Informe justificativo para la compra de Gestor de Seguridad de Información y Eventos (SIEM)

César Moliné Rodríguez y Nidson José Polanco
14-8-2023

Antecedentes. -

Los incidentes de ciberseguridad son cada vez más comunes y sofisticados, y pueden tener graves consecuencias para las organizaciones, incluyendo la pérdida de datos confidenciales, la interrupción de los servicios y la pérdida de la confianza del público en las instituciones gubernamentales. Actualmente, aunque ha habido avances en la capacidad de detección de amenazas y respuesta a incidentes en la institución, lo cierto es que todavía no contamos con todas las herramientas necesarias, lo que dificulta la identificación temprana de los incidentes y la respuesta efectiva a estos.

Esta preocupación fue recientemente recogida en el Decreto núm. 685-22 del Poder Ejecutivo de fecha 8 de noviembre de 2022. Este Decreto tiene por objeto establecer los principios y lineamientos generales que servirán de base a los entes y órganos de la Administración Pública para la adopción de controles, políticas y estándares para incrementar los niveles de madurez cibernética en el sector público, la notificación obligatoria de eventos e incidentes de ciberseguridad, así como el intercambio de información sobre amenazas cibernéticas, conforme a lo dispuestos en el Decreto núm. 313-22, del 14 de junio de 2022, que establece la Estrategia Nacional de Ciberseguridad 2030.

En el mismo se considera que el *Estado Dominicano necesita fortalecer la ciberseguridad del sector público para robustecer los sistemas de información y para asegurar la confianza de la población en estos sistemas como una opción viable para el desarrollo económico, social y la seguridad nacional.*

El propósito de este informe es sustentar por parte de la **Dirección de Ciberseguridad, Comercio Electrónico y Firma Digital**, los argumentos necesarios para justificar la adquisición de Gestor de Seguridad de Información y Eventos (SIEM) para el INDOTEL.

Sobre el Gestor de Seguridad de Información y Eventos (SIEM) y su pertinencia para la ciberseguridad del INDOTEL. -

El SIEM es una herramienta esencial para la gestión y supervisión de la seguridad de la información en una organización. Permite la monitorización en tiempo real de los eventos y la detección de posibles amenazas de seguridad, así como la gestión de incidentes y la realización de informes de seguridad.

Actualmente, nuestra organización no cuenta con una herramienta de este tipo, lo que implica una falta de visibilidad sobre los eventos y amenazas de ciberseguridad que pueden afectar a nuestros sistemas y datos. La falta de supervisión y análisis de los eventos de seguridad pone en peligro la integridad y confidencialidad de nuestra información, así como puede dañar la reputación de INDOTEL y generar costosos daños económicos.

Además, la implementación del SIEM ayuda a cumplir con los requisitos de cumplimiento normativo en materia de seguridad de la información y ciberseguridad establecidos por el precita Decreto núm. 685-22, en particular:

1. Cumplir con la obligación de adoptar e implementar normas, políticas y procedimientos en materia de ciberseguridad, según lo dispone el artículo 5;

2. Cumplir con la gestión de os riesgos cibernéticos en sus servicios, aplicaciones, sistemas de información e infraestructura tecnológica, de acuerdo con lo señalado por el artículo 6; y

3. Cumplir con la mejora en la prevención e identificación de los incidentes de ciberseguridad, de conformidad con el artículo 9.

En virtud de todo lo indicado previamente, con la adquisición de SIEM no solo nos permitirá tener una visibilidad completa de los eventos de seguridad en nuestra red, así como mejorar la capacidad de respuesta ante posibles incidentes, sino que además la herramienta nos permitirá detectar patrones de comportamiento sospechosos, identificar posibles vulnerabilidades y realizar un seguimiento detallado de la actividad de los usuarios. Todo esto sin contar que además se le estaría dando cumplimiento a las disposiciones de ciberseguridad establecidas por el Poder Ejecutivo.

Valor referencial

El valor referencial para este proceso corresponde a **ocho millones setecientos mil pesos dominicanos con 00/100 (RD$8,700,000.00),** aprobado en el POA de la Dirección de Ciberseguridad del año 2023.

En resumen, la compra de un SIEM es esencial para garantizar la seguridad de la información en nuestra organización y cumplir con los requisitos normativos. Además, permitirá mejorar la eficiencia y efectividad de nuestra estrategia de seguridad de la información y proteger nuestros activos críticos.

En consecuencia, quienes suscriben, recomendamos la adquisición del Gestor de Seguridad de Información y Eventos (SIEM) y quedamos a su disposición para cualquier consulta adicional o aclaración.

DCCEF-I-000022-23