INNOVACIÓN EN ACCIÓN

Beyond IT

SITES

Shared IT Enterprise Services

White Paper

Protección de Tenant O365: Parte I

ALEMAN Francisco Ingeniero de Nube [Microsoft Identity and Access Administrator]

SORIANO Karla Estefany Seguridad Informática [CompTIA Security+]

Resumen ejecutivo

Hemos trasladado nuestros documentos a la nube y a diario utilizamos diversas herramientas de comunicación para intercambiar mensajes, compartir objetos, realizar llamadas y planificar nuestro trabajo, entre otras actividades. Nuestra superficie de ataque crece constantemente, pero esto no implica que nuestras medidas de protección se implementen proactivamente y se validen de forma periódica. Muchos hemos decidido pasar por alto el hecho de que los fabricantes de los sistemas y de las aplicaciones que usamos cometen errores que exponen nuestros activos digitales, con mayor frecuencia que la esperada. Hace mucho tiempo que la seguridad informática dejó de ser un kit de herramientas para convertirse en un proceso, cuya propiedad de los controles debe ser compartida con los usuarios finales. Muchas veces, el conocimiento técnico requerido para habilitar las soluciones de seguridad no forma parte de las habilidades internas a la empresa, por lo que conviene colaborar con expertos en el tema que nos ayuden a lograr resultados en plazos óptimos.

En nuestra empresa hemos adquirido suscripciones de Microsoft Office 365 y las referencias comerciales del producto explican que las opciones de seguridad forman parte del pago mensual realizado. Dichas funciones de seguridad pueden adquirirse en planes diferentes, dependiendo del nivel de protección requerido y una vez que se han adquirido, un experto en ciberseguridad debería configurarlas para que las protecciones respondan al proceso de negocio.

Aunque las herramientas suministradas por Microsoft satisfacen buena parte de las demandas de protección, es indispensable alinear su configuración con las políticas de seguridad de la empresa y la manera en que los usuarios consumen los servicios de la nube. Muchas empresas, carecen de políticas y procesos de seguridad, con lo que se compromete el éxito de cualquier iniciativa de protección que se desee implementar.

Adicionalmente, el beneficio que brinda la nube de ampliar periódicamente las capacidades de las herramientas de usuario obliga a los gestores de seguridad de la nube a revisar nuevas necesidades de protección y nuevas funciones disponibles para implementar dicha protección, es decir, la seguridad no debe considerarse una paso para la adopción de la nube sino un control sujeto a verificaciones continuas.

Las oportunidades de ampliar las medidas de protección con herramientas de terceros se abordarán en la Parte II de este artículo.

Superficie de ataque de O365

La experiencia nos ha mostrado que cuando no se protege con el celo que merece “la moneda de cambio” de las empresas, incluso los más grandes de la industria caen, cual David contra Goliat; esta “moneda de cambio” resulta tan atractiva como una Helena de Troya, en riesgo constante de ser robada.

La moneda en cuestión no es otra que la información, ya sea empresarial y/o personal que reside en la nube, en recursos locales o en ambientes híbridos y es ambicionada por empresas competidoras

o por ciberdelincuentes.

Indistintamente del lugar donde resida, está claro que el primer paso para prevenir filtraciones, robos o abusos es identificar y clasificar los activos de información, y el segundo es estar consciente de las brechas y los puntos débiles en la seguridad, desde la infraestructura en donde se aloja hasta los protocolos o procedimientos con los que se accede, almacena, comparte, modifica, traslada y elimina, es decir, la superficie de ataque.

Conocer las brechas permite tomar las acciones pertinentes para controlarlas, mientras que conocer los puntos débiles constituye el punto de partida para mitigar y/o reforzar estas vulnerabilidades. En la nube de Microsoft O365 los componentes de la superficie de ataque son:

- Correo electrónico
- Dispositivos de usuario
- Identidad
- Políticas y procesos de gestión de la información
- Configuración del ambiente
- Aplicaciones autorizadas y no autorizadas (Shadow IT)
- Integración con terceros

Teniendo presente que la nube trabaja en base a responsabilidad compartida entre el proveedor de servicios en la nube (CSP por sus siglas en inglés) y la organización que la contrata, la seguridad en cada uno de estos elementos, también hereda esta característica de modo que ambos deben ser partícipes en la protección de la superficie de ataque desde sus responsabilidades.

