Gipuzkoako Ur Kontsortzioa
Gipuzkoako Urak

Blanca Vinuesa eraikina
Portuetxe, 16 - 1. solairua
20018 Donostia
Tfnoa: 902 30 22 22 - Faxa: 943 69 70 50
www.gipuzkoakour.com

**PLIEGO DE PRESCRIPCIONES TÉCNICAS PARA LA CONTRATACIÓN DEL SERVICIO DE GESTIÓN Y MONOTORIZACIÓN TANTO A NIVEL DE DISPOSITIVO COMO A NIVEL DE CIBERSEGURIDAD DE LA INFRAESTRUCTURA DE FIREWALL**

## 1.- OBJETO DEL CONTRATO

El presente documento tiene por objeto describir las especificaciones que han de regir la contratación en modo servicio de gestión y monitorización tanto a nivel de dispositivo como a nivel de ciberseguridad de la infraestructura de Firewall PA-820 (CENTRAL) y PA-N415 (Arriaran)

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

## 2.- SERVICIOS A CONTRATAR

Los equipos incluidos dentro de este servicio son**:** 2 Firewall PaloAlto y parcialmente 1 Fortinet Cloud de Euskaltel.

En el Firewall de Fortinet de Euskaltel solo se realizarán cambios en caso de ser necesaria añadir alguna regla derivado de la actuación en el PA820 o PA-N415. Este Firewall queda fuera de la monitorización, actualización, inyección de IOCs...

Las licencias incluidas dentro del servicio de monitorización en el Firewall PaloAlto 820 son:

1. Threat prevention.
2. Wildfire.
3. DNS Security.
4. URL Filtering.

Las licencias incluidas dentro del servicio de monitorización en el Firewall PA-N415 son:

1. Threat prevention.

Se plantean una serie de servicios que se detallan a continuación:

2.1 Servicio de monitorización de los Firewall Palo Alto:

- Los servicios de monitorización, gestión y alerta temprana en 24x7 de los firewalls incluirán la monitorización, gestión y alerta de cualquier incidente de seguridad que se identifique en estos puntos, estableciendo unos niveles de alerta en coordinación con el Gipuzkoako Urak, y un asesoramiento en 10x5, sobre el incidente detectado; para que se mitigue el incidente de la forma más efectiva y en el menor tiempo posible acorde a los SLAs establecidos. En el reporte de incidencias, se requiere especificar la dirección IP del equipo afectado.

Blanca Vinuesa eraikina
Portuetxe, 16 - 1. solairua
20018 Donostia
Tfnoa: 902 30 22 22 - Faxa: 943 69 70 50
www.gipuzkoakour.com



Si se trata del servidor DNS, se debe proporcionar la IP del equipo solicitante en lugar de la IP del servidor DNS.

- 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 Ural a nivel de Firewalls.
  - Se monitorizará diariamente el tráfico de red revisando que no se hayan producido o que se produzcan incidentes de seguridad (amenazas detectadas, malware, aplicaciones, vulnerabilidades, comportamientos extraños de un usuario, equipo o tráfico, etc.). Se monitorizara los siguientes ítems:
    - Amenazas
    - Aplicaciones no permitidas
    - Vulnerabilidades
    - Comportamientos extraños
    - Consumos excesivos
  - Se realizarán todas las tareas de gestión necesarias para el mantenimiento de la plataforma ya definida 8x5:
    - Modificación de reglas
    - Modificación de perfiles de acceso
    - Aplicación de la solución ante incidentes
    - Actualización y parches.
  - Se procederá a la recogida de información de los Firewall para la detección y análisis de posibles incidentes de seguridad.
  - Solucionar cualquier incidencia que pudiera surgir en los Palo Alto.
  - Asistencia en la gestión de las VLANs existentes y, eventualmente, en la creación de nuevas (incluyendo las modificaciones necesarias en los Switches).
  - Se procederá a la inyección de IoC (Indicadores de Compromiso) diariamente a los firewalls para mejorar la seguridad de Gipuzkoako Urak.
  - Informes Mensuales del estado Incidentes de Seguridad ocurridos y presentación de un resumen y los planes de mejora cada 3 meses.
  - Realización de Informe mensual, se valorará también la calidad del mismos.
  - Asistencia ante problemas e incidencias con el Fortinet.

