BLUEPRINT PARA ASEGURAR SU RED

Objetivo

Si desea mejorar la postura de seguridad de su red, pero no sabe cómo empezar, esta guía es para usted. Aquí podrá encontrar las áreas clave y recomendaciones que debe considerar dentro de su estrategia de ciberseguridad.

Visión General

El propósito de esta guía es brindar una descripción general de las áreas que debe tomar en cuenta al momento de implementar o revisar la postura de ciberseguridad de su entidad. De modo que no pase por alto alguna pieza crítica del rompecabezas a la hora de revisar o armar su arquitectura de seguridad de redes.

Con este enfoque, deseamos proporcionarle herramientas que le permitan conocer un listado de verificación de alto nivel para garantizar que se hayan abordado los componentes de seguridad más importantes, ya sea que estos sean o no elegidos dentro de la arquitectura.

Esta guía le brinda una referencia para cualquier red, esto se logra al reflejarse contra un listado de niveles que le permitirá conocer la ubicación y madurez de su red en temas de ciberseguridad.

También proporcionará el conocimiento de que una seguridad de red efectiva no es solo una colección de piezas. Debe ser una serie de herramientas entrelazadas planificadas para minimizar la exposición de la red corporativa.

Todas las áreas y posibles controles de seguridad deben ser parte de su análisis y estrategia de ciberseguridad. Cada posible acceso o superficie de riesgo debe evaluarse para determinar el valor de riesgo de no implementarse un mecanismo de seguridad. Este análisis generalmente viene dado al considerar el costo de una solución versus el costo de recuperar los datos, así como el costo de no disponer del servicio durante el tiempo de recuperación.

Áreas a Proteger

En este análisis explore un poco más todas las áreas que están involucradas en la seguridad junto a los riesgos que surgen en torno a ellas y como puede ir incorporándolas dentro de su estrategia de ciberseguridad.

Física

La seguridad física es, tal cual su nombre se describe, controlar el acceso físico a la infraestructura crítica de TI. Sin embargo, muchas entidades poseen dispositivos de red en ubicaciones no propicias como armarios, escritorios o cuartos no adecuados como un centro de datos. La seguridad física puede abarcar desde algo tan simple como una puerta cerrada con llave o tan elaborada como incluir lector de huellas y cámaras de vigilancia.

Pero más allá del centro de datos, la seguridad física requiere una atención significativa a los detalles, incluyendo desde el acceso inicial a sus instalaciones. Algunos ejemplos incluyen, pero no se limitan a:

1) Control y monitoreo físico para acceder al centro de datos
2) Análisis de espacios de trabajo de los colaboradores, ej. Evitar que miradas indiscretas o a través de ventanas puedan tener acceso a monitores y espacios de trabajo de empleados.
3) Estacionamientos con vigilancia, ej. Para evitar se realicen procedimientos de entrega de paquetes trampas, como dispositivos USB infectados ubicados donde podrán ser vistos y recogidos por los empleados.

Por otro lado, mucho menos controlado, también tiene que tomar en cuenta actos naturales como incendios, inundaciones, terremotos, tornados, etc. Lo cual generalmente conlleva a contar con un sitio alterno o de contingencia que sea geográficamente separado y totalmente independiente del sitio principal, que se conecte solo para sincronizar datos, pero pueda operar de forma autónoma ante un caso de desastre del sitio principal.

Poseer un control adecuado del acceso físico a la infraestructura conlleva a que cualquier intento de ataque tendrá que llegar a nivel de red forzosamente, donde podrá ser detectado usando las herramientas de inspección de red que veremos más adelante.

Puntos clave a analizar

- Acceso a Edificio o Áreas Críticas de TI
- Continuidad de Negocio (Contingencia o DR)
- Privacidad de Estaciones de Trabajo
- Descarte de Documentos o Activos

Host

Se basa en la seguridad del host o estación de trabajo propiamente. Defina una política que detalle el manejo de estos activos desde su adquisición, su manejo, hasta el procedimiento de descarte del mismo. En la adquisición debe validar que no traiga software malintencionado instalado de forma oculta, esto se corrige al formatear por defecto el sistema operativo.

