a devengarse únicamente cuando este se encuentre operativo al 100 %, es decir, completamente implantado y en funcionamiento. Nunca se facturará con anterioridad a ese hito.
- En caso de cambio de contratista respecto al adjudicatario anterior, se continuará abonando al contratista saliente hasta que el servicio completo del nuevo adjudicatario esté en marcha. A partir de ese momento, y solo entonces, se iniciará el pago al nuevo adjudicatario.
- En caso de que el adjudicatario resulte ser el mismo que venía prestando el servicio, se mantendrá el importe mensual que se abonaba hasta la fecha y se aplicará el nuevo precio del contrato únicamente cuando el servicio se haya implantado al 100 %.

Con ello se garantiza la continuidad del servicio y la ausencia de solapamiento o doble pago durante el período de transición, de modo que GIPUZKOAKO URAK no asuma el coste del nuevo contrato hasta disponer del servicio íntegramente operativo.

6.2 Estructura de la oferta económica

Los licitadores desglosarán su oferta económica en los siguientes conceptos, diferenciando el precio fijo recurrente de los precios unitarios por consumo:

- **Cuota fija (mensual/anual):** comprende la totalidad del servicio recurrente: monitorización 24x7 (apartado 4.1), gestión y operación rutinaria 8x5 (apartado 4.2), respuesta y contención de incidentes de prioridad Crítica o Alta en 24x7 (apartado 4.3), plataforma SIEM con ingesta ilimitada de eventos y logs de todas las fuentes (apartados 3 y 5), alta e integración de dichas fuentes e informes periódicos. La cuota fija no podrá variar en función del volumen de eventos ingerido. Incluye asimismo todos los costes de implantación, puesta en marcha y transición del servicio, que no podrán facturarse como conceptos independientes.
- **Precio unitario por hora de intervención RMA (apartado 4.2.1):** bolsa máxima de 160 horas anuales. Facturación exclusivamente por uso: solo se abonarán las horas efectivamente realizadas y validadas, sin mínimo garantizado.
- **Precio unitario por hora de asesoramiento CISO (apartado 4.4):** bolsa máxima de 200 horas anuales. Facturación exclusivamente por uso: solo se abonarán las horas efectivamente consumidas y validadas, sin mínimo garantizado.

El precio anual del contrato, a efectos de comparación homogénea de las ofertas y de determinación del presupuesto máximo de licitación, se calculará como: **(cuota fija mensual x 12) + (200 x precio unitario hora CISO) + (160 x precio unitario por hora de intervención RMA)**. No obstante, durante la ejecución del contrato únicamente se abonará la cuota fija más los consumos reales de los conceptos variables.



En todo caso, los conceptos variables (**horas de asesoramiento CISO y horas de intervención RMA**) se facturarán única y exclusivamente si se producen. La ausencia total o parcial de consumo de estos conceptos durante una anualidad no generará derecho a compensación, facturación ni reclamación alguna por parte del adjudicatario, que percibirá en tal caso únicamente la cuota fija del servicio.

7.- PARÁMETROS SLA MÍNIMOS

Los parámetros de nivel de servicio (SLA) que se relacionan a continuación constituyen los niveles mínimos exigidos para la prestación del servicio. Los tiempos indicados en la tabla son tiempos máximos de respuesta y de resolución, que en ningún caso podrán superarse: el licitador podrá comprometer en su oferta tiempos inferiores (mejora), pero nunca superiores a los aquí establecidos:

Prioridad	Riesgo de impacto	Tiempo máximo de respuesta	Tiempo máximo de resolución
Crítica	Caída del servicio	1 hora	8 horas
Alta	Caída del servicio	2 horas	8 horas
Media	Servicio en riesgo	4 horas	8 horas
Baja	Bajo impacto	8 horas	24 horas
Petición	Asistencia general / consulta	24 horas	24 horas

A dichos efectos, se entenderá por:

Prioridad Crítica: malware reconocido como de alto impacto (RAT, rootkits...), intrusiones externas efectivas, exfiltración de datos, DoS/DDoS contra servicios críticos, ciberincidentes industriales, servicios comprometidos, APT y campañas de malware.

Prioridad Alta: malware de medio impacto (virus, gusanos, troyanos...), DoS/DDoS contra servicios no críticos, intentos de intrusión externa, peticiones DNS a dominios relacionados con APT o campañas de malware, accesos no autorizados, suplantación, sabotaje, XSS, inyección SQL, spear phishing y pharming.

Prioridad Media: malware de bajo impacto (adware, spyware...), escaneo de vulnerabilidades, sniffing, defacements e ingeniería social.

Prioridad Baja: errores humanos, fallos HW/SW, software no actualizado, spam inofensivo sin adjuntos e incumplimiento de políticas de seguridad.

Petición de información: consultas relativas a configuraciones y a cómo proceder, modificación o alta de nuevas reglas, así como resolución de incidencias operacionales no críticas o asistencia para aclarar consultas y problemas no graves.