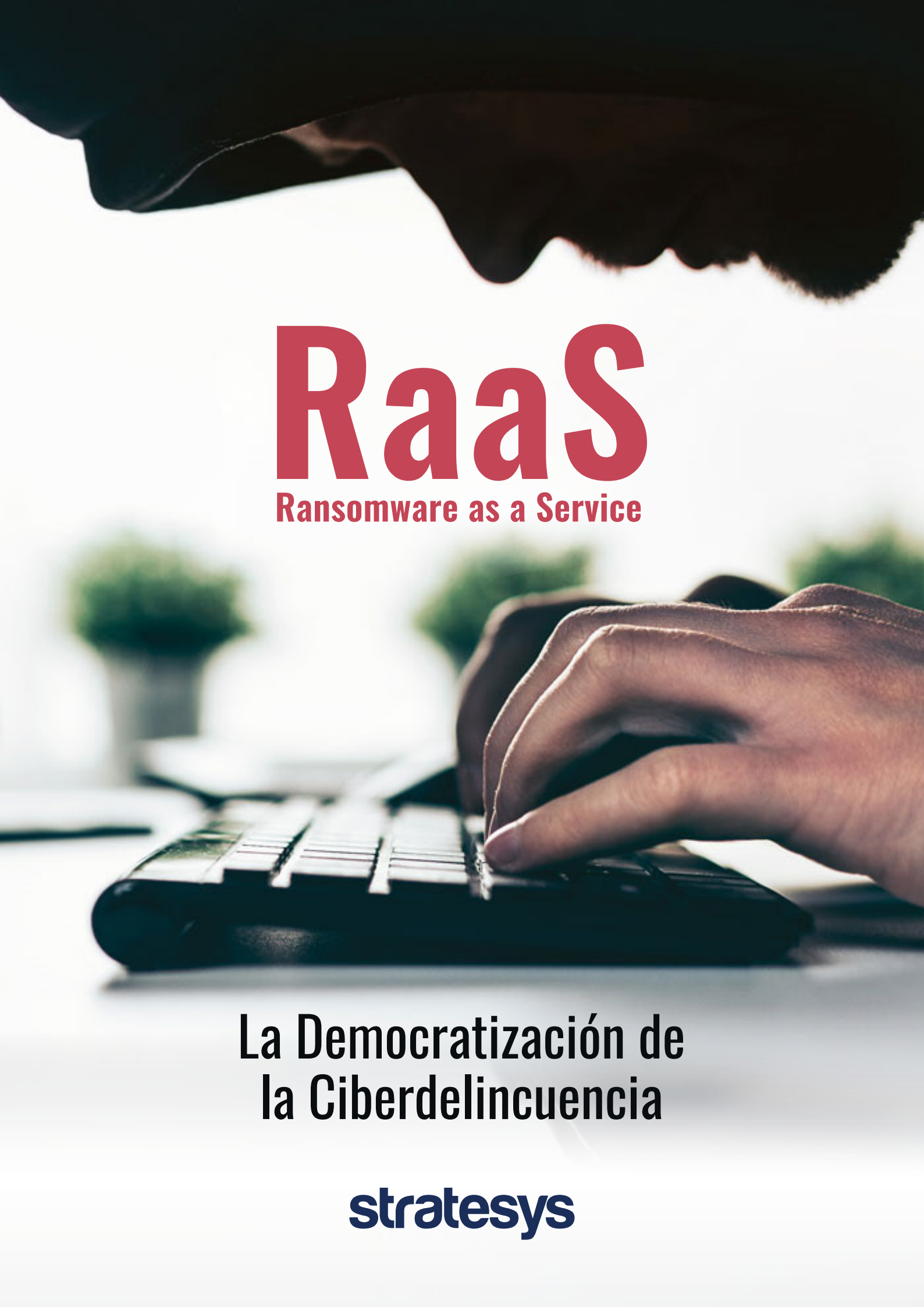


RaaS

Ransomware as a Service

La Democratización de la Ciberdelincuencia

stratesys

Para comprender mejor el alcance de este problema, empezaremos por aclarar que el RaaS es un tipo de servicio que ofrece kits de malware con instrucciones detalladas de uso, que permiten desplegar un ataque de ransomware a cualquiera que las adquiera. Es decir, es muy probable que individuos que tal vez no tengan la habilidad ni los medios técnicos para elaborar ataques avanzados, puedan conseguir las herramientas necesarias para llevar a cabo este tipo de ataques de forma económica y sencilla, en unos pocos clics.

