itera
it & business process

Microsoft Partner

Microsoft

Gold Desarrollo de aplicaciones
Gold Data Analytics
Gold Cloud Platform
Silver Application Integration

CLOUD SECURITY POSTURE

www.iteraprocess.com

CONTENIDO

¿Qué es Security Posture?

La postura de seguridad es algo que debemos tener siempre presente y ser conscientes del suelo que pisamos, sobre todo en estos tiempos. La postura de seguridad no es solo tener el conocimiento sobre cuales herramientas contamos sino también saber cómo están configuradas las soluciones, cada cuanto se actualizan, cómo trabaja en conjunto toda nuestra infraestructura.

Y, una vez conociendo todo ello, deberíamos preguntarnos si con lo que tenemos respaldando nuestra infraestructura es suficiente para poder defendernos de lo que está sucediendo allá afuera.

5 preguntas fundamentales para evaluar tu postura de seguridad

1. ¿Cuáles son los activos más valiosos de tu empresa?
2. ¿Conoces tu postura ante la Ciberseguridad de hoy?
3. ¿Son efectivos los controles de seguridad actuales?
4. ¿Tienes conocimiento de las últimas amenazas potenciales?
5. ¿Estás realizando la inversión adecuada para garantizar la resiliencia cibernética?

¿Cómo es posible medir esa postura?

Antes que nada, la primera palabra clave es: visibilidad. Posteriormente, podemos voltear para ver cómo es que protegemos todo aquello que sabemos que existe y, más adelante, dar paso al cómo reaccionamos.

¿Por qué es crítica la visibilidad?

La visibilidad es crucial, puesto que es imposible monitorear o proteger dispositivos e información que no puedes conocer.

Los enfoques de seguridad implican múltiples productos puntuales, procesos de cambio manual, políticas y datos monolíticos. Debido a esto, los activos críticos pueden pasarse por alto, lo que resulta en un informe incompleto.

En esta situación, es difícil orientar correctamente los análisis de vulnerabilidades y las evaluaciones de riesgos. Además resulta particularmente problemático para cubrir activos no tradicionales (como dispositivos personales, IoT, activos móviles y servicios en la nube).

