Guía de Controles Críticos de Ciberseguridad

Introducción:

Los Controles Críticos de Ciberseguridad son un conjunto de acciones, priorizadas, ampliamente analizadas y de efectividad probada que pueden ser tomadas por las organizaciones para mejorar su nivel de ciberseguridad. Esta guía nace como una iniciativa de estandarizar, ordenar, priorizar y medir los esfuerzos en ciberseguridad que están llevando a cabo los organismos paraguayos, de modo a construir un ciberespacio seguro y resiliente.

Metodología utilizada:

El CERT-PY basa sus esfuerzos en los siguientes principios:

- No reinventar la rueda: aprovechar y apoyarse en los conocimientos y esfuerzos aportados y compartidos por la comunidad para, de esta manera, crear más conocimiento y de mayor calidad

- Apoyarse en la experiencia en cuanto a incidentes y ataques reales observados en la región y específicamente en el país para la definición de estrategias de protección prácticas, reales y efectivas.

Es por ello que hemos decidido adoptar los "CIS Critical Security Controls" (Controles Críticos de Seguridad de CIS), un conjunto de 20 controles prioritarios, elaborados de manera consensuada por Center for Internet Security (CIS), una organización sin fines de lucro basada en Estados Unidos y una gran comunidad de actores claves del ecosistema de la ciberseguridad: organismos de gobierno, empresas de tecnología y de seguridad, auditores, equipos de respuesta a incidentes, usuarios, entre otros.

La metodología utilizada para la elaboración de los "CIS Critical Security Controls" se basa en:

- compartir conocimientos sobre ataques y atacantes, identificando las causas y traduciéndolas a acciones defensivas
- identificar problemas comunes en un modelo de colaboración de comunidad
- documentar experiencias de adopción y compartir herramientas para resolver problemas

- dar seguimiento a la evolución de las amenazas, las capacidades de los adversarios y los vectores de intrusión actuales
- mapear los controles a *frameworks* de regulación y cumplimiento

Los cinco principios fundamentales de un sistema efectivo de defensa cibernética como se refleja en los controles CIS son:

1. **La ofensa informa a la defensa:** utilice el conocimiento de los ataques reales que han comprometido los sistemas para proporcionar la base para aprender continuamente de estos eventos y construir defensas efectivas y prácticas. Incluya sólo aquellos controles demostrados para detener ataques conocidos del mundo real.

2. **Priorización:** Invierta primero en los controles que proporcionarán la mayor reducción de riesgos y protección contra los actores más peligrosos y que se pueden implementar de manera viable en su entorno informático.

3. **Mediciones y métricas**: establezca parámetros comunes para proporcionar un lenguaje compartido para ejecutivos, especialistas en TI, auditores y funcionarios de seguridad para medir la efectividad de las medidas de seguridad dentro de una organización, de modo que los ajustes necesarios se puedan identificar e implementar rápidamente.

4. **Diagnóstico y mitigación continuos**: realice mediciones continuas para probar y validar la efectividad de las medidas de seguridad actuales y para ayudar a dirigir la prioridad de los siguientes pasos.

5. **Automatización:** automatice las defensas para que las organizaciones puedan lograr mediciones confiables, escalables y continuas de su adhesión a los controles y las métricas relacionadas.

Al tomar como base los controles CIS y adaptarlos a nuestra realidad nacional, aprovechamos todo el conocimiento, la experiencia y las múltiples herramientas que han sido elaboradas a lo largo de los años por una enorme comunidad internacional, añadiéndole además las consideraciones propias para una organización paraguaya, así como también la retroalimentación con experiencias nacionales.

De esta manera, los controles están alineados a la protección efectiva a ataques reales conocidos. La metodología utilizada para la elaboración de la Guía de Controles

Críticos de Ciberseguridad hace posible que no se trate únicamente de una lista de buenas prácticas sino un conjunto de pocas acciones, priorizadas y focalizadas, que a su vez son implementables, usables, escalables y orientadas al cumplimiento de los requerimientos de seguridad de industrias y gobierno.

Estructura de la Guía de Controles Críticos de Ciberseguridad:

La presentación de cada control de este documento incluye lo siguiente:

- Descripción de la importancia de cada control **(¿Por qué es importante este control?)** en cuanto al bloqueo o identificación de un ataque y una explicación de cómo un atacante explota activamente la ausencia de dicho control
- Una tabla de acciones específicas **("sub-controles")** que una organización debe tomar para implementar el control
- **Procedimientos y herramientas** que permiten la implementación y automatización del control
- Ejemplo de **diagramas de relaciones de entidades** que muestran los componentes de la implementación.

Controles Básicos:

Control 1: Inventario de Dispositivos autorizados y no autorizados
Control 2: Inventario de Software autorizados y no autorizados
Control 3: Gestión continua de vulnerabilidades
Control 4: Uso controlado de privilegios administrativos
Control 5: Configuración segura para hardware y software en dispositivos móviles, computadoras portátiles, estaciones de trabajo y servidores
Control 6: Mantenimiento, monitoreo y análisis de logs de auditoría

Controles Fundacionales:

Control 7: Protección de correo electrónico y navegador web
Control 8: Defensa contra malware
Control 9: Limitación y control de puertos de red, protocolos y servicios
Control 10: Capacidad de recuperación de datos
Control 11: Configuración segura de los equipos de red, tales como cortafuegos, enrutadores y conmutadores
Control 12: Defensa de borde
Control 13: Protección de datos
Control 14: Control de acceso basado en la necesidad de conocer
Control 15: Control de acceso inalámbrico
Control 16: Monitoreo y control de cuentas

Controles Organizacionales:

Control 17: Implementar un programa de concienciación y capacitación en seguridad
Control 18: Seguridad del software de aplicación
Control 19: Respuesta y gestión de incidentes
Control 20: Pruebas de penetración y ejercicios de Equipo Rojo

Control 1: Inventario de Dispositivos autorizados y no autorizados

Gestione activamente todo dispositivo hardware en la red (inventario, seguimiento y corrección), de tal manera que solo los dispositivos autorizados obtengan acceso y que los dispositivos no autorizados y no gestionados sean detectados y se prevenga que obtengan acceso.

¿Por qué es importante este control?

Atacantes que pueden estar situados en cualquier parte del mundo están escaneando continuamente el espacio de direcciones de las organizaciones que desean atacar, esperando a que se conecten sistemas nuevos y desprotegidos a la red. Los atacantes tienen un interés particular en equipos que se conectan y desconectan de la red, tales como laptops o BYOD (*Bring-Your-Own-Devices*), los cuales podrían estar desincronizado de los parches o actualizaciones de seguridad o que ya podrían estar comprometidos. Los atacantes pueden aprovechar el hardware nuevo que se instala en la red un día pero que no se configuran y actualizan adecuadamente hasta el día siguiente. Incluso, los equipos que no están visibles desde Internet pueden ser utilizados por un atacante, que previamente ha ganado acceso a la red interna, como punto de pivot para otros ataques. Sistemas adicionales que son conectados a la red corporativa, tales como sistemas de demostración, de prueba temporales, de invitados, etc. deben ser gestionados cuidadosamente y/o aislados de modo a prevenir un acceso hostil a través de la vulneración de éstos.

Organizaciones grandes y complejas luchan, comprensiblemente, con el desafío de gestionar entornos intrincados y que cambian rápidamente. Pero los atacantes han demostrado la capacidad, la paciencia y la intención para "inventariar y controlar" nuestros activos a gran escala a fin de respaldar sus oportunidades.

El control gestionado de todos los equipos juega un rol crítico en la planificación y ejecución de copias de seguridad, respuesta a incidentes y recuperación de sistemas.

Control crítico #1: Inventario y control de activos hardware				
Sub-control	**Tipo de activo**	**Función de Seguridad**	**Control**	**Descripción**
1.1	Equipos	Identificar	Utilizar una herramienta de descubrimiento activo	Utilice una herramienta de descubrimiento activo para identificar equipos conectados a la red de la organización y actualizar el inventario de activos hardware.
1.2	Equipos	Identificar	Utilizar una herramienta de descubrimiento pasivo de activos	Utilice una herramienta de descubrimiento pasivo para identificar dispositivos conectados a la red de la organización y actualizar automáticamente el inventario de activos.
1.3	Equipos	Identificar	Utilizar DHCP Logging para	Utilice un sistema de logging de DHCP (Dynamic Host Configuration Protocol) en todos los servidores DHCP o

			actualizar el inventario de activos	herramientas de gestión de direcciones IPs para actualizar el inventario de activos hardware de la organización.
1.4	Equipos	Identificar	Mantener un inventario de activos detallado	Mantenga un inventario veraz y actualizado de todos los activos tecnológicos capaces de almacenar y/o procesar información. El inventario debe incluir todos los activos de hardware, estén o no conectados a la red de la organización.
1.5	Equipos	Identificar	Mantener la información del inventario de activos	Asegúrese que el inventario de activos de hardware registre, como mínimo, las direcciones de red, nombre, propósito, responsable, departamento de cada activo, así como también si el activo de hardware ha sido aprobado o no para ser conectado a la red.
1.6	Equipos	Responder	Gestionar los activos no autorizados	Asegúrese de que los activos no autorizados se eliminen de la red, se pongan en cuarentena o el inventario se actualice oportunamente.
1.7	Equipos	Proteger	Implementar control de acceso a nivel de puerto	Implemente control de acceso a nivel de puertos según el estándar 802.1x para limitar y controlar qué equipo puede autenticarse en la red. El sistema de autenticación debe estar vinculado a los datos de inventario de activos hardware para asegurar que sólo los equipos autorizados se pueden conectar a la red.
1.8	Equipos	Proteger	Utilizar certificados clientes para autenticar activos hardware	Utilice certificados clientes para autenticar los activos de hardware que se conectan a la red de confianza de la organización.

Control 1: Procedimientos y herramientas

Este control requiere tanto acciones técnicas como procedimentales, unidas en un proceso que rinda cuentas y gestione el inventario de hardware y toda la información asociada a lo largo del ciclo de vida. Vincula al gobierno corporativo estableciendo propietarios de información / activos que son responsables de cada componente de un proceso de negocio que incluye información, software y hardware. Las organizaciones pueden usar productos integrales de gran escala para mantener los inventarios de activos de TI. Otros utilizan herramientas más modestas para recopilar los datos al barrer la red y administrar los resultados por separado en una base de datos.

Mantener una visión actualizada y acertada de los activos de TI es un proceso continuo y dinámico. Las organizaciones pueden escanear la red activamente de forma regular, envidando una variedad de diferentes paquetes para identificar equipos conectados a la misma. Previo a dicho escaneo, la organización debería verificar que se cuente con un ancho de banda adecuado para dichos escaneos periódicos, verificando el historial de carga y la capacidad de la red.

Al realizar un escaneo de inventario, las herramientas de escaneo pueden enviar paquetes tradicionales de ping (ICMP Echo Request) de modo a esperar respuestas de ping que permitan identificar sistemas en una determinada IP. Teniendo en cuenta que algunos sistemas bloquean paquetes de ping, además del ping tradicional, los

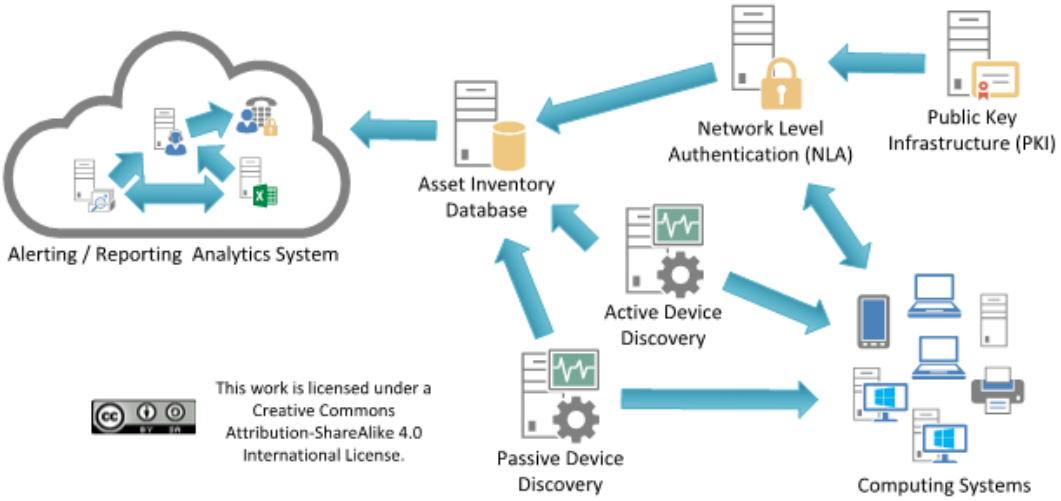
scanners pueden identificar equipos utilizando paquetes de sincronización (SYN) o de confirmación (ACK) TCP. Una vez que se hubiera identificado IPs de equipos en la red, algunos *scanners* proporcionan funcionalidades de *fingerprinting* robustas para determinar el tipo de sistema operativo del dispositivo descubierto.

Además de las herramientas de escaneo activo que barren la red, existen herramientas de identificación de activos que escuchan pasivamente una interfaz de red para descubrir equipos que anuncian su presencia mediante el envío de tráfico. Dichas herramientas pasivas pueden ser conectados a puertos espejos del *switch* en puntos estratégicos de la red de modo a visualizar todo el flujo de datos que pasa por dicho *switch*, maximizando la posibilidad de identificar sistemas que se comunican a través de éste.

Muchas organizaciones también extraen información de los activos de la red, como conmutadores y enrutadores, con respecto a las máquinas conectadas a la red. Mediante el uso de protocolos de administración de red autenticados y encriptados, las herramientas pueden recuperar direcciones MAC y otra información de dispositivos de red que se pueden conciliar con el inventario de servidores, estaciones de trabajo, computadoras portátiles y otros dispositivos de la organización. Una vez que se confirman las direcciones MAC, los *switches* deben implementar 802.1x y NAC para permitir que solo los sistemas autorizados que están configurados correctamente se conecten a la red.

Tanto los dispositivos inalámbricos como los portátiles cableados pueden unirse periódicamente a una red y luego desaparecer, lo que hace que el inventario de los sistemas actualmente disponibles sea muy dinámico. Del mismo modo, las máquinas virtuales pueden ser difíciles de rastrear en los inventarios de activos cuando se apagan o se detienen. Además, las máquinas remotas que acceden a la red usando tecnología de red privada virtual (VPN) pueden aparecer en la red por un tiempo y luego desconectarse de ella. Ya sea física o virtual, cada máquina que usa una dirección IP debe incluirse en el inventario de activos de una organización.

Control 1: Diagrama de relaciones de entidad de sistema



Control 2: Inventario de Software autorizados y no autorizados

Gestione activamente todo software en la red (inventario, seguimiento y corrección), de tal manera que solo software autorizado esté instalado y pueda ejecutarse, y que el software no autorizado y no gestionado sea encontrado y se prevenga su instalación y ejecución.

¿Por qué es importante este control?

Los atacantes escanean continuamente a las organizaciones objetivo en busca de versiones vulnerables de software que pueden explotarse de forma remota. Algunos atacantes también distribuyen páginas web, archivos de documentos, archivos multimedia y otros contenidos hostiles a través de sus propias páginas web o sitios de terceros de confianza. Cuando las víctimas desprevenidas acceden a este contenido con un navegador vulnerable u otro programa del lado del cliente, los atacantes comprometen sus máquinas, a menudo instalando programas de puerta trasera y *bots* que le dan al atacante un control a largo plazo del sistema. Algunos atacantes sofisticados pueden usar *exploits* de día cero, que aprovechan vulnerabilidades previamente desconocidas para las cuales el proveedor de software aún no ha publicado ningún parche. Sin el conocimiento o control adecuado del software que se encuentra desplegado en una organización, no se puede proteger adecuadamente los propios activos.

Los dispositivos poco controlados son tienen más posibilidades de ejecutar software innecesario desde el punto de vista de negocio (introduciendo posibles fallas de seguridad) o de ejecutar software malicioso introducido por un atacante después de que un sistema se vea comprometido. Una vez que se ha explotado una sola máquina, los atacantes a menudo la utilizan como punto de apoyo para recopilar información sensible del sistema comprometido y de otros sistemas conectados a ella. Además, las máquinas comprometidas se utilizan como un punto de partida para el movimiento por la red y las redes asociadas. De esta manera, los atacantes pueden pasar rápidamente de tener una máquina comprometida a tener muchas. Las organizaciones que no tienen inventarios de software completos no pueden encontrar los sistemas que ejecuten software vulnerable o malicioso para mitigar los problemas o eliminar a los atacantes.

El control administrado de todo el software también desempeña un papel fundamental en la planificación y ejecución de la copia de seguridad y la recuperación del sistema.

Control crítico #2: Inventario y control de activos software				
Sub-control	**Tipo de activo**	**Función de Seguridad**	**Control**	**Descripción**
2.1	Aplicaciones	Identificar	Mantener un inventario de software autorizado	Mantenga una lista actualizada de todo el software autorizado que es requerido en la organización para todos los fines de negocio y todos los sistemas de negocio.
2.2	Aplicaciones	Identificar	Asegurar que el software tenga soporte del fabricante	Asegure que en el inventario de software autorizado de la organización se incluya únicamente software (aplicaciones o sistemas operativos) que actualmente cuente con soporte del fabricante. El software que no cuenta con soporte debe ser marcado como no soportado en el sistema de inventario.
2.3	Aplicaciones	Identificar	Utilizar herramientas de inventario de software	Utilice herramientas de inventario de software en toda la organización para automatizar la documentación de todo el software en los sistemas de negocio.
2.4	Aplicaciones	Identificar	Rastrear información del inventario de software	El sistema de inventario de software debe obtener el nombre, la versión, el autor y la fecha de instalación de todo el software, incluidos los sistemas operativos autorizados por la organización.
2.5	Aplicaciones	Identificar	Integrar los inventarios de activos de hardware y software	El sistema de inventario de software debe estar vinculado al inventario de activos de hardware para que todos los dispositivos y el software asociado sean rastreados desde una sola ubicación.
2.6	Aplicaciones	Responder	Gestionar el software no aprobado	Asegúrese que el software no autorizado es removido, o que sea incluido en el inventario oportunamente.
2.7	Aplicaciones	Proteger	Utilizar lista blanca de aplicaciones	Utilice tecnología de lista blanca de aplicaciones en todos los activos para asegurar que solo el software autorizado se pueda ejecutar, y que se previene la ejecución de todo el software no autorizado en dichos activos.
2.8	Aplicaciones	Proteger	Implementar lista blanca de librerías	El sistema de lista blanca de aplicaciones de la organización debe garantizar que solo las librerías de software autorizadas (como * .dll, * .ocx, * .so, etc.) puedan cargarse en un proceso del sistema.
2.9	Aplicaciones	Proteger	Implementar lista blanca de scripts	El sistema de lista blanca de aplicaciones de la organización debe garantizar que solo los scripts autorizados y firmados digitalmente (como * .ps1, * .py, macros, etc.) puedan ejecutarse en un sistema.
2.10	Aplicaciones	Proteger	Separar física o lógicamente las aplicaciones de alto riesgo	Utilizar sistemas separados física o lógicamente para aislar y ejecutar aquel software que es requerido para fines de negocio, pero que conlleva un mayor riesgo para la organización.

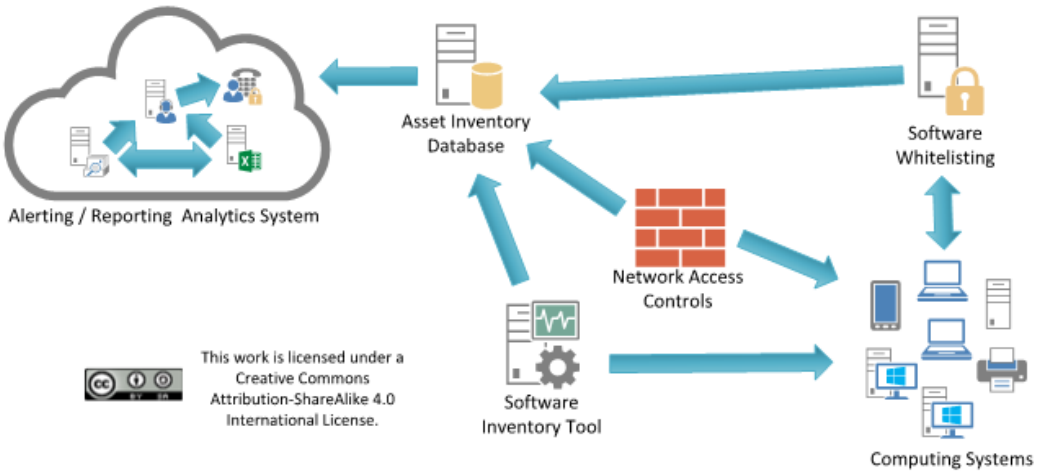
Control 2: Procedimientos y Herramientas

Las listas blancas se pueden implementar utilizando una combinación de herramientas comerciales de listas blancas, políticas o herramientas de ejecución de aplicaciones que vienen incluidas con paquetes de antivirus y sistemas operativos

populares. Herramientas comerciales de inventario de activos y de software están ampliamente disponibles y en uso hoy en día en muchas organizaciones. Las mejores de estas herramientas proporcionan una verificación de inventario de cientos de aplicaciones comúnmente utilizadas en organizaciones, extrayendo información sobre el nivel de parche de cada programa instalado para garantizar que sea la versión más reciente y, aprovechan los nombres estandarizados de aplicaciones, como las que se encuentran en la especificación de enumeración de plataforma común.

