colaboratic

Seguridad 365

2021/03

Seguridad en la nube: una asignatura pendiente

Falsas creencias de la nube

- Microsoft se ocupa de todo porque ya pago una suscripción

  FALSO: Las numerosas suscripciones existentes dan acceso a los servicios contratados como correo, videoconferencia, ofimática, etc. Pero junto con estos servicios, están también a las herramientas de gestión y análisis de la seguridad que están ahí para que cada cliente haga uso de ellas.

- La información esta en la nube así que está segura:

  FALSO: la nube proporciona mecanismos de seguridad avanzados, pero hemos de implementarlos nosotros porque es nuestra responsabilidad hacerlo. Si hay un robo de información mediante phishing, suplantación, robo de credenciales, etc. la responsabilidad será cosa nuestra. Recordemos que los medios para evitarlo están ahí…

- La información está en la nube, no es cosa mía si hay problemas:

  FALSO: una vez más la responsabilidad de la información depositada en los proveedores de nube, como Microsoft, es siempre del cliente. Es éste el que debe implementar los mecanismos de protección necesarios que varían según el servicio.

El problema entonces es que

- Pero los clientes NO tienen el tiempo ni los recursos para dedicarle tiempo a la gestión de la seguridad.

Hechos

- Los servicios en nube son enorme vector de entrada de ataques:
  - El correo electrónico supone una vía inagotable de intentos de fraude y robo.
  - Los demás servicios de la suite no hacen si no ampliar el abanico de posibilidades para un atacante.
  - El hecho de tener los servicios en la nube facilita el acceso a los mismos desde cualquier lugar del mundo … y por cualquiera que consiga el acceso.

- La actividad de usuarios y atacantes genera un elevado número de información:
  - Todos los días se registran innumerables alertas.
  - Los proveedores de nube a su vez también generan avisos y advertencias que atender.

- Los servicios en nube evolucionan constantemente
  - Por su naturaleza, cada poco tiempo aparecen nuevas funcionalidades o cambian las existentes.
  - Muchos de esos cambios afectan a la seguridad y también a las propias herramientas de gestión de la misma.
  - El cambio es una constante en la nube.

Entonces ¿cómo puedo mejorar la seguridad de mis usuarios en Microsoft 365?

Microsoft 365 ofrece distintos servicios de seguridad para sus productos (Exchange Online, OneDrive, Teams, Sharepoint, …):

- De base, hay una capa de protección mínima que se cubre con el pago de la suscripción.
- Se puede fortalecer la seguridad mediante diversos planes y herramientas adicionales.

Sin embargo, tanto la seguridad de base como la avanzada necesitan de atención y gestión.

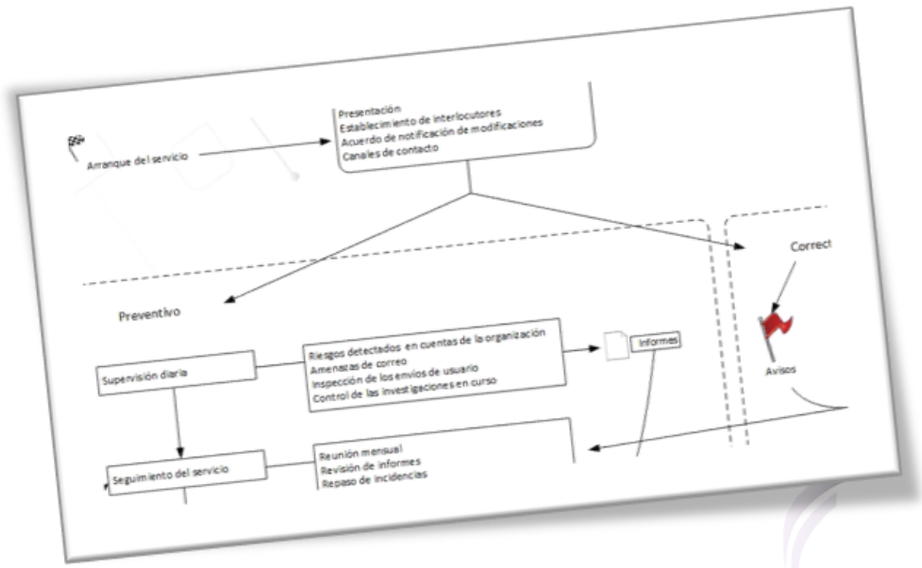
…pero los clientes NO tienen el tiempo ni recursos que dedicar a la gestionar la seguridad y estar al tanto de los numerosos cambios

Seguridad en la nube mediante Seguridad 365

Seguridad 365: descripción

- Seguridad 365 es un servicio de **Seguimiento**, **Gestión** y **Mejora** continuado de la Seguridad en Microsoft 365.

- Contratado de manera natural junto a cada suscripción de Microsoft o incluido dentro del Mantenimiento Integral de Sistemas y Comunicaciones.



Seguridad 365: que ofrece

Tranquilidad frente a las amenazas mediante:

- Supervisión diaria de riesgos y amenazas.
- Evolución de la seguridad de la empresa a medida que nuevas funcionalidades están disponibles.
- Adaptación a las necesidades de seguridad de la compañía.