Dentro de la etapa de manejo, debe considerar las herramientas de seguridad que red que le brindarán un acceso seguro a las herramientas de negocio a la vez que pueda detener o bloquear tráfico mal intencionado.

Finalmente, durante la etapa de descarte, asegúrese de eliminar o borrar propiamente los discos para evitar una fuga no intencional de información.

Regresando y expandiendo la etapa de manejo, la cantidad de soluciones que implemente en sus estaciones estarán definidas por algunas preguntas como:

- ¿Acceden sus colaboradores información confidencial?
- ¿Los colaboradores pueden llevarse y utilizar sus equipos de trabajo desde afuera de la organización?
- ¿Comparten estos dispositivos entre varios colaboradores?
- ¿Qué tan valioso es el dato que pueda almacenarse en sus equipos?

En la medida que todas estas preguntas sean afirmativas, se debe considerar una herramienta de mitigación de amenazas avanzadas en la estación de trabajo, probablemente con algún tipo de cifrado de disco y algún servicio que permita conectividad segura a aplicaciones de negocio como SASE. Recuerde que un IDS o Antivirus basado en host es la protección mínima que sus estaciones de trabajo deben tener, por encima de esto existen módulos adicionales que expanden la seguridad y minimizan el riesgo de sufrir un ataque.

Algunas otras consideraciones son respaldo y la salud del equipo propiamente. Un respaldo será necesario si los usuarios trabajan mucho con archivos *offline* que no están gestionados por un repositorio central. Además, es importante que dentro de su estrategia de seguridad se contemple una revisión y monitoreo constante de el nivel de parche del sistema operativo y actualizaciones de cualquier otro software que requiera para la operativa.

Una solución de seguridad Endpoint protege mucha de estas capas, no solo a nivel de acceso a la información del usuario, sino también de posibles intentos de comprometer su dispositivo para usarlo de *Botnet* o movimiento lateral para lograr acceso a un servidor saltando de un equipo a otro. Es por ello que, a pesar de sus usuarios no tengan información crítica o sensitiva en sus equipos, no debe descuidar la seguridad en estos.

Puntos clave a analizar

- Antivirus & Antibot
- Parchado de Sistema Operativo
- Firewall & IDS de host
- Acceso físico
- Acceso remoto seguro SASE
- Cifrado de disco
- Procesos seguros de adquisición y descarte

Perímetro

El perímetro lo podemos definir como lo que separa el interior de su red del exterior (Internet). El componente más común a tomar en consideración en esta área es el Firewall. Sin embargo, debe pensar también en otras áreas como: puntos de accesos inalámbricos, correo electrónico, navegación web, unidades USB.

En general, cada uno de estos elementos proporciona, de algún modo, una conectividad a la red interna, por lo tanto, contemplarlos dentro de su análisis es de gran importancia. Recuerde que una vez algún atacante gana algún tipo de acceso a su red interna puede continuar mejorando su control y presencia al realizar movimientos laterales entre sistemas dentro de su red.

A nivel de Red fija contemple un Firewall de siguiente generación (Next Generation Firewall) con capacidades de análisis avanzado de tráfico y mitigación de ataques conocidos y desconocidos, que no solo incluya una revisión de reglas estáticas, sino que pueda elevar el análisis para una inspección profunda de todo el tráfico de red entrante y saliente. Tenga en cuenta que perímetro no es solo el enlace de Internet, también lo puede ser una conectividad WAN hacia oficinas o VPN hacia aliados empresariales. Además, de ser posible, considere un sistema de mitigación de ataques distribuidos (Anti-DDoS) que permita extender las capacidades del Firewall para proteger contra ataques de negación de servicio.

Respecto a las redes inalámbricas, asegúrese de utilizar las mejores prácticas como estándares seguros de cifrado, usar contraseñas, así como segmentar el acceso a través de una red aislada de la red Interna.

En cuanto a los servicios que interactúen con el exterior (Internet u otra empresa) como correo electrónico, navegación web y servicios de nombre (DNS), protéjalos colocándolos en un área aislada, definida como (DMZ). Una DMZ es un área de red que tiene una presencia de firewall en cada entrada/salida de dicha área. Así como soluciones que brinden protección a estos servicios como AntiSpam, AntiPhishing, Firewall de Aplicaciones Web y Seguridad DNS.