Muchas suites modernas de seguridad de *endpoint* incluyen características que implementan listas blancas. Además, las soluciones comerciales agrupan cada vez más *antivirus*, *antispyware*, *firewall* personal y sistemas de detección de intrusiones (IDS) y sistemas de prevención de intrusiones (IPS) basados en host, junto con listas blancas y negras de aplicaciones. En particular, la mayoría de las soluciones de seguridad de *endpoint* pueden ver el nombre, la ubicación en el sistema de archivos y / o el hash criptográfico de un ejecutable dado para determinar si se debe permitir que la aplicación se ejecute en la máquina protegida. La más efectiva de estas herramientas ofrece listas blancas personalizadas basadas en ruta ejecutable, *hash* o coincidencia de expresiones regulares. Algunos incluso incluyen una función de lista gris que permite a los administradores definir reglas para la ejecución de programas específicos solo por ciertos usuarios y en ciertos momentos del día.

Control 2: Diagrama de relación de entidad de sistema



Control 3: Gestión continua de vulnerabilidades

Adquirir, evaluar y tomar medidas continuamente sobre nueva información para identificar vulnerabilidades, remediar y minimizar la ventana de oportunidad para los atacantes.

¿Por qué es importante este control?

Para la defensa cibernética se debe operar en un flujo constante de nueva información: actualizaciones de software, parches, avisos de seguridad, boletines de amenazas, etc. Comprender y gestionar las vulnerabilidades se ha convertido en una actividad continua, que requiere tiempo, atención y recursos significativos.

Los atacantes tienen acceso a la misma información y pueden aprovechar las brechas entre la aparición de nuevo conocimiento y la corrección. Por ejemplo, cuando los investigadores informan sobre nuevas vulnerabilidades, se inicia una carrera entre todas las partes, que incluye: atacantes (para convertir en "arma", desplegar un ataque, explotar), vendedores (para desarrollar, implementar parches o firmas y actualizaciones) y defensores (para evaluar riesgo, prueba de compatibilidad de parches, instalación).

Las organizaciones que no buscan vulnerabilidades y abordan de manera proactiva las fallas detectadas se enfrentan una probabilidad significativa de que sus sistemas informáticos se vean comprometidos. Los defensores enfrentan desafíos particulares para escalar la remediación en toda una organización y priorizar las acciones con prioridades conflictivas y, en ocasiones, efectos secundarios inciertos.

Control crítico #3: Gestión continua de vulnerabilidades				
Sub-control	**Tipo de activo**	**Función de Seguridad**	**Control**	**Descripción**
3.1	Aplicaciones	Detectar	Ejecutar herramientas de escaneo de vulnerabilidades automatizadas	Utilice una herramienta actualizada de escaneo de vulnerabilidades compatible con SCAP para escanear automáticamente todos los sistemas en la red de forma semanal o más frecuente para identificar todas las vulnerabilidades potenciales en los sistemas de la organización.
3.2	Aplicaciones	Detectar	Realizar análisis de vulnerabilidades autenticados	Realice escaneos de vulnerabilidades autenticados con agentes que se ejecutan localmente en cada sistema o con escáneres remotos que están configurados con derechos elevados en el sistema que se audita.
3.3	Aplicaciones	Proteger	Proteger las cuentas dedicadas a auditorías	Utilice una cuenta dedicada al escaneo de vulnerabilidades autenticado, la cual no debe ser utilizada para otras tareas administrativas y que debe ser vinculada a máquinas específicas en direcciones IPs específicas.
3.4	Aplicaciones	Proteger	Implementar	Implemente herramientas de actualización de software

			herramientas de gestión automatizada de parches del sistema operativo	automatizadas para garantizar que los sistemas operativos cuenten con las actualizaciones de seguridad más recientes provistas por el proveedor del software.
3.5	Aplicaciones	Proteger	Implementar herramientas de gestión automatizada de parches de software	Implemente herramientas de actualización de software automatizadas para garantizar que el software de terceros en todos los sistemas cuente con las actualizaciones de seguridad más recientes provistas por el proveedor del software
3.6	Aplicaciones	Responder	Comparar escaneos de vulnerabilidades consecutivos	Compare regularmente los resultados de escaneos de vulnerabilidades consecutivos para verificar que las vulnerabilidades se hayan remediado de manera oportuna.
3.7	Aplicaciones	Responder	Utilizar un proceso de calificación de riesgo	Utilice un proceso de calificación de riesgo para priorizar la corrección de vulnerabilidades descubiertas.

Control 3: Procedimientos y herramientas:

Existe una gran cantidad de herramientas de análisis de vulnerabilidades disponibles para evaluar la configuración de seguridad de los sistemas. También pueden resultar efectivos los servicios comerciales que utilizan dispositivos de escaneo gestionados remotamente. Para ayudar a estandarizar las definiciones de vulnerabilidades descubiertas en múltiples departamentos de una organización o incluso entre organizaciones, es preferible usar herramientas de análisis de vulnerabilidades que midan las fallas de seguridad y las mapeen a vulnerabilidades y problemas categorizados utilizando una o más de los siguientes esquemas o lenguajes de clasificación vulnerabilidades, configuración y plataformas, reconocidos por la industria: CVE, CCE, OVAL, CPE, CVSS y / o XCCDF.

Las herramientas avanzadas de análisis de vulnerabilidades pueden ser configuradas con credenciales de usuario para iniciar sesión en los sistemas escaneados y realizar escaneos más exhaustivos de lo que se puede lograr sin las credenciales de inicio de sesión. Sin embargo, la frecuencia de los escaneos debería aumentarse a medida que aumenta la diversidad de los sistemas de una organización, de modo a tener en cuenta los ciclos de parches variables de cada proveedor.

Además de las herramientas de escaneo que verifican las vulnerabilidades y las configuraciones incorrectas en la red, varias herramientas gratuitas y comerciales pueden evaluar las configuraciones de seguridad y las configuraciones de las máquinas locales en las que están instaladas. Dichas herramientas pueden proporcionar una visión granular sobre cambios no autorizados en la configuración o la introducción involuntaria de debilidades de seguridad por parte de los administradores.

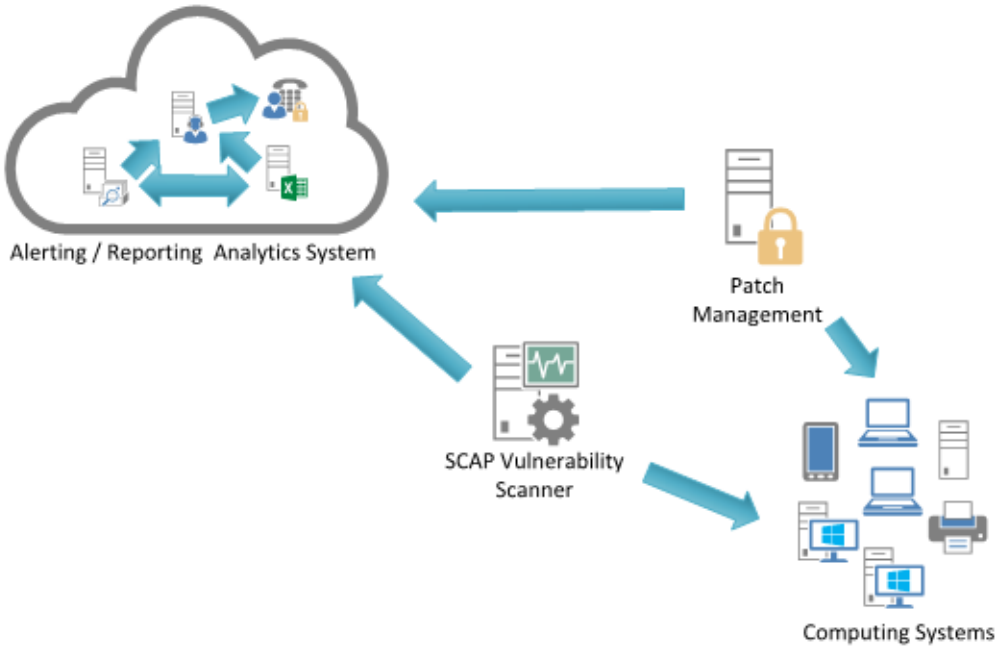
Las organizaciones efectivas vinculan sus escáneres de vulnerabilidad con sistemas de ticketing de problemas que automáticamente monitorean e informan el progreso en la solución de problemas, y eso hace que las vulnerabilidades críticas no mitigadas sean visibles para los niveles superiores de administración para asegurar que los problemas se resuelvan.

Las herramientas de escaneo de vulnerabilidades más efectivas comparan los resultados del escaneo actual con escaneos previos para determinar cómo las vulnerabilidades en el entorno han cambiado con el tiempo. El personal de seguridad usa estas características para conocer las tendencias de vulnerabilidad de mes a mes.

A medida que las herramientas de exploración descubren las vulnerabilidades relacionadas con los sistemas no parchados, el personal de seguridad debe determinar y documentar la cantidad de tiempo que transcurre entre la publicación de un parche para el sistema y la ejecución del análisis de vulnerabilidad. Si esta ventana de tiempo excede los límites de tiempo de la organización para el despliegue del parche según su nivel de criticidad, el personal de seguridad debe notar el retraso y determinar si se documentó formalmente una desviación para el sistema y su parche. De lo contrario, el equipo de seguridad debería trabajar con los administradores para mejorar el proceso de parchado.

Además, algunas herramientas de parchado automático pueden no detectar o instalar ciertos parches debido a un error del proveedor o administrador. Debido a esto, todas las revisiones de parches deben conciliar los parches del sistema con una lista de parches que cada proveedor ha anunciado en su sitio web.

Control 3: Diagrama de relación de entidad de sistema



Control 4: Uso controlado de privilegios administrativos

Los procesos y herramientas utilizados para rastrear, controlar, prevenir y corregir el uso, la asignación y la configuración de privilegios administrativos en computadoras, redes y aplicaciones.

¿Por qué es importante este control?

El uso indebido de privilegios administrativos es un método principal para que los atacantes se propaguen dentro de una organización objetivo. Dos técnicas de ataque muy comunes aprovechan los privilegios administrativos no controlados. En el primero, el usuario de una estación de trabajo ejecutándose como usuario privilegiado es engañado para abrir un archivo adjunto de un correo electrónico malicioso, descargar y abrir un archivo de un sitio web malicioso o simplemente navegar a un sitio web que alberga contenido del atacante que puede explotar automáticamente los navegadores. El archivo o *exploit* contiene un código ejecutable que se ejecuta automáticamente en la máquina de la víctima o engaña al usuario para que ejecute el contenido del atacante. Si la cuenta del usuario de la víctima tiene privilegios administrativos, el atacante puede controlar completamente la máquina de la víctima e instalar *keyloggers*, *sniffers* y software de control remoto para buscar contraseñas administrativas y otros datos confidenciales. Ataques similares ocurren con el correo electrónico. Un administrador inadvertidamente abre un correo electrónico que contiene un archivo adjunto infectado y esto se utiliza para obtener un punto de pivote dentro de la red que se usa para atacar a otros sistemas.

La segunda técnica común utilizada por los atacantes es la elevación de privilegios al adivinar o descifrar una contraseña de un usuario administrativo para obtener acceso a una máquina objetivo. Si los privilegios administrativos son distribuidos de manera amplia y descuidada, o idénticos a las contraseñas utilizadas en sistemas menos críticos, al atacante le resulta mucho más fácil obtener el control total de los sistemas, porque hay muchas más cuentas que pueden actuar como un medio para que los atacantes comprometan los privilegios administrativos.

Control crítico #4: Uso controlado de privilegios administrativos				
Sub-control	**Tipo de activo**	**Función de Seguridad**	**Control**	**Descripción**
4.1	Usuarios	Detectar	Mantener un inventario de cuentas administrativas	Use herramientas automatizadas para inventariar todas las cuentas administrativas, incluidas las cuentas de dominio y locales, para garantizar que solo las personas autorizadas tengan privilegios elevados.
4.2	Usuarios	Proteger	Cambiar contraseñas por defecto	Antes de implementar cualquier activo nuevo, cambie todas las contraseñas por defecto para que tengan valores consistentes con las cuentas de nivel administrativo

4.3	Usuarios	Proteger	Asegurar el uso de cuentas administrativas dedicadas	Asegúrese de que todos los usuarios con acceso a la cuenta administrativa utilicen una cuenta dedicada o secundaria para actividades elevadas. Esta cuenta solo se debe usar para actividades administrativas y no para la navegación por Internet, correo electrónico o actividades similares.
4.4	Usuarios	Proteger	Usar contraseñas únicas	Cuando no está soportada la autenticación multifactor (como el administrador local, root o cuentas de servicio), las cuentas usarán contraseñas que son únicas de ese sistema.
4.5	Usuarios	Proteger	Usar autenticación multifactor para todo acceso administrativo	Utilice autenticación de multifactor y canales encriptados para todos los accesos de cuentas administrativas.
4.6	Usuarios	Proteger	Usar máquinas dedicadas para toda tarea administrativa	Asegúrese de que los administradores utilicen una máquina dedicada para todas las tareas administrativas o tareas que requieren acceso administrativo. Esta máquina debe estar en un segmento de red diferente al principal de la organización y no se le permitirá el acceso a Internet. Esta máquina no se usará para leer correos electrónicos, manipular documentos o navegar en Internet.
4.7	Usuarios	Proteger	Limitar el acceso a herramientas de scripts	Limite el acceso a las herramientas de scripting (como Microsoft PowerShell y Python) solo a usuarios administrativos o de desarrollo que necesiten acceder a esas funcionalidades.
4.8	Usuarios	Detectar	Registrar y alertar cambios de miembros en grupos administrativos	Configure los sistemas para que generen una entrada de registro y una alerta cuando se agregue o elimine una cuenta a cualquier grupo que tenga asignados privilegios administrativos.
4.9	Usuarios	Detectar	Registrar y alertar los inicios de sesión fallidos a cuentas administrativas	Configure los sistemas para generar una entrada de registro y una alerta de inicios de sesión fallidos en una cuenta administrativa.

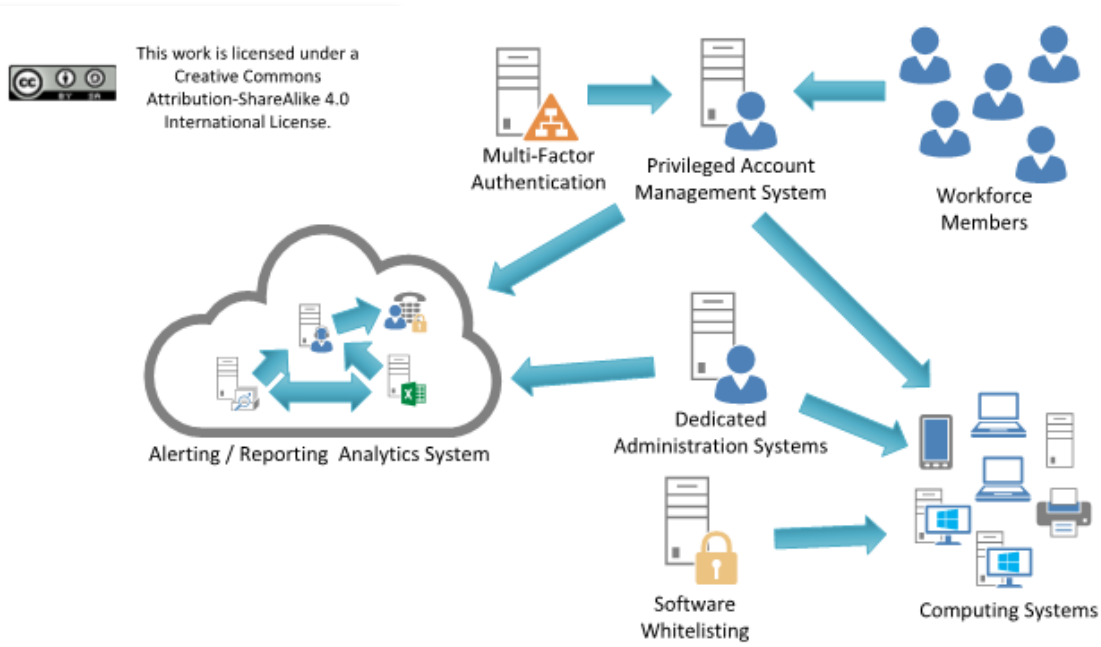
Control 4: Procedimiento y herramientas

Las funciones integradas del sistema operativo pueden extraer listas de cuentas con privilegios de superusuario, tanto localmente en sistemas individuales como en controladores de dominio en general. Para verificar que los usuarios con cuentas con privilegios altos no usen dichas cuentas para la navegación web diaria y la lectura de correos electrónicos, el personal de seguridad debe recopilar periódicamente una lista de procesos en ejecución para determinar si los navegadores o lectores de correo electrónico se están ejecutando con privilegios elevados. Esta recopilación de información se puede programar, con scripts de *shell* cortos que buscan una docena o más de navegadores diferentes, lectores de correo electrónico y programas de edición de documentos que se ejecutan con privilegios elevados en las máquinas. Algunas actividades legítimas de administración del sistema pueden requerir la ejecución de dichos programas a corto plazo, pero el uso a largo plazo o frecuente de dichos programas con privilegios administrativos podría indicar que un administrador no se está adhiriendo a este Control.

Para hacer cumplir el requisito de contraseñas seguras, se pueden configurar una longitud mínima de contraseñas mediante las características integradas del sistema operativo para evitar que los usuarios elijan contraseñas cortas. Para aplicar la complejidad de la contraseña (que requiere que las contraseñas sean una cadena de caracteres pseudoaleatorios), se pueden aplicar las configuraciones integradas del sistema operativo o herramientas de terceros de cumplimiento de complejidad de contraseñas. La robustez y la gestión de la contraseña (por ejemplo, la frecuencia del cambio) se deben considerar en un contexto de sistema y ciclo de vida. Una guía de referencia es:

- The NIST Digital Identity Guidelines (https://pages.nist.gov/800-63-3/)

Control 4: Diagrama de relación de entidad de sistema



Control 5: Configuración segura para hardware y software en dispositivos móviles, computadoras portátiles, estaciones de trabajo y servidores

Establezca, implemente y gestione activamente (rastree, informe, corrija) la configuración de seguridad de dispositivos móviles, computadoras portátiles, servidores y estaciones de trabajo utilizando una rigurosa gestión de configuraciones y un proceso de control de cambios para evitar que los atacantes exploten servicios y configuraciones vulnerables.

¿Por qué es importante este control?

Las configuraciones predeterminadas entregadas por los fabricantes y revendedores de sistemas operativos y aplicaciones normalmente están orientadas a la facilidad de implementación y la facilidad de uso, no a la seguridad. Controles básicos, servicios y puertos abiertos, cuentas o contraseñas predeterminadas, protocolos antiguos (vulnerables), preinstalación de software innecesario - todos pueden ser explotables en su estado predeterminado.

Desarrollar configuraciones con buenas propiedades de seguridad es una tarea compleja más allá de la capacidad de usuarios individuales, que requiere un análisis de cientos o miles de opciones para tomar buenas decisiones. Incluso si se desarrolla e instala una configuración inicial sólida, debe gestionarse continuamente para evitar la "degradación" de la seguridad a medida que se actualiza o repara el software, se informan nuevas vulnerabilidades de seguridad y se "afinan" las configuraciones para permitir la instalación de nuevo software o soporte nuevos requisitos operacionales. De lo contrario, los atacantes encontrarán oportunidades para explotar tanto los servicios accesibles a la red como el software del cliente.

