Estrategias para el endurecimiento de la ciberseguridad

Breve descripción:

El componente aborda los conceptos claves para la generación de estrategias en la mejora de los sistemas de computación referente a la seguridad de la información. Se describe el concepto de seguridad profunda, cómo se hace el diseño de controladores de puntos y técnicas específicas de seguridad para la mejora de la infraestructura de una red de datos.

Junio 2023

Tabla de contenido

Introducción

Bienvenido al componente formativo “Estrategias para el endurecimiento de la ciberseguridad”. Revise el siguiente video a manera de contextualización de las temáticas que se desarrollarán en este escenario de formación.

Video 1. Estrategias para el endurecimiento de la ciberseguridad

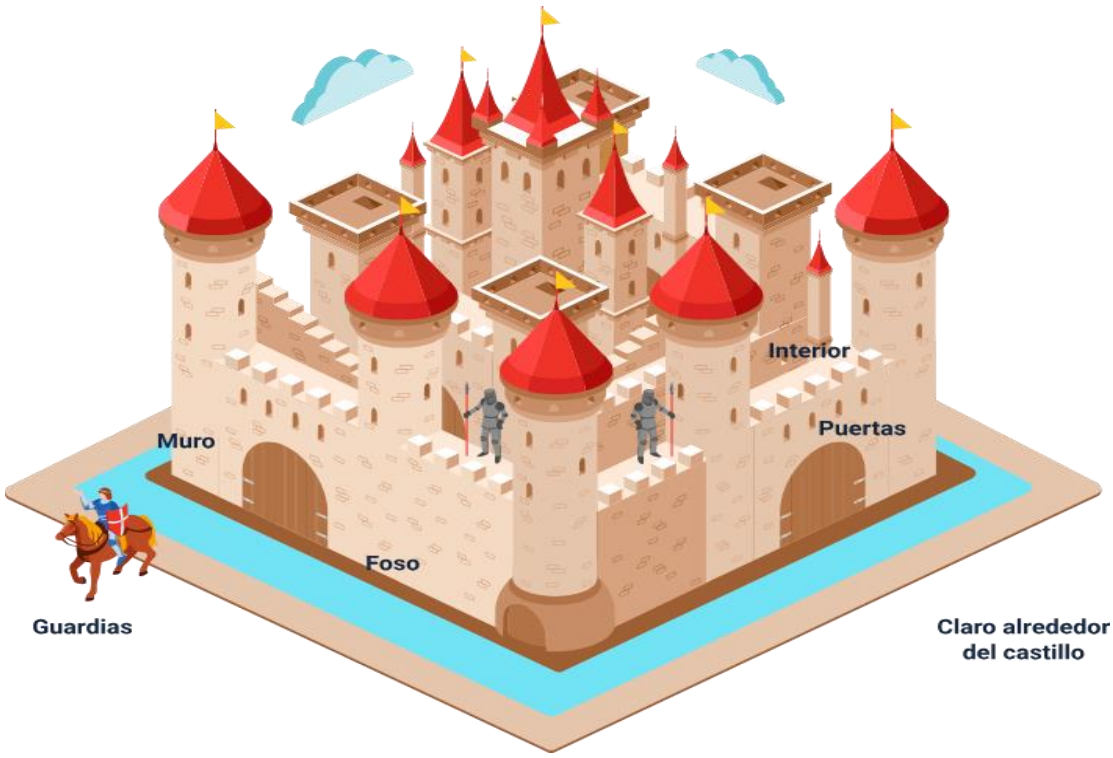
Enlace de reproducción del video

Síntesis del video: Estrategias para el endurecimiento de la ciberseguridad
El competitivo mercado mundial actual está influenciado por la dependencia de recursos naturales para el desarrollo económico y fluctuantes climas geopolíticos. Estas condiciones han contribuido a convertir las industrias en objetivos de ciberespionaje. A través de campañas orientadas a garantizar acceso a los últimos conocimientos técnicos y de inteligencia, se mantienen las ventajas competitivas y se prospera en una economía global impulsada por el mercado. Las estrategias de prevención de ciberataques y violaciones de datos deben considerarse parte integral de las operaciones diarias de las empresas. El principio clave de la defensa es asumir el compromiso y tomar contramedida. Endurecer los componentes de un sistema significa bloquear la funcionalidad de varios componentes dentro del sistema para evitar accesos o cambios no autorizados, eliminar funciones o características innecesarias y parchear cualquier vulnerabilidad conocida.

1. Defensa en profundidad

Ninguna solución única puede proteger realmente contra todos los vectores de ataque y tapar todos los agujeros de seguridad de un sistema. Aplicando un modelo de defensa en profundidad y estratificando las medidas de protección, las brechas en la seguridad de una capa pueden cerrarse con controles en otra capa, creando una postura de seguridad integral.

La superposición de medidas de protección en un sistema informático es muy parecida a la forma en que, en la Edad Media, se alzaban las medidas de seguridad en un castillo, observe con atención:



En el ejemplo del castillo medieval, los controles de seguridad aplicados son en su mayoría de naturaleza física, ya que implican principalmente impedir de forma física que la gente entre en el castillo o detectar una violación física del perímetro.

Ahora, tomemos en consideración que el rey del castillo hubiera encontrado una forma de hacer oro a partir del hierro mediante un proceso secreto de alquimia. En lugar de oro y joyas, la mazmorra alberga ahora un sofisticado proceso de fundición, controlado por un Sistema de Control Distribuido (DCS) de última generación. La fórmula secreta que convierte el hierro en oro está almacenada en un servidor en una de las cámaras de la torre.

El proceso de alquimia está a cargo de un puñado de empleados de confianza bien evaluados y todos los sistemas de control y supervisión del SCI (Sistema de control interno) están conectados entre sí a través de una red Ethernet con una solución de acceso remoto que permite la interacción a distancia. El rey tiene acceso a todo el ICS (Sistemas de control industrial) desde su trono, por lo que puede vigilar la rapidez con la que se enriquece e interactuar con los sistemas siempre que lo necesite.

Al instalar una red ICS accesible de forma remota ya no son eficientes sólo las defensas físicas contra los intrusos, lo que hace necesaria una estrategia defensiva que incluya entre otros los siguientes aspectos:

- Protección contra personas no autorizadas que utilicen acceso remoto.
- Restricción de acceso a usuarios autorizados mientras interactúan física o remotamente con los sistemas ICS.
- Trato adecuado para usuarios e invitados de la red.
- Protección de los datos en tránsito o almacenados en discos ante posible robo o manipulación.
- Defensa del sistema contra el tiempo de inactividad de la producción por manipulación de equipos ICS o ataques a la red.

- Protección ante riesgos de seguridad por manipulación o cambios que provoquen comportamiento inesperado en equipos y procesos.

La forma adecuada de abordar todas las preocupaciones relacionadas con la seguridad y la defensa de un ICS es mediante la implementación de una estrategia de defensa en profundidad.

A continuación, las capas a tener en cuenta para la elaboración de estrategias pertinentes:

- **Físico:** Limitar el acceso físico de personal autorizado a zonas de áreas, paneles de control, dispositivos, cableado y salas de control, mediante el uso de cerraduras, puertas, tarjetas llave y biometría. También implica el uso de políticas, procedimientos y tecnología para escoltar y rastrear a los visitantes.
- **Red:** Marco de seguridad: políticas de cortafuegos, políticas ACL (listas de control de acceso) para conmutadores y "routers", AAA, detección de intrusiones y sistemas de prevención.
- **Computación:** Gestión de parches, "software antimalware", eliminación de aplicaciones/protocolos/servicios no utilizados, cierre de puertos lógicos innecesarios y protección de puertos físicos.
- **Aplicación:** Autenticación, autorización y contabilidad (AAA), gestión de vulnerabilidades, gestión de parches y gestión del ciclo de vida del desarrollo seguro.
- **Dispositivo:** Endurecimiento de dispositivos, cifrado de comunicaciones y acceso restrictivo, gestión de parches, gestión del ciclo de vida de los dispositivos y gestión de la configuración y los cambios.

El modelo adopta un enfoque sistemático para asegurar todas las capas de un ICS. Cubrir todas las capas del modelo guiará al implementador a través del proceso de asegurar un ICS desde todos los aspectos.

1.1. Capas

A continuación, se revisan cada una de las capas del modelo, sus principales características, alcances e implicaciones.

Seguridad física

El objetivo de la seguridad física es mantener a las personas fuera de las zonas en las que no están autorizadas a estar. Esto incluye áreas restringidas, salas de control, áreas de alta seguridad, paneles eléctricos y de red, salas de servidores y otras áreas restringidas o sensibles. Si un atacante tiene acceso físico a la red o a los equipos de computación, es sólo cuestión de tiempo que consiga acceder a la red o al sistema de computación. La capa de defensa física incluye recomendaciones como la construcción de muros de tamaño suficiente, la aplicación de cerraduras en las puertas, la instalación de cámaras de CCTV y la definición de políticas y controles para tratar a los visitantes e invitados (Noonan, 2004).

Seguridad de la red

Al igual que la seguridad física, consiste en restringir el acceso a las áreas lógicas de la red ICS. La idea es dividir la red en zonas de seguridad, aplicando reglas de “firewall”, estableciendo listas de control de acceso e implementando sistemas de

detección de intrusos (IDS) para separar las partes más sensibles (zonas más seguras) de la red de las zonas menos seguras. Al controlar y supervisar estrechamente el tráfico que atraviesa las zonas de seguridad, se pueden detectar y gestionar eficazmente las anomalías.

La implementación de una seguridad sólida comienza literalmente desde los cimientos. Al aplicar una base sólida a una red ICS, se allana el camino para permitir una implementación más ágil del programa de seguridad de la red. Una base sólida viene en forma de decisiones de diseño de arquitectura de red centradas en la seguridad, por ejemplo:

- La provisión de puntos de control del tráfico de red en lugares estratégicos de la arquitectura de red, que faciliten la captura efectiva de paquetes, utilizada por herramientas de seguridad como los sistemas de detección de intrusiones (IDS).
- El diseño de una segmentación de la red que permita confinar y detectar los incidentes de seguridad y mantener las interrupciones, como las tormentas de difusión de paquetes, dentro de la zona, protegiendo la red en general.

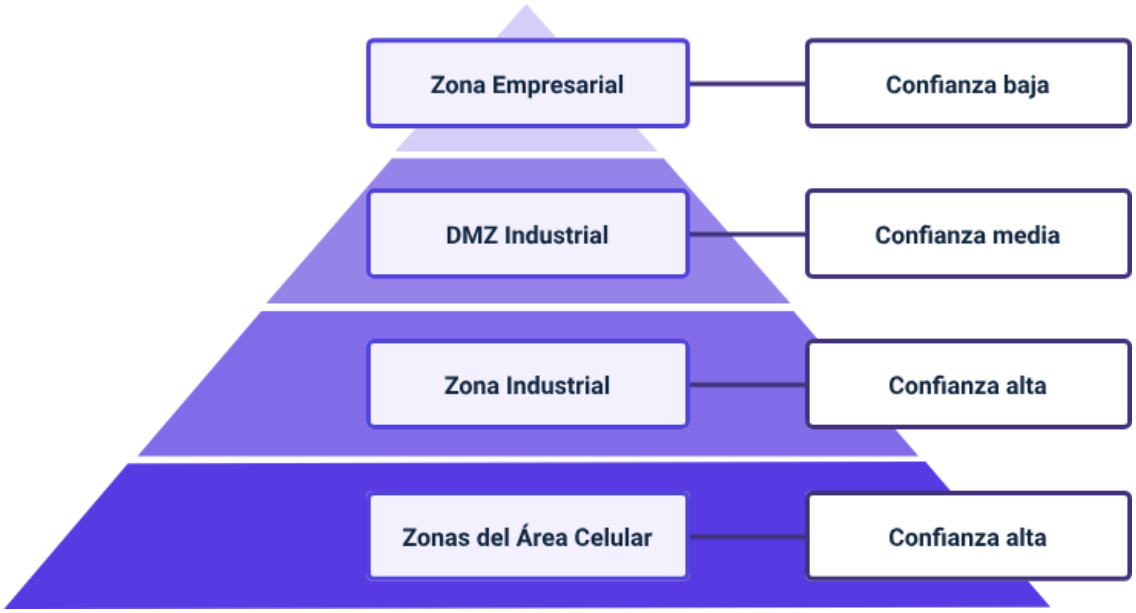
Segmentación de la red

El primer paso en el diseño de una arquitectura de red ICS consciente de la seguridad es definir la segmentación de la red. Un segmento de red, también conocido como zona de seguridad de la red, es una agrupación lógica de sistemas de información y automatización en una red ICS. La red ICS debe ser dividida en segmentos de red manejables con el fin de limitar el dominio de difusión, restringir el uso de ancho de

banda, y reducir la superficie de ataque. Una zona de seguridad de la red tiene un perímetro bien definido y una protección estricta de los límites.

Las zonas de seguridad reciben un nivel de confianza de seguridad (alto, bajo o medio) En el contexto de una red ICS, la Zona Industrial se considera la zona de alta seguridad y la Zona Empresarial la zona de baja seguridad. Esto permite que sistemas con requisitos de seguridad similares sean colocados dentro de la misma zona. Por ejemplo, una estación de trabajo suministrada por un fabricante de equipos originales, construida a medida por ese proveedor, se utiliza para controlar una parte crítica del proceso de producción que tiene prohibido por contrato que se le apliquen actualizaciones sin la estricta aprobación del proveedor, que se alojaría en la Zona Industrial, donde puede estar protegida del acceso directo desde zonas menos seguras por medio de la IDMZ. Por otro lado, un computador de mesa se utiliza simplemente para ejecutar informes de producción y no tiene restricciones de actualización ni valor particular para el proceso de producción y se situará en la Zona Empresarial, donde se puede restringir el acceso directo a los sistemas y dispositivos críticos de producción mediante la IDMZ.