2.2 Asesoramiento de un CISO (estimación de 300 horas anuales).

Elaboración de planes de Acción y mejoras relacionados con la Ciberseguridad. CISO

- Elaboración de planes de Acción y mejoras relacionados con la Ciberseguridad. CISO.
- La figura del CISO tiene como objetivo principal gestionar la adecuación, implantación, monitorización y mejora de dichos controles de seguridad, así como de las obligaciones y riesgos asociados. Dentro del marco del

Blanca Vinuesa eraikina
Portuetxe, 16 - 1. solairua
20018 Donostia
Tfnoa: 902 30 22 22 - Faxa: 943 69 70 50
www.gipuzkoakour.com



servicio de CISO el contratista debe disponer de un equipo multidisciplinar en materia de ciberseguridad, que garantice que en cada momento se cuenta con los conocimientos y experiencia necesaria para afrontar cada situación.

- Sus principales funciones serán:
  - Servicio de asesoría especializada y centralizada de ciberseguridad, en especial en la elaboración del Plan de Ciberseguridad.
  - Consultoría y cumplimiento normativo (PCI DSS, ENS, etc.)
  - Consultoría de infraestructura técnica IT/OT y asesoramiento experto en ciberseguridad IT/OT.
  - Cumplimiento con la legislación vigente, normas sectoriales, 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, etc.)
  - Redacción de políticas, procedimientos y procesos de ciberseguridad.
  - Formación

## 3.- CONDICIONES

- El adjudicatario deberá garantizar la transferencia del servicio sin interrupción del mismo, con 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.

- 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

Blanca Vinuesa eraikina
Portuetxe, 16 - 1. solairua
20018 Donostia
Tfnoa: 902 30 22 22 - Faxa: 943 69 70 50
www.gipuzkoakour.com



robusta, con tres niveles de seguridad:

- Acceso VPN sobre IPSEC o SSL.
- Una vez conectados mediante VPN, acceso mediante 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.

- Con el fin de obtener sinergias con los servicios previstos a futuro, la solución SIEM debe cumplir con 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 con la certificación Common Criteria EAL2 + ALC_FLR.1
    - Tecnología empleada por el CCN-CERT en los servicios de alerta temprana SAT y por otros Centros de Operaciones de Ciberseguridad integrados en la Red Nacional de Centros de Operaciones de Ciberseguridad, por lo que se trata de una solución plenamente interoperable con los servicios desplegados en la Administración General del Estado por el CCN-CERT. (SAT-INET y SAT-ICS)
    - Plataforma perteneciente al conjunto de herramientas comunes del CCN-CERT, sin coste de licencia para los organismos públicos nacionales.
    - La plataforma está diseñada para la monitorización tanto de entornos IT como de entornos OT y redes ICS (Sistemas de Control Industrial).
    - La plataforma debe integrarse nativamente con las soluciones del CCN-CERT: LUCIA, REYES, IRIS, CARMEN, CLAUDIA, MICROCLAUDIA

- La prestación de los servicios objeto del pliego conllevará el cumplimiento de una serie de niveles de servicio (SLA's). En la propuesta, el licitador deberá especificar los valores a los que se compromete con relación a los mismos.

## 4.- PARÁMETROS SLA MÍNIMOS

Los niveles de servicio (SLA's) máximos serán los siguientes:

| Prioridad | Riesgo de Impacto | Tiempo máximo de Respuesta | Tiempo máximo de Resolución |
|---|---|---|---|

Blanca Vinuesa eraikina
Portuetxe, 16 - 1. solairua
20018 Donostia
Tfnoa: 902 30 22 22 - Faxa: 943 69 70 50
www.gipuzkoakour.com



| | | | |
|---|---|---|---|
| Crítica | Caída del Servicio | 1 hora | 8 horas |
| Alta | Caída del Servicio | 2 hora | 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, APTs, 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 APTS o campañas de malware, accesos no autorizados, suplantación, sabotaje, XSS, inyección SQL, spear phishing, pharming.

- **Prioridad Media:** Malware de bajo impacto (adware, spyware…), escaneo de vulnerabilidades, sniffing, defacements, ingeniería social.

- **Prioridad Baja:** Errores humanos, fallos HW/SW, software no actualizado, spam inofensivo sin adjuntos, no cumplimiento de políticas de seguridad

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