Control crítico #5: Configuración segura para hardware y software en dispositivos móviles, computadoras portátiles, estaciones de trabajo y servidores				
Sub-control	**Tipo de activo**	**Función de Seguridad**	**Control**	**Descripción**
5.1	Aplicaciones	Proteger	Establecer configuraciones seguras	Mantenga estándares de configuración de seguridad estándar documentados para todos los sistemas operativos y software autorizados.
5.2	Aplicaciones	Proteger	Mantener imagenes seguras	Mantenga imágenes o plantillas seguras para todos los sistemas de la organización según los estándares de configuración aprobados por la organización. Cualquier implementación de sistema nuevo o sistema existente que se vea comprometido se debe volver a reconstruido con una de esas imágenes o plantillas.
5.3	Aplicaciones	Proteger	Almacenar las imágenes maestras de forma segura	Almacene las imágenes maestras y las plantillas en servidores configurados de forma segura, validados con herramientas de monitoreo de integridad, para garantizar que solo sean posibles los cambios autorizados en las imágenes.

5.4	Aplicaciones	Proteger	Implementar herramientas de gestión de configuración de sistema	Implemente las herramientas de gestión de configuración de sistema que automáticamente fuercen y vuelvan a implementar los parámetros de configuración en los sistemas a intervalos regulares programados.
5.5	Aplicaciones	Detectar	Implementar sistemas de monitoreo automatizado de configuración	Utilice un sistema de monitoreo de configuración compatible con el Protocolo de automatización de contenido de seguridad (SCAP) para verificar todos los elementos de configuración de seguridad, excepciones aprobadas por catálogo y que alerte cuando ocurran cambios no autorizados.

Control 5: Procedimientos y herramientas

En lugar de comenzar de cero desarrollando una línea base de seguridad para cada sistema de software, las organizaciones deberían comenzar desde referencia, guías o listas de verificación de seguridad que hayan sido desarrolladas, aprobadas y respaldadas públicamente. Excelentes recursos incluyen:

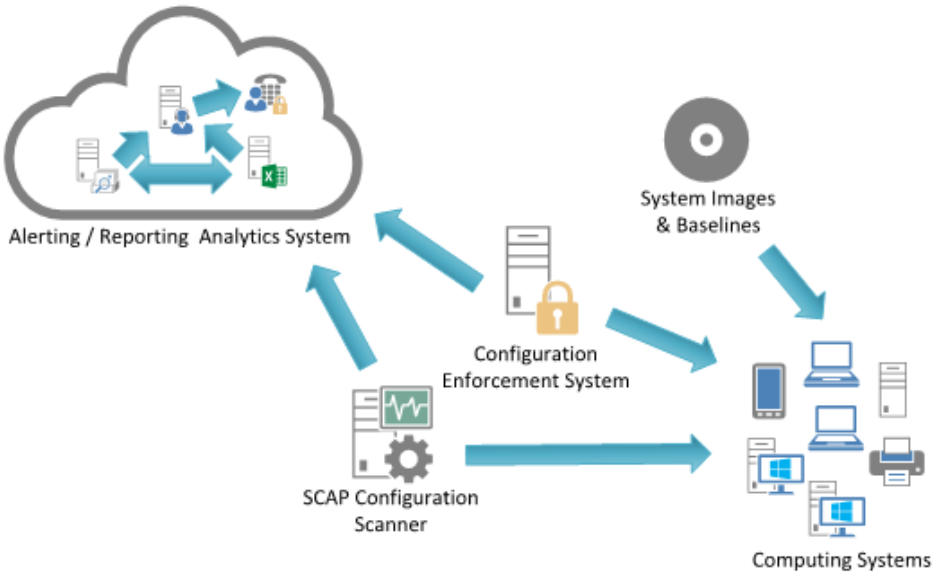
- El programa CIS Benchmarks™ (www.cisecurity.org)
- NIST National Checklist Program (https://nvd.nist.gov/ncp/repository)

Las organizaciones deberían aumentar o ajustar estas líneas base para satisfacer las políticas y los requisitos locales, pero las desviaciones y los fundamentos deberían documentarse para facilitar revisiones o auditorías posteriores.

Para una organización compleja, el establecimiento de una única configuración de línea base de seguridad (por ejemplo, una imagen de instalación única para todas las estaciones de trabajo en toda la organización) a veces no es práctica o se considera inaceptable. Es probable que necesite admitir diferentes imágenes estandarizadas, basadas en el endurecimiento adecuado para abordar los riesgos y la funcionalidad necesaria de la implementación prevista (por ejemplo, un servidor web en la DMZ frente a un correo electrónico u otro servidor de aplicaciones en la red interna). El número de variaciones se debe mantener al mínimo para comprender y gestionar mejor las propiedades de seguridad de cada una, pero las organizaciones deben estar preparadas para gestionar líneas de base múltiples.

Las herramientas de gestión de configuración comerciales y/o gratuitas pueden emplearse para medir la configuración de los sistemas operativos y las aplicaciones de las máquinas gestionadas para detectar desviaciones de las configuraciones de imagen estándar. Las herramientas de gestión de configuración típicas utilizan alguna combinación de un agente instalado en cada sistema gestionado o una inspección sin agente de los sistemas iniciando sesión de forma remota en cada máquina gestionada utilizando credenciales de administrador. Además, a veces se utiliza un enfoque híbrido mediante el cual se inicia una sesión remota, se implementa un agente temporal o dinámico en el sistema de destino para el escaneo y luego se elimina el agente.

Control 5: Diagrama de relación de entidad de sistema



Control 6: Mantenimiento, monitoreo y análisis de logs de auditoría

Reúna, administre y analice registros de auditoría de eventos que podrían ayudar a detectar, comprender o recuperarse de un ataque.

¿Por qué es importante este control?

Las deficiencias en el registro y análisis de seguridad permiten a los atacantes esconder su ubicación, software malicioso y actividades en las máquinas de las víctimas. Incluso si las víctimas saben que sus sistemas se han visto comprometidos, sin registros de auditoría protegidos y completos, están ciegos a los detalles del ataque y a las acciones posteriores tomadas por los atacantes. Sin registros de auditoría sólidos, un ataque puede pasar desapercibido indefinidamente y los daños particulares pueden ser irreversibles.

A veces, los registros de auditoría son la única evidencia de un ataque exitoso. Muchas organizaciones mantienen registros de auditoría para fines de cumplimiento, pero los atacantes confían en el hecho de que tales organizaciones rara vez miran los registros de auditoría, y no saben que sus sistemas se han visto comprometidos. Debido a procesos de análisis de registros pobres o inexistentes, los atacantes a veces controlan las máquinas de víctimas durante meses o años sin que nadie en la organización objetivo lo sepa, aunque la evidencia del ataque se haya registrado en archivos de registro no examinados.

Control crítico #6: Mantenimiento, monitoreo y análisis de logs de auditoría				
Sub-control	**Tipo de activo**	**Función de Seguridad**	**Control**	**Descripción**
6.1	Red	Detectar	Utilizar tres fuentes de tiempo sincronizadas	Use al menos tres fuentes de tiempo sincronizadas de las cuales todos los servidores y dispositivos de red recuperan información de tiempo regularmente para que las marcas de tiempo en los registros sean consistentes.
6.2	Red	Detectar	Activar registros de auditoría	Asegure que los registros locales se han activado en todos los sistemas y equipos de red.
6.3	Red	Detectar	Habilitar registros detallados	Habilite el registro del sistema para incluir información detallada, como origen de evento, fecha, usuario, marca de tiempo, direcciones de origen, direcciones de destino y otros elementos útiles.
6.4	Red	Detectar	Asegurar almacenamiento adecuado para registros	Asegúrese de que todos los sistemas que almacenan registros tengan el espacio de almacenamiento adecuado para los registros generados.
6.5	Red	Detectar	Gestión centralizada de registros	Asegúrese de que los registros apropiados se agreguen a un sistema central de gestión de registros para su análisis y revisión.
6.6	Red	Detectar	Desplegar	Implemente un sistema de Gestión de información de

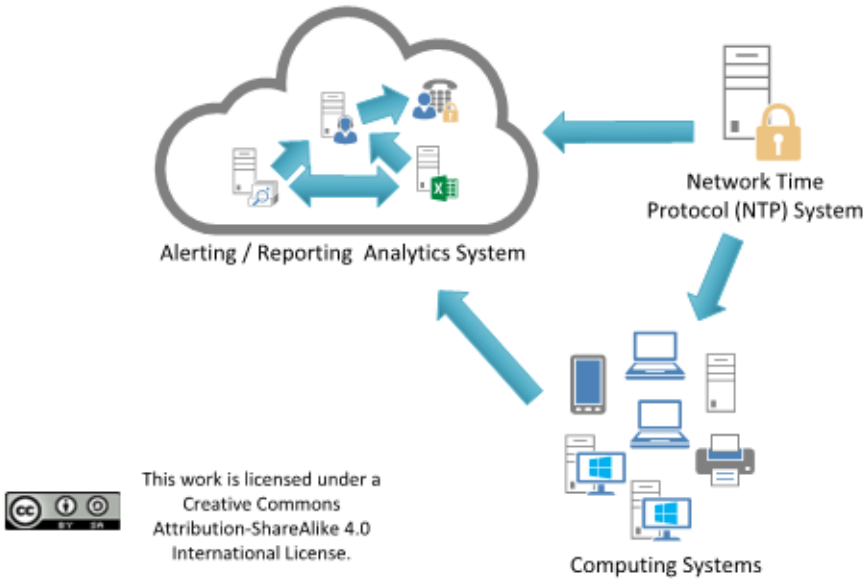
			herramientas SIEM o de Análisis de registros	seguridad y eventos (Security Information and Event Management - SIEM) o una herramienta de análisis de registros para la correlación y el análisis de los registros.
6.7	Red	Detectar	Revisar regularmente los registros	Regularmente, revise los registros para identificar anomalías o eventos anormales.
6.8	Red	Detectar	Ajustar regularmente el SIEM	Regularmente, ajuste el sistema SIEM para identificar mejor los eventos que requieren acción y disminuir el ruido.

Control 6: Procedimientos y herramientas:

La mayoría de los sistemas operativos, servicios de red y tecnologías de firewalls, libres y comerciales, ofrecen capacidades de registro. Tales registros deben ser activados y enviados a servidores de registro centralizados. Los *firewalls*, servidores *proxy* y sistemas de acceso remoto (VPN, *dial-up*, etc.) deben estar configurados para el registro detallado, almacenando toda la información disponible, en caso de que se requiera una investigación de seguimiento. Además, los sistemas operativos, especialmente los de los servidores, deben configurarse para crear registros de control de acceso cuando un usuario intenta acceder a los recursos sin los privilegios apropiados. Para evaluar si dicho registro está implementado, una organización debe examinar periódicamente sus registros y compararlos con el inventario de activos obtenido como parte del Control 1 para garantizar que cada elemento gestionado conectado activamente a la red genere registros periódicamente.

Los programas de análisis, como las soluciones SIEM para revisar los registros, pueden proporcionar valor, pero las capacidades empleadas para analizar los registros de auditoría son bastante extensas, incluyendo, incluso, un examen superficial de una persona. Las herramientas de correlación reales pueden hacer que los registros de auditoría sean mucho más útiles para la posterior inspección manual. Tales herramientas pueden ser bastante útiles para identificar ataques sutiles. Sin embargo, estas herramientas no son una panacea ni un reemplazo para el personal experto en seguridad de la información y los administradores del sistema. Incluso con herramientas automatizadas de análisis de registros, a menudo se requiere experiencia humana e intuición para identificar y comprender los ataques.

Control 6: Diagrama de relación de entidad de sistema



Control 7: Protección de correo electrónico y navegador web

Minimizar la superficie de ataque y la oportunidad para atacantes de manipular el comportamiento humano a través de su interacción con navegadores web y sistemas de correo electrónico.

¿Por qué es importante este control?

Los navegadores web y los clientes de correo electrónico son puntos de entrada y ataque muy comunes debido a su complejidad técnica, flexibilidad y su interacción directa con los usuarios y con los otros sistemas y sitios web. El contenido puede diseñarse para atraer o engañar a los usuarios para que tomen medidas que aumenten en gran medida el riesgo y permitan la introducción de códigos maliciosos, la pérdida de datos valiosos y otros ataques. Dado que estas aplicaciones son el principal medio para que los usuarios interactúen con entornos que no son de confianza, estos son objetivos potenciales tanto para la explotación del código como para la ingeniería social.

Control crítico #7: Protección de correo electrónico y navegador web				
Sub-control	**Tipo de activo**	**Función de Seguridad**	**Control**	**Descripción**
7.1	Aplicaciones	Proteger	Asegurar el uso de navegadores y clientes de correo electrónico que cuenten con soporte	Asegúrese de que solo los navegadores web y los clientes de correo electrónico que cuenten con soporte completo puedan ejecutarse en la organización, idealmente solo con la última versión de los navegadores y clientes de correo electrónico proporcionados por el proveedor.
7.2	Aplicaciones	Proteger	Deshabilitar plugins innecesarios de navegadores o clientes de correo electrónico	Desinstalar o deshabilitar cualquier plugin o aplicación add-on para navegador o cliente de correo electrónico no autorizados.
7.3	Aplicaciones	Proteger	Limitar el uso de lenguajes de scripting en navegadores web y clientes de correo electrónico	Asegúrese de que solo los lenguajes de scripting autorizados puedan ejecutarse en los navegadores web y clientes de correo electrónico.
7.4	Red	Proteger	Mantener y aplicar filtros de URL basados en red	Aplique los filtros de URL basados en red que limitan la capacidad de un sistema para conectarse a sitios web no aprobados por la organización. Este filtrado se aplicará para cada uno de los sistemas de la organización, ya sea que se encuentren físicamente en las instalaciones de una organización o no.
7.5	Red	Proteger	Suscribirse a servicios de categorización de URL	Suscríbase a servicios de categorización de URL para asegurarse de que estén actualizados con las definiciones de categoría de sitio web más recientes disponibles. Los sitios no categorizados deberían bloquearse de manera predeterminada.

7.6	Red	Detectar	Registrar todas las peticiones de URLs	Registre todas las solicitudes de URL de cada uno de los sistemas de la organización, ya sea en el sitio o en un dispositivo móvil, para identificar actividades potencialmente maliciosas y ayudar a los responsables de gestionar incidentes a identificar sistemas potencialmente comprometidos.
7.7	Red	Proteger	Utilizar servicios de filtrado DNS	Utilice servicios de filtrado de DNS para ayudar a bloquear el acceso a dominios maliciosos conocidos.
7.8	Red	Proteger	Implementar DMARC y habilitar verificación del lado del receptor	Para reducir la posibilidad de correos electrónicos falsificados o modificados de dominios válidos, implemente y verifique la política de Autenticación, Reporte y Conformidad de mensajes basada en dominio (Domain-based Message Authentication, Reporting and Conformance - DMARC), comenzando por implementar los estándares Sender Policy Framework (SPF) y DomainKeys Identified Mail (DKIM).
7.9	Red	Proteger	Bloquear tipos de archivos innecesarios	Bloquee todos los archivos adjuntos de correo electrónico que ingresen a la pasarela de correo electrónico de la organización si los tipos de archivos son innecesarios para los fines de negocio de la organización.
7.10	Red	Proteger	Utilizar técnicas de sandbox para todos los adjuntos de correo electrónico	Utilice técnicas de sandboxing para analizar y bloquear los archivos adjuntos de correo electrónico que tengan un comportamiento malicioso.

Control 7: Procedimientos y herramientas

Navegador web:

Los ciberdelincuentes pueden explotar los navegadores web de múltiples maneras. Si éstos tienen acceso a vulnerabilidades de navegadores vulnerables, pueden crear páginas web maliciosas que pueden explotar esas vulnerabilidades cuando son accedidas mediante un navegador no parcheado. Alternativamente, si las vulnerabilidades dentro del navegador no son accesibles, pueden apuntar a un sinfín de complementos de navegador web comunes que les permitan conectarse al navegador o incluso directamente al sistema operativo. Estos complementos, al igual que cualquier otra aplicación dentro de su entorno, necesitan ser gestionados y controlados, no solo para saber qué necesita actualizarse sino también para reducir la probabilidad de que los usuarios instalen de manera no intencional malware que pueda estar oculto en algunos de estos complementos y *add-ons*. Una simple configuración del navegador puede dificultar la instalación del malware tanto mediante la reducción de la capacidad de instalar *add-ons* y complementos y como también mediante la limitación de la ejecución automática de tipos específicos de contenido.

La mayoría de los navegadores populares emplean una base de datos de sitios de *phishing* y/o de malware para protegerse contra las amenazas más comunes. Asegúrese de que usted y sus usuarios habiliten estos filtros

de contenido y activen los bloqueadores de ventanas emergentes. Las ventanas emergentes no solo son molestas, sino que también pueden alojar malware incrustado directamente o atraer a los usuarios a hacer clic en algo utilizando trucos de ingeniería social. Para ayudar a imponer el bloqueo de dominios maliciosos conocidos, también considere suscribirse a los servicios de filtrado de DNS para bloquear los intentos de acceder a estos sitios web a nivel de red.

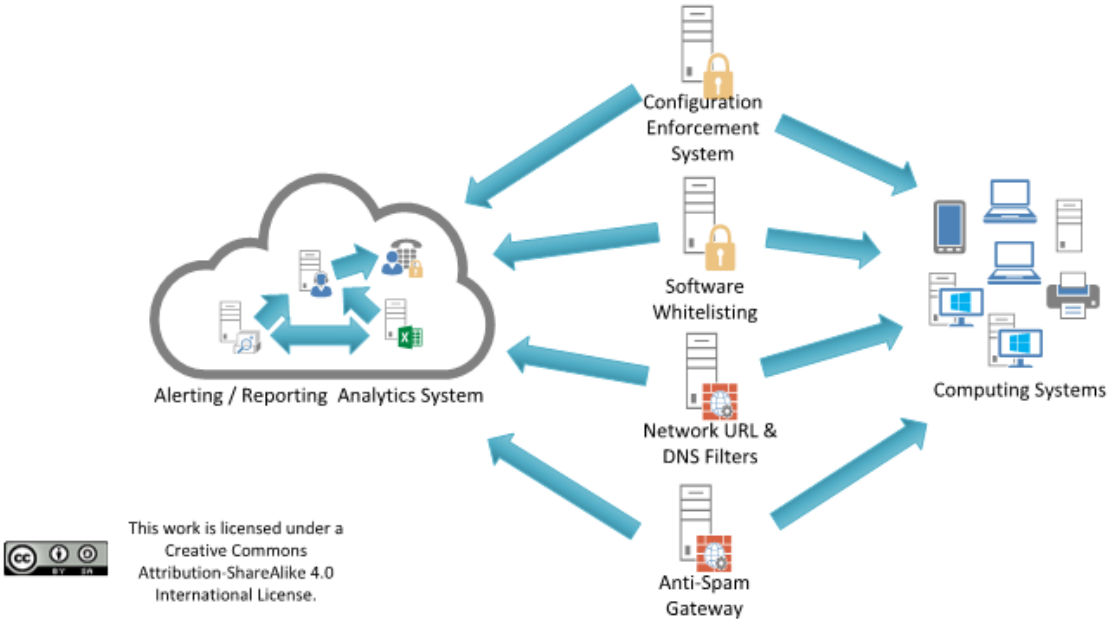
Correo electrónico:

El correo electrónico representa una de las formas más interactivas en que los humanos trabajan con computadoras; alentar el comportamiento correcto es tan importante como la configuración técnica.

El uso de una herramienta de filtrado de spam reduce la cantidad de correos electrónicos maliciosos que ingresan a su red. Iniciar un proceso de Autenticación, Reporte y Conformidad de Mensajes basado en Dominio (DMARC) ayuda a reducir el spam y las actividades de phishing. La instalación de una herramienta de cifrado para proteger el correo electrónico y las comunicaciones agrega otra capa de seguridad basada en el usuario y la red. Además del bloqueo basado en el remitente, también vale la pena permitir solo ciertos tipos de archivos que los usuarios necesitan para sus trabajos. Esto requerirá cierto nivel de interacción con diferentes unidades de negocio para comprender qué tipo de archivos reciben por correo electrónico para garantizar que no haya interrupciones en sus procesos.

