

Controles CIS

Versión 8

V8

CIS Controls Versión 8

Mayo 2021

Este trabajo está licenciado bajo una licencia pública internacional de Reconocimiento-No comercial-Sin Derivados 4.0 de Creative Commons (el enlace se puede encontrar en <https://creativecommons.org/licenses/by-nc-nd/4.0/legalcode>).

Para aclarar aún más la licencia de Creative Commons relacionada con el contenido de CIS Controls, está autorizado a copiar y redistribuir el contenido como un marco de trabajo para su uso, dentro de su organización y fuera de su organización para fines no comerciales únicamente, siempre que (i) se otorga el crédito apropiado a CIS, y (ii) se proporciona un enlace a la licencia. Además, si mezcla, transforma o construye sobre los Controles CIS, no puede distribuir los materiales modificados. También se requiere que los usuarios del marco de trabajo de controles CIS se refieran a (<http://www.cisecurity.org/controls/>) cuando se refieren a los controles CIS para garantizar que los usuarios estén utilizando la guía más actualizada. El uso comercial de los controles CIS está sujeto a la aprobación previa de CIS® (Center for Internet Security, Inc.).

Agradecimientos

CIS® (Center for Internet Security, Inc.) quisiera agradecer a los numerosos expertos en seguridad que ofrecen voluntariamente su tiempo y talento para apoyar Critical Security Controls (CIS Controls®) y otros trabajos de CIS. Los productos de CIS representan el esfuerzo de un verdadero ejército de voluntarios de toda la industria, que brindan generosamente su tiempo y talento en nombre de una experiencia en línea más segura para todos.

En agradecimiento a todos los voluntarios expertos en la comunidad de ciberseguridad por compartir su tiempo y talento con la organización CIS, y a la Selección Nacional CSIRT de Paraguay (Cert-PY) por traducir y difundir este documento a la comunidad de habla hispana.

Contenido

	Glossário	iii
	Acrónimos y Abreviaturas	vi
	Introducción	1
	Evolución de los Controles CIS	1
	Esta Versión de los Controles CIS	2
	El Ecosistema de los Controles CIS ("No se trata de un listado")	4
	Cómo empezar	4
	Adopción o transición de versiones anteriores de los Controles CIS	5
	Estructura de los Controles CIS	5
	Perfiles	5
Control 01	Inventario y Control de los Activos Empresariales	8
	¿Por qué es Crítico este Control?	8
	Procedimientos y Herramientas	9
	Salvaguardas	10
Control 02	Inventario y Control de Activos de Software	11
	¿Por qué es Crítico este Control?	11
	Procedimientos y Herramientas	12
	Salvaguardas	12
Control 03	Protección de los Datos	14
	¿Por qué es Crítico este Control?	14
	Procedimientos y Herramientas	15
	Salvaguardas	15
Control 04	Configuración Segura de Activos y Software Empresarial	17
	¿Por qué es Crítico este Control?	17
	Procedimientos y Herramientas	18
	Salvaguardas	19
Control 05	Administración de Cuentas	20
	¿Por qué es Crítico este Control?	20
	Procedimientos y Herramientas	20
	Salvaguardas	21
Control 06	Gestión de Control de Accesos	22
	¿Por qué es Crítico este Control?	22
	Procedimientos y herramientas	22
	Salvaguardas	23
Control 07	Gestión Continua de Vulnerabilidades	25
	¿Por qué este Control es Crítico?	25
	Procedimientos y Herramientas	26
	Salvaguardas	27
Control 08	Gestión de Registros de Auditoría	28
	¿Por qué es Crítico este Control?	28
	Procedimientos y Herramientas	28
	Salvaguardas	29
Control 09	Protección del Correo Electrónico y Navegador Web	30
	¿Por qué es Crítico este Control?	30
	Procedimientos y Herramientas	30
	Salvaguardas	31

Control 10	Defensas contra Malware	33
	¿Por qué es este Control Crítico?	33
	Procedimientos y Herramientas	33
	Salvaguardas	34
Control 11	Recuperación de Datos	35
	¿Por qué es Crítico este Control?	35
	Procedimientos y Herramientas	35
	Salvaguardas	36
Control 12	Gestión de la Infraestructura de Red	37
	¿Por qué es Crítico este Control?	37
	Procedimientos y Herramientas	37
	Salvaguardas	38
Control 13	Monitoreo y Defensa de la red	40
	¿Por qué es Crítico este Control?	40
	Procedimientos y Herramientas	41
	Salvaguardas	41
Control 14	Concientización en Seguridad y Formación de Habilidades	43
	¿Por qué es Crítico este Control?	43
	Procedimientos y Herramientas	43
	Salvaguardas	44
Control 15	Gestión de Proveedores de Servicios	46
	¿Por qué es Crítico este Control?	46
	Procedimientos y Herramientas	47
	Salvaguardas	47
Control 16	Seguridad en el Software de Aplicación	49
	¿Por qué es Crítico este Control?	49
	Procedimientos y Herramientas	50
	Salvaguardas	52
Control 17	Gestión de Respuesta a Incidentes	54
	¿Por qué es Crítico este Control?	54
	Procedimientos y Herramientas	54
	Salvaguardas	55
Control 18	Pruebas de Penetración	57
	¿Por qué es Crítico este Control?	57
	Procedimientos y Herramientas	58
	Salvaguardas	59
Apêndice A	Recursos y Referencias	A1
Apêndice B	Controls and Safeguards Index	B1