Puntos clave a analizar

- Next Generation Firewall
- Next Generation Threat Prevention
- Acceso Zero Trust
- Mitigación de Negación de Servicio (Anti DDoS)
- Sandboxing
- Seguridad Wireless
- NAT, DMZ, Segmentación
- AntiSPAM & AntiPhishing
- Firewall de Aplicaciones Web
- Seguridad DNS

Red, Servidores & Servicios

Internamente la protección de redes es proporcionada por segmentación, como vimos en el área de **Perímetro,** pero es complementada con un Firewall Interno o un sistema de detección o prevención de amenazas (IDS/IPS). Sin embargo, hoy día las amenazas han evolucionado y se extienden a comportamientos que parecen normales o legítimos para un IDS/IPS es requerido una tecnología basada en Inteligencia artificial que pueda aprender sobre el tráfico y alertar ante comportamientos maliciosos.

A nivel de servidores, puede considerar una solución de protección dedicada para servidores, que no solo incluya antivirus o IPS a nivel de host, sino que sea un agente especializado y enfocado a proteger servidores con mecanismos avanzados de análisis, detección de amenazas y parchado virtual.

Para los servicios publicados, que típicamente serán aplicativos web, considere una solución de seguridad de aplicaciones web (WAF). Segmentar el aplicativo web detrás de un firewall y un IPS no es suficiente porque los ataques de aplicaciones han evolucionado y se requiere una inspección a nivel de capa 7 para poder detectarlos y bloquearlos. Inclusive podría requerir de una solución basada en la nube que realice un filtro en la nube y le entregue únicamente el tráfico limpio en su aplicativo.

Otro componente clave es el control de acceso privilegiado. Este aspecto requiere la capacidad de autenticación, autorización y contabilidad (AAA). Basado en la criticidad de sus credenciales de alto privilegio como bases de datos, aplicaciones web, inclusive cuentas de redes sociales, puede requerir contemplar una solución de protección de cuentas privilegiadas que garantice la seguridad de estas cuentas de alto privilegio en una bóveda segura.

Finalmente, un puerto de red disponible y descuidado puede permitir la conectividad y acceso de activos externos a su red. Apague puertos no utilizados y de ser posible configure el puerto para que solo permitan que se conecte la tarjeta MAC adecuada. También puede contemplar una solución automatizada que le brinde visibilidad y control (NAC) de cualquier dispositivo IP que se conecte a su red.

Puntos clave a analizar

- Next Generation IPS
- Seguridad de Servidores
- Segmentación, Firewall Interno
- Firewall de Aplicaciones Web
- Gestión de Credenciales Privilegiadas
- Control de Acceso a la Red

Datos

Dado que la cantidad de datos que se crean y almacenan ha aumentado a un ritmo sin precedentes, la protección de datos es cada vez más importante. Además, las operaciones comerciales dependen cada vez más de los datos, e incluso un período corto de tiempo de inactividad o una pequeña pérdida de datos puede tener consecuencias importantes en una empresa.

Antes de implementar soluciones para asegurar los datos contemple las implicaciones de una filtración de datos o un incidente de pérdida de datos, en algunos casos pueden hacer que las organizaciones se pongan de rodillas. No proteger los datos puede causar pérdidas financieras, pérdida de reputación y confianza del cliente y responsabilidad legal. La protección de datos es uno de los desafíos clave de la transformación digital en organizaciones de todos los tamaños.

Debe evaluar los riesgos de seguridad que puedan surgir dentro y fuera de la organización:

Los riesgos internos incluyen errores en la configuración de TI o en las políticas de seguridad, falta de contraseñas seguras, autenticación y gestión del acceso deficiente, y acceso sin restricciones a los servicios o dispositivos de almacenamiento. Una amenaza creciente son los usuarios internos malintencionados o las cuentas comprometidas que han sido controladas por los actores de la amenaza.