El uso de una herramienta de filtrado de spam reduce la cantidad de correos electrónicos maliciosos que ingresan a su red. Iniciar un proceso de Autenticación, Reporte y Conformidad de Mensajes basado en dominio (*Domain-based Message Authentication, Reporting and Conformance* - DMARC) ayuda a reducir el spam y las actividades de phishing. La instalación de una herramienta de cifrado para proteger el correo electrónico y las comunicaciones agrega otra capa de seguridad basada en el usuario y la red. Además del bloqueo basado en el remitente, también vale la pena permitir solo ciertos tipos de archivos que los usuarios necesitan para sus trabajos. Esto requerirá cierto nivel de interacción con diferentes unidades de negocio para comprender qué tipo de archivos reciben por correo electrónico para garantizar que no haya interrupciones en sus procesos.

Control 7: Diagrama de relación de entidad de sistema



Control 8: Defensa contra malware

Controlar la instalación, propagación y ejecución de código malicioso en múltiples puntos de la organización, al mismo tiempo que optimizar el uso de automatización para permitir la actualización rápida de la defensa, la recopilación de datos y la acción correctiva.

¿Por qué es importante este control?

El software malicioso (malware) es un aspecto integral y peligroso de las amenazas en Internet, ya que está diseñado para atacar sus sistemas, dispositivos y sus datos. Se mueve rápidamente, cambia rápidamente y entra a través de múltiples y diversos puntos, como dispositivos de usuario final, archivos adjuntos de correo electrónico, páginas web, servicios en la nube, acciones del usuario y medios extraíbles. El malware moderno está diseñado para evitar las defensas y atacarlas o deshabilitarlas.

Las defensas contra malware deben ser capaces de operar en este entorno dinámico a través de la automatización a gran escala, la actualización rápida y la integración con procesos como la respuesta a incidentes. También deben implementarse en múltiples puntos posibles de ataque para detectar, detener el movimiento o controlar la ejecución de software malicioso. Las suites corporativas de seguridad de *endpoints* proporcionan funciones administrativas para verificar que todas las defensas estén activas y actualizadas en todos los sistemas administrados.

Control crítico #8: Defensa contra malware				
Sub-control	**Tipo de activo**	**Función de Seguridad**	**Control**	**Descripción**
8.1	Equipos	Proteger	Utilizar software antimalware de gestión centralizada	Utilice software antimalware gestionado centralmente para monitorear y defender continuamente cada una de las estaciones de trabajo y servidores de la organización.
8.2	Equipos	Proteger	Asegurar que el software antimalware y las firmas estén actualizadas	Asegúrese de que el software antimalware de la organización actualice su motor de exploración y la base de datos de firmas periódicamente.
8.3	Equipos	Proteger	Habilitar características anti-explotación de sistemas operativos / implementar tecnologías anti-explotación	Habilite las características anti-explotación como la Prevención de ejecución de datos (Data Execution Prevention - DEP) o Address Space Layout Randomization (ASLR) que están disponibles en los sistemas operativos o implemente los kits de herramientas adecuados que pueden configurarse para aplicar protección a un conjunto más amplio de aplicaciones y ejecutables.
8.4	Equipos	Detectar	Configurar escaneo antimalware de dispositivos removibles	Configure los dispositivos para que automáticamente realicen un análisis antimalware de los medios extraíbles cuando se inserten o se conecten.

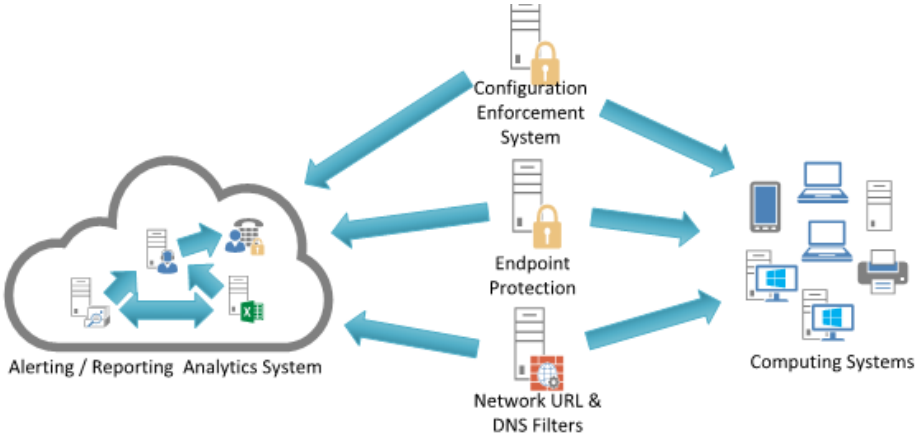
8.5	Equipos	Proteger	Configurar equipos para no auto-ejecutar contenido	Configure los equipos para no ejecutar automáticamente el contenido de medios extraíbles.
8.6	Equipos	Detectar	Centralizar los registros antimalware	Envíe todos los eventos de detección de malware a las herramientas de administración antimalware de la organización y a los servidores de registro de eventos para análisis y alertas.
8.7	Red	Detectar	Habilitar registros de consultas DNS	Habilitar los registros de las consultas al sistema de nombre de dominio (Domain Name System - DNS) para detectar búsquedas de nombres de host para dominios maliciosos conocidos.
8.8	Equipos	Detectar	Habilitar registros de auditoría de línea de comandos	Habilite el registro de auditoría de línea de comandos para shells de comandos, como Microsoft Powershell y Bash.

Control 8: Procedimientos y herramientas:

Para garantizar que las firmas antivirus estén actualizadas, las organizaciones usan la automatización. Utilizan las funciones administrativas integradas de las suites corporativas de seguridad de *endpoints* para verificar que las funciones de IDS basado en host, antivirus y antispyware estén activas en todos los sistemas administrados. Ejecutan evaluaciones automatizadas diariamente y revisan los resultados para encontrar y mitigar los sistemas que han desactivado dichas protecciones, así como los sistemas que no tienen las últimas definiciones de malware.

Ser capaz de bloquear aplicaciones maliciosas es solo una parte de este Control: también hay un gran enfoque en recopilar los registros para ayudar a las organizaciones a comprender lo que sucedió dentro de su entorno, lo que incluye asegurarse de que se encuentren habilitados los registros para varias herramientas de línea de comando, como Microsoft PowerShell y Bash. A medida que los actores malintencionados continúan desarrollando sus metodologías, muchos comienzan a adoptar un enfoque de "vivir de la tierra" para minimizar la probabilidad de ser atrapados. Al habilitar el registro, será mucho más fácil para la organización seguir los eventos y cómo sucedieron, qué sucedió y cómo sucedió.

Control 8: Diagrama de relación de entidad de sistema



Control 9: Limitación y control de puertos de red, protocolos y servicios

Administrar (rastrear/controlar/corregir) el uso operacional continuo de puertos, protocolos y servicios en dispositivos en red para minimizar las ventanas de vulnerabilidad disponibles para los atacantes.

¿Por qué es importante este control?

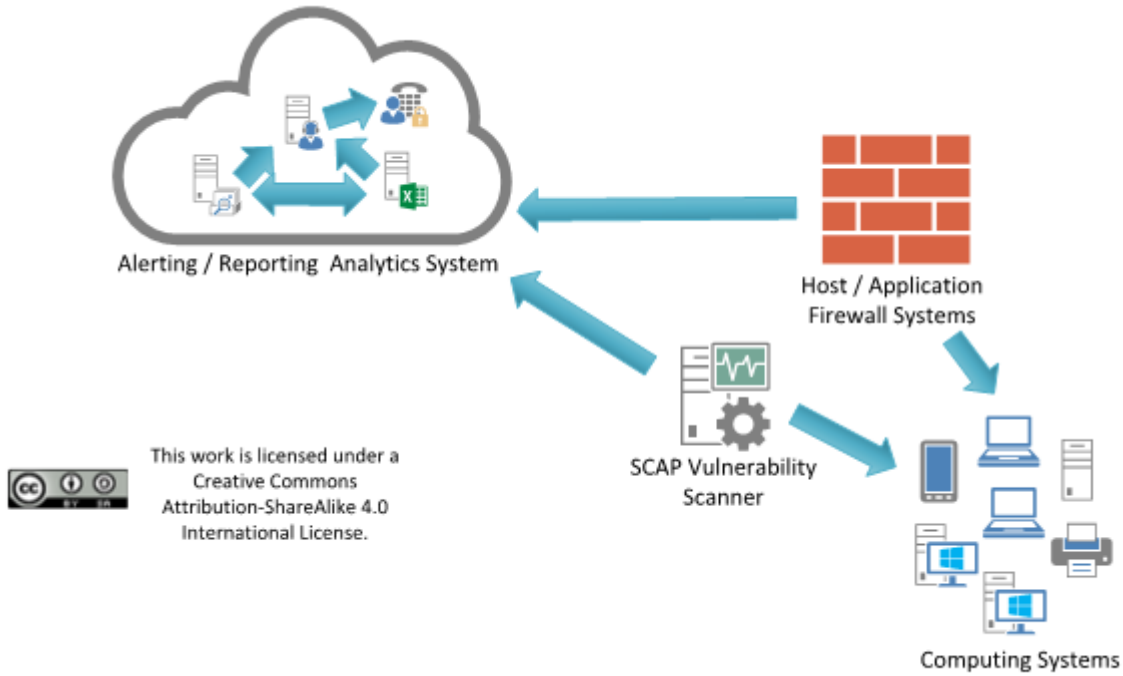
Los atacantes buscan servicios de red remotamente accesibles que sean vulnerables a la explotación. Ejemplos comunes incluyen servidores web mal configurados, servidores de correo, servicios de archivo e impresión y servidores de DNS instalados por defecto en una variedad de diferentes tipos de dispositivos, a menudo sin un propósito de negocio para el servicio dado. Muchos paquetes de software instalan servicios automáticamente y los activan como parte de la instalación del paquete de software principal sin informar a un usuario o administrador que los servicios se han habilitado. Los atacantes buscan estos servicios e intentan explotarlos, a menudo intentando explotar identificaciones de usuarios y contraseñas predeterminadas o códigos de explotación ampliamente disponibles.

Control crítico #9: Limitación y control de puertos de red, protocolos y servicios				
Sub-control	**Tipo de activo**	**Función de Seguridad**	**Control**	**Descripción**
9.1	Equipos	Identificar	Asociar puertos, servicios y protocolos activos al inventario de activos	Asocie puertos, servicios y protocolos activos a los activos de hardware en el inventario de activos.
9.2	Equipos	Proteger	Asegurar que solo puertos, protocolos y servicios aprobados se están ejecutando	Asegúrese de que en cada sistema se ejecuten solo los puertos de red, los protocolos y los servicios que se requieran con fines de negocio validados.
9.3	Equipos	Detectar	Realizar regularmente escaneos automatizados de puertos	Realice escaneos automáticos de puertos de forma regular contra todos los sistemas y advierta si se detectan puertos no autorizados en un sistema.
9.4	Equipos	Proteger	Aplicar firewalls basados en host o filtrado de puertos	Aplique firewalls basados en host o herramientas de filtrado de puertos en los sistemas finales, con una regla de denegación predeterminada que descarta todo el tráfico, excepto los servicios y puertos que están explícitamente permitidos.
9.5	Equipos	Proteger	Implementar firewalls de aplicación	Coloque firewalls de aplicaciones frente a servidores críticos para verificar y validar el tráfico que va al servidor. Cualquier tráfico no autorizado debe ser bloqueado y registrado.

Control 9: Procedimientos y herramientas:

Las herramientas de escaneo de puertos se utilizan para determinar qué servicios están escuchando en la red, para una variedad de sistemas objetivo. Además de determinar qué puertos están abiertos, los escáneres de puertos efectivos se pueden configurar para identificar la versión del protocolo y el servicio que se escucha en cada puerto descubierto. Esta lista de servicios y sus versiones se comparan con un inventario de servicios requerido por la organización para cada servidor y estación de trabajo en un sistema de gestión de activos. Características recientemente agregadas en estos escáneres de puertos se están utilizando para determinar los cambios en los servicios ofrecidos por las máquinas escaneadas en la red desde el escaneo anterior, ayudando al personal de seguridad a identificar las diferencias a lo largo del tiempo.

Control 9: Diagrama de relación de entidad de sistema



Control 10: Capacidad de recuperación de datos

Los procesos y herramientas utilizadas para respaldar adecuadamente la información crítica con una metodología comprobada para la recuperación oportuna de la misma.

¿Por qué es importante este control?

Cuando los atacantes comprometen máquinas, a menudo realizan cambios significativos en las configuraciones y el software. En ocasiones, los atacantes también realizan alteraciones sutiles de los datos almacenados en máquinas comprometidas, lo que puede poner en peligro la eficacia de la organización con información contaminada. Cuando se descubre a los atacantes, puede ser extremadamente difícil para las organizaciones sin una capacidad confiable de recuperación de datos eliminar todos los aspectos de la presencia del atacante en la máquina.

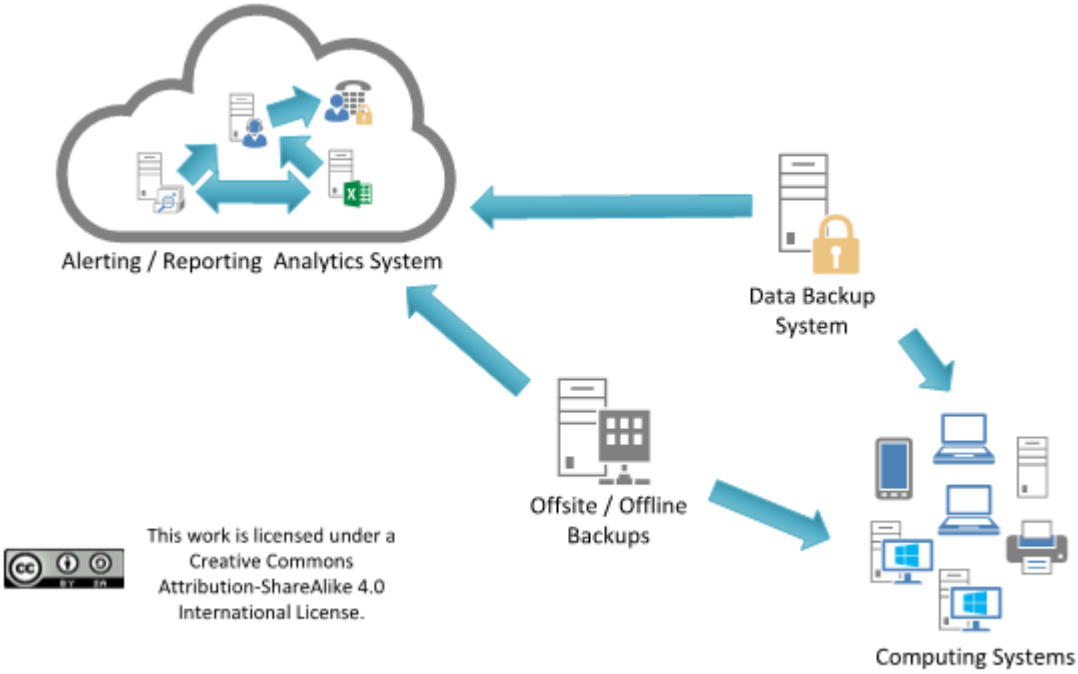
Control crítico #10: Capacidad de recuperación de datos				
Sub-control	**Tipo de activo**	**Función de Seguridad**	**Control**	**Descripción**
10.1	Datos	Proteger	Asegurar los respaldos regulares automatizados	Asegúrese de que se realizan regularmente copias de respaldo de todos los datos de sistemas de manera automatizadas
10.2	Datos	Proteger	Realizar respaldos de sistemas completos	Asegúrese de que cada uno de los sistemas clave de la organización se esté respaldado como un sistema completo, a través de procesos tales como imágenes, para permitir la recuperación rápida de un sistema completo.
10.3	Datos	Proteger	Probar los datos en los medios de respaldo	Pruebe la integridad de los datos en los medios de copia de respaldo de forma periódica mediante la realización de un proceso de restauración de datos para garantizar que la copia de respaldo funcione correctamente.
10.4	Datos	Proteger	Asegurar la protección de las copias de respaldo	Asegúrese de que las copias de seguridad estén protegidas adecuadamente a través de la seguridad física o el cifrado cuando se almacenan, así como también cuando se mueven a través de la red. Esto incluye copias de seguridad remotas y servicios en la nube.
10.5	Datos	Proteger	Asegurar que las copias de respaldo tengan al menos un destino discontinuo	Asegúrese que todas las copias de respaldo se almacenen en al menos un destino que no esté disponible si sea alcanzable de manera continua a través de llamadas del sistema operativo.

Control 10: Procedimientos y herramientas:

Una vez por trimestre (o cada vez que se compra un nuevo equipo de respaldo), un equipo de prueba debe evaluar una muestra aleatoria de copias de seguridad del sistema intentando restaurarlas en un entorno de pruebas. Los sistemas restaurados deben verificarse para garantizar que el sistema operativo, la aplicación y los datos de la copia de seguridad estén intactos y sean funcionales.

En caso de infección de malware, los procedimientos de restauración deben usar una versión de la copia de seguridad que se cree que es anterior a la infección original.

Control 10: Diagrama de relación de entidad de sistema



Control 11: Configuración segura de los equipos de red, tales como cortafuegos, enrutadores y conmutadores

Establecer, implementar y gestionar activamente (rastrear, reportar, corregir) la configuración de seguridad de la infraestructura de red utilizando un proceso de gestión de configuración y control de cambios riguroso para prevenir que los atacantes exploten servicios y configuraciones vulnerables.

¿Por qué es importante este control?

Según lo entregado por los fabricantes y revendedores, las configuraciones predeterminadas para dispositivos de infraestructura de red están orientadas a facilitar el despliegue y la facilidad de uso, no a la seguridad. Servicios y puertos abiertos, cuentas o contraseñas predeterminadas (incluidas cuentas de servicio), soporte para protocolos más antiguos (vulnerables), preinstalación de software innecesario: todos pueden ser explotables en su estado predeterminado. La gestión de las configuraciones seguras para dispositivos de red no es un evento único, sino que es un proceso que implica reevaluar regularmente no solo los elementos de configuración sino también los flujos de tráfico permitidos. Los atacantes aprovechan los dispositivos de red que se configuran de manera menos segura a lo largo del tiempo a medida que los usuarios exigen excepciones para necesidades de negocio específicas. En ocasiones, el riesgo de seguridad de las excepciones no se analiza ni se mide adecuadamente en relación con los fines de negocio asociados, y puede cambiar a lo largo del tiempo. Los atacantes buscan configuraciones predeterminadas, brechas o inconsistencias en el conjunto de reglas de cortafuegos, enrutadores y conmutadores y utilizan esos agujeros para penetrar las defensas. Explotan las fallas en estos dispositivos para obtener acceso a las redes, redirigir el tráfico en una red e interceptar información mientras están en transmisión. A través de tales acciones, el atacante obtiene acceso a datos confidenciales, altera información importante o incluso utiliza una máquina comprometida para hacerse pasar por otro sistema de confianza en la red.