Glossário

Cuentas de Administrador	Cuentas dedicadas con elevados privilegios y son utilizados para administrar las características de una computadora, dominio, o toda la infraestructura de tecnología de la información de la empresa. Los subtipos de cuentas de administrador frecuentes incluyen cuentas de root, Administrador local y cuentas de administración del dominio, y red o cuentas de administrador de dispositivos de seguridad.
Aplicación	Un programa, grupo de programas, alojado como un activo de la empresa y diseñado para los usuarios finales. Las aplicaciones son consideradas como un activo en este documento. Dentro de la definición están incluidos por ejemplo web, bases de datos, aplicaciones basadas en la nube y aplicaciones para móviles.
Sistemas de Autenticación	Un sistema o mecanismo utilizado para identificar a un usuario mediante la asociación de una solicitud entrante con un conjunto de credenciales de identificación. Las credenciales proporcionadas se comparan con las de un archivo de una base de datos de la información del usuario autorizado en un sistema operativo local, servicio de directorio de usuarios o dentro de un servidor de autenticación. Algunos ejemplos de sistemas de autenticación pueden ser Directorio Activo (AD), Múltiple Factor de Autenticación (MFA), biometría y tokens.
Sistemas de Autorización	Un sistema o mecanismo utilizado para determinar los niveles de acceso o los privilegios de usuario/cliente relacionados con los recursos del sistema, incluidos archivos, servicios, programas informáticos, datos y características de aplicaciones. Un sistema de autorización concede o deniega el acceso a un recurso en función de la identidad del usuario. Algunos ejemplos de sistemas de autorización pueden ser Active Directory, listas de control de acceso y listas de control de acceso basadas en roles.
Ambiente de Nube	Un entorno virtualizado que proporciona acceso de red ventajoso y bajo demanda a un grupo compartido de recursos configurables como red, informática, almacenamiento, aplicaciones y servicios. Hay cinco características esenciales para un ambiente de nube: on-demand self-service, broad network access, resource pooling, rapid elasticity, and measured service. Algunos servicios ofrecidos a través de entornos en la nube incluyen software como servicio (SaaS), plataforma como servicio (PaaS) e infraestructura como servicio (IaaS).
Base de Datos	Una recopilación organizada de datos, generalmente almacenados y accedidos electrónicamente desde un sistema informático. Las bases de datos pueden residir de forma remota o local. Los Sistemas de Gestión de Base de Datos (DMSs) se utilizan para administrar bases de datos y no se consideran parte de una base de datos para este documento.
Dispositivos de usuarios	Activos de tecnología de la información (TI) utilizados entre los miembros de una empresa durante el trabajo, fuera del horario laboral o cualquier otro propósito. Los dispositivos de usuario incluyen dispositivos móviles y portátiles como computadoras portátiles, teléfonos inteligentes y tabletas, así como computadoras de escritorio y estaciones de trabajo. Para el propósito de este documento, los dispositivos del usuario son un subconjunto de activos de la empresa.
Activos Empresariales	Activos con el potencial de almacenar o procesar datos. A los efectos de este documento, los activos empresariales incluyen dispositivos de usuario final, dispositivos de red, dispositivos no informáticos / Internet de las cosas (IoT) y servidores, en entornos físicos, virtuales y basados en la nube.
Activos Empresariales Expuestos Externamente	Se hace referencia a los activos de la empresa que son de cara al público y que se pueden detectar mediante el reconocimiento del sistema de nombres de dominio y el análisis de la red desde la Internet pública fuera de la red de la empresa.

