Informe Técnico

PAC Nº: 04/2024	**ID Nº:** 436.589
DESCRIPCIÓN DEL LLAMADO: LCO "CONTRATACIÓN DE SERVICIO EXTERNO DE UN SOCAAS (SECURITY OPERATION CENTER AS A SERVICE)" - PLURIANUAL - AD REFERENDUM - S.B.E."	
CONTRATO Nº: 48/2024	**PROVEEDOR:** CORPORATION SEKIURA S.A.C.E.I.
ORDEN DE SERVICIO Nº 3186	**MES DE OCTUBRE 2024**
Fecha de Recepción del Informe: 01/11/2024	

Este documento presenta un resumen del informe de aceptación mensual correspondiente al servicio de **Centro de Operaciones de Seguridad como Servicio (SOCaaS)** provisto por la empresa CORPORATION SEKIURA S.A.C.E.I. y es elaborado con el objetivo de proporcionar una visión general del rendimiento del servicio durante el mes de referido, protegiendo al mismo tiempo la confidencialidad y sensibilidad de la información tecnológica detallada en el informe completo.

Motivo de la Elaboración del Resumen

El informe completo del SOCaaS contiene información técnica sensible y confidencial de los recursos tecnológicos (Hardware y Software) de la Corte Suprema de Justicia (CSJ), incluyendo detalles sobre la infraestructura tecnológica y de seguridad, vulnerabilidades detectadas, incidentes gestionados y configuraciones específicas. La divulgación no controlada de esta información podría exponer a la organización a riesgos de seguridad. Por estas razones, se genera este resumen para asegurar la transparencia y la rendición de cuentas, sin comprometer la seguridad de la información.

Áreas Clave Cubiertas en el Informe Completo (resumidas aquí):

- Monitoreo y Detección de Amenazas: El informe completo detalla la actividad de monitoreo de seguridad realizada durante el mes, incluyendo el número promedio de eventos por segundo (EPS) y el número de detecciones y alertas de seguridad registrados, así como un mapa de calor de detecciones por fecha. Este resumen indica que el sistema de monitoreo operó de manera efectiva, recopilando un promedio de **10,13** eventos por segundo y detectando **27.136.300** eventos relevantes.

- Análisis de Vulnerabilidades: El informe completo presenta los resultados de los análisis de vulnerabilidades realizados durante el mes, incluyendo las vulnerabilidades detectadas y las recomendaciones de mitigación. Este resumen indica que se identificaron **5.834** vulnerabilidades, de las cuales **63** fueron consideradas críticas.

- Gestión de Incidentes: El informe completo describe los incidentes de seguridad que se gestionaron durante el mes, incluyendo su clasificación, impacto y las acciones de respuesta tomadas. Este resumen indica que se gestionaron **5** incidentes.

- Rendimiento del Servicio: El informe completo incluye indicadores de la evolución mensual del servicio, como ser: Equipos monitoreados, EPS, Incidentes reportados, Tickets creados, Tickets finalizados, Tickets pendientes en SOC, Tickets pendientes en CSJ; así como la

disponibilidad del servicio a través del registro en planilla del control de asistencia de los analistas en ciberseguridad.

- Mejoras y Recomendaciones: El informe completo presenta recomendaciones para mejorar la postura de seguridad y el rendimiento del servicio. Este resumen indica que se han identificado las siguientes áreas de mejora: proseguir con el despliegue de las configuraciones, establecer ventanas de trabajos, normalizar las versiones de Sistemas Operativos, abordar la remediación de las vulnerabilidades detectadas y considerar especialmente las detecciones que corresponden a cumplimiento de Marcos Normativos de Ciberseguridad, para la aplicación de sus recomendaciones de mejora.

- Reuniones de seguimiento semanales: donde son abordados temas puntuales acerca de la coordinación de equipos involucrados en la ejecución de las acciones de remediación, alternativas de adopciones de más activos o fuentes de información a ser correlacionadas para el análisis y monitoreo de actividades sospechosas.

Conclusión

El servicio SOCaaS proporcionado por CORPORATION SEKIURA S.A.C.E.I. durante el mes referido se considera satisfactorio según el análisis del informe completo. Este resumen proporciona una visión general del rendimiento del servicio, protegiendo al mismo tiempo la confidencialidad de la información técnica sensible.

Observación importante: Este es un resumen. El informe técnico completo está disponible en la DCPI-DGTIC para revisión por personal autorizado, bajo un acuerdo de confidencialidad.

Ing. Mg. Marcelo G. Demestri F.
Director Interino - Dirección de Ciberseguridad y Protección de la Información - DGTIC - CSJ