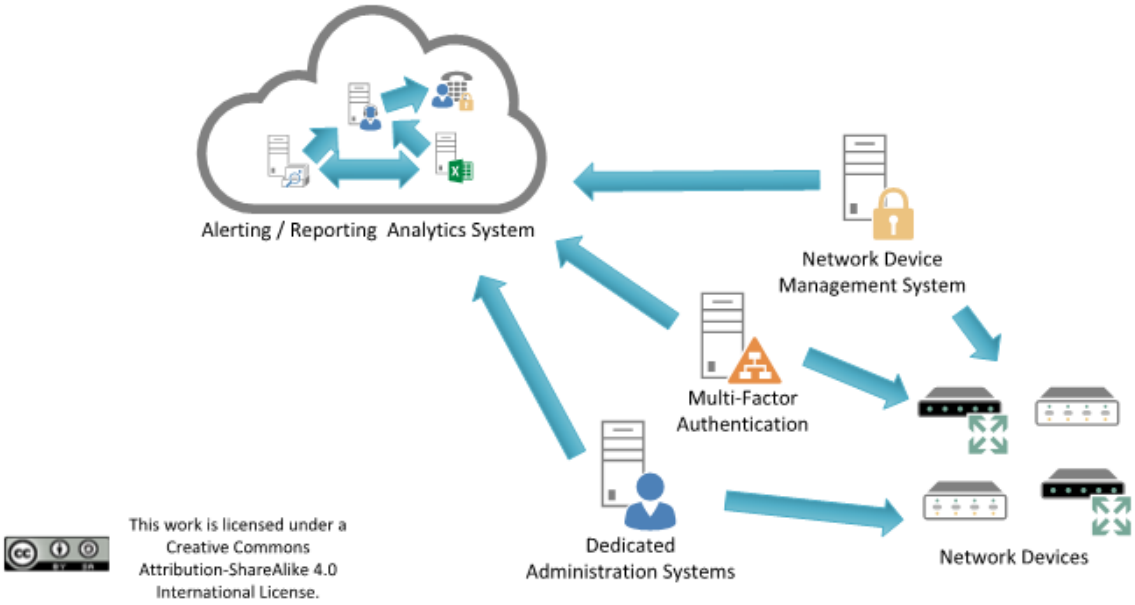
Control crítico #11: Configuración segura de los equipos de red, tales como cortafuegos, enrutadores y conmutadores				
Sub-control	**Tipo de activo**	**Función de Seguridad**	**Control**	**Descripción**
11.1	Red	Identificar	Mantener configuraciones de seguridad estandarizadas en equipos de red	Mantenga estándares de configuración de seguridad estándar y documentados para todos los equipos de red autorizados.
11.2	Red	Identificar	Documentar las reglas de configuración de tráfico	Todas las reglas de configuración que permiten que el tráfico fluya a través de dispositivos de red deben documentarse en un sistema de gestión de configuración con un fin de negocio específico para cada regla, el nombre de un individuo específico responsable de esa necesidad de negocio y una duración esperada de la necesidad

11.3	Red	Detectar	Utilizar herramientas automatizadas para verificar configuraciones de equipos y detectar cambios	Compare toda la configuración de equipos de red con las configuraciones de seguridad aprobadas definidas para cada dispositivo de red en uso y alerte cuando se descubran desviaciones.
11.4	Red	Proteger	Instalar la última versión estable de cualquier actualización de seguridad en todos los equipos de red	Instale la última versión estable de cualquier actualización de seguridad en todos los equipos de red
11.5	Red	Proteger	Gestionar equipos de red utilizando autenticación multi-factor y sesiones cifradas	Gestione los equipos de red utilizando autenticación multi-factor y sesiones cifradas
11.6	Red	Proteger	Utilizar máquinas dedicadas para todas las tareas administrativas en la red	Asegúrese de que los administradores de la red utilicen una máquina dedicada para todas las tareas administrativas o tareas que requieren un acceso elevado. Esta máquina se segmentará de la red principal de la organización y no se le permitirá el acceso a Internet. Esta máquina no debe usarse para leer correos electrónicos, componer documentos o navegar en Internet.
11.7	Red	Proteger	Administrar la infraestructura de red mediante una red dedicada	Administre la infraestructura de red a través de las conexiones de red que están separadas del uso de negocio de la red, mediante VLAN separadas o, preferiblemente, en una conectividad física completamente diferente para sesiones de administración para dispositivos de red.

Control 11: Procedimientos y herramientas

Algunas organizaciones usan herramientas comerciales que evalúan los conjuntos de reglas de los dispositivos de filtrado de red para determinar si son consistentes o si existe conflicto, proporcionando una verificación automatizada de sanidad de los filtros de red y búsqueda de errores en conjuntos de reglas o listas de control de acceso (ACL) que puedan permitir servicios involuntarios a través del dispositivo. Dichas herramientas se deben ejecutar cada vez que se realicen cambios significativos en los conjuntos de reglas del firewall, las ACL del enrutador u otras tecnologías de filtrado.

Control 11: Diagrama de relación de entidad de sistema



Control 12: Defensa de borde

Detectar/prevenir/corregir el flujo de información que transfieren redes de diferentes niveles de confianza con un enfoque en datos que dañan la seguridad.

¿Por qué es importante este control?

Los atacantes se centran en explotar los sistemas que pueden alcanzar a través de Internet, incluidos no solo los sistemas de la DMZ, sino también las estaciones de trabajo y las computadoras portátiles que extraen contenido de Internet a través de los límites de la red. Amenazas como grupos de crimen organizado y Estados utilizan la configuración y las deficiencias arquitectónicas que se encuentran en los sistemas perimetrales, los dispositivos de red y las máquinas cliente que acceden a Internet para obtener acceso inicial a una organización. Luego, con una base de operaciones en estas máquinas, los atacantes a menudo pivotan para profundizar dentro del límite para robar o cambiar información o para establecer una presencia persistente para ataques posteriores contra hosts internos. Además, se producen muchos ataques entre redes de socios comerciales, a veces denominadas extranets, ya que los atacantes saltan de una red de la organización a otra y explotan los sistemas vulnerables en perímetros de la extranet.

Para controlar el flujo de tráfico a través de los bordes de la red y supervisar el contenido buscando ataques y evidencia de máquinas comprometidas, las defensas de borde deben ser multi-capas, confiando en firewalls, *proxies*, redes perimetrales DMZ e IDS/IPS basados en red. También es fundamental filtrar el tráfico entrante y saliente.

Cabe señalar que las líneas divisorias entre las redes internas y externas están disminuyendo como resultado de una mayor interconectividad dentro y entre las organizaciones, así como del rápido aumento en el despliegue de las tecnologías inalámbricas. Estas líneas difusas a veces permiten a los atacantes obtener acceso dentro de las redes sin pasar por los sistemas de borde. Sin embargo, incluso con estos límites difusos, las implementaciones efectivas de seguridad aún dependen de defensas perimetrales cuidadosamente configuradas que separan las redes con diferentes niveles de amenaza, conjuntos de usuarios, datos y niveles de control.

Y a pesar de la difuminación de las redes internas y externas, una defensa multicapa eficaz de las redes perimetrales ayudan a reducir el número de ataques exitosos, permitiendo que el personal de seguridad se centre en los atacantes que han ideado métodos para eludir las restricciones de borde.

Control crítico #12: Defensa de borde				
Sub-control	**Tipo de activo**	**Función de Seguridad**	**Control**	**Descripción**
12.1	Red	Identificar	Mantener un inventario de los bordes de la red	Mantenga un inventario actualizado de todos los bordes de la red de la organización
12.2	Red	Detectar	Escanear de conexiones no autorizadas en los bordes confiables de la red	Realice regularmente escaneos desde el exterior del borde de cada red de confianza para detectar cualquier conexión no autorizada accesible a través del borde.
12.3	Red	Proteger	Denegar comunicaciones con direcciones IPs maliciosas conocidas	Denegar las comunicaciones con direcciones IP de Internet maliciosas conocidas o no utilizadas y limitar el acceso solo a los intervalos de direcciones IP confiables y necesarios en cada uno de los límites de la red de la organización.
12.4	Red	Proteger	Denegar comunicaciones sobre puertos no autorizados	Denegar la comunicación sobre los puertos TCP o UDP no autorizados o el tráfico de aplicaciones para garantizar que solo los protocolos autorizados puedan cruzar el límite de la red hacia o desde la red, en cada uno de los límites de la red de la organización.
12.5	Red	Detectar	Configurar sistemas de monitoreo para registro paquetes de red	Configure los sistemas de monitoreo para registrar los paquetes de red que pasan a través del límite en cada uno de los bordes de la red de la organización.
12.6	Red	Detectar	Desplegar sensores IDS basados en red	Despliegue sensores de sistemas de detección de intrusos (IDS) basados en red para buscar mecanismos de ataque inusuales y detectar el compromiso de estos sistemas en cada uno de los bordes de la red de la organización.
12.7	Red	Proteger	Desplegar IPS basado en red	Despliegue sistemas de prevención de intrusos (IPS) basados en red para bloquear el tráfico de red malicioso en cada uno de los bordes de la red de la organización.
12.8	Red	Detectar	Desplegar colectores NetFlow en equipos de borde de la red	Active la colección de NetFlow y registro de datos en todos los equipos de borde de la red.
12.9	Red	Detectar	Desplegar servidor proxy de filtrado de capa de aplicación	Asegúrese de que todo el tráfico de red hacia o desde Internet pase a través de un proxy de capa de aplicación autenticado que esté configurado para filtrar conexiones no autorizadas.
12.10	Red	Detectar	Descifrar el tráfico de red en el proxy	Descifre todo el tráfico de red cifrado en el proxy de borde antes de analizar el contenido. Sin embargo, la organización puede usar listas blancas de sitios permitidos a los que se puede acceder a través del proxy sin descifrar el tráfico.
12.11	Usuarios	Proteger	Requerir autenticación multi-factor en todos los inicios de sesión remotos	Requiera que todo acceso remoto a la red de la organización utilice cifrado de datos en tránsito y autenticación multi-factor.
12.12	Equipos	Proteger	Gestionar todos los dispositivos remotos que se conectan a la red interna	Analice todos los dispositivos que inician sesión remotamente en la red de la organización antes de acceder a la red para asegurarse de que cada una de las políticas de seguridad de la organización se haya aplicado de la misma manera que los dispositivos de red local.

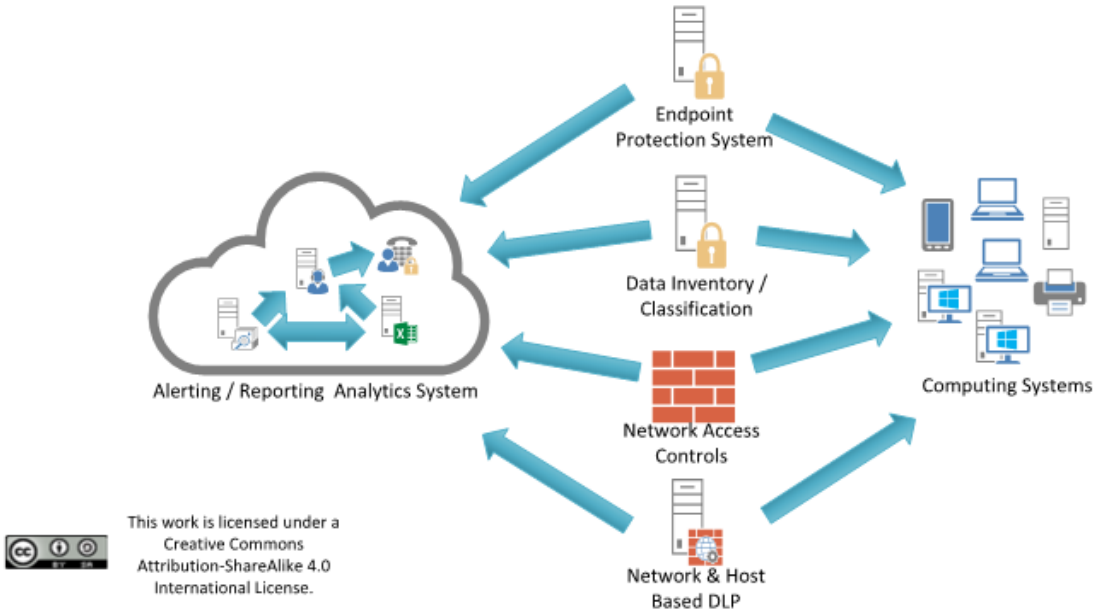
Control 12: Procedimientos y herramientas

Las defensas de borde incluidas en este Control se construyen sobre el Control 9. Las recomendaciones adicionales aquí se centran en mejorar la arquitectura general y la implementación de los puntos de borde de Internet y de la red interna. La segmentación de la red interna es fundamental para este Control porque una vez dentro de una red, muchos intrusos intentan apuntar a las máquinas más sensibles. Por lo general, la protección de la red interna no está configurada para defenderse contra un atacante interno. Configurar incluso un nivel básico de segmentación de seguridad en la red y proteger cada segmento con un proxy y un firewall reducirá en gran medida el acceso de un intruso a las otras partes de la red.

Un elemento de este Control puede implementarse usando IDS y *sniffers* gratuitos o comerciales para buscar ataques de fuentes externas dirigidas a la zona desmilitarizada (DMZ) y sistemas internos, así como ataques provenientes de sistemas internos contra la DMZ o Internet. El personal de seguridad debe probar regularmente estos sensores lanzando contra ellos herramientas de exploración de vulnerabilidades para verificar que el tráfico del escáner active una alerta apropiada. Los paquetes capturados de los sensores IDS deben ser revisados usando un script automatizado cada día para garantizar que el volumen de los registros esté dentro de los parámetros esperados y que los registros estén formateados correctamente y no estén dañados.

Además, los *sniffers* de paquetes deberían desplegarse en las DMZ para buscar tráfico HTTP que eluda los *proxies* HTTP. Al muestrear el tráfico regularmente, por ejemplo, durante un período de tres horas una vez a la semana, el personal de seguridad de la información puede buscar tráfico HTTP que no proviene ni está destinado a un proxy DMZ, lo que implica que se está pasando por alto el requisito del uso del proxy.

Control 12: Diagrama de relación de entidad de sistema



Control 13: Protección de datos

Los procesos y herramientas utilizadas para prevenir la exfiltración de datos, mitigar el efecto de la exfiltración de datos y asegurar la privacidad e integridad de la información sensible.

¿Por qué es importante este control?

Los datos residen en muchos lugares. La mejor manera de lograr la protección de esos datos es mediante la aplicación de una combinación de encriptación, protección de integridad y técnicas de prevención de pérdida de datos. A medida que las organizaciones continúan su avance hacia la computación en la nube y el acceso móvil, es importante que se tome la precaución adecuada para limitar e informar sobre la filtración de datos al tiempo que se mitigan los efectos del compromiso de los datos.

Algunas organizaciones no identifican ni separan cuidadosamente sus activos más sensibles y críticos de información menos sensible y de acceso público en sus redes internas. En muchos entornos, los usuarios internos tienen acceso a todos o la mayoría de los activos críticos. Los activos sensibles también pueden incluir sistemas que proporcionan administración y control de sistemas físicos (por ejemplo, SCADA). Una vez que los atacantes han penetrado en dicha red, pueden encontrar y extraer fácilmente información importante, causar daño físico o interrumpir operaciones con poca resistencia. Por ejemplo, en varias filtraciones de alto perfil en los últimos dos años, los atacantes pudieron obtener acceso a datos confidenciales almacenados en los mismos servidores con el mismo nivel de acceso que los datos menos importantes. También hay ejemplos de cómo usar el acceso a la red corporativa para obtener acceso para controlar los activos físicos y causar daños.

Control crítico #13: Protección de datos				
Sub-control	**Tipo de active**	**Función de Seguridad**	**Control**	**Descripción**
13.1	Datos	Identificar	Mantener un inventario de información sensible	Mantenga un inventario de toda la información sensible almacenada, procesada o transmitida por los sistemas de tecnología de la organización, incluidos los ubicados en la organización o en un proveedor de servicios remoto.
13.2	Datos	Proteger	Remover datos o sistemas sensibles que no son accedidos regularmente por la organización	Elimine datos o sistemas sensibles a los que la organización no accede regularmente desde la red. Estos sistemas solo se utilizarán como sistemas autónomos (desconectados de la red) por parte de la unidad de negocio que necesite utilizar el sistema de vez en cuando o completamente virtualizados y apagados hasta que sea necesario.
13.3	Datos	Detectar	Monitorear y bloquear el tráfico de red no autorizado	Implemente una herramienta automatizada en el perímetro de la red que monitoree la transferencia no autorizada de información sensible y bloquee dichas transferencias mientras alerta a los profesionales de seguridad de la información.

13.4	Datos	Proteger	Permitir solamente el acceso a proveedores de servicios de nube o correo autorizados	Permita solo el acceso a proveedores de servicio de almacenamiento en la nube o correo electrónico autorizados.
13.5	Datos	Detectar	Monitorear y detectar cualquier uso no autorizado de cifrado	Monitoree todo el tráfico que sale de la organización y detecte cualquier uso no autorizado de cifrado.
13.6	Datos	Proteger	Cifrar el disco duro de todos los dispositivos móviles	Utilice software de cifrado de disco completo aprobado para cifrar el disco duro de todos los dispositivos móviles.
13.7	Datos	Proteger	Gestionar dispositivos USB	Si se requieren dispositivos de almacenamiento USB, se debe usar software corporativo que pueda configurar sistemas para permitir el uso de dispositivos específicos. Se debe mantener un inventario de tales dispositivos.
13.8	Datos	Proteger	Gestionar las configuraciones de lectura/escritura de sistemas para medios removibles externos	Configure los sistemas para que no escriban datos en medios extraíbles externos, si no existe una necesidad de negocio para admitir dichos dispositivos.
13.9	Datos	Proteger	Cifrar los datos en dispositivos de almacenamiento USB	Si se requieren dispositivos de almacenamiento USB, todos los datos almacenados en dichos dispositivos se deben cifrar en reposo.

Control 13: Procedimientos y herramientas

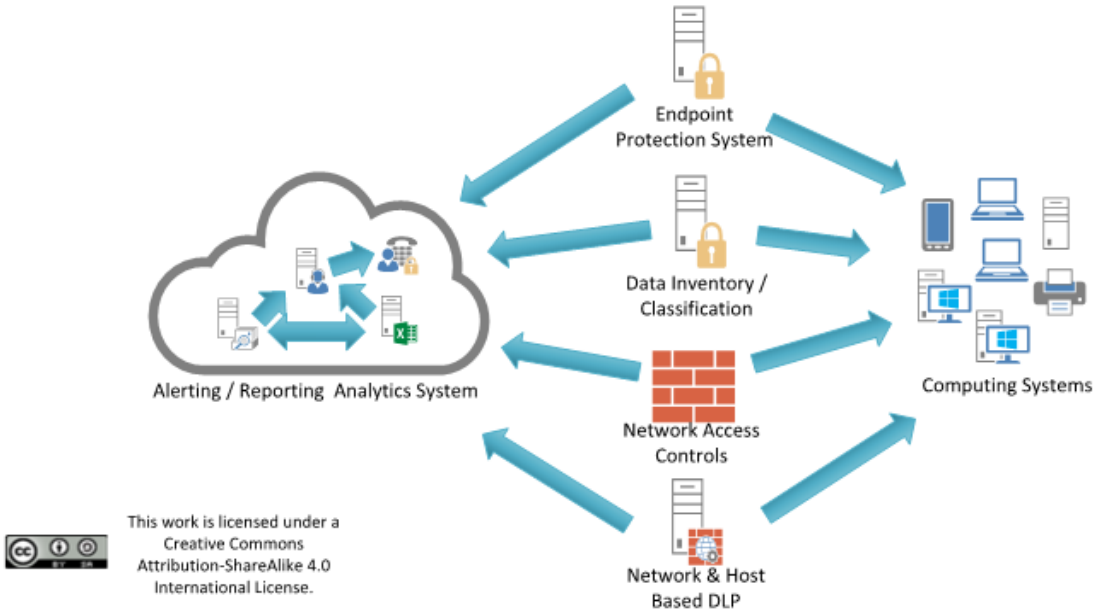
Es importante que una organización comprenda cuál es su información sensible, dónde reside y quién necesita acceder a ella. Para derivar niveles de sensibilidad, las organizaciones necesitan armar una lista de los tipos clave de datos y la importancia general para la organización. Este análisis se usaría para crear un esquema general de clasificación de datos para la organización. Las organizaciones deben definir etiquetas, tales como por ejemplo "Sensible", "Confidencial para el negocio" y "Pública", y clasificar sus datos según esas etiquetas. Una vez que se ha identificado la información privada, se puede subdividir en función del impacto que tendría para la organización si se viera comprometida.

Una vez que se ha identificado la sensibilidad de los datos, cree un inventario o mapeo de datos que identifique las aplicaciones de negocio y los servidores que albergan esas aplicaciones. Luego, la red debe segmentarse para que los sistemas del mismo nivel de sensibilidad estén en la misma red y segmentados de los sistemas con diferentes niveles de confianza. Si es posible, los firewalls deben controlar el acceso a cada segmento.

El acceso a los datos debe basarse en los requisitos del trabajo y en la necesidad de saberlo. Se deben crear requisitos de trabajo para cada grupo de usuarios para determinar a qué información necesita acceder el grupo para realizar sus trabajos. En

función de los requisitos, el acceso solo se debe otorgar a los segmentos o servidores de datos que se necesitan para cada función de trabajo. El registro detallado debe activarse para los servidores con el fin de rastrear el acceso y permitir que el personal de seguridad examine los incidentes en los que se accedió incorrectamente a los datos.