Visibilidad de lo que ocurre gracias a informes claros y concisos y reuniones de seguimiento.

Concienciación de usuarios de amenazas y herramientas a nuestra disposición.

Seguridad 365: informe ejemplo

[FECHA] INFORME MENSUAL SEGURIDAD MICROSOFT 365

Su puntuación segura — Incluir

Puntuación de seguridad: 24.14 %

Las zonas de calificación se personalizan en función de los objetivos de la organización y las definiciones de cada rango de resultados.

Tendencia de comparación

Comparación en el tiempo de la puntuación de seguridad de su organización con otras organizaciones.

Cambios de puntuación

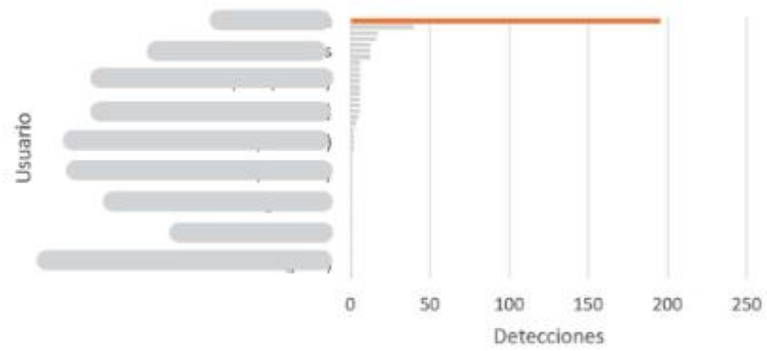
Incremento del 1.73 %

Cambios	Puntos
Puntos obtenidos	▲ 1
Puntos de regresión	0

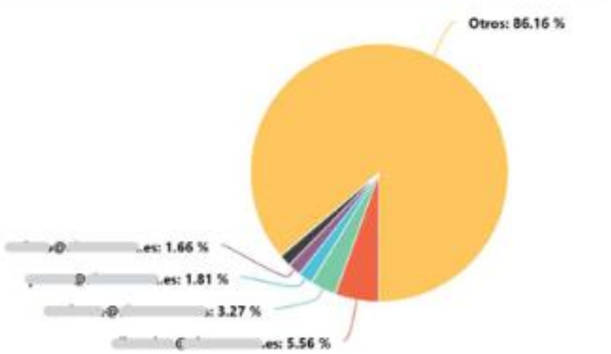
Tiene 61 de 2175 usuarios registrados y protegidos con MFA.

Hay 2173 de 2175 usuarios que no tienen habilitado el autoservicio de restablecimiento de contraseña.

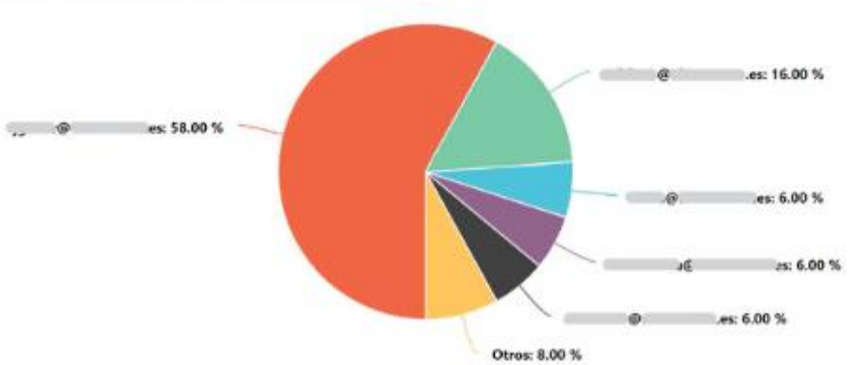
Detecciones de riesgo de inicio de sesión por usuario



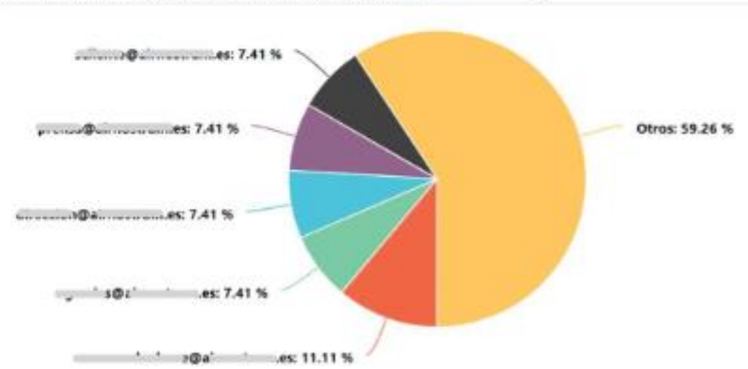
Principales destinatarios de correo no deseado



Principales destinatarios de malware (ATP)



Mostrar datos de Principales destinatarios de malware



LOGO EMPRESA

*** USO INTERNO - COLABORATIC - USO INTERNO ***

colaboratic