Figura 1. Zonas de seguridad de red



El establecimiento de un pequeño número de zonas de seguridad de la red con requisitos de seguridad claramente definidos limita la complejidad y elimina la ambigüedad a la hora de seleccionar una zona para nuevos sistemas y dispositivos. Observe la siguiente tabla que detalla cada una de las zonas de seguridad de una red ICS, sus principales características, sistemas y servicios:

Tabla 1. Zonas de seguridad en una red ICS

Nombre	Características	Sistemas y servicios
Zona empresarial	Donde residen los sistemas de los usuarios de la empresa incluidas estaciones de trabajo, impresoras, teléfonos VoIP. Usuarios y sistemas de esta zona requieren conectividad a Internet y acceso a correo electrónico y chat. Los controles de seguridad incluyen	• Sistemas ERP. • Estaciones de trabajo de usuarios finales con conectividad a Internet. • Sistemas de bases de datos de toda la empresa.

Nombre	Características	Sistemas y servicios
	protección de puntos finales, actualizaciones (automáticas) de Windows y de las aplicaciones, y esfuerzos de cumplimiento y exploración de vulnerabilidades.	• Soluciones de aterrizaje de acceso remoto (Citrix, VPN y RDP).
Zona industrial	Alberga sistemas y dispositivos críticos para la producción incluyendo estaciones de trabajo, servidores, bases de datos y automatización, y dispositivos de instrumentación y control. Un fallo en la disponibilidad, integridad o confidencialidad de cualquiera de los sistemas de esta zona podría afectar negativamente la productividad y la rentabilidad, la reputación o la seguridad de la empresa. Esta zona debe tener el más alto nivel de protección.	• Servidores de etiquetas. • Servidores de recogida de datos históricos. • Estaciones de trabajo, estaciones de operador y servidores relacionados con el sistema de producción. • Dispositivos de automatización y control, como PLCs, HMIs y VFDs. • Cualquier sistema relacionado con la producción que sea demasiado restrictivo para asegurarlo por medios convencionales.
Zonas de Área Celular	La Zona Industrial debe subdividirse en enclaves o Zonas de Área Celular, cada una con los sistemas y dispositivos que tengan una tarea común o un interés mutuo en el proceso de producción. Las Zonas de Área Celular	• Dispositivos de automatización como PLCs, HMIs y VFDs. • Actuadores inteligentes como motores, servos y

Nombre	Características	Sistemas y servicios
	permiten esquemas de control de seguridad más granulares y confinan más el tráfico de red relacionado.	bancos de válvulas neumáticas. • Dispositivos de instrumentación habilitados para Ethernet, como sondas de temperatura, sensores de presión y velocímetros. • Sistemas de cómputo suministrados por algún proveedor que interactúan directamente con el equipo de producción.
Operaciones del sitio de nivel 3	Sin ser técnicamente una zona de área celular, sino más bien una subzona dedicada de la zona industrial, las operaciones del sitio de nivel 3 consisten en todos los sistemas y recursos que deben compartirse entre los sistemas de producción de todas las zonas de área celular. Se convierte en la zona de aterrizaje para las interacciones con los usuarios y los sistemas de nivel 4 y superior, como el extremo industrial de una solución de pasarela de escritorio remoto o el servidor de entrega de una actualización de antivirus.	• Entornos de desarrollo de automatización y controles virtuales (infraestructura de escritorio virtual). • Servicios de red y seguridad para la zona industrial, que incluyen Directorio Activo DNS, DHCP, servicios de identidad (AAA, ISE). • Almacenamiento y recuperación. • Servicios de automatización y control: recogida de datos

Nombre	Características	Sistemas y servicios
		históricos, servidores de etiquetas. • Servicios de actualización de antivirus, Windows y aplicaciones. • Solución de red industrial inalámbrica.

La definición de lo que entra en una Zona de Área Celular depende del objetivo de los esfuerzos de seguridad para toda la red ICS, pudiendo establecerse por:

- **Áreas funcionales de un proceso de producción**: por ejemplo, la línea de producción 1 será una Zona de Área Celular separada, la línea de producción 2 será otra Zona de Área Celular, y las áreas de envío y recepción formarán Zonas de Área Celular separadas.
- **Capacidad de supervivencia**: por ejemplo, si ciertas partes de un proceso de producción están vinculadas a los mismos servicios públicos como el gas, la electricidad y el aire, entonces tiene sentido colocar esos sistemas con servicios públicos comunes en sus propias Zonas de Área Celular.
- **Ubicación**: en el caso de un proceso de producción que se extiende a través de edificios separados, incluso en ciudades separadas; entonces, podría asignarse áreas celulares a cada ubicación.

El modelo de zonas de seguridad de la red utiliza el concepto de confianza como base de su funcionamiento. A cada zona se le asigna un nivel de confianza. La confianza aumenta desde la zona exterior hasta la interior, que alberga los activos y datos de

producción más críticos de la empresa. Sólo se permite la comunicación entre los sistemas de las zonas adyacentes y no se permite saltarse las zonas. Se colocan controles de seguridad entre cada zona, como cortafuegos de inspección de estado, sistemas de prevención y detección de intrusiones y sólidos controles de acceso. Los controles de seguridad implementados dentro de una zona permiten la detección de actividades maliciosas entre los sistemas de una zona.

La direccionalidad del tráfico también se puede tener en cuenta a la hora de definir las reglas de comunicación entre zonas. Por ejemplo, se podría permitir que el tráfico HTTPS entre la Zona Empresarial y la Zona Industrial sólo se origine en los clientes de la Zona Empresarial.

Seguridad de computación

La seguridad de la computación consiste en evitar la infiltración en los sistemas computacionales (estaciones de trabajo, servidores, computadores portátiles, etc.). Esto se consigue aplicando estrategias de parcheo, realizando ejercicios de endurecimiento de los sistemas informáticos e instalando aplicaciones y soluciones de seguridad como antivirus, protección de puntos finales y software de detección/prevención de intrusiones en los hosts (HIDS / HIPS).

Los controles de seguridad de computación también incluyen la restricción o la prevención del acceso a los puertos de comunicación no utilizados de los dispositivos informáticos, como el bloqueo del acceso a los puertos USB y “FireWire” mediante bloqueadores de puertos físicos (o hot glue) así como la aplicación de una política de dispositivos con una solución de protección de puntos finales como “Symantec Endpoint Protection” (SCP) Mantener los sistemas de computación libres de

vulnerabilidades mediante la actualización y la aplicación de parches es también una forma de seguridad informática.

Veamos en qué consisten algunos de estos controles de seguridad:

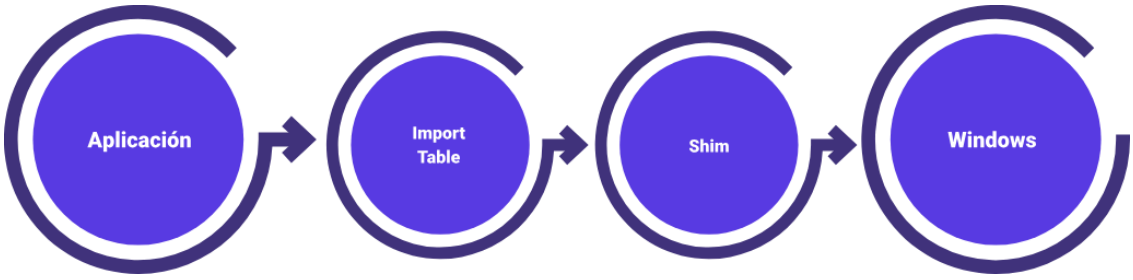
a. Endurecimiento de los endpoint: una parte integral de la seguridad informática de los ICS es el endurecimiento de los puntos finales, que tiene como objetivo reducir la superficie de ataque del punto final, así como limitar el impacto de un compromiso potencial del punto final.
b. Reducción de la superficie de ataque: el ejercicio implica revisar todos los sistemas y desactivar los servicios de Windows que no se utilicen, desinstalar las aplicaciones que no se usen y deshacerse de los scripts, programas, bases de datos y otros archivos instalados. Estas actividades realizadas al momento de la implementación del endpoint, deberían ser un ejercicio programado, realizado de forma regular después de la implementación del endpoint.
c. Limitar el impacto de un compromiso: limitar el impacto de una violación de la seguridad del punto final, por ejemplo, cuando un servicio o aplicación del sistema se ve comprometido, se logra restringiendo los permisos y privilegios dados al servicio o aplicación expuestos. Una forma de hacerlo es configurando los servicios y aplicaciones para que se ejecuten bajo cuentas de usuario dedicadas y restringidas.
d. Kit de herramientas de mitigación mejorada de Microsoft: otra forma de limitar el impacto de un compromiso es utilizar una solución de software de mitigación de seguridad, como el "Enhanced Mitigation Experience Toolkit" (EMET) de Microsoft o "AppLocker" de Microsoft. El EMET de Microsoft intercepta las llamadas a la interfaz de programación de

aplicaciones y aplica perfiles de protección a esas llamadas, evitando llamadas peligrosas o maliciosas.

El "Enhanced Mitigation Experience Toolkit" (EMET) no se ejecuta como un servicio y no se adjunta a una aplicación como un depurador. En su lugar, aprovecha una infraestructura de cuña integrada en Windows, llamada marco de compatibilidad de aplicaciones. Se trata de una interfaz de bajo nivel altamente optimizada y, como tal, EMET no presenta una sobrecarga adicional de recursos para las aplicaciones y servicios protegidos.

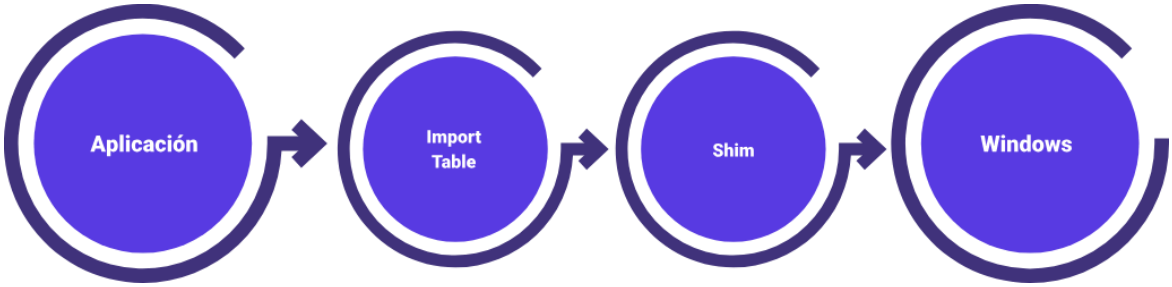
Una infraestructura de cuña implementa una forma de enganche de la interfaz de programación de aplicaciones. En concreto, aprovecha la naturaleza de la vinculación para redirigir las llamadas a la API de Windows a un código alternativo: la propia cuña. La especificación de Windows "Portable Executable" (PE) y "Common Object File Format" (COFF) incluye varias cabeceras, y los directorios de datos de esta cabecera proporcionan una capa de indirección entre la aplicación y el archivo vinculado.

Por ejemplo, si un ejecutable hace una llamada a una función de Windows, esta llamada a los archivos de la biblioteca externa tendrá lugar a través de la tabla de direcciones de importación (IAT), como se muestra en el siguiente diagrama:



Nota. Tomado de Li (2009).

Utilizando la infraestructura de cuña, puede modificar la dirección de la función de Windows resuelta en la tabla de importación, sustituyéndola por un puntero a una función en el código de cuña alternativo:



Nota. Tomado de Li (2009).

EMET aprovecha esta arquitectura de cuña para imponer sus perfiles de protección. Los perfiles de protección de EMET son archivos XML que contienen ajustes preconfigurados de EMET. Las empresas pueden proporcionar perfiles de protección de EMET adaptados para que funcionen con las aplicaciones y sistemas que venden. La empresa prueba y valida que la configuración del perfil de protección funcione para una variedad de sistemas operativos y aplicaciones.

Seguridad de las aplicaciones

Mientras que la seguridad de la información consiste en mantener a un intruso fuera de un sistema informático, la seguridad de las aplicaciones consiste en evitar que un usuario realice interacciones no autorizadas con los programas y servicios que se ejecutan en el sistema informático. Esto se consigue implementando la autenticación, la autorización y la auditoría. Aquí, la autenticación verifica que el usuario es quien dice ser, la autorización restringe las acciones del usuario y la auditoría registra todas las interacciones que el usuario tiene con el sistema. Mantener las aplicaciones libres de

vulnerabilidades mediante la detección y la aplicación de parches es también una forma de seguridad de las aplicaciones.

Seguridad de los dispositivos

La seguridad de los dispositivos implica las acciones y los controles de seguridad relativos a la tríada AIC de los dispositivos ICS, donde AIC significa disponibilidad, integridad y confidencialidad. En el caso de los sistemas y redes computacionales habituales, el orden de la tríada de seguridad es AIC, o sea, confidencialidad, integridad y disponibilidad, pero en el contexto de un ICS, la disponibilidad está por encima de las demás, ya que el tiempo de actividad (disponibilidad) es el objetivo número uno en la producción y el que más repercute en la rentabilidad.

La seguridad de los dispositivos incluye la aplicación de parches, el endurecimiento de los dispositivos, las restricciones de acceso físico y lógico, y el establecimiento de un programa de ciclo de vida de los dispositivos que incluya la definición de procedimientos para la adquisición, la implementación, el mantenimiento, la gestión de la configuración y los cambios, y la eliminación de los dispositivos.

Políticas, procedimientos y concienciación

Por último, están, las políticas, los procedimientos y la concienciación, elementos que unen todos los controles de seguridad. Las políticas son una directriz de alto nivel sobre cuál es la postura de seguridad esperada para los sistemas y dispositivos, por ejemplo, cifrando todas las bases de datos. Los procedimientos son instrucciones paso a paso sobre cómo lograr los objetivos de las políticas, como, por ejemplo, implementar el cifrado AES en las bases de datos. La toma de conciencia de los riesgos en seguridad ayuda a conseguir y mantener la atención sobre los aspectos relacionados con la

seguridad del ICS y su funcionamiento. La formación de conciencia suele consistir en una formación de seguridad anual que abarca temas como el spam, las amenazas internas y las prácticas de seguimiento (un intruso que sigue, de cerca, a un empleado legítimo en una instalación protegida por controles de acceso físico).

1.2. Conceptos

La plataforma en la nube es cada vez más atractiva para el mundo de la computación. Hoy en día, las técnicas de arquitectura orientada a servicios (SOA) y de programación orientada a aspectos (AOP) se utilizan ampliamente en las soluciones empresariales. Una pregunta que puede hacerse un equipo de gestión de TI o un equipo de desarrollo de "software" es: ¿cuál va a ser la próxima tendencia? La computación en nube parece ser la respuesta correcta. Se utilizan diferentes nombres para este tipo de plataforma, como computación de servicios, plataforma bajo demanda y plataforma como servicio. En relación con la computación en nube se ha extendido el uso de un conjunto de nuevas palabras de moda, como Programa como Servicio (PaaS) "software" como Servicio (SaaS) y cualquier cosa que se pueda imaginar como servicio (XaaS).