Control 13: Diagrama de relación de entidad de sistema



Control 14: Control de acceso basado en la necesidad de conocer

Los procesos y herramientas utilizados para rastrear/controlar/prevenir/corregir el acceso seguro a activos críticos (por ejemplo, información, recursos, sistemas) de acuerdo con la determinación formal de qué personas, computadoras y aplicaciones tienen una necesidad y derecho a acceder a estos activos críticos basado en una clasificación aprobada.

¿Por qué es importante este control?

El cifrado de datos proporciona un nivel de seguridad de que incluso si los datos se ven comprometidos, no es práctico acceder al texto plano sin recursos significativos; sin embargo, también deberían establecerse controles para mitigar la amenaza de la filtración de datos en primer lugar. Muchos ataques ocurrieron en la red, mientras que otros involucraron el robo físico de computadoras portátiles y otros equipos con información confidencial. Sin embargo, en muchos casos, las víctimas no sabían que datos sensibles abandonaban sus sistemas porque no estaban supervisando las salidas de datos. El movimiento de datos a través de los límites de la red, tanto electrónico como físicamente, debe analizarse cuidadosamente para minimizar su exposición a los atacantes.

La pérdida de control sobre los datos protegidos o sensibles por parte de las organizaciones es una grave amenaza para las operaciones de negocio y una amenaza potencial para la seguridad nacional. Mientras que algunos datos se filtran o pierden como resultado de robo o espionaje, la gran mayoría de estos problemas son el resultado de prácticas de datos poco entendidas, la falta de arquitecturas de políticas efectivas y errores del usuario. La pérdida de datos puede incluso ocurrir como resultado de actividades legítimas como e-Discovery durante un litigio, particularmente cuando las prácticas de retención de registros son ineficaces o inexistentes.

La adopción de cifrado de datos, tanto en tránsito como en reposo, proporciona mitigación contra el compromiso de datos. Esto es cierto si se han tenido los cuidados adecuados en los procesos y tecnologías asociados con las operaciones de cifrado. Un ejemplo de esto es la administración de las claves criptográficas utilizadas por los diversos algoritmos que protegen los datos. El proceso de generación, uso y destrucción de claves debe basarse en procesos probados, tal como se define en normas como NIST SP 800-57.

También se debe tener cuidado para garantizar que los productos utilizados dentro de una organización implementen algoritmos criptográficos bien conocidos y comprobados, según lo identificado por el NIST. También se recomienda volver a evaluar los algoritmos y tamaños de clave utilizados en la organización anualmente para garantizar que las organizaciones no se queden atrás en cuanto a la solidez de la protección aplicada a sus datos.

Para las organizaciones que trasladan datos a la nube, es importante comprender los controles de seguridad aplicados a los datos en el entorno de múltiples huéspedes (multi-tenant) en la nube y determinar el mejor curso de acción para la aplicación de los controles de cifrado y la seguridad de las claves. Cuando sea posible, las claves se deben almacenar dentro de contenedores seguros como los Módulos de seguridad de hardware (HSM).

La prevención de pérdida de datos (DLP) se refiere a un enfoque integral que abarca personas, procesos y sistemas que identifican, supervisan y protegen datos en uso (por ejemplo, acciones de *endpoint*), datos en movimiento (por ejemplo, acciones de red) y datos en reposo (ej., almacenamiento de datos) mediante una profunda inspección de contenido y con un *framework* centralizado. En los últimos años, se ha producido un cambio notable en la atención y la inversión, de asegurar la red a asegurar los sistemas dentro de la red, hasta asegurar los datos en sí. Los controles DLP se basan en políticas e incluyen la clasificación de datos sensibles, el descubrimiento de datos en una organización, la aplicación de controles y la creación de informes y auditorías para garantizar el cumplimiento de las políticas.

Control crítico #14: Control de acceso basado en la necesidad de conocer				
Sub-control	**Tipo de activo**	**Función de Seguridad**	**Control**	**Descripción**
14.1	Red	Proteger	Segmentar la red basado en sensibilidad	Segmente la red según la etiqueta o el nivel de clasificación de la información almacenada en los servidores, ubique toda la información confidencial en redes de área local virtual (VLAN) separadas.
14.2	Red	Proteger	Habilitar filtrado de firewall entre VLANs	Habilite el filtrado de firewall entre las VLAN para garantizar que solo los sistemas autorizados puedan comunicarse con otros sistemas necesarios para cumplir con sus responsabilidades específicas.
14.3	Red	Proteger	Deshabilitar comunicaciones entre estaciones de trabajo	Inhabilite todas las comunicaciones de estación de trabajo a estación de trabajo para limitar la capacidad de un atacante de moverse lateralmente y poner en peligro los sistemas vecinos, a través de tecnologías como VLAN privadas o microsegmentación.
14.4	Datos	Proteger	Cifrar toda la información sensible en tránsito	Cifre toda la información confidencial en tránsito.
14.5	Datos	Detectar	Utilizar una herramienta de descubrimiento activo para identificar datos sensibles	Utilice una herramienta de descubrimiento activo para identificar toda la información sensible almacenada, procesada o transmitida por los sistemas de tecnología de la organización, incluidos los ubicados en el sitio o en un proveedor de servicios remoto, y actualice el inventario de información sensible de la organización.
14.6	Datos	Proteger	Proteger la información mediante lista de control de acceso	Proteja toda la información almacenada en sistemas con listas de control de acceso específicas para sistema de archivos, uso compartido de redes, aplicaciones o bases de datos. Estos controles harán cumplir el principio de que solo las personas autorizadas deberían tener acceso a la información

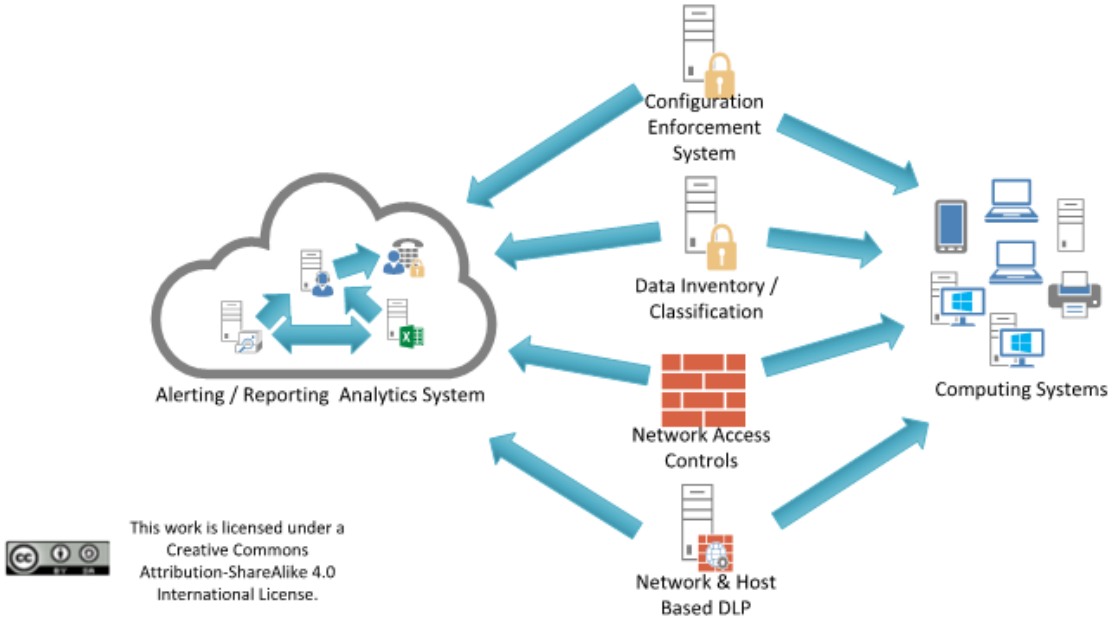
				en función de su necesidad de acceder a la información como parte de sus responsabilidades.
14.7	Datos	Proteger	Aplicar control de acceso a datos mediante herramientas automatizadas	Utilice una herramienta automatizada, como la prevención de pérdida de datos (Data Loss Prevention - DLP) basada en host, para hacer cumplir los controles de acceso a los datos, incluso cuando los datos se copian de un sistema.
14.8	Datos	Proteger	Cifrar información sensible en reposo	Cifre toda la información sensible en reposo utilizando una herramienta que requiere un mecanismo de autenticación secundario no integrado en el sistema operativo, para poder acceder a la información.
14.9	Datos	Detectar	Imponer el registro detallado para acceso o cambios en datos sensibles	Imponga el registro de auditoría detallado para acceder o realizar cambios en datos sensibles (utilizando herramientas como Monitoreo de Integridad de Archivos o sistemas SIEM).

Control 14: Procedimientos y herramientas

Están disponibles herramientas comerciales que permiten la gestión corporativa de cifrado y administración de claves dentro de una organización e incluyen la capacidad de soportar la implementación de controles de cifrado dentro de la nube y en entornos móviles. La definición de los procesos del ciclo de vida y las funciones y responsabilidades asociadas con la gestión de claves debe ser asumida por cada organización.

Están disponibles soluciones DLP comerciales para buscar intentos de exfiltración y detectar otras actividades sospechosas asociadas con una red protegida que contiene información sensible. Las organizaciones que implementen tales herramientas deben inspeccionar cuidadosamente sus registros y realizar un seguimiento de los intentos descubiertos de transmitir información confidencial de la organización sin autorización, incluso aquellos que se bloquearon con éxito.

Control 14: Diagrama de relación de entidad de sistema



Control 15: Control de acceso inalámbrico

Los procesos y herramientas utilizados para rastrear/controlar/prevenir/corregir el uso seguro de las redes de área local inalámbricas (WLAN), puntos de acceso y sistemas de clientes inalámbricos.

¿Por qué es importante este control?

Los principales robos de datos han sido iniciados por atacantes que han obtenido acceso inalámbrico a la organización desde el exterior del edificio físico, sobrepasando el perímetro de seguridad de la misma, conectándose de forma inalámbrica a los puntos de acceso dentro de la organización. Los clientes inalámbricos que acompañan a los viajeros se infectan regularmente a través de la explotación remota, mientras se encuentran en redes inalámbricas públicas de los aeropuertos y cafeterías. Estos sistemas explotados se utilizan como puertas traseras cuando se vuelven a conectar a la red de una organización objetivo. Otras organizaciones han reportado el descubrimiento de puntos de acceso inalámbrico no autorizados en sus redes, plantados y, a veces, ocultos para el acceso irrestricto a una red interna. Debido a que no requieren conexiones físicas directas, los dispositivos inalámbricos son vectores convenientes para que los atacantes mantengan el acceso a largo plazo en un entorno objetivo.

Control crítico #15: Control de acceso inalámbrico				
Sub-control	**Tipo de activo**	**Función de Seguridad**	**Control**	**Descripción**
15.1	Red	Identificar	Mantener un inventario de puntos de acceso inalámbrico autorizados	Mantenga un inventario de los puntos de acceso inalámbrico autorizados conectados a la red cableada.
15.2	Red	Detectar	Detectar puntos de acceso inalámbricos conectados a la red cableada	Configure las herramientas de exploración de vulnerabilidades de red para detectar y alertar sobre puntos de acceso inalámbrico no autorizados conectados a la red cableada.
15.3	Red	Detectar	Usar un sistema de detección de intrusión inalámbrica	Use un sistema inalámbrico de detección de intrusos (WIDS) para detectar y alertar sobre puntos de acceso inalámbrico no autorizados conectados a la red.
15.4	Equipos	Proteger	Deshabilitar el acceso inalámbrico en dispositivos si no se requiere	Deshabilite el acceso inalámbrico en dispositivos que no tienen un propósito de negocio para el acceso inalámbrico.
15.5	Equipos	Proteger	Limitar el acceso inalámbrico en dispositivos cliente	Configure el acceso inalámbrico en máquinas cliente que tienen un propósito de negocio inalámbrico esencial, para permitir el acceso solo a redes inalámbricas autorizadas y para restringir el acceso a otras redes inalámbricas.

15.6	Equipos	Proteger	Inhabilitar las capacidades de red inalámbrica punto a punto en clientes inalámbricos	Inhabilite las capacidades de redes inalámbricas punto a punto (adhoc) en clientes inalámbricos.
15.7	Red	Proteger	Usar estándar de cifrado avanzado (AES) para cifrar datos inalámbricos	Aproveche el estándar de cifrado avanzado (Advanced Encryption Standard - AES) para cifrar datos inalámbricos en tránsito.
15.8	Red	Proteger	Usar protocolos de autenticación inalámbrica que requieran autenticación mutua multi-factor	Asegúrese de que las redes inalámbricas utilicen protocolos de autenticación como Protocolo de autenticación extensible / Seguridad de capa de transporte (Extensible Authentication Protocol-Transport Layer Security - EAP / TLS), que requiere autenticación mutua de múltiples factores.
15.9	Equipos	Proteger	Deshabilitar el acceso periférico inalámbrico de dispositivos	Deshabilite el acceso periférico inalámbrico de dispositivos (como Bluetooth y NFC), a menos que dicho acceso sea necesario para fines de negocio.
15.10	Red	Proteger	Crear una red inalámbrica separada para dispositivos personales y no confiables	Cree una red inalámbrica separada para dispositivos personales o que no sean de confianza. El acceso de la organización desde esta red debe tratarse como no confiable y debe filtrarse y auditarse en consecuencia.

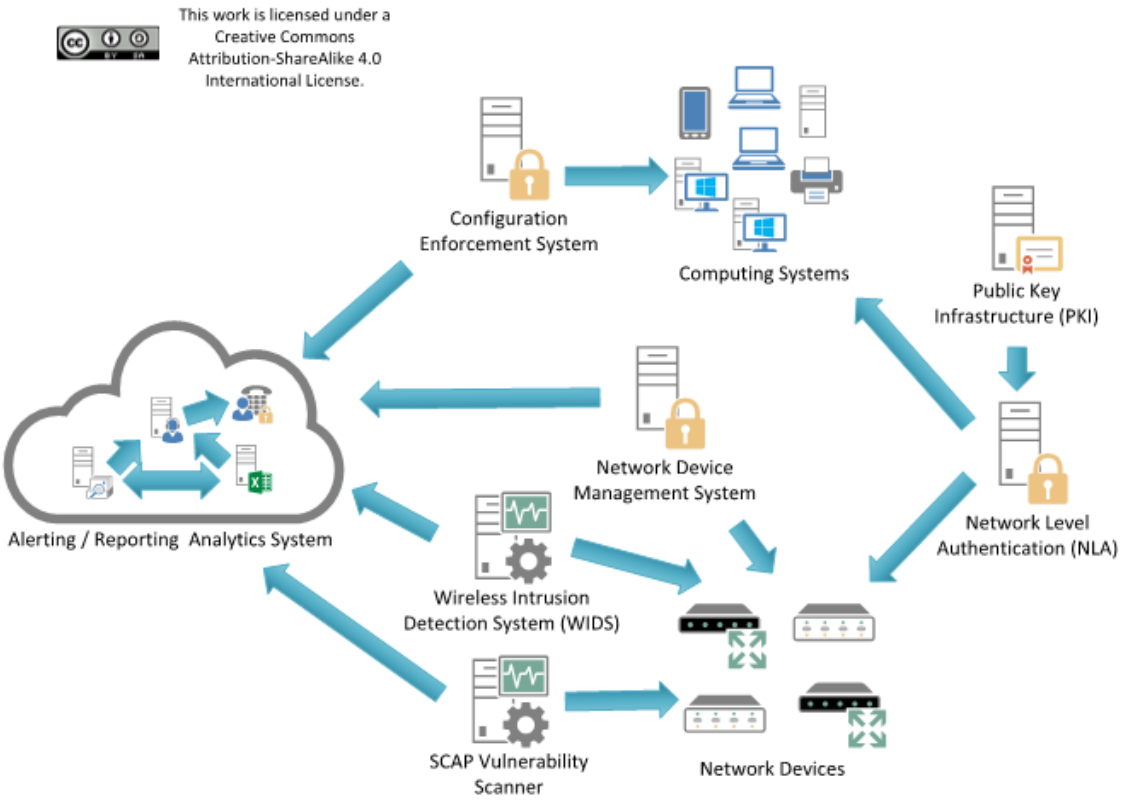
Control 15: Procedimientos y herramientas

Las organizaciones eficaces ejecutan herramientas comerciales de escaneo, detección y descubrimiento inalámbrico, así como sistemas de detección de intrusiones inalámbricas comerciales.

Además, el equipo de seguridad debe capturar periódicamente el tráfico inalámbrico desde los bordes de una instalación y utilizar herramientas de análisis gratuitas y comerciales para determinar si el tráfico inalámbrico se transmitió utilizando protocolos o cifrado más débiles que los mandatos de la organización. Cuando se identifican dispositivos con una configuración de seguridad inalámbrica débil, deben encontrarse dentro del inventario de activos de la organización y re-configurarse de forma más segura o denegar el acceso a la red de la organización.

Además, el equipo de seguridad debe emplear herramientas de administración remota en la red cableada para extraer información sobre las capacidades inalámbricas y los dispositivos conectados a los sistemas administrados.

Control 15: Diagrama de relación de entidad de sistema



Control 16: Monitoreo y control de cuentas

Gestione activamente el ciclo de vida de las cuentas del sistema y de aplicaciones (su creación, uso, latencia, eliminación) con el fin de minimizar las oportunidades para que los atacantes las aprovechen.

¿Por qué es importante este control?

Los atacantes frecuentemente descubren y explotan cuentas de usuarios legítimas pero inactivas para suplantar a usuarios legítimos, lo que dificulta el descubrimiento del comportamiento de los atacantes para el personal de seguridad. Las cuentas de contratistas y empleados que ya no trabajan para la organización y las cuentas que habían sido configuradas para las pruebas del Equipo Rojo (pero que luego no se eliminan) a menudo se han utilizado de forma incorrecta. Además, algunas personas internas o ex-empleados malintencionados han accedido a cuentas que han sido dejadas en un sistema mucho después de la expiración del contrato, manteniendo su acceso al sistema informático de una organización y datos confidenciales para fines no autorizados y en ocasiones maliciosos.

Control crítico #16: Monitoreo y control de cuentas				
Sub-control	**Tipo de activo**	**Función de Seguridad**	**Control**	**Descripción**
16.1	Usuarios	Identificar	Mantener un inventario de sistemas de autenticación	Mantenga un inventario de cada uno de los sistemas de autenticación de la organización, incluidos los ubicados en el sitio o en un proveedor de servicios remoto.
16.2	Usuarios	Proteger	Configurar un punto de autenticación centralizado	Configure el acceso para todas las cuentas a través de la menor cantidad posible de puntos de autenticación centralizados, incluidos los sistemas de red, de seguridad y en la nube.
16.3	Usuarios	Proteger	Requerir Autenticación Multi-factor	Requiera autenticación de múltiples factores para todas las cuentas de usuario, en todos los sistemas, ya sea que se administren localmente en la organización o por un proveedor de terceros.
16.4	Usuarios	Proteger	Cifrar o hashear todas las credenciales de autenticación	Utilice técnicas de cifrado o hash combinado con salt con todas las credenciales de autenticación cuando se almacenan.
16.5	Usuarios	Proteger	Cifrar la transmisión de nombres de usuario y credenciales de autenticación	Asegúrese de que todos los nombres de usuario y las credenciales de autenticación de la cuenta se transmitan a través de redes que utilizan canales cifrados.
16.6	Usuarios	Identificar	Mantener un inventario de	Mantenga un inventario de todas las cuentas organizadas por sistema de autenticación.

