

SERVICIOS

Gestión de Protección Integral en EndPoint:

El servicio está diseñado para gestionar la seguridad de las plataformas endpoint de las organizaciones en la protección de los datos y dispositivos tanto corporativos como personales.

Proceso

Inicialmente, recopilará información sobre los usuarios, los requisitos de seguridad de la organización y definirá los procesos, las reglas o políticas que se requieren.

Los resultados de la evaluación serán luego revisados por un Consultor Certificado de Azure, quien hará sugerencias basadas en:

- Gestión de amenazas e incidentes
- Mantener un ambiente de trabajo seguro.
- Gestión segura de documentos y aplicaciones.
- Necesidad de autenticación híbrida.

Administración del Servicio

Basados en una comprensión clara de las metas y objetivos comerciales del Cliente para evaluar el alcance y la dirección del trabajo con precisión.

Se gestionará:

Los endpoints: aprovisionamiento e inscripción

Seguridad unificada con controles Zero-Trust. Acceso seguro a los recursos corporativos mediante evaluaciones continuas y políticas basadas en el uso que controlan las aplicaciones de acceso condicional con tecnología de Azure Active Directory (Azure AD) y la integración nativa Microsoft Endpoint Manager.

Protección de datos laborales: Garantiza el cumplimiento del dispositivo y la aplicación para controlar el flujo de datos fuera de las aplicaciones móviles de confianza a través de las directivas de administración de aplicaciones móviles (MAM) y administración de dispositivos móviles (MDM).

Licenciamiento mínimo necesario:

M365 E3 + E5 Security Add-on

M365 E5.

M365 F3 + F5 Security

M365 F3 + F5 Security+Compliance