Activos Empresariales internos	Se refiere a los activos empresariales no públicos que solo se pueden identificar mediante exploraciones de red y reconocimiento desde dentro de la red de una empresa a través de acceso autorizado o no autorizado.
Librerías	Código elaborado, clases, procedimientos, scripts, datos de configuración y más, que se utilizan para desarrollar aplicaciones y programas de software. Está diseñado para ayudar tanto al programador como al compilador del lenguaje de programación a crear y ejecutar software.
Dispositivos móviles de usuarios	Pequeños, dispositivos de usuarios emitidos por la empresa con capacidad de conectarse de forma inalámbrica a una red, por ejemplo, teléfonos inteligentes y tabletas. Dispositivos móviles de usuarios son un subconjunto de dispositivos portátiles de usuarios, incluso computadoras portátiles, que puedan requerir hardware externo para conectividad. Para el propósito de este documento dispositivos móviles de usuarios son un subconjunto de dispositivos de usuarios.
Dispositivos de Red	Dispositivos electrónicos necesarios para la comunicación y la interacción entre dispositivos de una red informática. Los dispositivos de red incluyen puntos de acceso inalámbricos, cortafuegos, puertas de enlace físicas/virtuales, enrutadores y conmutadores. Estos dispositivos constan de hardware físico, así como dispositivos virtuales y basados en la nube. A los efectos de este documento, los dispositivos de red son un subconjunto de los activos empresariales.
Infraestructura de Red	Se refiere a todos los recursos de una red que hacen posible la conectividad, la gestión, las operaciones comerciales y la comunicación de la red o de Internet. Consiste en hardware y software, sistemas y dispositivos, y permite la informática y la comunicación entre usuarios, servicios, aplicaciones y procesos. La infraestructura de red puede ser en la nube, física o virtual.
Dispositivos no informáticos/Internet de las cosas (IoT)	Dispositivos integrados con sensores, software y otras tecnologías con el fin de conectar, almacenar e intercambiar datos con otros dispositivos y sistemas a través de Internet. Si bien estos dispositivos no se utilizan para procesos computacionales, respaldan la capacidad de una empresa para realizar procesos comerciales. Ejemplos de estos dispositivos incluyen impresoras, pantallas inteligentes, sensores de seguridad física, sistemas de control industrial y sensores de tecnología de la información. A los efectos de este documento, los dispositivos no informáticos / de IoT son un subconjunto de los activos empresariales.
Sistemas Operativos	Es el software en los activos de la empresa que administra los recursos de software y hardware de la computadora, y proporciona servicios comunes para los programas. Los sistemas operativos se consideran un activo de software y pueden ser de una o varias tareas, de un solo usuario y de varios usuarios, distribuidos, con plantillas, integrados, en tiempo real y de biblioteca.
Entorno físico	Se refiere a partes de hardware físico que componen una red, incluidos cables y enrutadores. El hardware es necesario para la comunicación y la interacción entre dispositivos en una red.
Dispositivos portátiles de usuarios	Son dispositivos transportables para el usuario que tienen la capacidad de conectarse de forma inalámbrica a una red. A los efectos de este documento, los dispositivos portátiles para el usuario pueden incluir computadoras portátiles y dispositivos móviles como teléfonos inteligentes y tabletas, todos los cuales son un subconjunto de los activos de la empresa.
Dispositivos remotos	Puede ser cualquier activo de la empresa capaz de conectarse a una red de forma remota, generalmente desde Internet público. Esto puede incluir activos empresariales como dispositivos de usuario, dispositivos de red, dispositivos no informáticos / Internet de las cosas (IoT) y servidores.

Sistemas de archivo remoto	Cuando se habilita una aplicación que se ejecuta en un activo empresarial para acceder a archivos almacenados en un activo diferente. Los sistemas de archivos remotos a menudo hacen que otros recursos, como dispositivos remotos no informáticos, sean accesibles desde un activo. El acceso remoto al archivo se realiza mediante algún tipo de red de área local, red de área amplia, enlace punto a punto u otro mecanismo de comunicación. Estos sistemas de archivos a menudo se denominan sistemas de archivos de red o sistemas de archivos distribuidos.
Medios Extraíbles	Cualquier tipo de dispositivo de almacenamiento que se pueda quitar de una computadora mientras el sistema está funcionando y que permita que los datos se muevan de un sistema a otro. Ejemplos de medios extraíbles incluyen discos compactos (CD), discos versátiles digitales (DVD) y discos Blu-ray, copias de seguridad en cinta, así como disquetes y unidades de bus serie universal (USB).
Servidor	Un dispositivo o sistema que proporciona recursos, datos, servicios o programas a otros dispositivos en una red de área local o una red de área extensa. Los servidores pueden proporcionar recursos y utilizarlos desde otro sistema al mismo tiempo. Algunos ejemplos son los servidores web, los servidores de aplicaciones, los servidores de correo y los servidores de archivos.
Cuentas de Servicio	Una cuenta dedicada con privilegios elevados que se utiliza para ejecutar aplicaciones y otros procesos. Las cuentas de servicio también se pueden crear solo para poseer datos y archivos de configuración. No están destinados a ser utilizados por personas, excepto para realizar operaciones administrativas.
Servicios	Se refiere a una funcionalidad de software o un conjunto de funcionalidades de software, como la recuperación de información especificada o la ejecución de un conjunto de operaciones. Los servicios proporcionan un mecanismo para habilitar el acceso a una o más capacidades, donde el acceso se proporciona mediante una interfaz prescrita y en función de la identidad del solicitante según las directivas de uso de la empresa.
Ingeniería Social	Se refiere a una amplia gama de actividades maliciosas realizadas a través de interacciones humanas en varias plataformas, como el correo electrónico o el teléfono. Se basa en la manipulación psicológica para engañar a los usuarios para que cometan errores de seguridad o entreguen información confidencial.
Activos de Software	En este documento, también se hace referencia a los programas y otra información operativa que se utilizan dentro de un activo empresarial. Los activos de software incluyen sistemas operativos y aplicaciones.
Cuentas de usuarios	Una identidad creada para una persona en una computadora o sistema informático. A los efectos de este documento, las cuentas de usuario se refieren a cuentas de usuario "estándar" o "interactivas" con privilegios limitados y se utilizan para tareas generales como leer el correo electrónico y navegar por la web. Las cuentas de usuario con privilegios escalados están cubiertas por cuentas de administrador.
Ambiente Virtual	Simula el hardware para permitir que un entorno de software se ejecute sin la necesidad de utilizar una gran cantidad de hardware real. Los entornos virtualizados se utilizan para hacer que un pequeño número de recursos actúen como muchos con mucha capacidad de procesamiento, memoria, almacenamiento y red. La virtualización es una tecnología fundamental que permite que la computación en la nube funcione.