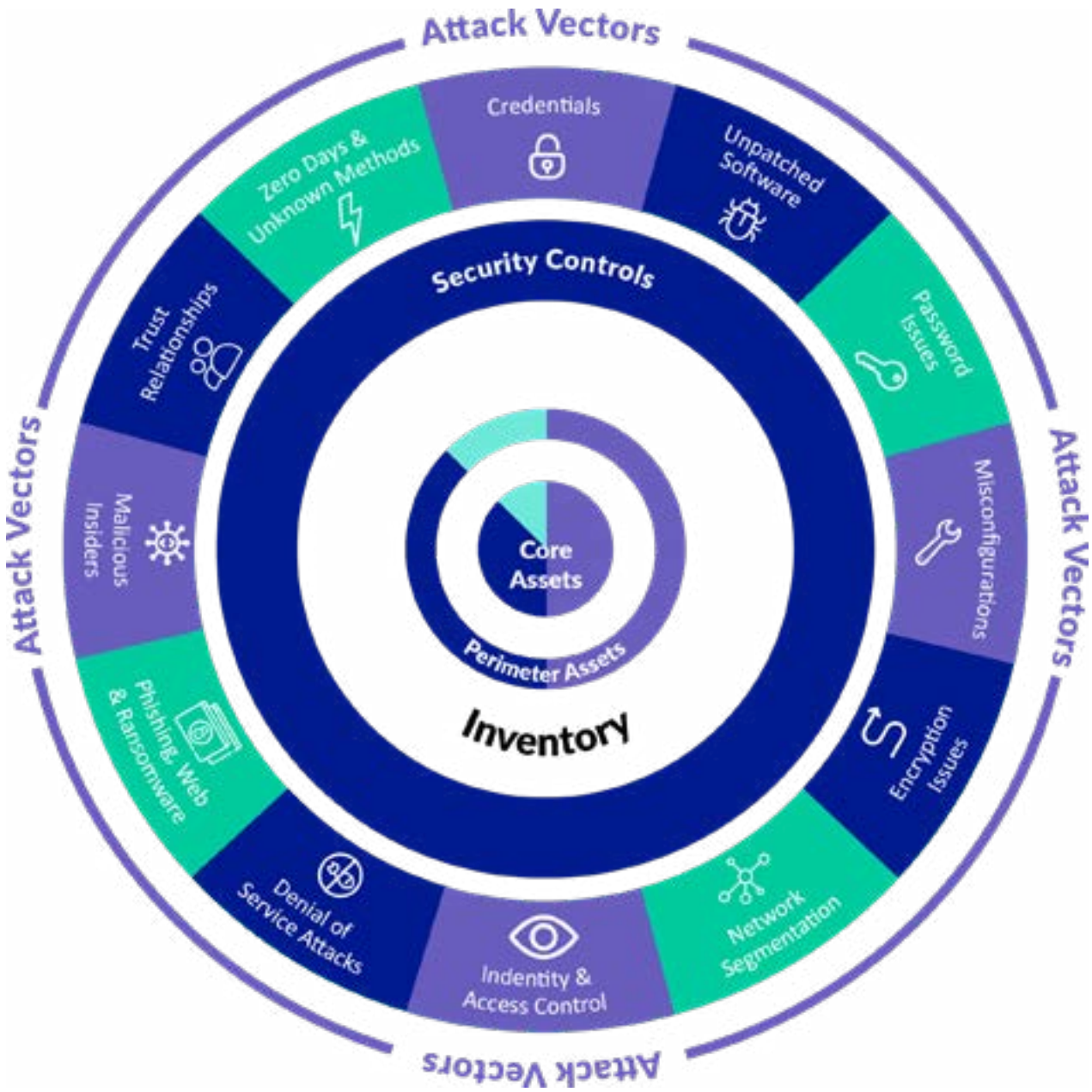
Profundicemos un poco: uno de los puntos más críticos por los que todos hemos sufrido y seguramente padeceremos en un futuro, suele ser el tema de tener un inventario completo de la infraestructura. Siempre nos faltan PC que están apagadas o laptops en un cajón que se vuelven a encender semanas después, servidores temporales o de ambientes no productivos que se crearon para alguna actividad en específico, pero por alguna razón aún no son eliminados o retirados de la red.

Todos estos activos pueden presentar un riesgo potencial debido a que no se les actualiza correctamente programas o parches a nivel de sistema operativo. Pero si esto lo extendemos más allá podríamos hablar de temas de red, por ejemplo: siempre hay reglas en los firewalls que fueron de prueba y no se eliminaron, o bien rangos muy amplios que se abrieron y no se documentaron correctamente, como tampoco fueron depurados en algún proceso de recertificación de reglas.

Pero la idea de todo esto principalmente es siempre tener a la vista los Core Assets, o como los conocemos comúnmente, *las joyas de la corona*. Estos son los activos sobre los cuales siempre tenemos que vigilar y poner mayor atención acerca de lo que está pasando en ellos y en su entorno.

Después, tenemos alrededor la capa de protección, en ella colocamos todas las políticas de seguridad, las configuraciones de hardening, governance y también las soluciones de seguridad que protegen dichos assets. Ahí van el antivirus, firewalls, DLP y demás soluciones que hayamos adquirido para proteger la infraestructura.

Y en cuanto al entorno de monitoreo, resulta muy importante contar con SIEMS, soluciones que proactivamente te mantienen en alerta y en simulación de lo que ocurre constantemente dentro y fuera de tu infraestructura.