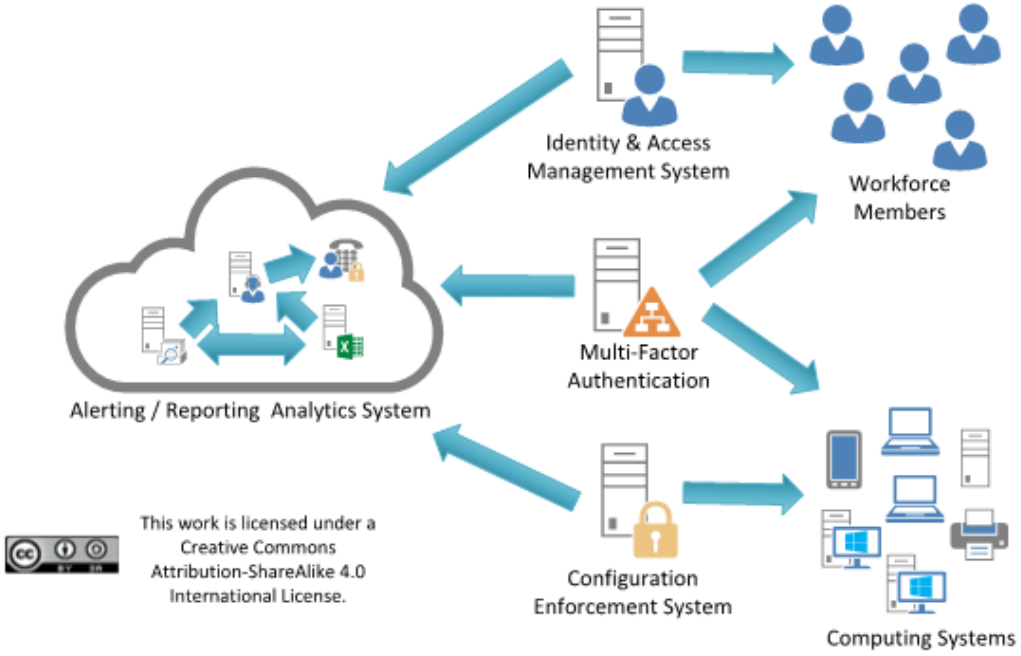
			cuentas	
16.7	Usuarios	Proteger	Establecer un proceso para revocar el acceso	Establezca y siga un proceso automatizado para revocar el acceso a sistemas mediante la desactivación de cuentas inmediatamente después de la terminación o el cambio de responsabilidades de un empleado o contratista. Desactivar estas cuentas, en lugar de eliminar cuentas, permite preservar los registros de auditoría.
16.8	Usuarios	Responder	Deshabilitar cualquier cuenta no asociada	Deshabilite cualquier cuenta que no pueda asociarse con un proceso de negocio o un propietario de la organización.
16.9	Usuarios	Responder	Desactivar cuentas inactivas	Deshabilite automáticamente las cuentas inactivas después de un período de inactividad establecido.
16.10	Usuarios	Proteger	Asegurar que todas las cuentas tengan fecha de caducidad	Asegúrese de que todas las cuentas tengan una fecha de vencimiento monitoreada y forzada.
16.11	Usuarios	Proteger	Bloquear sesiones de estaciones de trabajo tras inactividad	Bloquee automáticamente las sesiones de la estación de trabajo después de un período estándar de inactividad.
16.12	Usuarios	Detectar	Monitorear los intentos de acceso a cuentas desactivadas	Monitoree los intentos de acceso a cuentas desactivadas a través de los registros de auditoría.
16.13	Usuarios	Detectar	Alertar sobre desviación de comportamiento de inicio de sesión de cuentas	Alerte cuando los usuarios se desvían del comportamiento normal de inicio de sesión , como la hora y/o el día, la ubicación de la estación de trabajo y la duración.

Control 16: Procedimientos y herramientas

Aunque la mayoría de los sistemas operativos incluyen capacidades para registrar información sobre el uso de cuentas, estas funciones algunas veces están deshabilitadas de manera predeterminada. Incluso cuando tales funciones están presentes y activas, a menudo, por defecto, no proporcionan detalles precisos sobre el acceso al sistema. El personal de seguridad puede configurar sistemas para registrar información más detallada sobre el acceso a cuentas, y utilizar scripts propios o herramientas de análisis de registros de terceros para analizar esta información y perfilar el acceso de usuarios de varios sistemas.

Las cuentas también deben ser monitoreadas muy de cerca. Cualquier cuenta que esté inactiva debe ser desactivada y eventualmente eliminada del sistema. Todas las cuentas activas se deben remontar a los usuarios autorizados del sistema, y deben utilizar la autenticación de múltiples factores. Los usuarios también deben desconectarse del sistema después de un período de inactividad para minimizar la posibilidad de que un atacante use su sistema para extraer información de la organización.

Control 16: Diagrama de relación de entidad de sistema



Nota especial con respecto a los Controles 17 – 20:

- Control 17: Implementar un programa de concienciación y capacitación en seguridad
- Control 18: Seguridad del software de aplicación
- Control 19: Respuesta y gestión de incidentes
- Control 20: Pruebas de penetración y ejercicios de Equipo Rojo

Todos estos temas son una parte crítica y fundamental de cualquier programa de ciberdefensa, pero tienen un carácter diferente al de los Controles 1-16. Si bien tienen muchos elementos técnicos, estos están menos enfocados en los controles técnicos y más enfocados en las personas y los procesos. Son amplios en cuanto a que deben considerarse en toda la organización y en todos los Controles 1-16. Sus mediciones y métricas de éxito son impulsadas más por las observaciones sobre los pasos y resultados del proceso, y menos por la recolección de datos técnicos. También son temas complejos por derecho propio, cada uno con un cuerpo existente de literatura y orientación.

Por lo tanto, presentamos los Controles 17-20 de la siguiente manera: para cada Control, identificamos una pequeña cantidad de elementos que creemos que son críticos para un programa efectivo en cada área. A continuación, describimos procesos y recursos que pueden utilizarse para desarrollar un tratamiento corporativo más completo de cada tema. Aunque hay muchos recursos comerciales excelentes disponibles, proporcionamos fuentes abiertas y sin fines de lucro siempre que sea posible. Las ideas, los requisitos y los procesos expresados en las referencias están bien respaldados por el mercado comercial.

Control 17: Implementar un programa de concienciación y entrenamiento de seguridad

Para todos los roles funcionales en la organización (priorizando aquellos que son misionales para la organización y su seguridad), identificar los conocimientos, habilidades y capacidades específicos necesarios para soportar la defensa de la organización; desarrollar y ejecutar un plan integral para evaluar, identificar brechas y remediar a través de políticas, planificación organizacional, capacitación y programas de concienciación.

¿Por qué es importante este control?

Es tentador pensar en la defensa cibernética principalmente como un desafío técnico, pero las acciones de las personas también juegan un papel crítico en el éxito o el fracaso de una organización. Las personas cumplen funciones importantes en cada etapa del diseño, implementación, operación, uso y supervisión del sistema.

Los ejemplos incluyen: desarrolladores de sistemas y programadores (que pueden no entender la oportunidad de resolver vulnerabilidades de causa raíz al principio del ciclo de vida del sistema); profesionales de operaciones de TI (que pueden no reconocer las implicaciones de seguridad de los artefactos y registros de TI); usuarios finales (que pueden ser susceptibles a esquemas de ingeniería social como el phishing); analistas de seguridad (que luchan por mantenerse al día con una explosión de nueva información); y ejecutivos y propietarios de sistemas (que luchan por cuantificar el papel que desempeña la seguridad cibernética en el riesgo operacional y misional general, y no tienen una forma razonable de tomar decisiones de inversión relevantes).

Los atacantes son muy conscientes de estos problemas y los utilizan para planificar sus explotaciones, por ejemplo: elaborando cuidadosamente mensajes de phishing que parecen tráfico de rutina y esperado para un usuario incauto; explotando las brechas o las grietas entre la política y la tecnología (por ejemplo, políticas que no tienen aplicación técnica); trabajando dentro de la ventana de tiempo de parcheo o revisión de registro; utilizando sistemas nominalmente no críticos para la seguridad como puntos de salto o *bots*.

Ningún enfoque de defensa cibernética puede abordar eficazmente el riesgo cibernético sin un medio para abordar esta vulnerabilidad fundamental. Por el contrario, empoderar a las personas con buenos hábitos de defensa cibernética puede aumentar significativamente la preparación.

Control crítico #17: Implementar un programa de concienciación y entrenamiento de seguridad				
Sub-control	**Tipo de activo**	**Función de Seguridad**	**Control**	**Descripción**
17.1	N/A	N/A	Realizar un análisis de brecha de habilidades	Lleve a cabo un análisis de la brecha de habilidades para comprender las habilidades y los comportamientos a los que los miembros de la fuerza de trabajo no se están adhiriendo, usando esta información para construir una hoja de ruta base de educación.
17.2	N/A	N/A	Realizar capacitación para llenar la brecha de habilidades	Realice capacitaciones para abordar el vacío de habilidades identificado para impactar positivamente el comportamiento de seguridad de los miembros de la fuerza laboral.
17.3	N/A	N/A	Implementar un programa de concienciación de seguridad	Cree un programa de concientización de seguridad para que todos los miembros de la fuerza laboral lo completen regularmente para asegurarse de que entienden y exhiben los comportamientos y las habilidades necesarias para ayudar a garantizar la seguridad de la organización. El programa de concientización de seguridad de la organización debe comunicarse de manera continua y atractiva.
17.4	N/A	N/A	Actualice el contenido de concienciación con frecuencia	Asegúrese de que el programa de concientización de seguridad de la organización se actualice con frecuencia (al menos una vez al año) para abordar nuevas tecnologías, amenazas, estándares y requisitos de negocio.
17.5	N/A	N/A	Entrenar a la fuerza laboral en la autenticación segura	Capacite a los miembros de la fuerza de trabajo sobre la importancia de habilitar y utilizar la autenticación segura.
17.6	N/A	N/A	Capacitar a la fuerza laboral en la identificación de ataques de ingeniería social	Capacite a los empleados sobre cómo identificar diferentes formas de ataques de ingeniería social, como phishing, fraudes telefónicos y llamadas de suplantación.
17.7	N/A	N/A	Capacitar a la fuerza laboral en manejo de datos sensibles	Capacite a los empleados sobre cómo identificar y almacenar, transferir, archivar y destruir información confidencial de manera adecuada.
17.8	N/A	N/A	Capacitar a la fuerza laboral sobre las causas de la exposición involuntaria a los datos	Capacite a los miembros de la fuerza de trabajo para que conozcan las causas de las exposiciones involuntarias de datos, cómo perder sus dispositivos móviles o enviar correos electrónicos a la persona equivocada debido al autocompletado en el correo electrónico.
17.9	N/A	N/A	Capacite a la fuerza laboral sobre cómo identificar y reportar incidentes	Capacitar a los empleados para que puedan identificar los indicadores más comunes de un incidente y poder informar tal incidente.

Control 17: Procedimientos y recursos

Un programa de capacitación eficaz en toda la organización debería tener un enfoque holístico y considerar las políticas y la tecnología al mismo tiempo que la capacitación

de las personas. Las políticas deben diseñarse con mediciones y cumplimiento técnicos y deben reforzarse con capacitación para llenar las lagunas en la comprensión; se pueden implementar controles técnicos para proteger los sistemas y los datos, y minimizar la posibilidad de que las personas cometan errores. Con controles técnicos implementados, la capacitación puede enfocarse en conceptos y habilidades que no pueden ser manejados técnicamente.

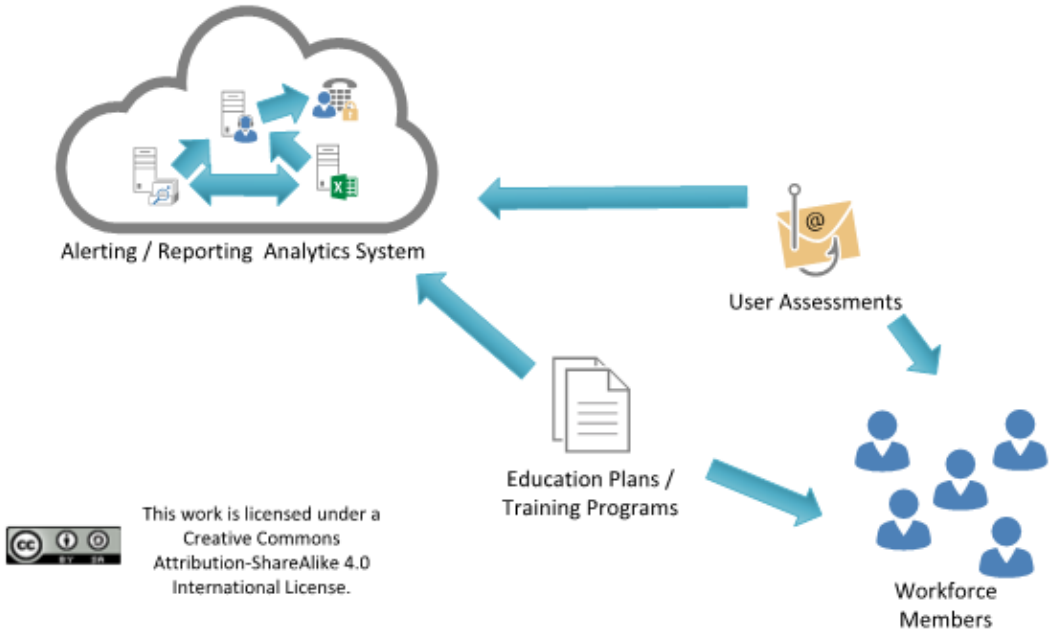
Un programa efectivo de capacitación en defensa cibernética es más que un evento anual; es una mejora continua del proceso con los siguientes elementos clave:

- La capacitación es específica, personalizada y enfocada en función de los comportamientos y habilidades específicos que necesita la fuerza de trabajo, según su función y responsabilidad laboral.
- El entrenamiento se repite periódicamente, se mide y se prueba su efectividad y se actualiza regularmente.
- Aumentará la toma de conciencia y desalentará las chapuzas arriesgadas al incluir racionalidad para los buenos comportamientos y habilidades de seguridad.

En las acciones convocadas en este Control, hemos identificado algunos elementos críticos de un programa de capacitación exitoso. Para un tratamiento más completo de este tema, sugerimos los siguientes recursos para ayudar a la organización a construir un programa efectivo de concienciación de seguridad:

- NIST SP 800-50 Infosec Awareness Training https://csrc.nist.gov/publications/detail/sp/800-50/final
- ENISA https://www.enisa.europa.eu/publications/archive/copy_of_new-users-guide (Este documento es de 2010, por lo que es muy antiguo, pero es un recurso europeo, por lo que puede ser mejor para un público más amplio.)
- EDUCAUSE https://library.educause.edu/search#?q=security%20awareness%20and%20training
- NCSA https://staysafeonline.org/
- SANS https://www.sans.org/security-awareness-training/resources

Control 17: Diagrama de relación de entidad de sistema



Control 18: Seguridad del software de aplicación

Gestione el ciclo de vida de seguridad de todo el software interno desarrollado y adquirido para prevenir, detectar y corregir las debilidades de seguridad.

¿Por qué es importante este control?

Los ataques a menudo aprovechan las vulnerabilidades que se encuentran en el software basado en la web y en otras aplicaciones. Las vulnerabilidades pueden estar presentes por muchas razones, incluidos los errores de programación, los errores de lógica, los requisitos incompletos y la falta de pruebas de condiciones inusuales o inesperadas. Los ejemplos de errores específicos incluyen: la falla al verificar el tamaño de la entrada del usuario; no filtrar las secuencias de caracteres innecesarios, pero potencialmente maliciosos de los flujos de entrada; falla al inicializar y borrar variables; y una gestión de memoria deficiente que permite que los defectos en una parte del software afecten a partes no relacionadas (y más críticas desde el punto de vista de seguridad).

Existe una avalancha de información pública y privada sobre estas vulnerabilidades disponible para los atacantes y defensores por igual, así como un mercado robusto de herramientas y técnicas para permitir la "militarización" de vulnerabilidades en *exploits*. Los atacantes pueden inyectar vulnerabilidades específicas, incluidos desbordamientos de búfer, ataques de inyección de lenguaje estructurado de consulta (Structured Query Language - SQL), *cross-site* scripting (XSS), *cross-site request forgery* (CSRF) y *click-jacking* de código para obtener control sobre máquinas vulnerables. En un ataque, más de 1 millón de servidores web fueron explotados y convertidos en motores de infección para los visitantes de esos sitios que usan inyección SQL. Durante ese ataque, se usaron sitios web confiables de los gobiernos estatales y otras organizaciones comprometidas por los atacantes para infectar a cientos de miles de navegadores que accedieron a esos sitios web. Regularmente se descubren muchas más vulnerabilidades de aplicaciones web y no web.

Control crítico #18: Seguridad del software de aplicación				
Sub-control	**Tipo de activo**	**Función de Seguridad**	**Control**	**Descripción**
18.1	N/A	N/A	Establecer prácticas seguras de codificación	Establezca prácticas seguras de codificación apropiadas para el lenguaje de programación y el entorno de desarrollo que se utiliza.
18.2	N/A	N/A	Asegurar que la verificación explícita de errores se realice para todo el software desarrollado internamente	Para el software desarrollado internamente, asegúrese de que se realice y documente la verificación de errores explícita para todas las entradas, incluidos el tamaño, el tipo de datos y los rangos o formatos aceptables. .

18.3	N/A	N/A	Verificar que el software adquirido aún tiene soporte	Verifique que la versión de todo el software adquirido desde fuera de su organización aún cuente con soporte del desarrollador o esté debidamente securizada en función de las recomendaciones de seguridad del desarrollador.
18.4	N/A	N/A	Usar sólo componentes de terceros actualizados y de confianza	Utilice únicamente componentes de terceros actualizados y de confianza para el software desarrollado por la organización.
18.5	N/A	N/A	Usar únicamente algoritmos de cifrado revisados y estandarizados	Utilice únicamente algoritmos de cifrado ampliamente revisados y estandarizados.
18.6	N/A	N/A	Asegurar que el personal de desarrollo de software esté capacitado en programación segura	Asegúrese de que todo el personal de desarrollo de software reciba capacitación para escribir código seguro para su entorno de desarrollo y responsabilidades específicas.
18.7	N/A	N/A	Aplicar herramientas de análisis de código estático y dinámico	Aplique herramientas de análisis estático y dinámico para verificar que se cumplan las prácticas de codificación segura para el software desarrollado internamente. .
18.8	N/A	N/A	Establecer un proceso para aceptar y tratar los reportes de vulnerabilidades del software	Establezca un proceso para aceptar y tratar los reportes de las vulnerabilidades del software, incluido proporcionar un mecanismo para que las entidades externas se comuniquen con su grupo de seguridad.
18.9	N/A	N/A	Sistemas separados de producción y no producción	Mantenga entornos separados para sistemas de producción y no producción. Los desarrolladores no deberían tener acceso no supervisado a entornos de producción.
18.10	N/A	N/A	Implementar Firewall de aplicación Web (WAFs)	Proteja las aplicaciones web mediante la implementación de firewalls de aplicaciones web (WAF) que inspeccionan todo el tráfico que fluye a la aplicación web para ataques comunes de aplicaciones web. Para aplicaciones que no están basadas en web, se deben implementar firewalls de aplicaciones específicas si tales herramientas están disponibles para el tipo de aplicación dado. Si el tráfico está cifrado, el dispositivo debe colocarse detrás del cifrado o ser capaz de descifrar el tráfico antes del análisis. Si ninguna de las opciones es adecuada, se debe implementar un firewall de aplicaciones web basado en host.
18.11	N/A	N/A	Usar plantillas de configuración de hardening estándar para bases de datos	Para aplicaciones que dependen de una base de datos, use plantillas de configuración de hardening estándar. Todos los sistemas que son parte de procesos de negocio críticos también deben ser probados.

Control 18: Procedimientos y recursos

La seguridad de las aplicaciones desarrolladas internamente o adquiridas *out-of-the-box* (listas para usarse) es una actividad compleja que requiere un programa completo que englobe las políticas, la tecnología y el rol de las personas en toda la organización.

Todo el software debe ser probado regularmente para detectar vulnerabilidades. La práctica operativa de escanear vulnerabilidades de aplicaciones se ha consolidado en el Control 3: Gestión continua de vulnerabilidades. Sin embargo, el enfoque más efectivo es implementar un programa de seguridad de la cadena de suministro completo para el software adquirido externamente y un Ciclo de vida de desarrollo de software seguro para el software desarrollado internamente. Esos aspectos se abordan en este Control.

Para el software desarrollado internamente o personalizado y desarrollado externamente por contrato, un programa efectivo para aplicaciones de software debe abordar la seguridad durante todo el ciclo de vida e integrar la seguridad como parte natural del establecimiento de requerimientos, capacitación, herramientas y pruebas. Los ciclos y métodos de desarrollo modernos no permiten enfoques secuenciales. Los criterios de aceptación siempre deben incluir como requisito que se ejecuten las herramientas de testing de vulnerabilidades de la aplicación y se documenten todas las vulnerabilidades conocidas. Es seguro suponer que el software no será perfecto, por lo que un programa de desarrollo debe planificar de antemano el informe y la solución de fallas como una función de seguridad esencial.