Herramientas de seguridad O365

Ahora que conocemos la superficie de ataque es momento de establecer el sistema de defensa. El siguiente cuadro introduce, el valor de las herramientas que Microsoft ha incorporado al servicio de O365 para proteger los *tenants*.

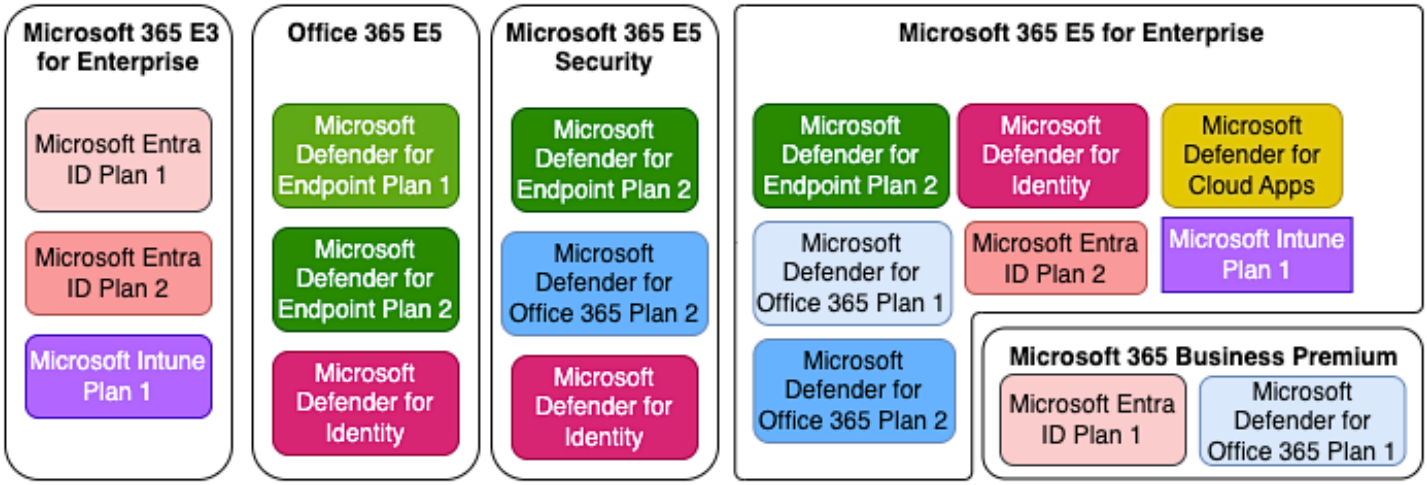
Herramienta	Descripción
Microsoft Defender for Office 365	Aporta protección integrada para prevenir, detectar, investigar y dar respuesta a amenazas sobre las herramientas de colaboración y correo de Office 365.
Microsoft Defender for Endpoint	Mantiene los dispositivos empresariales protegidos detectando y tomando acción de manera continua, contra eventos que intenten vulnerar la seguridad de los mismos.
Microsoft Intune	Realiza la gestión de dispositivos, incluyendo el ciclo de actualizaciones de sistema operativo y aplicaciones, y controla lo que se instala en ellos. Mantiene los equipos en un estado esperado bajo una línea base de seguridad establecida, lo que permite tomar acción para los dispositivos que no están alineados a la misma.
Microsoft Entra ID	Gestiona el ciclo de vida de las identidades de usuarios, dispositivos y aplicaciones, integra herramientas que añaden seguridad a las cuentas y al proceso de autenticación, como lo es MFA y acceso condicional.
Microsoft Defender for Identity	Monitorea y detecta amenazas a través de señales generadas por las identidades para protegerlas y reducir la superficie de ataque.
Multifactor Authenticator	Fortalece la autenticación, añadiendo métodos al tradicional usuario y contraseña para validar la identidad de un usuario al momento de autenticarse, lo cual brinda mayor seguridad al no depender de un único método de validación.
Microsoft Defender for Cloud Apps	Brinda protección para las aplicaciones empresariales y sus datos.