Acrónimos y Abreviaturas

AAA	Authentication, Authorization, and Auditing
ACL	Access Control List
AD	Active Directory
AoC	Attestation of Compliance
API	Application Programming Interface
BEC	Business Email Compromise
C2	Command and Control
CCE	Common Configuration Enumeration
CDM	Community Defense Model
CIA	Confidentiality, Integrity, and Availability
CIS	Center for Internet Security
CIS-CAT	CIS Configuration Assessment Tool
COTS	Commercial off-the-Shelf
CPE	Common Platform Enumeration
CREST	Council of Registered Security Testers
CSA	Cloud Security Alliance
CSP	Cloud Service Provider
CVE	Common Vulnerabilities and Exposures
CVSS	Common Vulnerability Scoring System
DBIR	Data Breach Investigations Report
DEP	Data Execution Prevention
DG	Development Group
DHCP	Dynamic Host Configuration Protocol
DKIM	DomainKeys Identified Mail
DLP	Data Loss Prevention
DMARC	Domain-based Message Authentication, Reporting, and Conformance
DMS	Database Management System
DNS	Domain Name System
DPI	Deep Packet Inspection
EDR	Endpoint Detection and Response
EOL	End of Life
FFIEC	Federal Financial Institutions Examination Council
FISMA	Federal Information Security Modernization Act
GRC	Governance Risk and Compliance
HECVAT	Higher Education Community Vendor Assessment Toolkit

HIPAA	Health Insurance Portability and Accountability Act
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IaaS	Infrastructure as a Service
IAM	Identity and Access Management
IDS	Intrusion Detection System
IG	Implementation Group
IOCs	Indicators of Compromise
IoT	Internet of Things
IP	Internet Protocol
IPS	Intrusion Prevention System
ISAC	Information Sharing and Analysis Center
ISO	International Organization for Standardization
IT	Information Technology
LotL	Living off the Land
MDM	Mobile Device Management
MFA	Multi-Factor Authentication
MITRE ATT&CK	MITRE Adversarial Tactics, Techniques, and Common Knowledge®
MS-ISAC	Multi-State Information Sharing and Analysis Center
NaaS	Network-as-a-Service
NCSA	National Cyber Security Alliance
NIDS	Network Intrusion Detection System
NIST	National Institute of Standards and Technology
OS	Operating System
OSS	Open Source Software
OVAL	Open Vulnerability and Assessment Language
OWASP	Open Web Application Security Project
PaaS	Platform as a Service
PAM	Privileged Access Management
PCI	Payment Card Industry
SaaS	Software as a Service
SAFECode	Software Assurance Forum for Excellence in Code
SCADA	Supervisory Control and Data Acquisition

SCAP	Security Content Automation Protocol
SIEM	Security Information and Event Management
SIP	System Integrity Protection
SMS	Short Messaging Service
SOC	Security Operations Center
SOC 2	Service Organization Control 2
SPAM	Something Posing as Mail
SPF	Sender Policy Framework
SQL	Structured Query Language
SSDF	Secure Software Development Framework
SSH	Secure Shell

SSO	Single Sign-On
Telnet	Teletype Network
TLS	Transport Layer Security
TTPs	Tactics, Techniques, and Procedures
U.K.	United Kingdom
URL	Uniform Resource Locator
USB	Universal Serial Bus
VPN	Virtual Private Network
WDEG	Windows Defender Exploit Guard
WPA2	Wi-Fi Protected Access 2
XCCDF	Extensible Configuration Checklist Description Format

Introducción

Los Controles CIS® empezaron como una simple actividad de base para identificar los ciberataques más comunes e importantes del mundo real que afectan a las empresas todos los días, traducir ese conocimiento y experiencia en acciones positivas, constructivas para los defensores, para luego compartir con una audiencia más amplia esa información. Las metas originales eran modestas – ayudar a las personas y empresas a enfocar su atención y comenzar con los pasos más importantes para defenderse de los ataques que realmente importan.