A continuación, se presentan algunos servicios de computación en la nube y sus principales características.

Azure

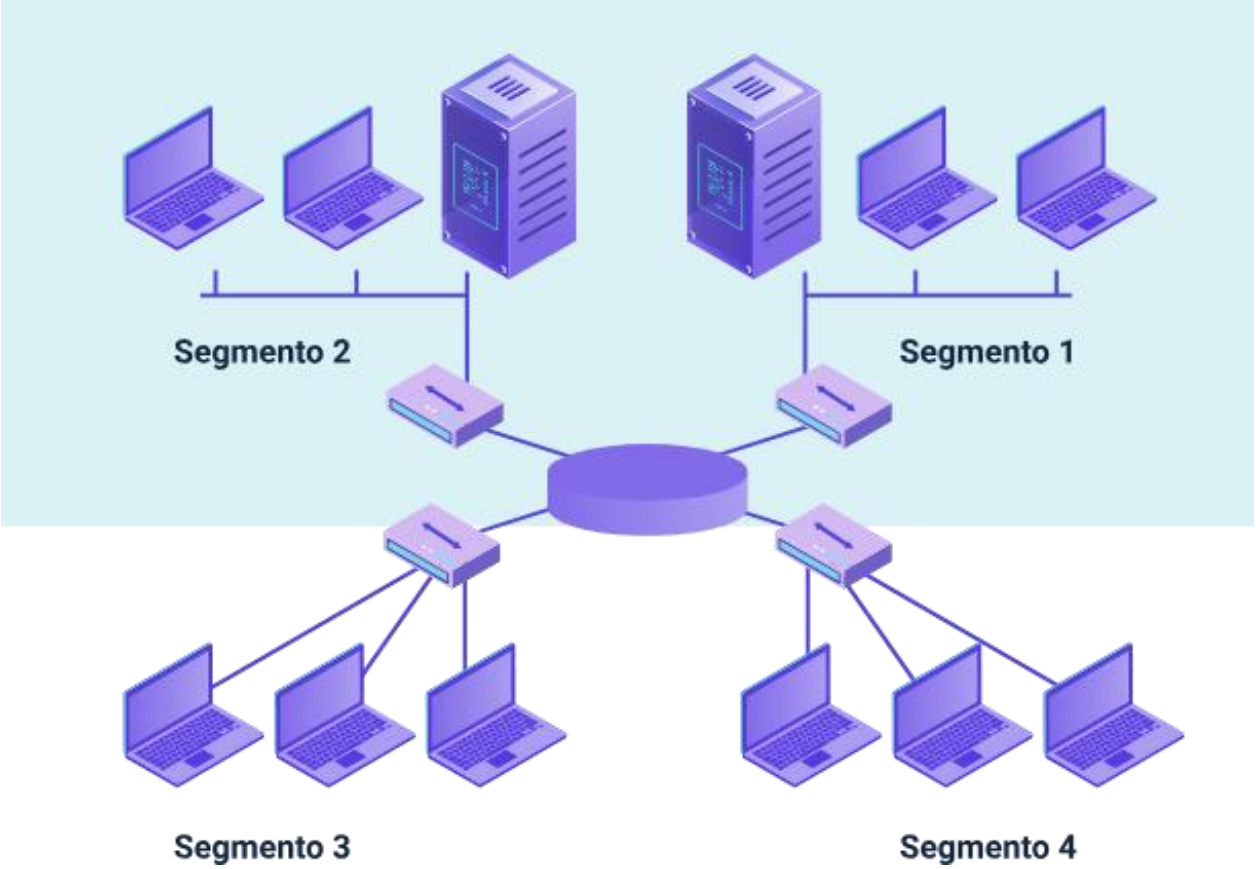
Azure es un nuevo sistema en la nube de Microsoft que permite que las aplicaciones se ejecuten desde un sistema conectado de forma remota, alojado en un

centro de datos de Microsoft, y que almacene los datos en la nube. La plataforma consta de tres partes:

- **Tiempo de ejecución de desarrollo:** simula el tiempo de ejecución permitiendo probar, depurar y ajustar la aplicación en un entorno de desarrollo local antes de desplegarla en la nube.
- **Tiempo de ejecución:** incluye la estructura, el servicio de almacenamiento y el sistema operativo de Windows Azure.
- **Aplicaciones:** las aplicaciones se ejecutan desde el tiempo de ejecución de Azure. Un conjunto de servicios basados en Internet funciona como bloques de construcción para desarrollar aplicaciones. El paquete de servicios incluye .NET *Services* (antes "BizTalk Services") SQL Azure y "Live Services".

La figura 2 describe el concepto de la plataforma Azure. Cualquier aplicación de tipo "on-premise" construida en una organización podría también aprovechar los servicios proporcionados por Azure a través de Internet. Sin embargo, para alojar y ejecutar aplicaciones desde la plataforma en la nube de Azure, las aplicaciones deben ser desarrolladas utilizando el .NET "Framework". Tanto las aplicaciones de Azure como las locales pueden acceder al servicio de almacenamiento de Azure utilizando un enfoque de transferencia de estado representativo (RESTful) El almacenamiento en la nube ya no se basa en el modelo relacional para cumplir con los requisitos de escalabilidad de Internet. Hay tres tipos de almacenamiento disponibles en la plataforma Azure: almacenamiento de blobs, almacenamiento de colas y almacenamiento de tablas.

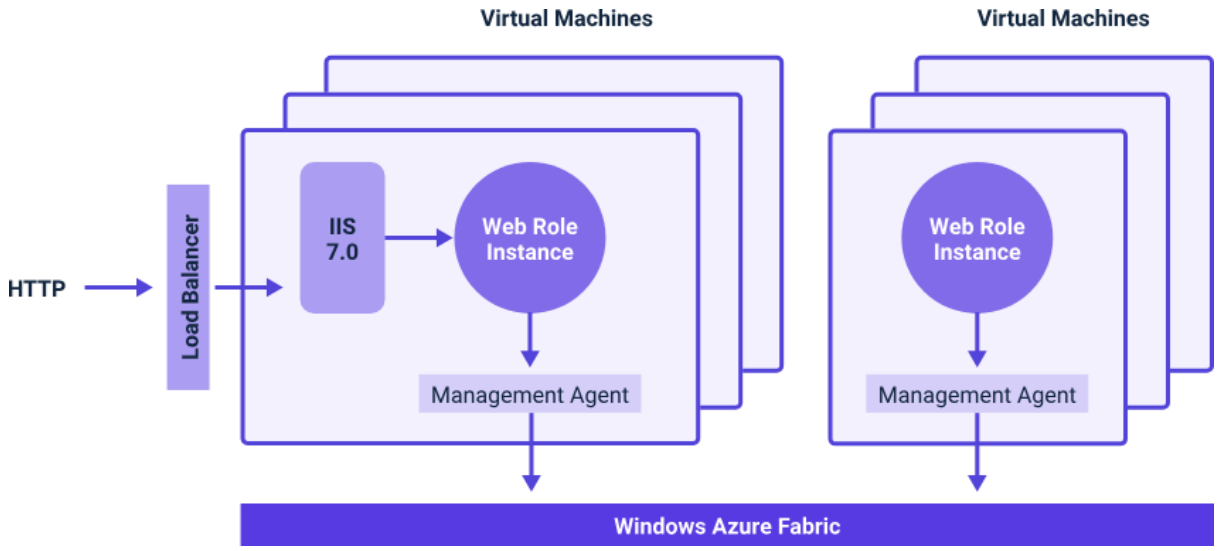
Figura 2. Concepto de la plataforma Azure



Nota. Tomada de Introduction to Windows Azure (p. xvii), por H. Li, 2009, H. (2009), Apress.

Azure Fabric es una tecnología innovadora y puede entenderse como el contexto de ejecución de Azure. El concepto de una aplicación Azure (ver figura 3) muestra que, para alcanzar el objetivo de escalabilidad en Internet, cada instancia de rol web y de rol trabajador tiene su núcleo de procesador dedicado. El número de instancias por defecto está configurado en uno cuando se crea una aplicación en la nube desde Visual Studio. El propietario de la cuenta puede aumentarlo a través del archivo de configuración *Web.config* incluso después del despliegue.

Figura 3. Aplicación Azure



Nota. Tomada de Introduction to Windows Azure (p. xvii), por H. Li, 2009, H. (2009), Apress.F.

El marco de Azure también proporciona un entorno de simulación de red local para simular el entorno de la nube, lo que permite depurar, probar y ajustar la aplicación localmente antes de desplegarla en producción. La red local puede iniciarse manualmente.

Las funciones de la red se resumen en la siguiente lista:

- **Monitorizar el estado de la aplicación:** cada aplicación de Azure tiene un propietario que controla algunos aspectos de la aplicación cambiando la configuración para gobernar la seguridad y la escalabilidad (número de instancias) La estructura Azure supervisa el estado de la configuración de la aplicación para satisfacer las solicitudes de las aplicaciones en tiempo de ejecución.

- **Garantizar el rendimiento de las aplicaciones**: una aplicación en la nube se ejecuta en una máquina virtual (VM). Azure mantiene relación de uno a uno entre la VM y un núcleo de procesador físico. Si una aplicación solicita aumentar el número de instancias, la red asignará nuevos recursos de VM desde la nube a los núcleos.
- **Gestión de la conmutación por error**: la estructura supervisa el estado de ejecución de la aplicación. Cuando una instancia falla, el tejido iniciará una nueva instancia desde un nuevo recurso VM.
- **Registro y seguimiento**: cuando una aplicación se ha desplegado en la nube, la única forma de registrar la información en tiempo de ejecución y enviar alertas o notificaciones al propietario de la aplicación es a través del tejido.

Google Cloud

Google Compute Engine es un servicio que proporciona máquinas virtuales (VM) que se ejecutan en la infraestructura de Google. Se pueden crear máquinas virtuales con una variedad de configuraciones utilizando un gran número de sistemas operativos disponibles. Los datos de la instancia se almacenan y se mantienen en un almacenamiento de bloques persistente que se replica para la redundancia y persiste más allá del ciclo de vida de la VM. El acceso a la red puede configurarse para permitir que las máquinas virtuales se comuniquen entre sí, con Internet o con una red privada propia.

Google Compute Engine proporciona varias herramientas para interactuar y gestionar las instancias y configuraciones de Compute Engine. Por ejemplo, se puede

iniciar y detener instancias, adjuntar almacenamiento en disco y configurar el acceso a la red utilizando cada uno de estos puntos de acceso. Las herramientas incluyen:

- Consola de desarrolladores de Google (https://console.cloud.google.com/getting-started?pli=1) que proporciona una interfaz de usuario (UI) basada en la web con formularios HTML para la creación y la configuración de instancias.
- Gcloud compute, una interfaz de línea de comandos que puede utilizarse de forma interactiva o en scripts para una automatización sencilla.
- API de Compute Engine, una API RESTful para la integración en su propio código y en aplicaciones de gestión de la nube.

Para empezar a trabajar con Google Compute Engine, primero se debe crear un proyecto Compute Engine en la Consola de Desarrolladores. Un proyecto de Compute Engine es una colección de información sobre la aplicación y actúa como un contenedor para los recursos y configuraciones de Compute Engine. Los discos, los cortafuegos, las redes y las instancias están asociados a un único proyecto y contenidos en él. La facturación se aplica a un proyecto en función de la cantidad de recursos utilizados. Los miembros del equipo pueden añadirse al proyecto con permisos específicos para acceder a los recursos de Compute Engine del proyecto.

El siguiente video ilustra paso a paso el proceso para desplegar una aplicación en Google Cloud:

Video 2. Amazon Web Services (AWS)

Enlace de reproducción del video

Síntesis del video: Amazon Web Services (AWS)
El instructor SENA desarrolla y explica los pasos para desplegar una aplicación en Google Cloud. Paso cero: crear máquina virtual de desarrollo y clonar la aplicación de ejemplo. Paso uno: crear imagen Docker para su aplicación (Dockerfile). Paso dos: construcción de "framework" de la UI. Paso tres: construcción de la interfaz del usuario. Paso cuatro: implementación del maestro.

Paso cinco: implementación del esclavo.

Desplegar una aplicación en Google Cloud.

Amazon Web Services (AWS) es una plataforma de servicios web que ofrece soluciones de computación, almacenamiento y redes, en diferentes capas de abstracción. Puede utilizar estos servicios para alojar sitios web, ejecutar aplicaciones empresariales y extraer enormes cantidades de datos. El término servicio web implica que los servicios pueden controlarse a través de una interfaz web que puede ser utilizada por máquinas o por humanos a través de una interfaz gráfica de usuario. Los servicios más destacados son EC2, que ofrece servidores virtuales, y S3, que ofrece capacidad de almacenamiento. Los servicios de AWS funcionan bien juntos; pueden ser utilizados para replicar la configuración local existente o diseñar una nueva configuración desde cero. Los servicios se cobran según un modelo de precios de pago por uso.

Un cliente de AWS, puede elegir entre diferentes centros de datos distribuidos en Estados Unidos, Europa, Asia y Sudamérica. Por ejemplo, puede iniciar un servidor virtual en Japón de la misma manera que puede iniciar un servidor virtual en Irlanda, lo que permite atender a clientes de todo el mundo con una infraestructura global.

Figura 4. Centros de datos

Nota. Tomada de Introduction to Windows Azure (p. xvii), por H. Li, 2009, H. (2009), Apress.F

Detalle a través de la situación descrita en el siguiente video, las posibilidades que ofrece AWS en el proceso de implementación de una arquitectura de sistema tolerante a fallos.