Planes de licenciamiento y opciones de seguridad

Es posible que algunas de las herramientas previamente mencionadas ya existan dentro de los planes de licenciamiento contratado por su empresa, lo cual no significa que se este aprovechando todo su potencial, y que se encuentran a la espera de ser implementadas como parte de una lista de deseos para reforzar la estrategia de seguridad de la empresa.

Microsoft ofrece distintos tipos de licenciamiento de acuerdo a las necesidades y las características que se requieran implementar basado en la postura de seguridad, el licenciamiento es basado en suscripciones que engloba diferentes planes de productos o suscripciones individuales para productos específicos.

A continuación, se resumen las suscripciones Microsoft 365 y Office 365, populares en el mercado al momento de publicar el presente artículo. Cada suscripción incluye un conjunto de planes, productos y herramientas de seguridad:



Suscripciones grupales y planes de seguridad Microsoft

Cada elemento contenido en una suscripción debe desglosarse para poder entender el potencial de las herramientas disponibles, tal como se muestra en el cuadro a continuación:

Producto	**Plan 1**	**Plan 2**
Entra ID	• Conditional access • MFA • Password protection	• Risk-based conditional access • Identity protection
Defender for Endpoint	• Next gen protection • Mobile threat protection • Defender for cloud app integration • Web content filtering	• Advanced hunting • Endpoint detection and response • Threat analytics • Vulnerability management • Endpoint advanced notifications
Defender for Office 365	• Advanced anti-phishing • Exchange online protection • Safe links • Safe attachments	• Automated investigation and response • Threat tracker • Threat explorer • Compromised user detection
Intune	• Device management • Application management • Configuration manager • Endpoint analytics	• Advanced app management • Advanced endpoint analytics • Endpoint privileges management • Remote help
Defender for Identity	• Identity threat detection (ITDR) • Identity suspicious activities across the cyber-attack kill-chain • Detect threats across modern identity environments	
Defender for Cloud Apps	• Continuous threat protection in eXtended detection and response (XDR) • App-to-app protection • Information protection • SaaS security posture management	

Microsoft también ofrece las suscripciones anteriores para que puedan ser adquiridas por separado, para complementar un plan con una suscripción existente.

Proyectos de aseguramiento de O365

En esta sección se expone una iniciativa de protección liderada por SITES para uno de sus clientes, con el objetivo de ayudar a los interesados a que tengan una idea bastante cercana a la realidad del tiempo y esfuerzo necesario para proteger un tentant de O365.

Perfil de la empresa

Centro de Servicios Compartidos: SSC, Co.

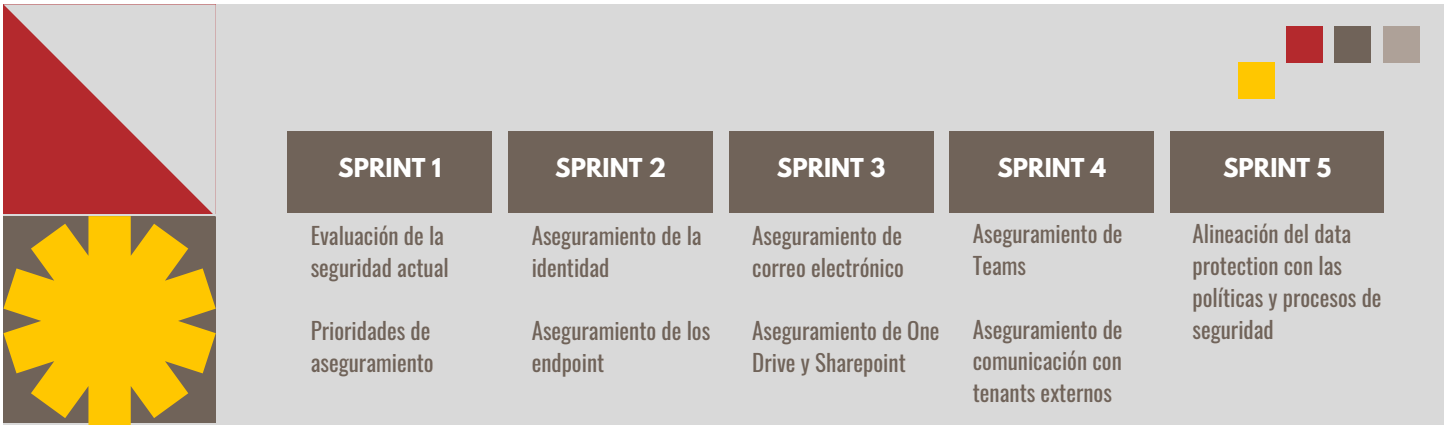
Tamaño del equipo	130 personas
Ubicaciones de acceso	Oficinas propias, oficinas de clientes en distintos países de América Latina, ubicaciones públicas (aeropuertos, centros de convenciones, hoteles y similares), oficina de casa y en el camino.
Dispositivos de acceso	Equipo portátil (Windows, MacOS), teléfonos y dispositivos móviles de la empresa (iOS).