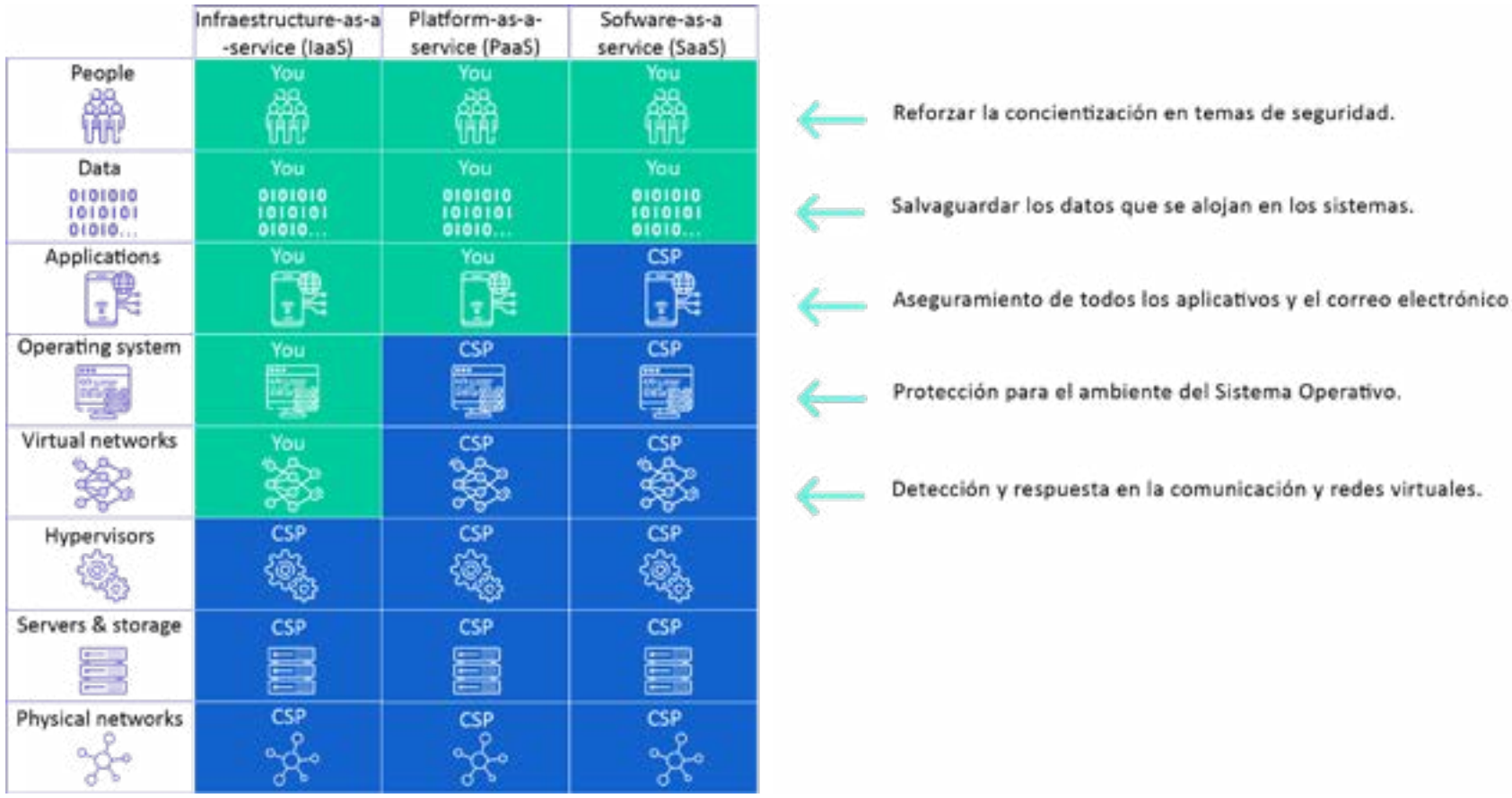
Ahora viene lo interesante: alrededor de todos esos assets tenemos 12 diferentes tipos de vectores de ataques. Y hay que poner especial atención en ello, porque no son 12 maneras diferentes de atacar, sino 12 categorías dentro de las cuales existen diversas formas o medios que buscan de cualquier manera posible hacerles daño a las empresas, a la operación y a sus activos.

Peligro latente

Con miles de activos en tu empresa y cada uno susceptible a a diferentes vectores de ataque, hay millones de formas en las que tu organización puede ser violada.

Tan solo la mala higiene de ciberseguridad, como una débil contraseña o un sistema expuesto a Internet sin parches, es una puerta abierta para los atacantes.

Responsabilidad compartida



En este punto enfoquémonos en la tecnología cloud.