Video 3. AWS: Posibilidades de uso

Enlace de reproducción del video

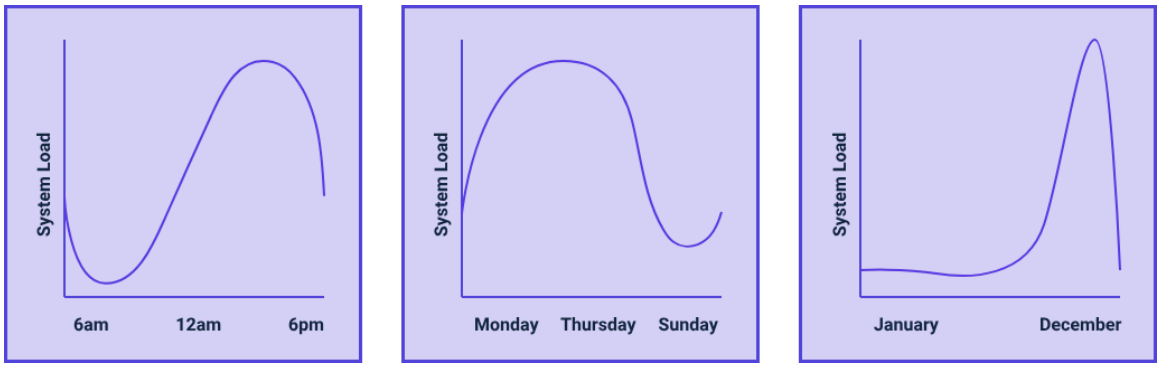
Síntesis del video: AWS: posibilidades de uso
Alexa es una ingeniera de software que trabaja en una empresa de rápido crecimiento. Sabe que la Ley de Murphy se aplica a la infraestructura de TI: todo lo que puede salir mal, saldrá mal. Alexa está trabajando duro para construir un sistema tolerante a fallos para evitar que las interrupciones arruinen el negocio. Ella sabe que hay dos tipos de servicios en AWS: los servicios tolerantes a fallos y los servicios que se pueden utilizar de forma tolerante a fallos. Alexa construye un sistema con una arquitectura tolerante a fallos. El servicio de base de datos se ofrece con manejo de replicación y conmutación por error. Alexa utiliza servidores virtuales que actúan como servidores web, aunque sabe que no son tolerantes a fallos por defecto. Por eso utiliza un balanceador de carga con lo que puede lanzar múltiples servidores en diferentes centros de datos a fin de lograr la tolerancia a fallos. Hasta ahora, Alexa ha protegido al "startup" de las principales interrupciones. Sin embargo, ella y su equipo siempre están planificando los fallos.

Con la idea general de lo que se puede hacer con AWS, a continuación, se destacan los beneficios más importantes que ofrece la plataforma en cuanto a capacidad y servicios:

Capacidad flexible (escalabilidad)

La capacidad flexible libera de la planificación, pudiendo escalar de un servidor a miles de servidores. Su almacenamiento puede crecer de gigabytes a petabytes, sin tener que predecir futuras necesidades de capacidad para los próximos meses y años. Si se dirige una tienda web, se tiene patrones de tráfico estacionales, como se muestra en la figura 5. Se puede pensar en el día frente a la noche, y en los días laborables frente a los fines de semana o las vacaciones. ¿No sería bueno poder añadir capacidad cuando el tráfico crece y eliminar capacidad cuando el tráfico disminuye? En eso consiste exactamente la capacidad flexible. Se pueden poner en marcha nuevos servidores en cuestión de minutos y desecharlos unas horas después. La nube casi no tiene limitaciones de capacidad. Ya no tiene que pensar en el espacio de los bastidores, los conmutadores y las fuentes de alimentación: puede añadir tantos servidores como se quiera. Si el volumen de datos crece, siempre puede añadir nueva capacidad de almacenamiento.

Figura 5. Patrones de gráfico

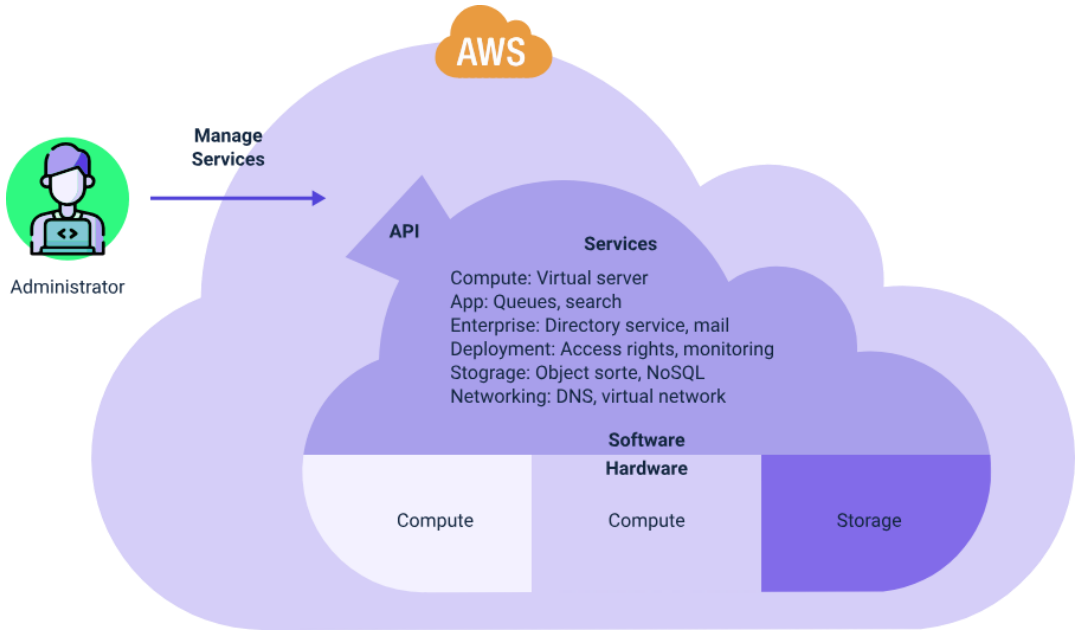


Nota. Tomada de Amazon web services in action (p. 11), por M. Wittig & A. Wittig, 2018, Manning.

Los servicios de AWS

El “hardware” para la computación, el almacenamiento y las redes es la base de la nube de AWS. AWS ejecuta servicios de “software” sobre el “hardware” para proporcionar la nube (Ver figura 6). Una interfaz web, la API, actúa como una interfaz entre los servicios de AWS y sus aplicaciones. Se puede gestionar los servicios enviando peticiones a la API manualmente a través de una GUI o programando los eventos a través de un SDK. Para ello, se puede utilizar una herramienta como la consola de administración, una interfaz de usuario basada en la web o una herramienta de línea de comandos.

Figura 6. Servicios AWS

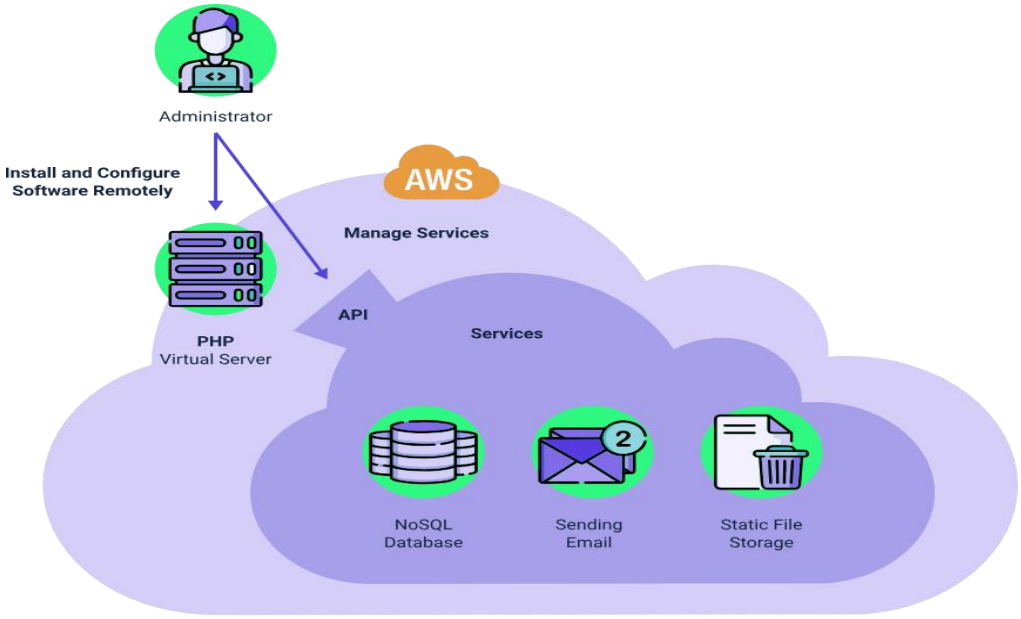


Nota. Tomada de Amazon web services in action (p. 16), por M. Wittig & A. Wittig, 2018, Manning.

Los servidores virtuales tienen una peculiaridad: se puede hacer la conexión a los servidores virtuales a través de SSH, por ejemplo, y obtener acceso de administrador.

Esto significa que se puede instalar el software que quiera en un servidor virtual. Otros servicios, como el servicio de base de datos NoSQL, ofrecen sus características a través de una API y ocultan todo lo que ocurre entre bastidores. La Figura 7 muestra un administrador instalando una aplicación web PHP personalizada en un servidor virtual y gestionando servicios dependientes como una base de datos NoSQL utilizada por la aplicación web PHP.

Figura 7. Administrador instalando una aplicación web PHP

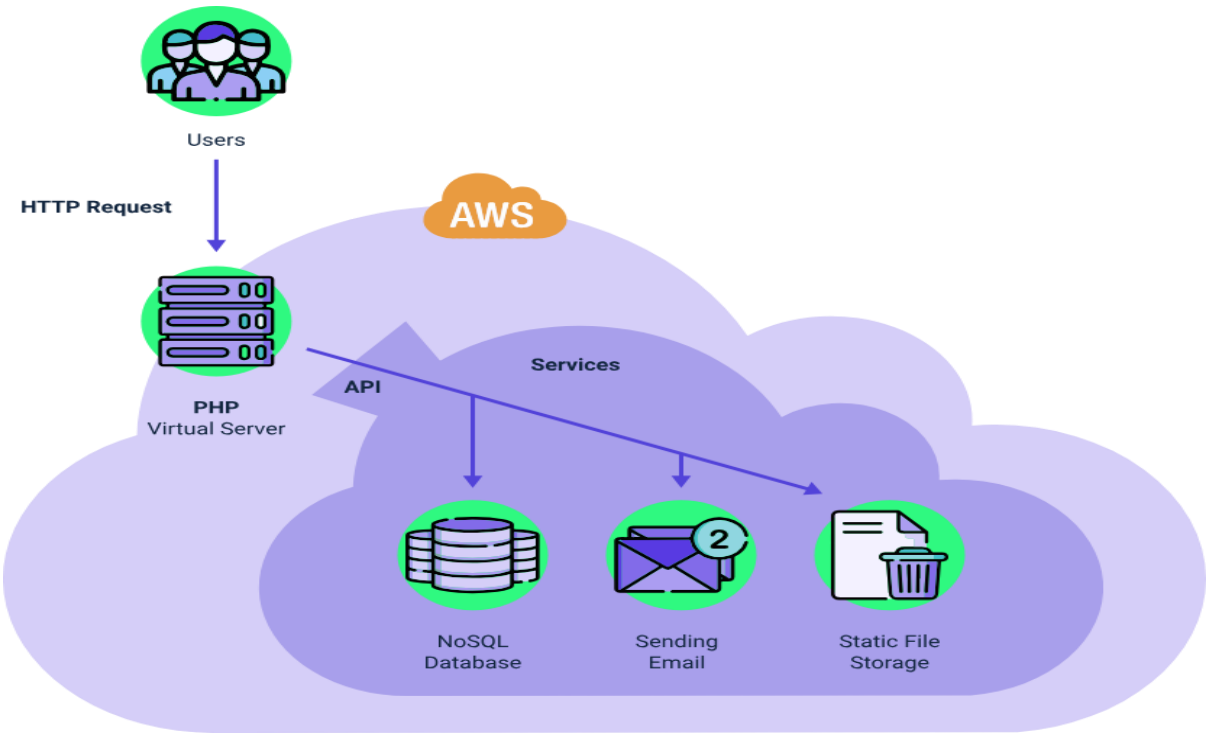


Nota. Tomada de Amazon web services in action (p. 17), por M. Wittig & A. Wittig, 2018, Manning.

Los usuarios envían peticiones HTTP a un servidor virtual. En este servidor virtual se instala un servidor web junto con una aplicación web PHP personalizada. La aplicación web necesita hablar con los servicios de AWS para responder a las solicitudes HTTP de los usuarios. Por ejemplo, la aplicación web necesita consultar datos de una base de datos NoSQL, almacenar archivos estáticos y enviar correos electrónicos. La

comunicación entre la aplicación web y los servicios de AWS se gestiona mediante la API, como muestra la siguiente figura.

Figura 8. Comunicación entre procesos



Nota. Tomada de Amazon web services in action (p. 17), por M. Wittig & A. Wittig, 2018, Manning.

La cantidad de servicios disponibles puede asustar al principio. La siguiente categorización de los servicios de AWS le ayudará a orientarse en la jungla:

- Los servicios de computación ofrecen potencia de cálculo y memoria. Puede iniciar servidores virtuales y utilizarlos para ejecutar sus aplicaciones.

- Los servicios de aplicaciones ofrecen soluciones para casos de uso comunes como colas de mensajes, temas y búsqueda de grandes cantidades de datos para integrarlos en sus aplicaciones.
- Los servicios para empresas ofrecen soluciones independientes como servidores de correo y servicios de directorio.
- Los servicios de implementación y administración funcionan sobre los servicios mencionados hasta ahora. Le ayudan a conceder y revocar el acceso a los recursos de la nube, a supervisar sus servidores virtuales y a desplegar aplicaciones.
- El almacenamiento es necesario para recoger, persistir y archivar datos. AWS ofrece diferentes opciones de almacenamiento: un almacén de objetos o una solución de almacenamiento conectado a la red para su uso con servidores virtuales.
- El almacenamiento de bases de datos tiene algunas ventajas sobre las soluciones de almacenamiento simples cuando se necesitan gestionar datos estructurados. AWS ofrece soluciones para bases de datos relacionales y NoSQL.
- Los servicios de red son una parte elemental de AWS. Puede definir redes privadas y utilizar un DNS bien integrado.