Aplicaciones de ofimática y colaboración utilizadas

Las operaciones de SSC, Co. requieren del uso de las aplicaciones de oficina (Word, PowerPoint y Excel) y aplicaciones de colaboración (Teams, SharePoint y OneDrive) disponibles en la licencia de O365 para empresas tipo E5. Las aplicaciones de O365 son accedidas desde sus interfaces Web, programas descargables y aplicaciones para dispositivos móviles.

Ruta de protección para O365

El servicio de protección para O365 con las soluciones suministradas por Microsoft, fue atendido por un equipo de especialistas autodirigido, apoyado por un Scrum Máster. Las funcionalidades de seguridad que SSC, Co. seleccionó se liberaron gradualmente, en sprints de tres semanas, siguiendo la ruta que se describe en el siguiente diagrama. Cada sprint representado en la ruta contiene múltiples historias, las cuales fueron ajustadas para responder a las necesidades de la organización.



Durante la ejecución de dichos sprints el equipo de SITES se mantuvo en comunicación con el equipo de administradores de O365 de SSC, Co. a quienes se les hizo participes del proceso de aseguramiento, debido a su rol en la gestión de seguridad del mismo.

La comunicación fue necesaria no solo durante la fase de planeación sino también durante la implementación, lo que permitió a SITES entender claramente el rubro de trabajo del cliente, su modelo de negocio, el dimensionamiento de la empresa, el nivel de implementación de sus políticas y procesos de seguridad para la nube, así como la disponibilidad y experticia del equipo de seguridad de SSC, Co. En resumen, el trabajo colaborativo tuvo como resultado configuraciones de seguridad a la medida de SSC, Co.

Equipo Scrum para la entrega del servicio

La entrega del servicio de aseguramiento de un tenant de O365, involucró a un equipo de trabajo multidisciplinario integrado por SITES y SSC, Co. El marco seleccionado para gestionar el trabajo fue Scrum, lo que permitió a SITES dar una respuesta eficiente a las diferentes necesidades de adopción del servicio de seguridad de O365 que se atendieron a lo largo del proyecto. Los roles que contribuyeron a alcanzar el objetivo se listan en la tabla siguiente:

