CRAYON IT CYBERSECURITY

Evaluación de Seguridad Microsoft 365

Alcance

La Evaluación de Seguridad de Microsoft 365 es un servicio ejecutivo que entrega una visión objetiva y profunda del estado de seguridad del ambiente Microsoft 365, de su organización. A partir de un levantamiento técnico especializado y el análisis de nuestros consultores, usted obtiene claridad sobre los riesgos actuales y un camino concreto para mitigarlos.

DURACION Y MODALIDAD

Duración: 6 semanas

Este servicio está dirigido a organizaciones de cualquier tamaño que utilicen Microsoft 365

STAKEHOLDERS CLAVE

Requiere: Stakeholders del cliente con conocimientos técnicos y operacionales del negocio.

Orientado a CISO, CTO, CIO que deseen contar con una evaluación objetiva del nivel de seguridad de sus ambientes Microsoft 365.

NUESTRO PROCESO

01 **Levantamiento técnico automatizado**

Ejecución de scripts especializados que recopilan información de configuración y estado de seguridad del ambiente Microsoft 365.

02 **Entrevistas y validación**

Entrevistas con responsables internos para entender el contexto de la configuración, aclarar dudas y descartar potenciales falsos positivos.

03 **Análisis y evaluación de riesgos**

Revisión detallada de la información recopilada para determinar el estado de seguridad del ambiente y clasificar los hallazgos según su impacto potencial para el negocio.

04 **Informe y plan de remediación**

Elaboración de un informe completo que describe el estado actual, los riesgos identificados y un plan de remediación priorizado, alineado a las necesidades de la organización.

CRAYON IT
CYBERSECURITY

Evaluación de Seguridad Microsoft 365

Valor de Negocio

- Contar con una visión objetiva e independiente del nivel de seguridad de su ambiente Microsoft 365.
- Identificar y priorizar riesgos antes de que se materialicen incidentes que afecten la continuidad del negocio.
- Disponer de un plan claro para mejorar la postura de seguridad en función de la criticidad de los hallazgos.
- Dar al directorio y a la gerencia claridad sobre qué se debe corregir y por dónde comenzar.
- Contribuir a proteger los servicios y datos críticos que su organización entrega a clientes y colaboradores.

Resuelve

Ausencia de priorización clara de riesgos críticos, altos, medios y bajos dentro del entorno Microsoft 365.

Riesgos en la seguridad del correo electrónico, incluyendo exposición a phishing y ataques de suplantación.

Configuraciones débiles o incorrectas en identidad y control de acceso (Azure AD / Entra ID).

Falta de un plan estructurado para remediar vulnerabilidades y mejorar progresivamente la postura de seguridad.

Evaluación de Seguridad Microsoft 365

Áreas evaluadas en Microsoft 365

1. Identidad y control de acceso (usuarios, roles, autenticación, MFA, etc.).
2. Seguridad de correo electrónico (protección contra phishing, malware, spam, políticas de seguridad).
3. Servicios de colaboración: SharePoint, OneDrive y Microsoft Teams.
4. Configuraciones y controles de seguridad relevantes de la plataforma Microsoft 365.

Cómo trabajamos

Semana 1-2: Kick-off y recolección de información.

Semana 3-4: Análisis y preparación de informes y presentaciones.

Semana 5: Presentación preliminar de resultados.

Semanas 6: Presentación ejecutiva y entrega de documentos y resultados.

ENTREGABLES

- **Informe final personalizado,** con evaluación de Seguridad de Microsoft 365, que incluye el detalle de hallazgos técnicos, su criticidad y su impacto potencial.
- **Plan de remediación priorizado, con acciones concretas para:**
    1. Riesgos Críticos
    2. Riesgos Altos
    3. Riesgos Medios
    4. Riesgos Bajos
- **Presentación ejecutiva para directorio y alta gerencia detallado**, donde se resumen los hallazgos más relevantes, los riesgos para el negocio y las principales líneas de acción recomendadas.

www.crayonit.com
contacto@crayonit.com
+56 2 3215 1077
linkedin/company/crayonit