Comparación de alternativas

AWS no es el único proveedor de computación en la nube. Microsoft y Google también tienen ofertas en la nube. OpenStak es diferente porque es de código abierto y está desarrollado por más de 200 empresas, entre ellas IBM, HP y Rackspace. Cada una de estas empresas utiliza OpenStack para operar sus propias ofertas de nube, a veces

con complementos de código cerrado. Comparar los proveedores de nubes no es fácil, porque la mayoría de los estándares abiertos están ausentes. Funcionalidades como las redes virtuales y las colas de mensajes se realizan de forma diferente. Si se sabe qué características se necesita para una aplicación en particular, se puede comparar los detalles y tomar una decisión.

Tabla 2. Proveedores de computación en la nube

Nombre	AWS	Microsoft Azure	Google Cloud	OpenStack
Número de servicio	La mayoría	Muchos	Suficiente	Pocos
Número de ubicaciones (varios centros de datos por ubicación)	9	13	3	Sí (depende del proveedor de OpenStack)
Cumplimiento	Normas comunes (ISO 27001, HIPAA, FedRAMP, SOC), IT Grundschutz (Alemania), G-Cloud (Reino Unido)	Normas comunes (ISO 27001, HIPAA, FedRAMP, SOC), ISO 27018 (seguridad en la nube), G-Cloud (Reino Unido)	Normas comunes (ISO 27001, HIPAA, FedRAMP, SOC)	Q)

Nombre	AWS	Microsoft Azure	Google Cloud	OpenStack
Idiomas del SDK	Android, Navegadores (JavaScript), iOS, Java, .NET, Node.js (JavaScript), PHP, Python, Ruby, Go	Android, iOS, Java, .NET, Node.js (JavaScript), PHP, Python, Ruby	Java, Navegadores (JavaScript), .NET, PHP, Python	
Integración en el proceso de desarrollo	Medio, no vinculado a ecosistemas específicos	Alta, vinculada al ecosistema de Microsoft (por ejemplo, el desarrollo de .NET)	Alta, vinculada al ecosistema de Google (por ejemplo, Android)	
Almacenamiento a nivel de bloque (conectado a través de la red)	Sí	Sí (puede ser utilizado por varios servidores virtuales simultáneamente)	No	Sí (puede ser utilizado por varios servidores virtuales simultáneamente)
Base de datos relacional	Sí (MySQL, Postgr- eSQL, Oracle Data-base, Microsoft SQL Server)	Sí (Azure SQL Data-base, Microsoft SQL Server)	Sí (MySQL)	Sí (depende del proveedor de OpenStack)

Nombre	AWS	Microsoft Azure	Google Cloud	OpenStack
Base de datos NoSQL	Si (propietario)	Si (propietario)	Si (propietario)	No
DNS	Sí	No	Sí	No
Red virtual	Sí	Sí	No	Sí
Herramientas de aprendizaje automático	Sí	Sí	Sí	No
Herramientas de despliegue	Sí	Sí	Sí	No
Integración en el centro de datos local	Sí	Sí	Sí	No

1.3. Características

A lo largo de los últimos cincuenta años, ciertas tendencias clave crearon cambios fundamentales en la forma de prestar servicios de computación. El procesamiento de mainframe impulsó los años sesenta y setenta. Los computadores personales, la digitalización del escritorio físico y la tecnología cliente/servidor encabezaron los años ochenta y noventa. Internet, el auge y la burbuja, abarcó el siglo pasado y el actual y continúa en la actualidad. Pero estamos en medio de otra de esas tendencias que

cambian el modelo: la virtualización, una tecnología disruptiva, que rompe el statu quo de cómo se manejan los computadores físicos, se prestan los servicios y se asignan los presupuestos.

Para entender por qué la virtualización ha tenido un efecto tan profundo en el entorno computacional actual, es necesario comprender mejor lo que ha sucedido en el pasado. La palabra virtual ha sufrido un cambio en los últimos años, su uso se ha ampliado junto con la expansión de la computación, especialmente con el uso generalizado de Internet y los teléfonos inteligentes. Las aplicaciones en línea han permitido comprar en tiendas virtuales, examinar posibles lugares de vacaciones a través de visitas virtuales, e incluso guardar libros virtuales en bibliotecas virtuales. Muchas personas invierten tiempo y dinero en explorar y aventurarse por mundos enteros que sólo existen en la imaginación de alguien y en un servidor de juegos.

La virtualización en computación suele referirse a la abstracción de algún componente físico en un objeto lógico. Al virtualizar un objeto, se puede obtener una mayor utilidad del recurso que proporciona el objeto. Por ejemplo, las LAN (redes de área local) virtuales, o VLAN, proporcionan un mayor rendimiento de la red y una mejor capacidad de gestión al estar separadas del hardware físico. Del mismo modo, las redes de área de almacenamiento (SAN) proporcionan una mayor flexibilidad, una mejor disponibilidad y un uso más eficiente de los recursos de almacenamiento al abstraer los dispositivos físicos en objetos lógicos que pueden manipularse rápida y fácilmente. Sin embargo, el análisis se centrará en la virtualización de ordenadores completos.

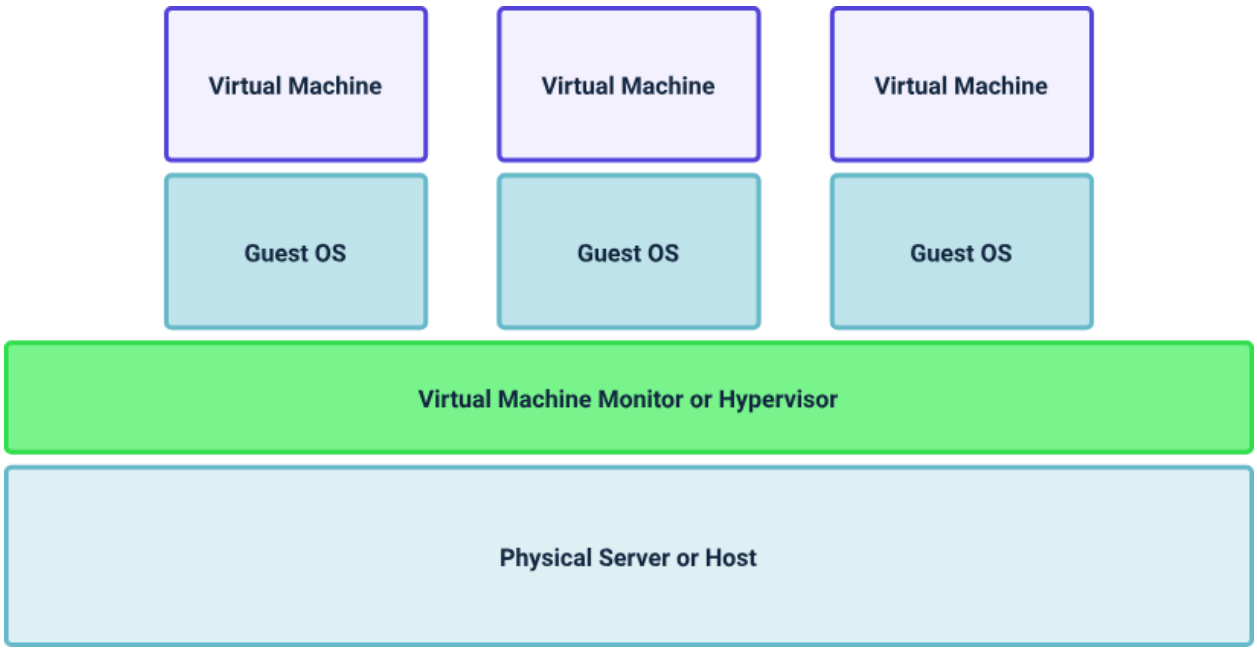
Si todavía no está familiarizado con la idea de la virtualización computacional, es posible que sus primeros pensamientos sean los de la realidad virtual, la tecnología

que, mediante el uso de sofisticadas proyecciones visuales y retroalimentación sensorial, puede dar a una persona la experiencia de estar realmente en ese entorno creado. En un nivel fundamental, esto es exactamente lo que es la virtualización computacional: es como una aplicación computacional experimenta su entorno creado.

La primera virtualización generalizada se realizó en los mainframes de IBM en los años 60, pero fueron Gerald Popek y Robert Goldberg quienes en 1974 codificaron el marco que describe los requisitos para que un sistema computacional soporte la virtualización. Su artículo "Formal requirements for virtualizable third generation architectures" describe las funciones y propiedades de las máquinas virtuales y de los monitores de máquinas virtuales que se siguen utilizando en la actualidad (Popek & Goldberg, 1974).

Por su definición, una máquina virtual (VM) puede virtualizar todos los recursos de hardware, incluidos los procesadores, la memoria, el almacenamiento y la conectividad de red. Un monitor de máquina virtual (VMM), que hoy en día se denomina comúnmente hipervisor, es el software que proporciona el entorno en el que operan las VM. La siguiente figura ilustra de forma sencilla un VMM.

Figura 9. Diagrama de una máquina virtual



Nota. Tomada de Virtualization essentials (Vol. 19), por M. Portnoy, 2012, John Wiley & Sons. Según Popek y Goldberg.

Un VMM debe presentar tres propiedades para satisfacer correctamente su definición:

- **Fidelidad**: el entorno que se crea para la VM es esencialmente idéntico al de la máquina física original (“hardware”).
- **Aislamiento o seguridad**: el VMM debe tener un control total de los recursos del sistema.
- **Rendimiento**: debe haber poca o ninguna diferencia de rendimiento entre la VM y un equivalente físico.

Aquí es donde se unen las dos historias. Hubo una explosión salvaje de centros de datos repletos de servidores; pero con el paso del tiempo, en una combinación del

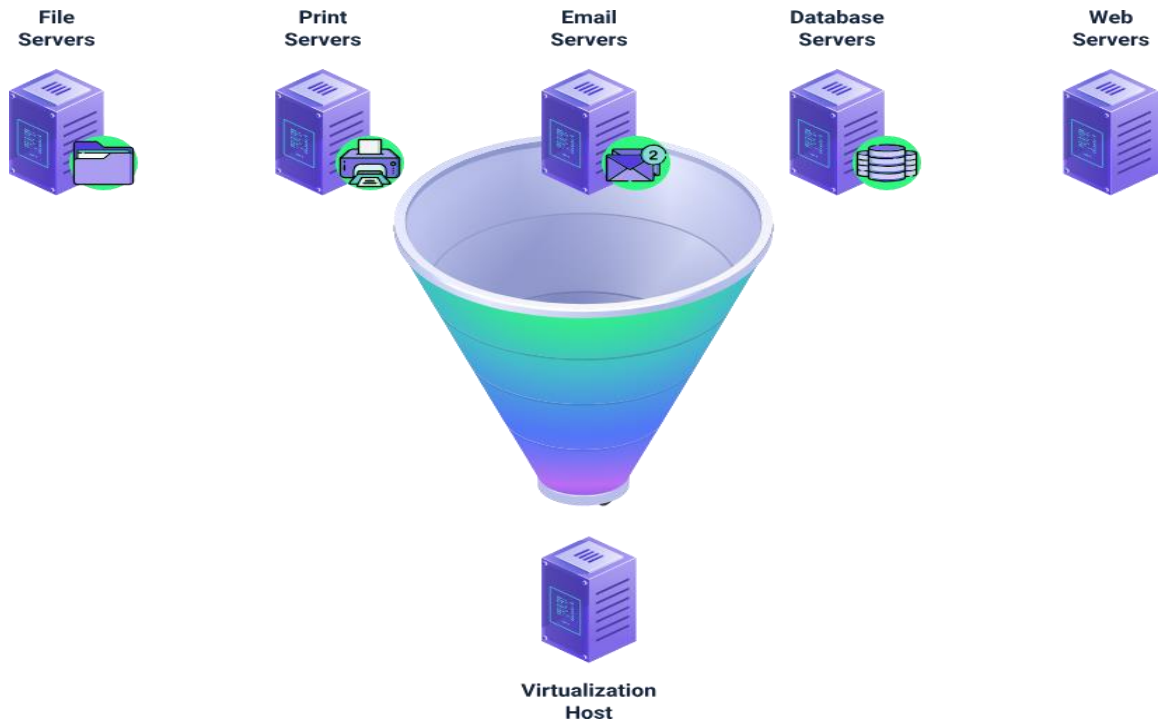
efecto de la Ley de Moore y el modelo "un servidor, una aplicación", esos servidores hicieron cada vez menos trabajo. Afortunadamente, la ayuda llegó en forma de virtualización. La idea y la ejecución de la virtualización no eran nuevas, ya funcionaba en los mainframes de IBM a principios de los años 70, pero se actualizó para los sistemas informáticos modernos.

Siguiendo la definición de Popek y Goldberg (1974), la virtualización permite que muchos sistemas operativos se ejecuten en el mismo "hardware" de servidor al mismo tiempo, manteniendo cada máquina virtual funcionalmente aislada de todas las demás. Así, la primera solución comercialmente disponible para proporcionar virtualización para ordenadores x86 vino de la mano de VMware en 2001. Y dos años después, llegó una oferta paralela de código abierto llamada Xen. Estas soluciones (VMMs, o hipervisores) tomaron la forma de una capa de software que vivía entre un sistema operativo y las máquinas virtuales (VMs) o se instalaba directamente en el hardware, al igual que un sistema operativo tradicional como Windows o Linux.

Lo que la virtualización aportó a esos centros de datos sobrecargados y a los servidores infrautilizados fue la capacidad de condensar varios servidores físicos en un servidor que ejecutará muchas máquinas virtuales, lo que permitiría que ese servidor físico funcionará a una tasa de utilización mucho mayor. Esta condensación de servidores se denomina consolidación (Ver figura 10). Una medida de la consolidación se denomina ratio de consolidación y se calcula contando el número de máquinas virtuales en un servidor; por ejemplo, un servidor que tiene ocho máquinas virtuales funcionando en él tiene una ratio de consolidación de 8:1. La consolidación fue una bendición para los asediados centros de datos y los gestores de operaciones porque resolvió una serie de problemas cruciales justo cuando se había alcanzado un umbral

crítico. Incluso un modesto ratio de consolidación de 4:1 podría eliminar tres cuartas partes de los servidores de un centro de datos.

Figura 10. Consolidación de virtualización



Nota. Tomada de Virtualization essentials (Vol. 19), por M. Portnoy, 2012, John Wiley & Sons.