Dirigido por el Center for Internet Security® (CIS®), los Controles CIS han madurado hasta convertirse en una comunidad internacional de personas voluntarias e instituciones que:

- Comparten información sobre ataques y atacantes, identificar el origen que los causa, y traducirlos en lecciones para acciones defensivas
- Crear y compartir herramientas, guías de trabajo e adopción historias y resolución de problemas
- Mapear los Controles CIS a los marcos de cumplimiento y regulatorio para garantizar su alineación y darles prioridad y enfoque colectivos
- Identificar barreras y problemas en común (Tales como la evaluación inicial y la implementación de hojas de ruta), y resolverlas como comunidad

Los Controles CIS reflejan el conocimiento combinado de expertos de cada parte del ecosistema (compañías, gobiernos, individuos), de cada perfil (analistas de amenazas, tecnólogos, tecnología de la información (TI), operadores y defensores, buscadores de vulnerabilidades, creadores de herramientas, proveedores de soluciones, usuarios, redactores de políticas, auditores, etc.), y a través de varios sectores (gobierno, energético, defensa, finanzas, transporte, universidades, consultor, seguridad, TI, etc.), quienes se han unido para crear, adoptar y respaldar los Controles CIS.

Evolución de los Controles CIS

Los Controles CIS iniciaron como muchas actividades similares – reunimos a expertos, discutimos y compartimos hasta ponernos de acuerdo. Esto puede ser muy valioso, dependiendo de las personas de la mesa y su experiencia. A través de la documentación y compartiéndola, las empresas pueden beneficiarse del trabajo de las personas que estas no podrían contratar o ni siquiera conocer. Puedes mejorar el resultado (y su confianza en él) a través de la selección de una amplia gama de conocimientos, aportar coherencia al proceso y garantizar el uso de la mejor información posible (particularmente sobre ataques). Al final, depende del buen juicio de un grupo relativamente pequeño de personas, redactado de una manera informal y narrativa.

En CIS, hemos recorrido un camino de varios años para traer más datos, rigor y transparencia al proceso de recomendaciones de mejores prácticas (Los CIS Benchmarks™ y los CIS Controls). Todos estos elementos son esenciales para la maduración de una ciencia que subyace a la defensa cibernética, y todos los necesario para permitir la “adaptación” y “negociación” de las acciones de seguridad aplicables en cada caso específico, y según sea necesario a través de marcos de seguridad específicos, regulaciones y esquemas de supervisión similares.

En las primeras versiones de los Controles CIS, utilizamos una lista de ataques públicamente conocidos como una prueba simple e informal utilizadas como recomendaciones específicas. A partir del 2013, trabajamos con el equipo de Verizon Data Breach Investigations Report (DBIR) para mapear los resultados de sus análisis de datos a gran escala directamente a los

Controles CIS, como una manera de equiparar sus resúmenes de ataques en un programa estándar de mejora defensiva.

CIS ha lanzado recientemente el Modelo de Defensa Comunitaria (CDM), es nuestro enfoque más orientado hacia los datos hasta el momento. En su versión inicial, el CDM analiza las conclusiones más recientes del DBIR de Verizon, junto con los datos del Multi-State Information Sharing And Analysis Center® (MS-ISAC®), para identificar cuáles creemos que son los cinco tipos de ataques más importantes. Describiremos esos ataques utilizando el marco MITRE Adversarial Tactics, Techniques y Common Knowledge® (MITRE ATT&CK®) para crear patrones de ataque (o combinaciones específicas de Tácticas y Técnicas utilizadas en esos ataques).

Esto nos permite analizar individualmente el valor de acciones defensivas (es decir. Salvaguardas¹) contra esos ataques. Específicamente, nos proporciona una manera consistente y explicable de ver el valor de seguridad de un conjunto de acciones defensivas sobre el ciclo de vida de un ataque, y proporciona una base de estrategia para defensa en profundidad. Los detalles de este análisis se encuentran disponibles en el sitio web de CIS. La conclusión es que hemos dado un paso importante hacia la identificación del valor de seguridad de los controles CIS, o cualquier subconjunto de ellos. Si bien estas ideas aún siguen evolucionando, CIS estamos comprometidos con la idea de recomendaciones de seguridad basadas en datos, presentadas de manera transparente. Para obtener información adicional consulte <https://www.cisecurity.org/controls/v8/>.