¿Cómo se produce un ataque de RaaS?

Todo empieza cuando grupos organizados de ciberdelincuentes con conocimientos avanzados de informática, redes corporativas y malware, desarrollan este tipo de programas maliciosos y los ponen a disposición de quien quiera adquirirlos a través del mercado negro (la Deep Web) con todo tipo de detalle e instrucciones de uso.

A partir de ese momento, cualquier individuo u organización con malas intenciones puede adquirirlo y perpetrar un ataque de ransomware contra su objetivo.

Lo primero que buscarán estos individuos será encontrar la puerta de entrada a su objetivo. Habitualmente, este tipo de ataques comienzan con la ayuda humana de la propia víctima y el phishing a través del correo electrónico sigue siendo el vector de ataque más sencillo y al mismo tiempo más fructífero; a través de técnicas de ingeniería social, consiguen engañar a los usuarios e infectar uno o varios

equipos de la víctima y a partir de ahí, el propio programa malicioso que han adquirido hace el resto: el ataque se va extendiendo por toda la red de la empresa, identificando y exfiltrando información confidencial, encriptando archivos y bloqueando el acceso legítimo a los sistemas, de forma que estos quedan totalmente inoperativos.

Una vez conseguido el objetivo de comprometer los sistemas de la víctima, el atacante tratará de sacar un beneficio económico utilizando la extorsión.

Normalmente se ponen en contacto con la víctima a través del correo electrónico, es habitual que contacten directamente con miembros del Comité de Dirección si se trata de una gran Compañía, y les informan de que si quieren recuperar el acceso y la operativa de sus sistemas deberán pagar un rescate, en criptomonedas, para evitar dejar ningún rastro que pueda poner en peligro su identidad.

Las empresas víctimas de este tipo de ataques NUNCA deberían plantearse ceder al chantaje y pagar el rescate.

Primero de todo, porque de esta manera se estaría contribuyendo a fomentar este nuevo tipo de terrorismo, y por otro lado porque nadie les puede asegurar que los criminales vayan a desaparecer sin más; los ciberdelincuentes han desarrollado técnicas de persistencia para mantener el acceso a los sistemas infectados, ya sea a través de la manipulación de herramientas legítimas de la red o configuraciones en los sistemas, dejando abiertas a través de las que poder recuperar el acceso y volver a repetir el ataque cuando ellos lo deseen.

Consecuencias del RaaS

El impacto que puede tener un ataque de Ransomware sobre una compañía es incalculable. No solo se trata del pago del rescate (algo que NUNCA deberían hacer las empresas), sino del impacto económico directo asociado a la pérdida de operativa del negocio durante el tiempo que tarde en recuperarse, y el indirecto por el impacto negativo que el ataque puede tener en la imagen de marca de la compañía, en sus clientes, por las multas o sanciones regulatorias si fuera el caso, etc.

Además, hay que tener en cuenta que cuando el objetivo de los ataques de RaaS son instituciones o servicios públicos, la ciudadanía en general también se ve afectada.

Hemos sufrido recientemente el ataque al SEPE, que afectó a miles de ciudadanos que no podían cobrar sus pensiones en plena pandemia. También algunos ayuntamientos, universidades e incluso HOSPITALES han sido afectados por este tipo de ataques, viendo cómo sus sistemas se quedan bloqueados durante semanas y teniendo que cancelar, por tanto, consultas y cirugías ya programadas.