Los riesgos externos incluyen estrategias de ingeniería social como phishing, distribución de malware y ataques a la infraestructura corporativa, como inyección SQL o denegación de servicio distribuida (DDoS). Los atacantes suelen utilizar estas y la mayoría de las amenazas de seguridad para obtener acceso no autorizado a datos confidenciales y filtrarlos.

Para asegurar los datos primero debe conocer dónde está su información, esto puede ser datos estructurados (Bases de Datos) o datos no estructurados (Sistemas de Archivos). Dependiendo de la ubicación de sus datos se enfoca la solución que va a requerir. Estas soluciones le brindarán: auditoría, monitoreo, alertas, bloqueo y cifrado de sus datos.

Por otro lado, si no posee un repositorio centralizado y sus datos residen en los equipos de trabajo, ej. Firma de abogados donde los documentos están en las laptops, la recomendación es aplicar un cifrado de la estación de trabajo, la cual puede realizarse con el cifrado propietario del equipo o una solución externa. Aunque la recomendación más segura, es que eviten tener estas islas de datos y tengan todo centralizado.

Puntos clave a analizar

- Monitoreo de Actividad de Uso de Datos
- Seguridad de Base de Datos
- Seguridad de Sistemas de Archivos
- Cifrado de Datos

Nube

Agilidad empresarial, productividad, eficiencia operativa, flexibilidad y rentabilidad son, sin duda, los factores clave detrás de la adopción de la nube pública empresarial. La nube pública permite que los recursos de la red de almacenamiento informático se adquieran e implementen más rápidamente.

Sin embargo, al mismo tiempo, Security of the Cloud Primer de Gartner 2019 afirma que la seguridad en la nube sigue siendo una de las principales preocupaciones. Esto no es sorprendente si tenemos en cuenta que los servicios de nube pública son compartidos, siempre conectados y dinámicos por naturaleza. Además, Gartner ha predicho que "hasta 2025, el 99% de las fallas de seguridad en la nube serán culpa del cliente". De hecho, la mayoría de las brechas en la nube se remontan a simples errores humanos en lugar de ataques concertados. Por ejemplo, la investigación muestra que hasta 10,000 empresas son vulnerables debido a una configuración incorrecta generalizada en Grupos de Google. Por un lado, estas son estadísticas alarmantes. Sin embargo, también implican que las empresas pueden mejorar significativamente su postura de seguridad si implementan una estrategia de seguridad eficaz.

Su análisis de seguridad debe contener principios arquitectónicos que deben abordar cualquier implementación de nube de nivel empresarial si va a cumplir con los desafíos de visibilidad limitada, necesidad de autorización granular y administración de privilegios, integración fluida con procesos automatizados, consistencia a través de sitios y cumplimiento de regulaciones.

El proveedor es responsable de la seguridad "de" la nube, mientras que el cliente debe asumir la responsabilidad de proteger lo que está "en" la nube. Para ello, contemple una seguridad de red con protección contra amenazas avanzada, que le permita segmentación y control de tráfico norte-sur, este-oeste. Deben protegerse los datos en reposo en recursos de almacenamiento en la nube como Amazon S3, Azure Storage y Google Cloud Storage Bucket. La identidad en entornos de nube comprende el acceso al entorno de nube (p. Ej., Aprovisionar una nueva máquina), así como el acceso a cada recurso específico (p. Ej., Acceso RDP a esta nueva máquina). Protección al plano de accesos debe implementarse para los servicios de control de acceso de proveedores o usuarios privilegiados, para ello contemple soluciones como Administración de Acceso de Identidad (IAM) y/o Administración de Acceso Privilegiado (PAM). Además, si publica servicios a través de la nube, recuerde la responsabilidad compartida, la nube es responsable que los recursos del servicio estén disponibles, pero usted es responsable de proteger dicho servicio ante ataques o fuga de información. Por lo tanto, debe contemplar alguna solución de seguridad de aplicaciones web y/o protección de negación de servicios. Finalmente, debe mantener una visibilidad de la configuración de la nube, debido a que muchas brechas de seguridad se han dado por mala configuración de la nube.