Estas actividades garantizan que las Mejores Prácticas de Seguridad de CIS (que incluyen los controles CIS y los puntos de referencia CIS) son más que una lista de verificación de “cosas buenas que hacer” y “cosas que podrían ayudar”; en cambio, son un conjunto de acciones prescriptivas, priorizadas y altamente enfocadas que tienen una red de apoyo comunitario para hacerlas implementables, utilizables, escalables y alineadas con todos los requisitos de seguridad gubernamentales o de la industria.

Esta Versión de los Controles CIS

Cuando comenzamos el trabajo de una nueva versión, primero nos sentamos a establecer los “principios de diseño” que se utilizará para guiar el proceso. Estos sirven como un “Punto de referencia” para recordarnos lo que es realmente importante y los objetivos de los Controles CIS. Si bien estas han sido bastante consistentes desde las primeras versiones de los Controles CIS, hemos refinado nuestro pensamiento sobre las últimas versiones para enfocarnos en el papel que juegan los controles CIS en la imagen total de la seguridad empresarial.

Nuestros principios de diseño incluyen: va

- **Ofensiva Informa a la Defensa**
 - Los Controles CIS se seleccionan, descartan y priorizan en función de los datos, y del conocimiento específico del comportamiento del atacante y cómo detenerlo
- **Objetivo**
 - Ayudar a los defensores a identificar los puntos más críticos que deben hacer para detener los ataques más importantes
 - **Evite sentirse tentado a resolver todos los problemas de seguridad:** evite agregar “cosas buenas que hacer” o “cosas que podría hacer”
- **Factibilidad**
 - Todas las recomendaciones individuales (Salvaguardas) deben ser específicas y prácticas de implementar

¹ “Las Salvaguardas” las conocíamos como “Sub-Controles” antes de la Version 8 de los Controles CIS.

- Métricas
 - Todos los Controles CIS, especialmente para el Grupo de Implementación 1, deben ser medibles
 - Reduzca o elimine el lenguaje ambiguo para evitar una interpretación inconsistente
 - Algunas Salvaguardas pueden tener un límite
- Adaptado
 - Crear y demostrar una “coexistencia pacífica” con otros esquemas, marcos y estructuras de gobernanza, regulación, gestión de procesos, marco y estructuras
 - Cooperar y señalar las normas y recomendaciones de seguridad existentes e independiente cuando existen, por ejemplo, el Instituto Nacional de Normas y Tecnología® (NIST), Alianza de Seguridad Cloud (CSA), Foro de Aseguramiento de Software para la Excelencia en Código (SAFECode), ATT&CK, Proyecto de Seguridad para Aplicaciones Web Open Source® (OWASP)

Además, desde la Versión 7, todos hemos visto cambios significativos en la tecnología y el ecosistema de ciberseguridad. La tendencia hacia la computación basada en la nube, la virtualización, la movilidad, la subcontratación, el trabajo desde el hogar y las tácticas cambiantes de los atacantes han sido fundamentales en cada discusión. Los dispositivos físicos, los límites fijos y las islas discretas de implementación de seguridad son menos importantes, por lo que reflejamos, que contrastamos eso en la Versión 8, a través de términos verificados y con la agrupación de Salvaguardas. Además, de ayudar a los usuarios en la implementación de la Versión 8, los Controles, CIS creó un glosario para eliminar la ambigüedad de la terminología. Algunas ideas han sido combinadas o agrupadas de manera diferente para reflejar de una forma más natural la evolución de la tecnología, en lugar de como se podrían organizar los equipos o responsabilidades empresariales, referenciando siempre a nuestros principios rectores.

El documento de los Controles CIS es solo un paso de un proceso que incluye el diseñar, implementar, medir, informar y administrar la seguridad empresarial. Teniendo en cuenta este flujo de trabajo mientras redactamos los Controles CIS, podemos abarcar el proceso total de gestión empresarial mediante: asegurarnos de que cada Salvaguarda pida “una cosa”, siempre que sea posible, de manera clara y que requiera una mínima interpretación; enfocándose en acciones medibles, y definimos la medición como parte del proceso; y, que simplificamos el lenguaje para evitar duplicaciones.

En CIS, siempre hemos tratado de ser bastante consientes del equilibrio entre abordar temas actuales y la estabilidad de un programa general de mejora defensiva. Siempre hemos tratado de enfocarnos en los cimientos de una buena defensa cibernética y siempre hemos tratado de mantener la vista en las nuevas tecnologías defensivas emergentes, mientras evitamos los “juguetes nuevos resplandecientes” o la tecnología compleja que se encuentra fuera del alcance de la mayoría de las empresas.