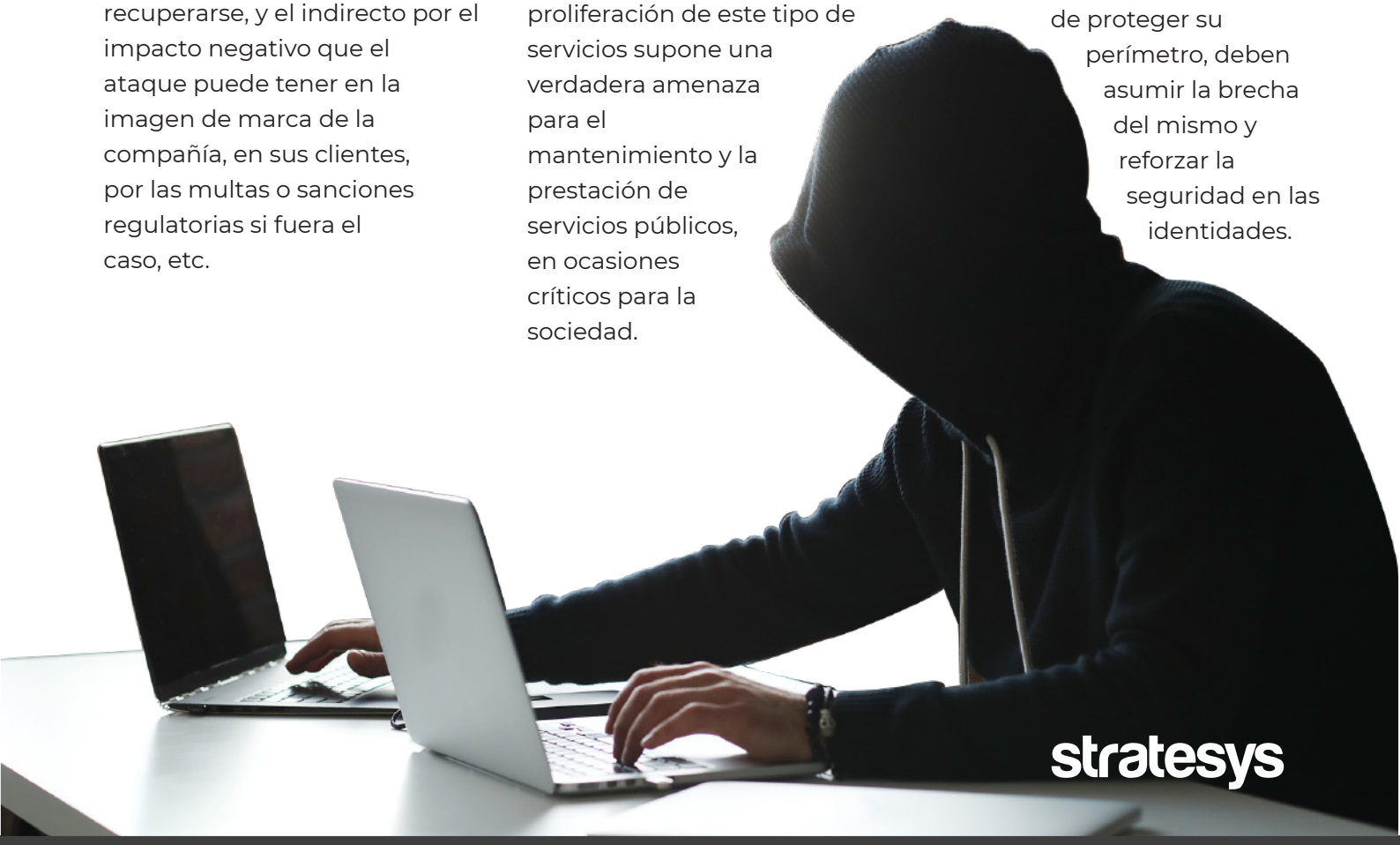
Por lo tanto, es importante reseñar que las pérdidas económicas son una de las consecuencias más graves para las empresas y que la proliferación de este tipo de servicios supone una verdadera amenaza para el mantenimiento y la prestación de servicios públicos, en ocasiones críticos para la sociedad.

¿Cómo estar preparado frente a este tipo de ataques?

1. Adoptar una filosofía ZERO TRUST y reforzar los servicios Cloud

Zero-Trust supone un cambio en la mentalidad de las empresas, eliminando los conceptos de “zona segura” dentro del perímetro o red interna y “zona insegura” en el exterior.

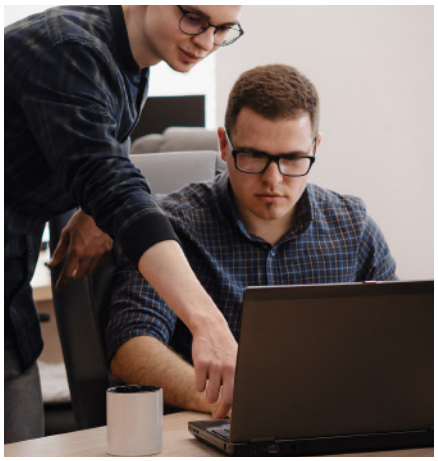
Con la proliferación del Cloud y el uso de servicios descentralizados, el perímetro se ha difuminado y ha dejado de tener sentido tratar de basar la seguridad SOLO en él. En cambio, las empresas, además de proteger su perímetro, deben asumir la brecha del mismo y reforzar la seguridad en las identidades.



Esto supone verificar la “triada” usuario + dispositivo + contexto para cada acceso o transacción ocurrido en nuestros sistemas o plataforma tecnológica, por ejemplo, con políticas de acceso condicional o el uso de MFA.

