REQUERIMIENTO

Los procesos de tecnología de la información han evolucionado en los últimos años con el fin de volverse fundamental para mantener el crecimiento, innovación y transformación en los servicios de madurez de seguridad y soporte de las operaciones comerciales en curso de las organizaciones, es por eso por lo que nace la necesidad de un servicio que identifica los riesgos de seguridad en Microsoft 365.

Las amenazas de seguridad son una tensión constante para las organizaciones.

La seguridad de la entidad es un objetivo en movimiento con nuevas vulnerabilidades identificadas diariamente. Para mantener una buena postura de seguridad, las personas, los procesos y la tecnología de la organización debe trabajar de forma conjunta. Una debilidad en cualquiera de estos dominios puede conducir a una brecha de seguridad.

Para que un programa general de ciberseguridad sea efectivo, primero es necesario tener una comprensión clara de la infraestructura de TI al interior de la entidad.

El servicio solicitado en debe brindar una vista general para identificar áreas de riesgo potencial y brindar orientación de alto nivel sobre programas y políticas de ciberseguridad para ayudar a habilitar una buena gestión de activos de software de TI.

ALCANCE DEL SERVICIO

Se debe realizar una ejecución de las actividades en tres fases:

Onboarding	Recopilación y análisis de datos	Consolidación & Presentación
• Presentar recursos.	• Temas de descubrimiento basados en hallazgos con partes interesadas clave. • Detección basada en herramientas en todas las cuentas dentro del alcance.	• Resumen ejecutivo e informe de problemas detallado. • Plan de remediacion de gaps de licenciamiento. • Plan de inversion de hardenizacion de uso de la solucion actualmente contratada.

DESCRIPCIÓN DE FASES

- Onboarding: Se debe realizar un análisis donde se revisan el conjunto de prácticas definidas, políticas y controles que incorporan estrategias comprobadas para un óptimo funcionamiento de la plataforma. Dentro de las actividades principales se analizarán las policitas definidas de acuerdo con el licenciamiento contratado, para lo cual se llevará a cabo las siguientes actividades:
    - Presentar recursos y partes interesadas.

- Ejecutar el proceso y requisitos previos.
- Desarrollar cuestionario.
- Acordar el esquema del taller, el horario y los asistentes.

- Recopilación y análisis de datos: En esta fase se debe ejecutar las actividades relacionadas con la recopilación de información concerniente a vulnerabilidades y políticas y controles aplicados de acuerdo con el uso del licenciamiento contratado.
    - Temas de descubrimiento basados en hallazgos con partes interesadas clave:
        - Revisión de marco de políticas y controles de seguridad.
        - Seguridad organizacional.
        - Core de seguridad.
        - Extensión de seguridad.
    - Detección basada en herramientas en todas las cuentas dentro del alcance para:
        - Validación de temas de infraestructura de talleres.
        - Vulnerabilidades de la infraestructura y el medio ambiente.
        - Validación del cumplimiento normativo de la infraestructura.
    - Consolidación y presentación: En esta fase se consolidará toda la información recopilada, se analizará y se alistara el informe técnico detallado con los hallazgos los cuales estarán detallados de la siguiente manera:
        1. Análisis de Seguridad Microsoft 365.
        2. Análisis de licenciamiento.
        3. Análisis de riesgos.
        4. Análisis de oportunidades.
        5. Puntuación de seguridad y recomendaciones.
        6. Análisis de seguridad por workload.
        7. Recomendaciones de hardenización del licenciamiento actual.

Nota: El servicio esta dimensionado para un máximo de 5000 usuarios.