Puntos clave a analizar

- Cloud Next Generation Firewall
- Seguridad de Aplicaciones Web
- Seguridad de Base de Datos
- Administración de Acceso de Identidad (IAM)
- Administración de Acceso Privilegiado (PAM)
- Cloud Security Posture Management

Madurez y Niveles de Seguridad

Una arquitectura de seguridad completa debe disponer de muchas soluciones de seguridad. Muchas veces los clientes se sienten confundidos porque no saben por donde comenzar. Por ello, hemos definido los Niveles de Seguridad, que le permitirán revisar de forma ordenada las soluciones que hemos estado mencionando, siguiendo un orden de madurez de red. Hemos nombrado los niveles: Esencial, Avanzado, Visionario y Estricto.

1) Esencial 2) Avanzado 3) Visionario 4) Estricto

Detallamos a continuación los niveles, su alcance y soluciones que debe contemplar:

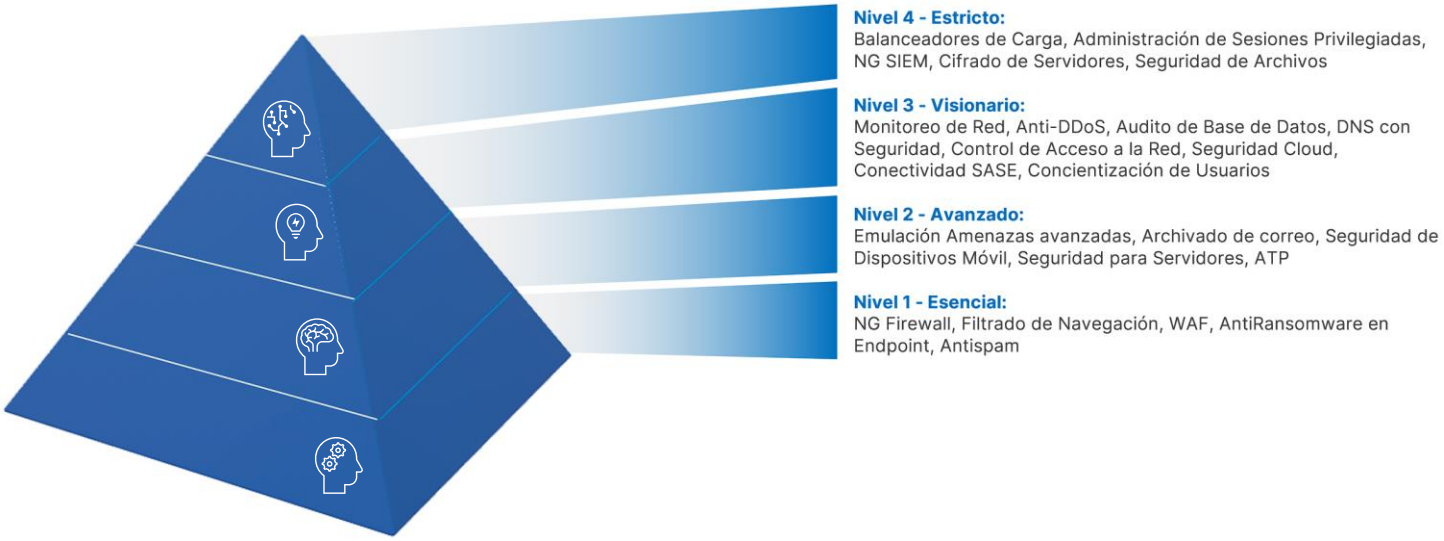
1) **Esencial** – Es la seguridad básica que toda organización debe cumplir, se compone de las soluciones de seguridad básicas para asegurar la red, correos, aplicativos y usuarios.
   - ✓ Next Generation Firewall
   - ✓ Filtrado de Navegación Web
   - ✓ Seguridad de Aplicaciones Web, WAF
   - ✓ Anti-Ransomware en Estaciones de usuarios, Endpoint
   - ✓ Seguridad de Correo Electrónico, Anti-Spam

2) **Avanzado** – Seguridad que aplica a organizaciones que se preocupan por asegurar con capaz adicionales a su correo electrónico, tal vez archivarlo para tener auditoría histórica. También aquellas que se preocupan por asegurar a sus servidores y dispositivos móviles mientras realiza también una inspección avanzada en el firewall de red local.
   - ✓ Emulación Amenazas, Sandboxing
   - ✓ Archivado de correo
   - ✓ Seguridad de Dispositivos Móvil
   - ✓ Seguridad para Servidores
   - ✓ Seguridad de Amenazas Avanzadas, ATP