En los centros de datos más grandes, donde se alojaban cientos o incluso miles de servidores, la virtualización proporciona una forma de retirar gran parte de los servidores lo que redujo el espacio total de un centro de datos y los requisitos de energía y refrigeración, además de eliminar la necesidad de construir centros de datos adicionales. Por extensión, con menos servidores, menos costos de mantenimiento del "hardware" menos tiempo de los administradores de sistemas dedicado a la realización de muchas otras tareas rutinarias.

Además de la consolidación, se produjo un segundo avance. A medida que las empresas empezaron a ver las ventajas de la virtualización, dejaron de comprar nuevos

equipos cuando terminaban sus contratos de alquiler o, si eran propietarios de estos, cuando caducaron sus licencias de mantenimiento de "hardware". En su lugar, virtualización esas cargas de trabajo del servidor, lo que se conoce como contención. La contención benefició a las empresas de múltiples maneras: ya no tenían que renovar grandes cantidades de "hardware" año tras año y todos los costos de gestión y mantenimiento de esos servidores (energía, refrigeración, etc.) se eliminaban.

Hasta el momento en que la virtualización se hizo comercialmente viable, la Ley de Moore iba en contra del modelo existente de aplicación/servidor/centro de datos; después de que se hizo factible, en realidad ayudó. Los ratios de consolidación de la primera generación de hipervisores x86 eran del orden de 5:1. Con el paso del tiempo, los chips más potentes y la memoria más grande permitieron ratios de consolidación mucho más altos, en los que un solo servidor físico podía albergar docenas o cientos de máquinas virtuales. En lugar de eliminar tres de cada cuatro servidores, la virtualización actual puede eliminar cómodamente nueve de cada diez; o con servidores suficientemente configurados, noventa y nueve de cada cien. Como resultado, la mayoría de los centros de datos corporativos han recuperado gran parte del espacio que habían perdido antes de la virtualización.

Observe a continuación los usos y posibilidades que ofrece el modelo de virtualización:

a) **Virtualización de servidores**: el hipervisor abstrae la capa física para uso de servidores virtualizados o máquinas virtuales. Los hipervisores son la base de los entornos virtuales y las máquinas virtuales, los motores que impulsan las aplicaciones, conteniendo todo lo que sus homólogas físicas (sistemas operativos, aplicaciones, conexiones de red, acceso al almacenamiento), pero

empaquetado en un conjunto de archivos de datos. Este empaquetamiento hace que las máquinas virtuales sean mucho más flexibles y manejables (pueden clonarse, actualizarse, incluso trasladarse) sin interrumpir las aplicaciones de los usuarios.

b) **Virtualización de escritorios**: alternativa para la computación de escritorios que para las empresas resulta costosa e ineficiente (requiere personal para actualizaciones de "software", soporte de "hardware", asistencia técnica). Los escritorios virtuales se ejecutan en servidores del centro de datos al igual que las aplicaciones a las que se conectan los usuarios, lo que reduce enormemente el tráfico de red y amplía los recursos. En cuanto a la seguridad, máquinas virtuales específicamente diseñadas que residen en cada host, protegen todos los escritorios virtuales que allí se ejecutan.

c) **Virtualización de aplicaciones**: ofrece facilidad de despliegue con herramientas que gestionan y automatizan miles de aplicaciones diferentes y sus actualizaciones de forma repetida y fiable. También proporciona apoyo en cuanto a la interacción de las aplicaciones. Es difícil saber cómo una actualización puede afectar a otras, incluso las actualizaciones más sencillas pueden resultar problemáticas. Algunos tipos de virtualización de aplicaciones pueden mitigar o incluso evitar este problema al encapsular todo el programa y el proceso.

2. Diseño de controles

El debido cuidado profesional en materia de ciberseguridad implica la realización de todas las prácticas razonables necesarias para cumplir un estándar mínimo de diligencia que garantice un rendimiento fiable de la seguridad a largo plazo. Si estas prácticas se llevan a cabo de forma adecuada, se puede decir que la organización ha cumplido con sus obligaciones legales y éticas de protección de la información (Kohnke, Shoemaker & Sigler, 2016).

En la práctica, la norma de atención adoptada debe incorporar todos los elementos conocidos necesarios para hacer frente a las amenazas e incidentes probables. Y dado que las consecuencias prácticas del fracaso son reales y pueden ser drásticas, la ignorancia de lo que hay que hacer no es una defensa contra la responsabilidad. De todos modos, es mucho esperar que los profesionales de la ciberseguridad conozcan y sean capaces de satisfacer los requisitos de la debida atención profesional. Por lo tanto, sería útil disponer de un modelo general de buenas prácticas de ciberseguridad para ayudar a esa comprensión. Idealmente, este modelo debería ser universal en su aplicación y comúnmente aceptado como correcto dentro de la comunidad de profesionales.

Las recomendaciones del modelo deben incorporar todas las mejores prácticas actualmente conocidas para garantizar la confidencialidad, la integridad y la disponibilidad de la información. Además, estas recomendaciones deben expresarse de forma que permitan a un profesional competente desarrollar un conjunto concreto de contramedidas para proteger la información que tiene a su cargo.

2.1. Tipos

Para simplificar la terminología, las áreas de amenaza común que podrían requerir algún tipo de control o contramedida radican según Kohnke, Shoemaker & Sigler (2016), en lo siguiente:

- Política.
- Control de la gobernanza.
- Seguridad del personal.
- Seguridad física y del entorno.
- Gestión de activos.
- Control de acceso.
- Seguridad de las operaciones.
- Seguridad de la red.
- Seguridad informática.
- Seguridad en el desarrollo y mantenimiento del software.
- Adquisición.
- Gestión de incidentes.
- Cumplimiento de la normativa.
- Continuidad.
- Elementos de los factores humanos, como la formación y la educación.

Los controles sugeridos por cada una de estas normas pueden servir como punto de referencia para desarrollar una respuesta de ciberseguridad a medida. Sin embargo, ninguno de ellos será eficaz a menos que la organización lleve a cabo un análisis exhaustivo del entorno de amenazas utilizando algún tipo de lista de comprobación u

otra orientación estándar que normalmente se desarrolla a partir del conjunto de controles recomendados.

El término que se utiliza normalmente para describir marcos como este es "modelo paraguas", en el sentido de que su propósito es definir el conjunto completo de competencias asociadas al trabajo de ciberseguridad. El uso de cualquiera de estos modelos consiste en estandarizar conceptos y términos en un conjunto de prácticas profesionales recomendadas. Dicha estandarización centra entonces la formulación de prácticas de control en objetivos de control específicos que existen dentro de cada una de las categorías estándar.

Implementación del proceso

La aplicación de cualquiera de estos modelos en un entorno práctico se posibilita y se sostiene a través de un plan estratégico de gestión de la ciberseguridad que enumera las áreas generales y actividades de control que constituirán el proceso global de gobierno de la ciberseguridad. Esto incluye el desglose de los procedimientos específicos que se seguirán para realizar el trabajo, además de todas las funciones, responsabilidades e interrelaciones de la organización que deben estar explícitamente definidas y asignadas por este plan. El producto final de este proceso es un enfoque estratégico completo y totalmente documentado de la seguridad de la información.

La siguiente secuencia presenta algunos elementos de consideración para la implementación del proceso:

a) **Establecer el esquema formal de identificación de activos**: integra todos los activos de información de la organización en una representación de base coherente para la asignación del control. En tanto el esquema de

identificación es la documentación del objetivo de control en sí mismo, define la forma del sistema de gobierno operativo para la gestión de la ciberseguridad.

b) **Acordar y explicitar los criterios para la identificación de los elementos del activo**: incluye un desglose de todos los criterios de decisión que se emplearán para definir las distintas cualidades del activo. Afirmaciones como "El elemento de información debe ser directamente rastreable y apoyar un proceso de negocio", podrían utilizarse como base para decidir si un elemento de información tiene valor para la organización.

c) **Garantizar que las personas responsables del etiquetado sigan los criterios establecidos**: importante contar con un procedimiento que posibilite el seguimiento.

d) **Identificación y etiquetado de activos**: cada activo de información se identifica y se etiqueta adecuadamente. Es esencialmente un proceso de documentación asociado al caso de negocio.

e) **Descripción de una línea de base de alto nivel de elementos**: esta línea de base desglosa los elementos que componen una determinada función del mundo real, como las facturas y las cuentas que forman parte del libro mayor. Estas líneas de base de alto nivel son más descriptivas que detalladas y se centran en el nivel de los gestores y usuarios.

f) **Detalle de elementos individuales**: se detallan todos los elementos individuales que componen los grandes elementos de la línea de base de alto nivel. Cada uno de estos elementos de datos componentes también se identifica individualmente y se etiqueta de forma única. El resultado es una descripción de elementos del mundo real que requieren control.

g) **A cada objetivo de control un conjunto de controles de comportamiento**: dado que los comportamientos de control varían en su propósito y efecto, es importante que a cada objetivo de control se le asigne un conjunto de controles de comportamiento cuidadosamente elaborados.

h) **Gestión de la configuración**: función de análisis y autorización aplicable al conjunto de objetivos de control y controles asociados. Es necesario un proceso exhaustivo considerando la constante evolución de los objetivos de control y la estructura de control que cambia en función de las alteraciones de la política y de la forma del propio activo.

2.2. Características

Con el objetivo de establecer y mantener una imagen correcta y en continua evolución de la forma de los objetivos de control y sus controles asociados, se hace necesario adelantar acciones de documentación y mantenimiento mediante una función de seguimiento y contabilidad de la línea de base. Este registro se mantiene normalmente en algún tipo de repositorio electrónico, o "libro de contabilidad" que es utilizado por la función de seguimiento y contabilidad de la línea de base de control para realizar el análisis de impacto antes de la autorización del cambio y se actualiza oportunamente una vez que el cambio ha sido aprobado e implementado.

El proceso de mantenimiento del conjunto de controles se extiende a todo el proceso de ciberseguridad y exige un análisis de los requisitos precisos de seguridad. Para ello, la organización debe adelantar las siguientes acciones:

a) **Definir comportamientos de control apropiados:** avanzar elemento por elemento a través de la línea base y decidir qué comportamientos de control

son apropiados y factibles para proteger la integridad y disponibilidad de los componentes de la información. Esta actividad se basa en el grado de riesgo estimado, cuya evaluación formal o informal, debe identificar todas las debilidades lógicas.

b) **Evaluar los tipos de amenaza: l**os tipos de amenaza se evalúan y clasifican en forma de tabla bidimensional dependiendo de si son físicos o lógicos y la fuente interna o externa, de donde provengan.

c) **Evaluar la viabilidad de los controles**: evaluar la viabilidad de cada uno de los controles que se desplegarán para responder a cada amenaza identificada. El resultado práctico del proceso de identificación de activos y formulación de la línea de base de control es un sistema de gobernanza de ciberseguridad que funciona.

d) **Formular normas, procedimientos o comportamientos de control:** estos comportamientos dictarán con precisión cómo los controles específicos de ciberseguridad interactúan entre sí dentro del esquema de gobierno. La ejecución de los comportamientos de control requeridos para cada elemento de información debe explicarse en forma de prácticas de trabajo detalladas, a las que se hace referencia en los documentos de política y procedimiento pertinentes.

e) **Especificar comportamientos concretos:** asegurarse de incluir la especificación de comportamientos concretos para dictar:

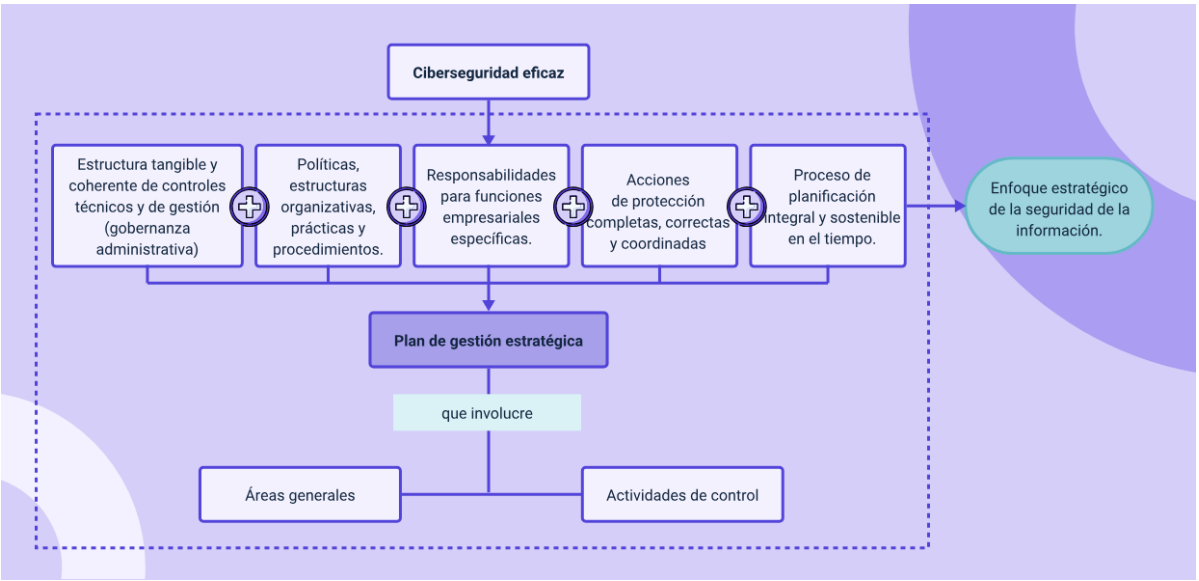
- Secuencia y calendario de utilización del control.
- Prácticas específicas de control.
- Responsabilidades.
- Documentación e informes.

- Responsabilidad en la resolución de problemas.

El campo de la ciberseguridad abarca las medidas adecuadas para garantizar que los datos electrónicos se mantengan a salvo de accesos no autorizados o de daños. Los procesos, las tecnologías y las prácticas en el campo de la ciberseguridad se desarrollan al servicio de este propósito. Un conjunto eficaz de controles de ciberseguridad debe:

- Identificar y autenticar con precisión a todas las entidades que desean acceder a un sistema.
- Autorizar el acceso sólo a los objetos que el nivel de confianza de la entidad permite.
- Supervisar y controlar las actividades durante el tiempo en que se concede el acceso a la entidad.
- Asegurar el acceso no autorizado o la manipulación de los datos.
- Asegurar la manipulación no autorizada de los objetos del sistema.