La nube nos ha vendido el tema de que es un ambiente no solo económico y escalable, sino también muy seguro. Y de cierta forma es verdad, solo tenemos que analizar a qué se refieren cuando se habla de seguridad. La nube es segura en las redes físicas, en los hostings y sus métodos de almacenamiento, así como en los hypervisores. Y justo a partir de ahí es donde empezamos a marcar la línea de responsabilidad.

Si utilizamos un ambiente IAAS, somos responsables de las Redes virtuales, del sistema operativo, de las aplicaciones (al igual que en ambiente PAAS). Por último, los datos y la gente que ocupa los ambientes de nube.

A todo esto, le llamamos responsabilidad compartida. Los proveedores de nube son responsables de cuidar la funcionalidad, estabilidad y seguridad de una parte de la nube, pero también nosotros somos responsables de la otra parte que ocupamos.

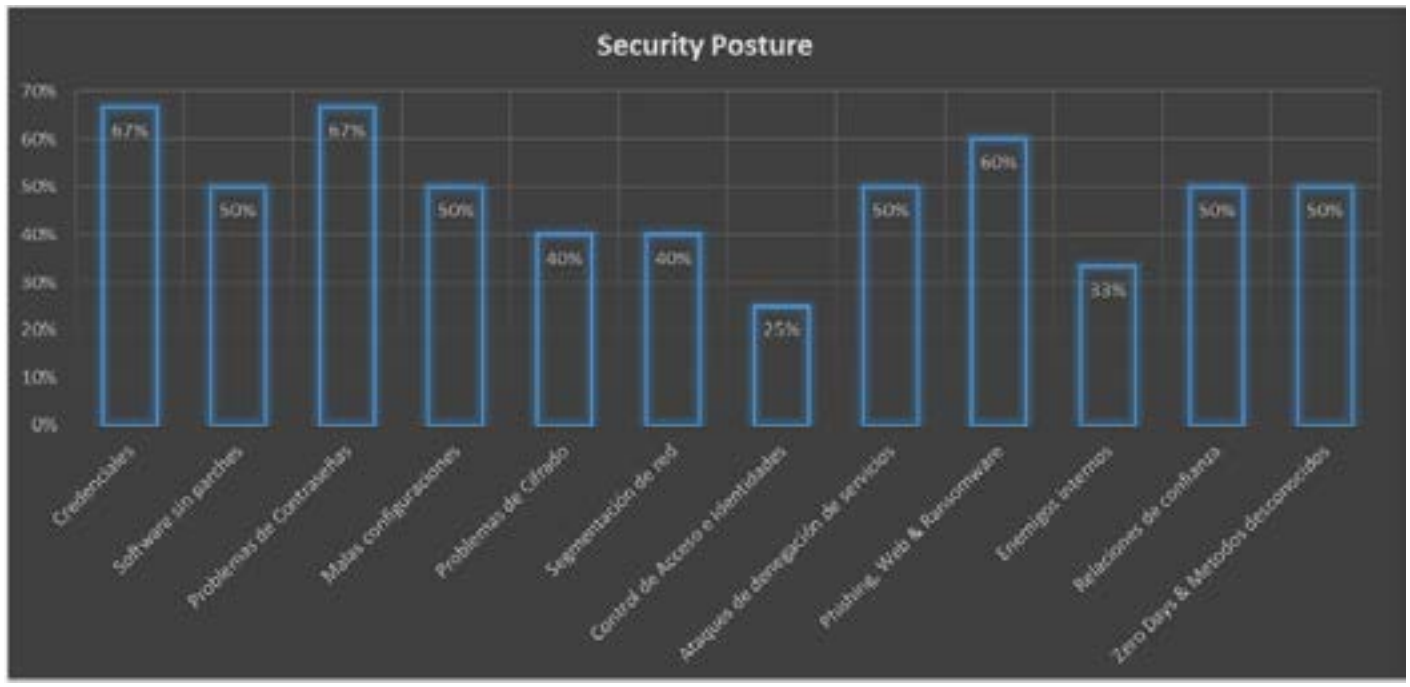
Volviendo al punto de la postura de seguridad: ¿estamos protegiendo correctamente las redes virtuales, el sistema operativo, las aplicaciones, los datos y la gente ante dichos vectores de ataque?