3) **Visionario** – Es la seguridad que aplican los que requieren de la visibilidad de lo que ocurre en su red, para ello necesitan poseer visibilidad de la red, así como los servidores, accesos a datos, nube, conectividad a usuarios y control de acceso a la red. También aquellos que implementan mecanismos para proteger su infraestructura de ataques de negación de servicio distribuido, ya sea en premisas o nube.
   - ✓ Monitoreo de Red
   - ✓ Mitigador de Negación de Servicio, Anti-DDoS
   - ✓ Audito de Base de Datos
   - ✓ DNS con Seguridad
   - ✓ Control de Acceso a la Red

- ✓ Seguridad de Nube
- ✓ Conectividad SASE
- ✓ Concientización de Usuarios

4) **Estricto** – Es la máxima seguridad, donde el cliente, además de la seguridad antes mencionada requiere un control total de la entrega de sus servicios, gestiona de forma centralizada y segura todas las credenciales de alto privilegio, posee un analizador de eventos de siguiente generación, cifra y asegura el acceso a los datos sensitivos de la organización.
   - ✓ Balanceadores de Carga
   - ✓ Administración de Sesiones Privilegiadas, PAM/IAM
   - ✓ Next Generation SIEM
   - ✓ Cifrado de Servidores
   - ✓ Seguridad de Base de Datos y Sistemas de Archivos



Tome en cuenta que cada nivel contempla las soluciones definidas por el nivel inferior, también de que algunas soluciones pueden no aplicarle si no posee los servicios que estas protegen, por **ej**. Si no posee cargas de trabajo en la nube, puede ser nivel **Visionario** sin tener soluciones de seguridad de nube.

Nuestra recomendación es que analice todas las soluciones del nivel Esencial e implemente si posee un área de riesgo que cubrir y luego avance al siguiente nivel. Muchos clientes no saben como comenzar su análisis porque piensan en distintas soluciones de seguridad de forma aislada, y fácilmente se extravían entre tantas capas de seguridad que se pueden implementar.

Resumen

El desafío para los CISO es cómo respaldar las necesidades del negocio y transformación digital sin comprometer la seguridad o la velocidad.

En esta guía explicamos por qué usted debe repensar su estrategia de seguridad e implementar arquitecturas de seguridad que incluyan:

- Soluciones de seguridad flexibles y ágiles
- Los beneficios de operar en la nube, pero de manera segura
- Protección integral contra amenazas avanzada sin afectar el rendimiento

Las herramientas que ofrecen los proveedores de servicios para ayudar a realizar implementaciones seguras a menudo son inadecuadas frente a las amenazas avanzadas actuales. Es por ello que debe considerar soluciones líderes en ciberseguridad.

Dada la sofisticación y el alcance del panorama de amenazas actual, la seguridad de red debe adoptar un enfoque de confianza cero, en el que no se confía automáticamente en los usuarios o los dispositivos. Los usuarios deben recibir solo los privilegios mínimos, es decir, aquellos permisos que realmente necesitan para llevar a cabo sus tareas y rechazar el resto. Todo el tráfico debe verificarse y las superficies de ataque deben minimizarse mediante una segmentación eficaz de la red. Estos pasos le ayudarán a mejorar su postura de seguridad.

Aunque nos gustaría poder entregarles algunos diagramas recomendados de red, la realidad es que no existe dicho diagrama, porque las necesidades y retos de cada cliente son distintas. Sin embargo, al ir aplicando las recomendaciones de esta guía, su red va a irse transformado en una arquitectura segura hecha a la medida de sus propias necesidades.

Referencias

Algunas referencias, textos y formatos fueron obtenidos de las siguientes fuentes:

1. Cloud Security Blueprint 2.0 – ©Check Point Software Technologies
2. Network Security Blueprint – © SANS Institute/GIAC Practical Repository
3. Data Protection - ©Imperva