La aplicación estratégica de los principios de ciberseguridad se centra en la cuestión de decidir qué se necesita para determinar el valor de la seguridad para una organización y a partir de allí, considerar aspectos de relevancia como los que se destacan en la siguiente infografía:


Ciberseguridad eficaz
Estructura tangible y coherente de controles técnicos y de gestión (gobernanza administrativa)
Políticas, estructuras organizativas, prácticas y procedimientos.
Responsabilidades para funciones empresariales específicas.
Acciones de protección completas, correctas y coordinadas
Proceso de planificación integral y sostenible en el tiempo.
Enfoque estratégico de la seguridad de la información.
Plan de gestión estratégica
que involucre
Áreas generales
Actividades de control

3. Endurecimiento del servicio

El endurecimiento del sistema es el proceso de asegurar un servidor o sistema computacional minimizando su superficie de ataque, o superficie de vulnerabilidad, y sus potenciales vectores de ataque. Es una forma de protección contra los ciberataques que consiste en cerrar las brechas del sistema que los ciber atacantes suelen utilizar para explotar el sistema y acceder a los datos sensibles de los usuarios.

Una definición oficial de endurecimiento del sistema, según el Instituto Nacional de Normas y Tecnología (NIST), es que se trata de **"un proceso destinado a eliminar un medio de ataque mediante la aplicación de parches a las vulnerabilidades y la desactivación de servicios no esenciales".**

Parte del proceso de eliminación del endurecimiento del sistema consiste en eliminar o desactivar las aplicaciones del sistema, los permisos, los puertos, las cuentas de usuario y otras características innecesarias para que los atacantes tengan menos oportunidades de acceder a la información sensible de un sistema informático de misión crítica o de infraestructura crítica.
Ackerman, P. (2017).

Pero en esencia, el endurecimiento del sistema es un método para proteger un sistema contra los ataques perpetrados por los ciberdelincuentes. Consiste en asegurar el software de un sistema de cómputo, principalmente, pero también su “firmware”, redes y otros elementos del sistema para reducir las vulnerabilidades y un posible compromiso de todo el sistema.

Existen cinco tipos principales de endurecimiento del sistema:

- Endurecimiento de servidores.

- Endurecimiento de aplicaciones de “software”.
- Endurecimiento del sistema operativo.
- Endurecimiento de la base de datos.
- Endurecimiento de la red.

Es importante tener en cuenta que los tipos de endurecimiento del sistema son lo suficientemente amplios como para ser universales y traducirse bien a través de diferentes configuraciones de servidores y sistemas computacionales; sin embargo, los métodos y herramientas utilizados para lograr prácticamente un estado endurecido o seguro por diseño varían ampliamente.

3.1. Características

Endurecer la infraestructura de una red es un proceso, no una tarea. Es algo que, una vez iniciado, no termina. Se debe permanecer constantemente atento a las amenazas que se ciernen sobre la red y emprender de forma continua acciones para prevenir cualquier peligro. Debido a la escala de una empresa, el endurecimiento de la infraestructura de la red no es un esfuerzo que deba emprender a la ligera. Dependiendo del tamaño y la complejidad de su entorno, podría pasar semanas o incluso meses planificando antes de realizar cualquier cambio. (Ackerman, 2017).

Al mismo tiempo, si se está estudiando cómo reforzar la red, probablemente se pueda reconocer que hay problemas de seguridad que deben ser abordados, incluso si no se está seguro de cuáles son exactamente esos problemas o cómo solucionarlos. Esto puede ser un inconveniente, ya que puede tener problemas que realmente

necesitan ser abordados inmediatamente, antes de que comience el proceso de endurecimiento a gran escala.

Hay muchas tareas que se pueden realizar como parte del proceso de endurecimiento sistemático. Por lo general, todas ellas de gran envergadura, como por ejemplo, el endurecimiento de los routers y switches o la implementación de DMZ (Zonas desmilitarizadas) y dispositivos de red perimetral. Estas tareas llevan tiempo, a veces meses, desde la fase inicial de planificación y diseño hasta la implementación. Y aunque todas son necesarias, se debería realizar seis tareas, en particular, antes de hacer cualquier otra cosa en su red, tome nota:

- **Revisar el diseño de la red**: el primer paso para reforzar la red es comprenderla: cómo están interconectados los dispositivos, cómo fluyen los datos en la empresa.
- **Implantar un cortafuego**: tiene el mayor impacto de cualquier tarea que se pueda realizar para endurecer la infraestructura de red porque permite definir un perímetro.
- **Implementar listas de control de acceso (ACL)**: se debería restringir y controlar todo el tráfico que entra y sale de la red al exterior y entre los segmentos de la red interna. Si no hay justificación comercial para el tráfico, hay que bloquearlo. Filtrar el tráfico con ACL en los cortafuegos y routers tanto internos como externos.
- **Desactivar funciones y servicios innecesarios**: aunque tradicionalmente se trata del ámbito de los servidores y las aplicaciones, los servicios innecesarios también afectan a los dispositivos de la infraestructura de red.

Si no hay una razón para ejecutar un servicio concreto en el equipo de red, no hay que hacerlo.

- **Implementar la protección contra virus**: los gusanos y virus actuales provocan a menudo ataques de denegación de servicio distribuido (DDoS) contra los router y los conmutadores. La forma más fácil de protegerse es con protección antivirus que incluya dispositivos de entrada y pasarelas SMTP, para evitar los virus y gusanos basados en el correo electrónico.
- **Asegurar las conexiones inalámbricas**: la conectividad inalámbrica presenta un problema único para asegurar la red. Si no está seguro de por qué utiliza una red inalámbrica, apáguela. Si se tiene que utilizar, asegúrese de implementar el cifrado y la autenticación para evitar que usuarios no autorizados se conecten y/o intercepten sus comunicaciones inalámbricas.

3.2. Marcos y técnicas de endurecimiento

La seguridad de las aplicaciones engloba los controles y actividades destinados a encontrar, solucionar y prevenir las vulnerabilidades de las aplicaciones y su entorno de ejecución. Las vulnerabilidades que suelen encontrarse en las aplicaciones pueden dividirse en las categorías que se presentan a continuación.

Vulnerabilidades de validación de entrada

La debilidad más común en la seguridad de las aplicaciones es no validar adecuadamente la entrada procedente de un usuario o del entorno en el que se ejecuta la aplicación antes de utilizarla. Al no escudriñar la entrada en su aplicación, se puede

desencadenar un comportamiento inesperado de la aplicación al forzarla a ejecutar fragmentos de un lenguaje de scripting o reenviar comandos sensibles del sistema.

Las aplicaciones ICS pueden sufrir este tipo de vulnerabilidades tanto como cualquier otro "software". Los programas HMI personalizados, la lógica de los controladores y las utilidades caseras a menudo no tienen en cuenta la validación de las entradas y son los principales candidatos a los ataques. Además, los dispositivos ICS a menudo vienen con páginas web integradas para fines de diagnóstico que se ejecutan en servidores web mal implementados con todo tipo de vulnerabilidades propias. Estos servidores web a menudo ejecutan aplicaciones web que utilizan una pobre validación de entrada, preparándose para ataques de inyección SQL, XSS y desbordamiento de búfer.

Los ataques más comunes asociados a las vulnerabilidades de validación de entrada son:

- Desbordamiento del búfer.
- Secuencia de comandos en sitios cruzados.
- Inyección de código.
- Inyección de SQL.
- Canonización de comandos del sistema operativo.

Nunca hay que confiar en los datos externos, investigue las técnicas de validación de entrada adecuadas para su aplicación y haga que las pruebas de validación de entrada formen parte de su proceso de desarrollo de aplicaciones.

Manipulación del software

La manipulación del "software" consiste en realizar modificaciones en el código de la aplicación antes o durante su ejecución. Al cambiar el código de una aplicación en la memoria o en el disco duro, se pueden eludir los controles de protección. Estas modificaciones pueden, por ejemplo, permitir al atacante eludir los mecanismos de autenticación o eludir las restricciones de licencia. Además, el "firmware" de un dispositivo puede ser alterado para permitir a un atacante el acceso por la puerta trasera al funcionamiento interno de un dispositivo. Con este tipo de acceso, el atacante puede buscar más vulnerabilidades en áreas del "firmware" que normalmente no son accesibles. Como ejemplo, en 2015 la empresa de seguridad ICS, CyberX, utilizó esta técnica para modificar el código del servidor web del" firmware" *de un PLC Micrologix 1100 de Rockwell Automation* para darles acceso al funcionamiento interno del PLC. Este acceso, a su vez, les permitió descubrir la vulnerabilidad *FrostyURL*.

Los ataques más comunes asociados a las vulnerabilidades de manipulación de software son:

- Modificación del comportamiento en tiempo de ejecución de una aplicación para realizar acciones no autorizadas.
- Explotación mediante parches binarios, sustitución de código o extensión de código. Crackeo de licencias de "software".
- Troyanización de aplicaciones.

Siempre se debe obtener el software de fuentes fiables. Si se descarga “software” pirata, se obtienen las actualizaciones de lugares aleatorios o se utilizan medios de instalación que se han pasado, se está exponiendo a ataques de “software” "troyanizado" o a un firmware manipulado. Siempre que sea posible, sus dispositivos de automatización deberían permitirle ejecutar imágenes de “firmware” firmadas criptográficamente. Esto implica que el dispositivo tenga la capacidad de verificar la integridad y validez del “firmware” antes de arrancarlo. Para evitar que su “software” sea manipulado, siga estas recomendaciones de buenas prácticas:

- Ejecute siempre cualquier aplicación como usuario restringido en un entorno restringido.
- Mantenga las aplicaciones y el “firmware” actualizados.
- Descargue siempre los instaladores de “software” y las imágenes de “firmware” del sitio web del proveedor. Restrinja el acceso al ordenador o dispositivo que ejecuta el “software” o “firmware” en la medida de lo posible, impidiendo acceso a puertos periféricos, como USB y “Firmware”, a los puertos de diagnóstico y depuración, y acceso físico al ordenador o dispositivo.

Vulnerabilidades de autenticación

Las vulnerabilidades de esta categoría incluyen el no comprobar adecuadamente la autenticación del usuario o eludir el sistema de autenticación por completo. Al igual que las vulnerabilidades de validación de entrada, suelen estar causadas por los programadores que asumen que los usuarios se comportarán de una determinada

manera y no prevén las consecuencias de que los usuarios hagan algo inesperado. Un ejemplo muy básico de una vulnerabilidad de autenticación, que se encuentra en las aplicaciones web o en los equipos de red, es cuando la aplicación simplemente pide un nombre de usuario y una contraseña en la página de inicio de sesión y luego permite a los usuarios autorizados el acceso sin restricciones a otras páginas web sin ninguna otra comprobación.

El problema con esto es que asume que la única manera de llegar a las páginas de configuración es a través de la página de inicio de sesión. Por otro lado, ¿qué pasa si los usuarios pueden ir directamente a las páginas de configuración escribiendo la URL, saltándose la autenticación?

Muchos productos de proveedores de ICS han sufrido vulnerabilidades de derivación de autenticación. Un ejemplo es una vulnerabilidad de derivación de autenticación encontrada en varios productos de Siemens. La vulnerabilidad permite a un atacante eludir la autenticación del usuario en el proceso de inicio de sesión de SYMANTEC.

Los ataques más comunes asociados a las vulnerabilidades de autenticación son los siguientes:

- Evasión del inicio de sesión.
- Manipulación de parámetros fijos Ataques de fuerza bruta y de diccionario.
- Repetición de “Kcookies”.
- Ataques “Pass-the-hash”.

Una medida eficaz, utilizada para detener los ataques de autenticación (automatizados), es añadir contenido aleatorio a la página de inicio de sesión presentada al cliente o usuario que se autentifica. El usuario debe ser capaz de enviar con éxito este contenido aleatorio como parte del proceso de autenticación para poder continuar en el sitio web o la aplicación. Otras medidas preventivas o correctivas incluyen procedimientos de autenticación rigurosos, el uso de "tokens" de autenticación sensibles al tiempo y restricciones a los intentos de autenticación fallidos.

Vulnerabilidades de autorización

La autorización es el concepto de permitir el acceso a los recursos sólo a aquellos que están autorizados a utilizarlos. Es el proceso que viene después de una autenticación exitosa, por lo que el usuario, en este punto, tendrá credenciales válidas asociadas a un conjunto bien definido de roles y privilegios. Las vulnerabilidades de esta categoría implican la verificación de los roles y privilegios. Al usuario se le permite más acceso a la aplicación o al sistema de lo necesario para realizar la tarea.

Los ataques más comunes asociados a las vulnerabilidades de autorización son:

- Elevación de privilegios.
- Manipulación de datos.
- Divulgación de datos confidenciales
- Ataques de seducción

Ante este tipo de vulnerabilidad, tenga en cuenta:

- Utilizar privilegios y funciones granulares para los usuarios.

- Adhiérase a las mejores prácticas de necesidad de conocimiento y de mínimo privilegio cuando configure cuentas o funciones de usuario.
- Imponga tiempos de espera en las sesiones iniciadas y realice comprobaciones.

Vulnerabilidades de configuración inseguras

Las configuraciones desempeñan un papel fundamental en la seguridad de una aplicación. A menudo, los sistemas y las aplicaciones se ejecutan con una configuración por defecto, extraída del manual del proveedor o de Internet. Esto hace que adivinar las contraseñas, eludir las páginas de inicio de sesión y encontrar vulnerabilidades de configuración bien conocidas sea muy fácil. Otra forma de gestión de la configuración insegura es cuando una configuración es simplemente errónea, ya sea desde el principio o después de haber realizado cambios que comprometen la seguridad de la aplicación o el sistema. Esta configuración defectuosa puede acabar utilizándose en cualquier lugar de la empresa.

Los ataques más comunes asociados a las vulnerabilidades en la gestión de la configuración son los siguientes:

- Defectos en el "software" del servidor o configuraciones erróneas que permiten el listado de directorios y los ataques de cruce de directorios.
- Archivos innecesarios por defecto, de copia de seguridad o de muestra, incluyendo scripts, aplicaciones, archivos de configuración y páginas web.
- Permisos inadecuados de archivos y directorios.
- Servicios innecesarios habilitados, incluyendo la gestión de contenidos y la administración remota.