También se deben proteger los accesos y credenciales privilegiadas, otorgando los accesos mínimos tanto en privilegios como en duración (lo que se conoce como Just-Enough-Access y Just-In-Time). El rotado frecuente de este tipo de credenciales es también esencial.

En este sentido, muchas organizaciones necesitan revisar su estrategia de ciberseguridad y adaptarla a los tiempos que corren.



2. Sensibilización de empleados frente a ataques de Ingeniería Social

Los usuarios son la primera barrera de protección de las empresas, su “firewall humano”, y es clave realizar actividades de sensibilización y capacitación en ciberseguridad, particularmente en ingeniería social (ataques dirigidos a las personas).

Una buena opción es comenzar con una simulación de ataque de phishing entre los empleados y en base a los resultados, definir un plan de formación y concienciación básica.

3. Mantener actualizados los sistemas y ponerlos a prueba de forma periódica o constante con RED TEAM

Mantener la plataforma tecnológica al día significa gestionar de forma apropiada y continua las vulnerabilidades de esta. Esto es esencial para evitar que los atacantes puedan detectar y explotar vulnerabilidades conocidas en la misma.

Por otro lado, los ejercicios de seguridad ofensiva (Hacking Ético, Pentesting, Red Team) se hacen cada vez más necesarios para poner a prueba y entrenar tanto las medidas técnicas como a los equipos de detección y defensa de las empresas.

4. Estar preparado para una rápida recuperación

El nivel de preparación y trabajo PREVIO a sufrir un ataque de ransomware determinará el tiempo de recuperación de los sistemas e información, y por tanto el impacto económico en las empresas.

Es fundamental contar con una estrategia definida y herramientas de respaldo y recuperación que se ajusten a las necesidades del negocio (Recovery-Time-Objective y Recovery-Point-Objective). Estas estrategias (3-2-1-1-0) deben incluir copias de los datos importantes para el negocio en diferentes soportes y el almacenamiento y protección de algunas de ellas en servicios Cloud como Azure, de forma que pueda recuperarse o levantarse la infraestructura necesaria si se han visto afectados los servicios onpremise.

stratesys

stratesys

ÁNGEL GARCÍA PALOMO
Executive Manager
Resp. Línea Microsoft
stratesys

JAVIER CASTRO BRAVO
Associate Director
Resp. Línea Ciberseguridad
stratesys

Microsoft Partner
Microsoft

Gold Cloud Platform
Gold Data Analytics
Gold Data Platform
Gold Application Development
Gold Application Integration
Silver Datacenter

¿Cómo podemos ayudarte?

Las organizaciones deben adoptar un enfoque de seguridad integral para evitar la amenaza de la nueva economía de ransomware.

Desde Stratesys podemos ayudarte con nuestros servicios de consultoría especializados en ciberseguridad

Pregúntanos en **ciberseguridad@stratesys-ts.com**

Servicios de seguridad ofensiva

Contamos con un equipo de hackers éticos especializados en servicios de Red Team, ejercicios de Hacking Ético a infraestructura y pentesting web y de aplicaciones.

Formación y concienciación de empleados

Pregúntanos por nuestros servicios de simulación de ataques de phishing ético, podemos organizar una simulación gratuita.

Planes estratégicos de Ciberseguridad

Te ayudamos a evaluar tus capacidades de ciberseguridad y a adaptar tu estrategia a las nuevas tecnologías y servicios cloud.

Continuidad de negocio y resiliencia operativa

Pregunta por nuestros servicios de infraestructura, smart storage y disaster recovery que proporcionamos a través de BESH, nuestra división especializada en soluciones de Data Center.

Servicios de seguridad orientados a Microsoft Azure

- **Microsoft 365 Defender**
  Le ayudará a detectar ataques en las identidades, puntos de conexión, aplicaciones, correos electrónicos, datos y aplicaciones en la nube con funciones XDR.
- **Microsoft Sentinel**
  Es la herramienta de administración de eventos e información de seguridad (SIEM) nativa de la nube de Microsoft. Agrega los datos de seguridad de prácticamente cualquier fuente y aplica la IA para separar el ruido de los eventos legítimos, correlacionar las alertas a través de complejas cadenas de ataques y acelerar la respuesta a las amenazas.
- **Microsoft Defender for Cloud**
  Le ayudará a proteger sus cargas de trabajo en nubes múltiples e híbridas con capacidades XDR integradas, además de proteger sus servidores, almacenamiento, bases de datos, contenedores, etc...