El Ecosistema de los Controles CIS (“No se trata de un listado”)

Ya sea que utilice los Controles CIS u otra guía para su programa de seguridad, debe reconocer que “no se trata de un listado”. Usted puede obtener una lista de controles aceptable de recomendaciones de seguridad de muchas fuentes; es mejor pensar en la lista como un punto de partida. Es importante buscar un ecosistema que crezca en torno a la lista. ¿Dónde podría recibir capacitación, información complementaria, explicaciones? ¿Cómo otros han implementado y utilizado estas recomendaciones; hay algún mercado de herramientas y servicios de proveedores para elegir? ¿Cómo podría medir el progreso o la madurez? ¿Cómo se alinea esto contra la multitud de otros marcos regulatorios y de cumplimiento que se aplican a mí? El verdadero poder de los Controles CIS no se trata de crear la mejor lista de controles, se trata de aprovechar la experiencia de la comunidad de individuos y empresas para hacer mejoras de seguridad a través del intercambio de ideas, herramientas, lecciones y acción colectiva.

Para respaldar todo eso, CIS actúa como catalizador y centro de nivelación para ayudar a todos a aprender unos de otros. Desde la Versión 6, ha habido una explosión de información complementaria, productos y servicios disponibles de CIS, y de la industria en general. Póngase en contacto con el CIS para obtener los siguientes tipos de ayudas para el trabajo y otros materiales de apoyo, <https://www.cisecurity.org/controls/v8/>:

- Mapear los Controles CIS a una amplia variedad de marcos formales de gestión de riesgos (como NIST®, Ley Federal de Modernización de la Seguridad de la Información (FISMA), Organización Internacional de Estándares (ISO), etc.)
- Casos de uso de adopción empresarial
- Una lista de continuas referencias a los Controles CIS en estándares nacionales e internacionales, legislación y regulación estatal y nacional, comercio y asociación profesional, etc.
- Información adaptada a las pequeñas y medianas empresas
- Medición y métricas para los Controles CIS
- Sugerencias para documentos técnicos de los proveedores y otros materiales que respaldan los Controles CIS
- Documentación alineada con el NIST® Marco de Ciberseguridad

Cómo empezar



Históricamente, los controles CIS fueron organizados en secuencia para enfocar actividades de ciberseguridad de una empresa, como un subconjunto de los primeros seis Controles CIS denominados “Higiene Cibernética”. Sin embargo, esto resultó ser demasiado simplista. Las empresas, especialmente las pequeñas, podrían tener problemas con algunas de las primeras medidas de seguridad y nunca podrían llegar a implementar los Controles CIS posteriores (por ejemplo, tener una estrategia de respaldo para ayudar a recuperarse del ransomware). Como resultado, comenzando con la versión 7.1, creamos los grupos de implementación de los Controles CIS (IGs) como nuestra guía recomendada para priorizar la implementación.

Los IGs de los Controles CIS son categorías de autoevaluación para las empresas. Cada IG identifica un subconjunto de Controles CIS que la comunidad ha evaluado ampliamente como aplicable a una empresa con un perfil de riesgo y recursos similares para esmerarse por implementar estos. IGs representan una mirada horizontal a través de los Controles CIS adaptados a diferentes tipos de empresas. Específicamente, hemos definido IG1 como “Ciber Higiene Básico” El conjunto fundamental de Salvaguardas de ciberdefensa que toda empresa debe aplicar para protegerse contra los ataques más comunes (<https://www.cisecurity.org/controls/v8/>). Cada IG se basa en el anterior: IG2 incluye a IG1, e IG3 incluye todas las Salvaguardas CIS en IG1 e IG2.

Adopción o transición de versiones anteriores de los Controles CIS

Creemos que la versión 8 de los Controles CIS es la mejor que hemos producido. También apreciamos que las empresas utilizan activamente versiones anteriores de los Controles CIS como parte clave de su estrategia defensiva podrían ser reacias a pasar a la Versión 8. Nuestra recomendación es si está utilizando la Versión 7 o la Versión 7.1, usted siguiendo un plan de seguridad eficaz y usable, y con el tiempo debe considerar pasar a la Versión 8. Si usted está utilizando la Versión 6 (anterior), nuestra recomendación es que usted debería empezar a planear la transición a la Versión 8 tan pronto como le sea posible.

Para las versiones anteriores de los Controles CIS, pudimos proporcionar sólo las herramientas más sencillas para ayudar en la transición de versiones anteriores, básicamente a un registro de cambios en una hoja de cálculo. Para la Versión 8, hemos adoptado un enfoque mucho más holístico y hemos trabajado con numerosos socios para garantizar que el ecosistema de Controles CIS esté listo para apoyar su transición, <https://www.cisecurity.org/controls/v8/>.