¿Cómo nos impacta en la nube?

Empecemos a hacer un match entre esos puntos de los que somos responsables y los vectores de ataque que existen en Internet.

- Problemas de cifrado: la información que almacenamos tanto de nuestra empresa, de los clientes o la misma información en tránsito muchas veces no se encuentra cifrada.
- Credenciales: políticas poco robustas para proteger las credenciales de acceso o problemas por parte de los usuarios para almacenarlas de forma segura.
- Acceso e Identidades: monitoreo de acceso a las instancias o información, validación periódica de accesos privilegiados y no privilegiados de usuarios.
- 0 Day: todos aquellos ataques a los que nadie está preparado para protegerse o contener en caso de un incidente de seguridad.
- Software sin Parches: es un software que muchas veces no sabemos en qué versión se encuentra o ni siquiera que está instalado en la infraestructura.
- Problemas de Contraseñas: contraseñas inseguras, reutilizadas o compartidas.
- Malas Configuraciones: errores en configuraciones, no solo en servidores, redes o aplicaciones mal configuradas, sino también en una posible mala configuración en los dispositivos de seguridad.
- Phishing, Web & Ransomware: las agresiones más comunes o preferidas por los hackers para ser utilizadas al inicio de un ataque o para secuestrar información.
- DDOS: ataques en los cuales buscan que nuestros servicios sean totalmente inoperables.

En resumen, esta tabla muestra todo aquello en lo que somos vulnerables hoy en día, ¿interesante, no es así?



El desafío para tener una comprensión precisa de la postura de seguridad, proviene de 4 factores:

1. Falta de visibilidad
2. Falta de estructura
3. Falta de claridad
4. Falta de datos actualizados

4 claves acerca de la postura de seguridad de tu organización

1. Enfoque orientado a proyectos

La postura de seguridad actual de la mayoría de las organizaciones consiste en herramientas que se han implementado como resultado del abordaje de proyectos de seguridad. Este enfoque de seguridad orientado a proyectos es uno donde los equipos solo se concentran en completar proyectos de seguridad fuera de las listas de tareas pendientes, sin tener una idea real sobre si estos proyectos tienen o no un impacto significativo en la postura de seguridad de la organización. Lo cual deriva en prácticas con un enfoque bastante limitado.

2. Tácticas reactivas

Casi todos los nuevos gastos y esfuerzos de seguridad están dirigidos a detectar un ataque en progreso o respondiendo a uno que ya ha ocurrido. Mientras se apagan los "incendios" de seguridad es una práctica esencial, pero la mayor parte de tus inversiones en seguridad no deberían ser reactivas.

3. No estar alineados con los vectores de ataque

¿Estás gastando la mayor parte de tus esfuerzos de seguridad en arreglar los indicadores de compromiso (IoC)? Sin saber realmente las respuestas a preguntas como: ¿cuáles de tus activos son más críticos? ¿Qué amenazas están activas en este momento? O ¿cuáles de tus activos son más vulnerables? Continuar dedicando tiempo, recursos y presupuesto para solucionar problemas sin tener una comprensión clara de cómo esas acciones reducen el riesgo cibernético general de la empresa, definitivamente no es fructífero. Tus prácticas de seguridad existentes deben evaluarse con una perspectiva nueva para comprender tu postura de seguridad actual, encontrar brechas y luego tomar medidas para cerrarlas.

4. Lejos del cumplimiento y de las mejores prácticas

No contar con una guía de cientos de reglas listas para usar, las cuales corresponden con los estándares de cumplimiento de la industria y con las mejores prácticas de seguridad, te aparta para resolver rápidamente las vulnerabilidades. Esa guía además te permite dar cumplimiento ante auditorías al reportar una infraestructura segura.

Tu primera línea de defensa contra el adversario es una buena postura de ciberseguridad

itera
it & business process

¡Hagamos que suceda!

www.iteraprocess.com

info.mx.df@iteraprocess.com

info.pe.li@iteraprocess.com

info.co.bog@iteraprocess.com

info.es.mad@iteraprocess.com

info.cl.sant@iteraprocess.com