Roles	Contribución	Habilidades
Scrum Máster	Apoya al equipo a superar las barreras o impedimentos que pudieran presentarse en la ejecución del plan de aseguramiento del tenant, a fin de que puedan alcanzarse los objetivos dentro de los plazos establecidos en el sprint.	• Comunicación asertiva • Pensamiento estratégico • Colaboración • Gestión del estrés • Planificación y organización • Facilitador en el manejo de problemas y conflictos
Dueño del Producto	Es el punto de contacto con el cliente y es el responsable de tomar los requerimientos para trasladarlos al plan de aseguramiento del tenant, así como al equipo implementador, y también velar por que en la ejecución se respeten los intereses del cliente (administración de backlog).	• Escucha activa • Comunicación asertiva • Negociación • Facilidad en la toma de decisiones • Liderazgo • Pensamiento critico
Ingeniero de Nube	Aporta los conocimientos de administración de la nube, en este caso la nube de Microsoft, que permitirán al equipo determinar la estimación de esfuerzos en la ejecución del sprint en base al orden y las dependencias de las configuraciones involucradas en cada historia.	• Dominio de administración de la nube Microsoft sus productos y servicios • Comunicación asertiva • Responsable • Anticipación de escenarios
Ingeniero de Seguridad	Contribuye a determinar la estimación de esfuerzos en la ejecución del plan de aseguramiento del tenant a la luz de sus conocimientos en seguridad, para alinear la ejecución del proyecto con las mejores prácticas de seguridad para la nube de acuerdo con el modelo de servicio del cliente.	• Dominio de las practicas de seguridad en la nube • Anticipación de escenarios • Resolución de problemas • Pensamiento analítico
Analista de Riesgos	Trae a la mesa los conocimientos de análisis, identificación, gestión y mitigación de riesgos, de modo que la ejecución del plan de aseguramiento contemple la reducción de los riesgos existentes en la nube del cliente.	• Pensamiento analítico • Anticipación de escenarios • Manejo y análisis de datos
Soporte Técnico a Usuarios	Apoya con la instalación y configuración de software en equipos de usuario final y servidores de acuerdo a la demanda del proyecto.	• Resolución de problemas • Pensamiento analítico • Comunicación asertiva

Proceso de protección de O365

Requisitos

Solicitar un servicio de protección para un tenant de O365, implica proporcionar acceso a las configuraciones del tenant al agente que realizará la evaluación y/o el aseguramiento; esto no significa que deba creársele un usuario permanente en el tenant. Otro aspecto a tener presente, es conocer el licenciamiento inicial, para determinar las capacidades de protección con que cuenta la empresa y tener clara la prioridad de protección, para no incurrir en un “big bang” que sea difícil de gestionar a nivel de cambio organizacional.

Pasos requeridos

1. Inventario de licenciamiento de la situación actual
2. Identificar prioridades y documentar incidentes activos
3. Integrar equipo de trabajo con administradores de seguridad y nube
4. Estimar el tiempo requerido para implementar la ruta de protección
5. Establecer la linea de base de seguridad luego de las protecciones
6. Actualizar le mapa de calor de riesgos y documentar el riesgo residual

Roles de seguridad de O365

En la nube de Microsoft los actores que participan de la estrategia de defensa equivalen a los “Roles”, en especial los roles de seguridad y administración de servicios. Antes de implementar un programa de protección, las empresas deben tener claridad de su alcance e importancia, para

delegar la responsabilidad asociada a los mismos durante la implementación y labor de operación posterior.

Rol	Descripción	Habilidades
Global Admin	Administrador Global del tenant de Microsoft, implícitamente cuenta con acceso de administración a las herramientas de Seguridad de Microsoft.	Conocimientos avanzados de todo el stack de productos y servicios de Microsoft 365.
Security Administrator	Administrador global de toda la solución de seguridad dentro del tenant de Microsoft.	Conocimiento avanzado de Seguridad y de todas las herramientas de seguridad de Microsoft.
Security Operator	Gestiona eventos y reportes de seguridad del tenant.	Alto grado de comprensión sobre las diferentes técnicas de hacking y que sea capaz de analizar los eventos para actuar de manera oportuna.
Security Reader	Permisos de lectura de información y reportes referidos a eventos de seguridad.	Conocimiento del portal de administración de seguridad de Microsoft y comprensión básica de eventos de seguridad y procesos de escalamiento.
Exchange Administrator SharePoint Administrator Teams Administrator	Administra todos los aspectos de cada servicio de colaboración y correo, cada portal de administración puede contener diferentes apartados de seguridad que es necesario configurar.	Conocimiento del funcionamiento de cada servicio y como se integran las herramientas de colaboración y correo de Microsoft O365.

Servicios de apoyo

SITES ofrece un abanico de servicios asociado a la protección de un tenant de O365 de: análisis, asesoría de aseguramiento y/o administración de correo electrónico, herramientas colaborativas (Sharepoint, Teams y One Drive), inicios de sesión, equipo de usuario final, identidad, entre otros.

Información de contacto

Para asesoría en este tema

www.sitescorp.com | Alameda Manuel Enrique Araujo, Calle Nueva 1, Edificio PALIC 4a Planta | +503 2250-2800 | info@sitescorp.com.sv