- Cuentas por defecto con sus contraseñas por defecto.
- Funciones administrativas o de depuración habilitadas o accesibles.
- Mensajes de error demasiado informativos (más detalles en la sección de gestión de errores).
- Certificados SSL y ajustes de cifrado mal configurados.
- Uso de certificados autofirmados para lograr la autenticación y la protección “man-in-the-middle”.
- Uso de certificados por defecto.
- Autenticación incorrecta con sistemas externos

La mejor defensa contra las vulnerabilidades de la configuración insegura es la gestión rigurosa de sus configuraciones. Debe adherirse a un estricto proceso de gestión de la configuración, definiendo los procedimientos en torno a la creación, el cambio y la verificación de las configuraciones. Debe detallar cómo deben configurarse las aplicaciones antes de su despliegue, cómo abordar los cambios de configuración y cómo verificar periódicamente que las configuraciones están actualizadas y siguen siendo relevantes desde el punto de vista de la seguridad.

Vulnerabilidades en la gestión de sesiones

Una sesión de red es una secuencia de transacciones de solicitud y respuesta asociadas al mismo usuario. Las sesiones proporcionan la capacidad de establecer variables, como derechos de acceso y ajustes de localización, que se aplicarán a cada interacción que un usuario tenga con la aplicación web durante la duración de la sesión. Las aplicaciones web, por ejemplo, pueden crear sesiones para hacer un seguimiento de los usuarios conectados después del proceso de inicio de sesión. Esto asegura la

capacidad de identificar al usuario en cualquier solicitud posterior, así como permite aplicar controles de seguridad de acceso, autorizar el acceso a los datos privados del usuario y aumentar la usabilidad de la aplicación. Las vulnerabilidades en esta categoría están relacionadas con la creación, el seguimiento y la eliminación de los identificadores de sesión. Mediante una mala gestión de la sesión, un atacante puede adivinar o reutilizar una clave/ID de sesión y apoderarse de la sesión y de la identidad de un usuario legítimo.

Los ataques más comunes asociados a las vulnerabilidades de la gestión de sesiones incluyen:

- Secuestro de sesión
- Repetición de sesión
- Ataques de intermediario (“Man-in-the-middle”).

Asegúrese de que utiliza técnicas adecuadas de gestión de sesiones, adhiriéndose a buenas prácticas como la generación aleatoria de sesiones (claves) el seguimiento adecuado de las sesiones y la finalización adecuada de las mismas. Añada valores únicos para el usuario a una clave de sesión para minimizar el riesgo de interceptación y reutilización de las claves de sesión.

Vulnerabilidades de manipulación de parámetros

Las vulnerabilidades de manipulación de parámetros permiten manipular los parámetros intercambiados entre un cliente y el servidor con el fin de modificar los datos de la aplicación, como las credenciales y los permisos de los usuarios, el precio y la cantidad de los productos. Esta información puede almacenarse en “cookies”, en campos de formularios ocultos o en cadenas de consulta de URL.

En los primeros días de las tiendas web en línea, los programadores cometieron el costoso error de codificar el precio de un artículo como un campo de formulario oculto en sus páginas HTML. Los atacantes simplemente descargaban el archivo HTML de la tienda web, cambiaban el precio y hacían el pedido con un enorme descuento. Este es un ejemplo clásico de una vulnerabilidad de manipulación de parámetros.

Los ataques más comunes asociados a las vulnerabilidades de manipulación de parámetros son los siguientes:

- Manipulación de cadenas de consulta.
- Manipulación de campos de formulario Manipulación de "cookies".
- Manipulación de cabeceras HTTP.
- La defensa contra este tipo de vulnerabilidades incluye prácticas de codificación adecuadas y una estricta validación de entradas.

Pruebas de seguridad de las aplicaciones

Entonces, ¿cómo descubrir si alguna de estas vulnerabilidades está presente en las aplicaciones desplegadas en una red ICS? La respuesta es probando todas las aplicaciones instaladas en busca de vulnerabilidades. Se hace hincapié en todas las aplicaciones instaladas porque primero hay que conocer todas las aplicaciones que se están ejecutando en la red ICS. Aquí es donde los procedimientos de gestión de activos ayudarán. No se puede asegurar aquello que no se sabe que se tiene. Mantener una lista de activos actualizada con información que incluya versiones de "software", niveles de parches y revisiones de "firmware" debería ser la mayor prioridad.

Una lista precisa de activos permite comparar la revisión y los niveles de parches de cada aplicación en la red ICS contra una lista de vulnerabilidades conocidas para la

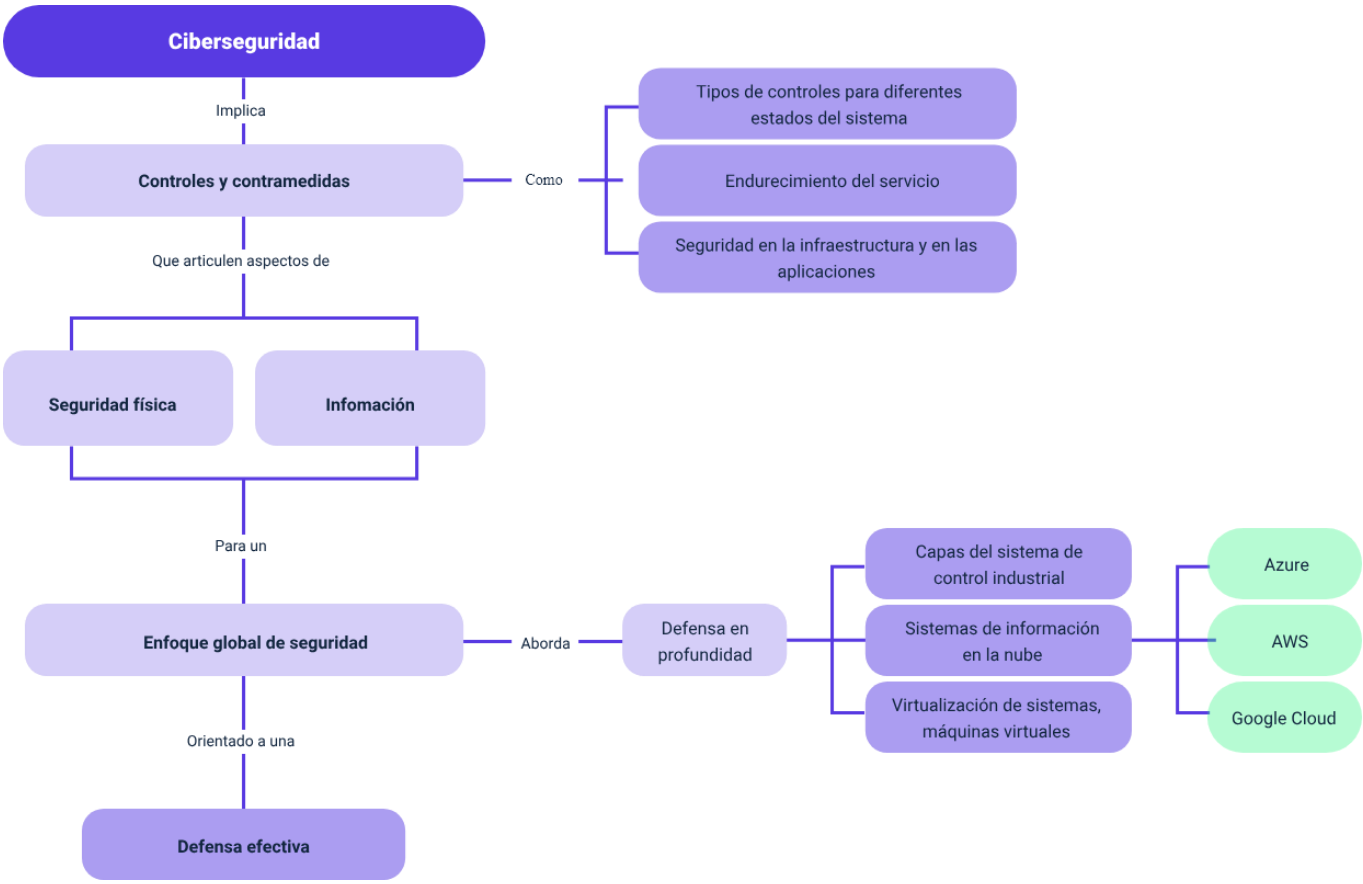
aplicación. Este proceso se puede hacer manualmente o con la ayuda de una herramienta automatizada como el escáner de vulnerabilidad Nessus.

Otra área de las pruebas de vulnerabilidad de las aplicaciones implica una comparación de la configuración de las aplicaciones con una base de datos de mejores prácticas y configuraciones seguras conocidas, mientras se buscan discrepancias. Una vez más, esto puede ser un proceso manual, o se puede lograr con la ayuda de una herramienta automatizada.

Los métodos de prueba mencionados anteriormente funcionan bien para aplicaciones conocidas que tienen listas y bases de datos de problemas y configuraciones conocidas. En el caso de las aplicaciones que no son bien conocidas - pensemos en las aplicaciones caseras o las construidas a medida- es necesario un enfoque diferente. Este tipo de aplicaciones necesitan ser verificadas manualmente para detectar la presencia de cualquiera de las vulnerabilidades discutidas en la sección anterior. Esto puede ser un proceso manual en el que, por ejemplo, una persona prueba todos los campos de entrada posibles de una aplicación para una validación de entrada adecuada.

Síntesis

Revise el siguiente esquema que a manera de síntesis articula los elementos principales abordados en el desarrollo del componente formativo.



Material complementario

Tema	Referencia	Tipo de material	Enlace del recurso
Defensa en profundidad	Hadlington, L. (2017). Human factors in cybersecurity; examining the link between Internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours. Heliyon, 3(7), 1-18.	Artículo	https://sena-primo.hosted.exlibrisgroup.com/primo-explore/fulldisplay?docid=TN_cdi_doaj_primary_oai_doaj_org_article_c3640829408444539879ceeb75d871ba&vid=SENA&search_scope=sena_completo&tab=sena_completo&lang=es_ES&context=PC
Defensa en profundidad	Rios Insua, D., Couce-Vieira, A., Rubio, J., Pieters, W., Labunets, K., & G Rasines, D. (2021). An Adversarial Risk Analysis Framework for Cybersecurity. Risk Analysis, 41(1), 16-36.	Artículo	https://sena-primo.hosted.exlibrisgroup.com/primo-explore/fulldisplay?docid=TN_cdi_crossref_primary_10_1111_risa_13331&vid=SENA&search_scope=sena_completo&tab=sena_completo&lang=es_ES&context=PC

Glosario

AAA: autenticación, autorización y contabilidad.

ACL: listas de control de acceso.

AWS: nube de Amazon.

AZURE: nube de Microsoft.

DHCP: protocolo de configuración dinámica de host.

DNS: protocolo de sistema de nombres de dominio.

***Dockerfile*:** archivo para configurar contenedores de Docker.

DOS: ataque de negación de servicio.

IDS: sistemas de detección de intrusos.

PLC: controlador lógico programable.

SCD: sistema de control distribuido.

SCI: sistema de control interno.

Sistemas ERP: estaciones de trabajo de usuarios finales.

UI: interfaz de usuario.

Referencias bibliográficas

Ackerman, P. (2017). *Industrial cybersecurity: efficiently secure critical infrastructure systems. Packt Publishing Ltd*

Cohen, M., Hurley, K. & Newson, P. (2014). *Google compute engine: managing secure and scalable cloud computing.*

Kohnke, A., Shoemaker, D., & Sigler, K. E. (2016). *The complete guide to cybersecurity risks and controls. CRC Press.*

Li, H. (2009). *Introduction to windows azure. Apress.*

Noonan, W. (2004). *Hardening Network Infrastructure: Bulletproof Your Systems Before You Are Hacked!. Osborne.*

Popek, G. J., & Goldberg, R. P. (1974). Formal requirements for virtualizable third generation *architectures. Communications of the ACM, 17(7), 412-421.*https://doi.org/10.1145/361011.361073

Portnoy, M. (2012). *Virtualization essentials (Vol. 19). John Wiley & Sons.*

Wittig, M. & Wittig, A. (2018). *Amazon web services in action. Manning.*

Créditos

Nombre	Cargo	Regional y Centro de Formación
Claudia Patricia Aristizábal	Líder del Ecosistema	Dirección General
Rafael Neftalí Lizcano Reyes	Responsable de Línea de Producción	Centro Industrial del Diseño y la Manufactura - Regional Santander
Joaquín Fernando Sánchez	Experto Temático	Centro de la Industria, la Empresa y los Servicios - Regional Norte de Santander
Maribel Avellaneda Nieves	Diseñadora Instruccional	Centro de la Industria, la Empresa y los Servicios - Regional Norte de Santander
Silvia Milena Sequeda Cárdenas	Asesora Pedagógica y Metodológica	Centro de diseño y Metrología - Regional Distrito Capital
Sandra Patricia Hoyos Sepúlveda	Correctora de Estilo	Centro de diseño y Metrología - Regional Distrito Capital
Francisco José Lizcano Reyes	Desarrollador Fullstack	Centro Industrial del Diseño y la Manufactura - Regional Santander
Juan Daniel Polanco Muñoz	Diseñador de Contenidos Digitales	Centro Industrial del Diseño y la Manufactura - Regional Santander
Wilson Andrés Arenales Cáceres	Storyboard e Ilustración	Centro Industrial del Diseño y la Manufactura - Regional Santander
Carmen Alicia Martínez Torres	Animador y Productor Multimedia	Centro Industrial del Diseño y la Manufactura - Regional Santander
Emilsen Alfonso Bautista	Actividad Didáctica	Centro Industrial del Diseño y la Manufactura - Regional Santander
Zuleidy María Ruíz Torres	Validador de Recursos Educativos Digitales	Centro Industrial del Diseño y la Manufactura - Regional Santander

Nombre	Cargo	Regional y Centro de Formación
Luis Gabriel Urueta Álvarez	Validador de Recursos Educativos Digitales	Centro Industrial del Diseño y la Manufactura - Regional Santander
Daniel Ricardo Mutis	Evaluador para Contenidos Inclusivos y Accesibles	Centro Industrial del Diseño y la Manufactura - Regional Santander