Para el software que se adquiere (comercial, de código abierto, etc.), los criterios de seguridad de la aplicación deben formar parte de los criterios de evaluación y se deben realizar esfuerzos para comprender las prácticas de origen del software, las pruebas y la gestión e informe de errores. Siempre que sea posible, se debe exigir a los proveedores que demuestren que se utilizaron herramientas o servicios de prueba de software comercial estándar y que no existen vulnerabilidades conocidas en la versión actual.

Las acciones en este control proporcionan pasos específicos de alta prioridad que pueden mejorar la seguridad del software de aplicaciones. Además, recomendamos el uso de algunos de los excelentes recursos integrales dedicados a este tema:

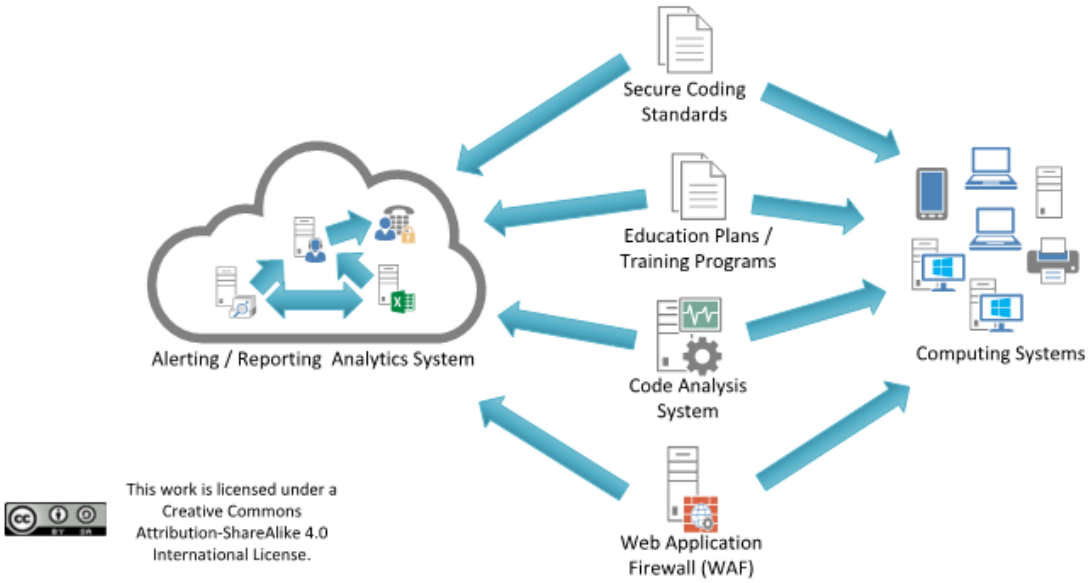
- The Open Web Application Security Project (OWASP)

  OWASP es una comunidad abierta que crea y comparte una gran colección de herramientas de software y documentación sobre seguridad de aplicaciones. https://www.owasp.org

- Software Assurance Forum for Excellence in Code (SAFECODE)

  SAFECODE crea y fomenta la adopción general de la industria de prácticas comprobadas de seguridad, integridad y autenticidad del software. https://www.safecode.org/

Control 18: Diagrama de relación de entidad de sistema



Control 19: Respuesta y manejo de incidentes

Proteger la información de la organización, así como su reputación, desarrollando e implementando una infraestructura de respuesta a incidentes (por ejemplo, planes, funciones definidas, capacitación, comunicaciones, supervisión de la gestión) para descubrir rápidamente un ataque y luego contener de manera efectiva el daño, erradicando la presencia del atacante y restaurando la integridad de la red y los sistemas.

¿Por qué es importante este control?

Hoy en día, los incidentes cibernéticos son ya parte de nuestra forma de vida. Incluso empresas grandes, bien financiadas y técnicamente sofisticadas luchan por mantenerse al día con la frecuencia y complejidad de los ataques. La cuestión de un ciberataque exitoso contra una organización no es "si" sino "cuándo".

Cuando ocurre un incidente, es demasiado tarde para desarrollar los procedimientos correctos, informes, recopilación de datos, responsabilidad de gestión, protocolos legales y estrategia de comunicaciones que permitan a la organización comprender, gestionar y recuperarse con éxito. Sin un plan de respuesta a incidentes, una organización puede no descubrir un ataque en primer lugar o, si se detecta el ataque, la organización puede no seguir buenos procedimientos para contener el daño, erradicar la presencia del atacante y recuperarse de manera segura. Por lo tanto, el atacante puede tener un impacto mucho mayor, causando más daño, infectando más sistemas y posiblemente extrayendo datos más sensibles de lo que de otro modo sería posible si un plan de respuesta a incidentes fuera efectivo.

Control crítico #19: Respuesta y manejo de incidentes				
Sub-control	**Tipo de activo**	**Función de Seguridad**	**Control**	**Descripción**
19.1	N/A	N/A	Documentar los procedimientos de respuesta de incidentes	Asegúrese de que haya planes escritos de respuesta a incidentes que definan las funciones del personal, así como las fases de manejo/gestión de incidentes. .
19.2	N/A	N/A	Asignar cargos y responsabilidades para la respuesta a incidentes	Asigne los cargos y responsabilidades para el manejo de incidentes cibernéticos a personas específicas y asegure el seguimiento y la documentación durante todo el incidente hasta la resolución.
19.3	N/A	N/A	Designar personal de gestión para apoyar el manejo de incidentes	Designe al personal de gestión, así como a sus suplentes, que apoyen el proceso de manejo de incidentes actuando en roles claves de toma de decisiones.
19.4	N/A	N/A	Idear estándares para toda la organización para	Diseñe estándares para toda la organización con respecto a los tiempos requerido para que los administradores de sistemas y otros miembros de la fuerza laboral informen

			reporte de incidentes	eventos anómalos al equipo de manejo de incidentes, los mecanismos para dichos informes y el tipo de información que debe incluirse en la notificación de incidente.
19.5	N/A	N/A	Mantener información de contacto para reportar incidentes de seguridad	Reúna y mantenga información sobre la información de contacto de terceros que se utilizará para informar un incidente de seguridad, como los organismos de aplicación de ley, organismos gubernamentales pertinentes, proveedores, socios de ISAC.
19.6	N/A	N/A	Publicar información relacionada con la notificación de anomalías e incidentes informáticos	Publique información para todos los miembros de la fuerza laboral, con respecto a reportar anomalías e incidentes informáticos al equipo de manejo de incidentes. Dicha información debe incluirse en las actividades de concientización rutinarias de los empleados.
19.7	N/A	N/A	Llevar a cabo sesiones periódicas de escenarios de incidentes para el personal	Planifique y realice ejercicios y escenarios rutinarios de respuesta a incidentes para la fuerza laboral involucrada en la respuesta a incidentes para mantener la conciencia y la comodidad a la hora de responder a las amenazas del mundo real. Los ejercicios deben evaluar las capacidades técnicas de los canales de comunicación, la toma de decisiones y los responsables de responder al incidente, utilizando las herramientas y los datos disponibles para ellos.
19.8	N/A	N/A	Crear un esquema de priorización y puntuación de incidentes	Cree un esquema de puntuación y priorización de incidentes basado en el impacto conocido o potencial para su organización. Utilice una puntuación para definir la frecuencia de las actualizaciones de estado y los procedimientos de escalación.

Control 19: Procedimientos y herramientas

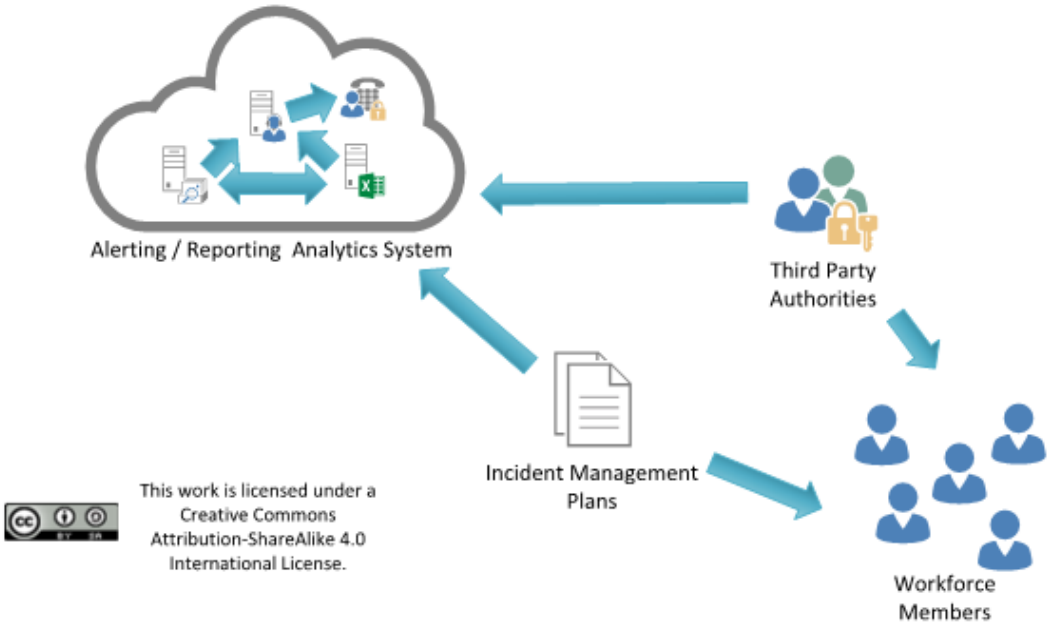
Después de definir los procedimientos detallados de respuesta a incidentes, el equipo de respuesta al incidente debe participar en una capacitación periódica basada en escenarios, trabajando a través de una serie de escenarios de ataque ajustados a las amenazas y vulnerabilidades que enfrenta la organización. Estos escenarios ayudan a garantizar que los miembros del equipo comprendan su rol en el equipo de respuesta a incidentes y también ayudan a prepararlos para manejar los incidentes. Es inevitable que los escenarios de ejercicio y capacitación identifiquen las brechas en los planes y procesos, y las dependencias inesperadas.

Las acciones en este Control brindan pasos específicos, de alta prioridad, que pueden mejorar la seguridad de la organización y deben formar parte de cualquier plan integral de incidentes y respuestas. Además, recomendamos el uso de algunos de los excelentes recursos exhaustivos dedicados a este tema:

- CREST Cyber Security Incident Response Guide

  CREST brinda orientación, estándares y conocimiento sobre una amplia variedad de temas de defensa cibernética. https://www.crest-approved.org/wp-content/uploads/2014/11/CSIR-Procurement-Guide.pdf

Control 19: Diagrama de relación de entidad de sistema



Control 20: Pruebas de penetración y ejercicios de equipo rojo

Probar la fortaleza general de la defensa de una organización (la tecnología, los procesos y las personas) simulando los objetivos y las acciones de un atacante.

¿Por qué es importante este control?

Los atacantes a menudo explotan la brecha entre los buenos diseños defensivos y las buenas intenciones y su implementación o mantenimiento. Los ejemplos incluyen: la ventana de tiempo entre el anuncio de una vulnerabilidad, la disponibilidad de un parche del proveedor y la instalación real en cada máquina. Otros ejemplos incluyen: políticas bien intencionadas que no tienen mecanismo de aplicación (especialmente aquellas destinadas a restringir las acciones humanas riesgosas); la falla en la aplicación de buenas configuraciones a las máquinas que entran y salen de la red; y la incapacidad de comprender la interacción entre múltiples herramientas defensivas o con operaciones normales de sistemas que tienen implicaciones de seguridad.

Una postura defensiva exitosa requiere un programa integral de políticas y gobernanza efectivas, defensas técnicas fuertes y acciones apropiadas por parte de las personas. En un entorno complejo en el que la tecnología evoluciona constantemente y atacantes con nuevas capacidades aparecen regularmente, las organizaciones deben evaluar periódicamente sus defensas para identificar los vacíos y evaluar su preparación mediante la realización de pruebas de penetración.

Las pruebas de penetración comienzan con la identificación y evaluación de las vulnerabilidades que se pueden identificar en la organización. A continuación, las pruebas se diseñan y ejecutan para demostrar específicamente cómo un adversario puede subvertir los objetivos de seguridad de la organización (por ejemplo, la protección de propiedad intelectual específica) o alcanzar objetivos adversos específicos (por ejemplo, establecer una infraestructura encubierta de comando y control). Los resultados proporcionan una visión más profunda, a través de la demostración, de los riesgos de negocio de diversas vulnerabilidades.

Los ejercicios de Equipo Rojo tienen un enfoque exhaustivo en todo el espectro de políticas, procesos y defensas de la organización con el fin de mejorar la preparación de la organización, mejorar el entrenamiento de los practicantes defensivos e inspeccionar los niveles de rendimiento actuales. Los Equipos Rojos independientes pueden proporcionar información valiosa y objetiva sobre la existencia de vulnerabilidades y la eficacia de las defensas y los controles de mitigación ya existentes e incluso de los planeados para su implementación futura.

Control crítico #20: Pruebas de penetración y ejercicios de equipo rojo				
Sub-control	**Tipo de activo**	**Función de Seguridad**	**Control**	**Descripción**
20.1	N/A	N/A	Establecer un programa de prueba de penetración	Establezca un programa para pruebas de penetración que incluya un alcance completo de ataques combinados, como ataques inalámbricos, basados en cliente y aplicaciones web.
20.2	N/A	N/A	Llevar a cabo pruebas periódicas de penetración externa e interna	Realice pruebas periódicas de penetración externa e interna para identificar vulnerabilidades y vectores de ataque que puedan utilizarse para explotar con éxito los sistemas de la organización.
20.3	N/A	N/A	Realizar Ejercicios Periódicos del Equipo Rojo	Realice ejercicios periódicos del Equipo Rojo para evaluar la preparación de la organización para identificar y detener ataques o para responder de manera rápida y efectiva.
20.4	N/A	N/A	Incluir pruebas de presencia de información y artefactos no protegidos de sistema	Incluya pruebas de la presencia de información de sistemas y artefactos no protegido que serían útiles para los atacantes, incluidos diagramas de red, archivos de configuración, informes de pruebas de penetración anteriores, correos electrónicos o documentos que contienen contraseñas u otra información crítica para el funcionamiento de sistemas.
20.5	N/A	N/A	Crear banco de pruebas para elementos que normalmente no se prueban en producción	Cree un banco de pruebas que imite un entorno de producción para pruebas de penetración específicas y ataques del Equipo Rojo contra elementos que normalmente no se prueban en producción, como ataques contra control de supervisión y adquisición de datos y otros sistemas de control.
20.6	N/A	N/A	Usar herramientas de prueba de penetración y exploración de vulnerabilidades en conjunto	Utilice herramientas de exploración de vulnerabilidades y pruebas de penetración en conjunto. Los resultados de las evaluaciones de escaneo de vulnerabilidad deben usarse como punto de partida para guiar y enfocar los esfuerzos de prueba de penetración.
20.7	N/A	N/A	Asegurar que los resultados de la prueba de penetración estén documentados usando estándares abiertos y legibles por máquina	Siempre que sea posible, asegúrese de que los resultados de los Equipos Rojos estén documentados utilizando estándares abiertos y legibles por máquina (por ejemplo, SCAP). Diseñe un método de puntuación para determinar los resultados de los ejercicios del Equipo Rojo para que los resultados puedan compararse a lo largo del tiempo.
20.8	N/A	N/A	Controlar y monitorear las cuentas asociadas con las pruebas de penetración	Las cuentas de usuario o de sistema utilizadas para realizar las pruebas de penetración deben monitorearse y controlarse para garantizar que solo se utilicen con fines legítimos y se eliminen o restablezcan a la función normal una vez finalizadas las pruebas.

Control 20: Procedimientos y recursos

Históricamente, las pruebas de penetración y las pruebas del Equipo Rojo se llevan a cabo:

- como una demostración "dramática" de un ataque, por lo general para convencer a los tomadores de decisiones de la vulnerabilidad de su organización;
- como un medio para probar el correcto funcionamiento de las defensas de la organización ("verificación"); y
- para probar que la organización ha construido las defensas correctas en primer lugar ("validación").

En general, este tipo de pruebas son costosas, complejas y pueden presentar sus propios riesgos. Pueden proporcionar un valor significativo, pero solo cuando ya existen medidas defensivas básicas y cuando estas pruebas se realizan como parte de un programa integral y continuo de gestión y mejora de la seguridad. Los eventos de prueba son una forma muy costosa de descubrir que su organización hace un mal trabajo con parches y administración de configuración, por ejemplo.

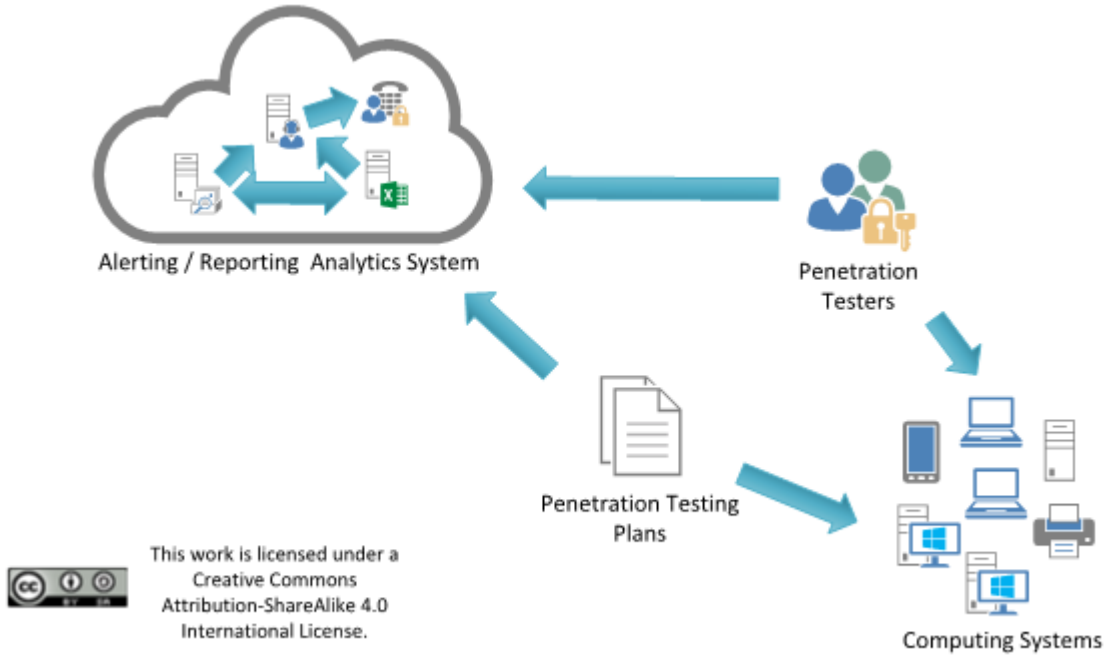
Cada organización debe definir un alcance claro y reglas de participación para las pruebas de penetración y los análisis del Equipo Rojo. El alcance de tales proyectos debe incluir, como mínimo, aquellos sistemas de información de mayor valor de la organización y la funcionalidad de procesos de negocio. También se pueden probar otros sistemas de menor valor para ver si se pueden usar como puntos de pivote para comprometer objetivos de mayor valor. Las reglas de participación para las pruebas de penetración y los análisis del Equipo Rojo deben describir, como mínimo, las horas del día para las pruebas, la duración de las pruebas y el enfoque general de la prueba.

Las acciones en este Control proporcionan pasos específicos de alta prioridad que pueden mejorar la seguridad de la organización y que deben ser parte de cualquier prueba de penetración y del programa del Equipo Rojo. Además, recomendamos el uso de algunos de los excelentes recursos integrales dedicados a este tema para ayudar a la planificación, gestión e informes de pruebas de seguridad:

- OWASP Penetration Testing Methodologies
  https://www.owasp.org/index.php/Penetration_testing_methodologies

- PCI Security Standards Council
  https://www.pcisecuritystandards.org/documents/Penetration-Testing-Guidance-v1_1.pdf

Control 20: Diagrama de relación de entidad de sistema



Notas de Cierre

Todas las referencias a herramientas u otros productos en este documento se proporcionan sólo con fines informativos, y no representan el respaldo a ninguna compañía, producto o tecnología en particular.

Si está interesado en ser voluntario y/o tiene preguntas o comentarios, o ha identificado formas, etc. para mejorar esta guía, por favor escribanos a cert@cert.gov.py.

Información de contacto

CERT-PY – SENATICs
Complejo Santos Bloque E
+595 21 2179000
www.cert.gov.py
cert@cert.gov.py