Estructura de los Controles CIS

La presentación de cada Control en este documento incluye los siguientes elementos:

- **Resumen:** Una breve descripción de la intención del Control y su utilidad como acción defensiva
- **¿Por qué es Crítico este Control?** Una descripción de la importancia del Control en el bloqueo, mitigación o identificación de ataques, y la explicación de cómo los atacantes activamente explotan la ausencia de este control
- **Procedimientos y Herramientas:** Una descripción técnica de los procesos y tecnologías disponibles y automatización para este Control
- **Salvaguardas:** Un listado de acciones específicas que las empresas deben tomar para implementar el Control

Perfiles



IG1

Una empresa IG1 es de tamaño pequeña a mediana con experiencia limitada en TI y ciberseguridad para dedicarse a proteger los activos y personal de TI. La principal preocupación de estas empresas es mantener el negocio operativo, ya que tienen una tolerancia limitada de inactividad. La sensibilidad de la información que ellas tratan de proteger es baja y principalmente incluye información de empleados e información financiera.

Las Salvaguardas seleccionadas para IG1 deberían ser implementables con limitada experiencia en ciberseguridad y estar dirigidas a frustrar ataques generales y no dirigidos. Estas Salvaguardas normalmente se diseñan para trabajar en conjunto con software y hardware que ya existe y se encuentra disponible de fuentes comerciales (COTS).



IG2 (Incluye IG1)

Una empresa IG2 emplea a individuos responsables de administrar y proteger la infraestructura de TI. Estas empresas se apoyan de múltiples departamentos con distintos perfiles de riesgo en base a la función del puesto y misión. Las empresas IG2 almacenan procesos e información sensible sobre el cliente o información empresarial y pueden soportar breves interrupciones de servicios. La mayor preocupación es la pérdida de la confianza del público si se produce una brecha.

Las Salvaguardas seleccionadas para IG2 ayudan a los equipos de seguridad a hacer frente al incremento de la complejidad operacional. Algunas Salvaguardas están sujetas al grado de tecnología y nivel empresarial, experiencia especializada para ser instaladas y configuradas correctamente.



IG3 (Incluye IG1 y IG2)

Una empresa IG3 emplea expertos en seguridad los cuales se especializan en diferentes facetas de la ciberseguridad (por ejemplo, gestión de riesgo, pruebas de penetración, seguridad en las aplicaciones). Los activos e información IG3 contienen información sensible o funciones que están sujetas a supervisión regulatoria y de cumplimiento. Una empresa IG3 debe abordar la disponibilidad y la confidencialidad e integridad de los datos sensibles. La materialización de los ataques puede causar un daño significativo al bienestar público.

Las Salvaguardas seleccionadas para IG3 deben reducir los ataques dirigidos por un adversario sofisticado y reducir el impacto de los ataques de día cero.

Inventario y Control de los Activos Empresariales

SALVAGUARDAS

5

IG1

2/5

IG2

4/5

IG3

5/5

RESUMEN

Gestione activamente (inventario, seguimiento y corrección) todos los activos de la empresa (dispositivos de usuarios finales, incluidos equipos portátiles y teléfonos móviles; dispositivos de red; Dispositivos no informáticos/Internet de las Cosas (IoT); y servidores) conectados a la infraestructura física, virtualmente, remotamente, y aquellos del ambiente de la nube, para conocer con precisión la totalidad de los activos que necesitan ser monitoreados y protegidos dentro de la empresa. Esto también apoyará la identificación de activos no autorizados y no administrados para eliminar o remediar.

¿Por qué es Crítico este Control?

Las empresas no pueden defender aquello que no saben que tienen. El control administrado de todos los activos de la empresa también desempeña un papel crítico en el monitoreo de la seguridad, respuesta a incidentes, el respaldo de sus sistemas y recuperación. Las empresas deben saber que los datos son críticos para sí mismas, la administración adecuada ayudará a identificar aquellos activos empresariales que contienen o administran estos activos críticos, de modo que se puedan aplicar los controles de seguridad adecuados.

Los atacantes externos escanean continuamente el espacio de direcciones de internet de las empresas objetivo, ya sea en las instalaciones o en la nube, identificando activos posiblemente desprotegidos conectados a la red de una empresa. Los atacantes pueden aprovechar los nuevos activos que están instalados, pero aún no parcheados y configurados de forma segura. Internamente, los activos no identificados también pueden tener configuraciones de seguridad débiles que pueden hacerlos vulnerables al malware basado en la web o el correo electrónico; y los adversarios pueden aprovechar las configuraciones de seguridad débiles para atravesar la red, una vez que están dentro.

Activos adicionales conectados a la red empresarial (por ejemplo, sistemas de demostración, sistemas de prueba temporales, redes de invitados) deben ser identificados y/o aislados para evitar el acceso de adversarios que puedan afectar la seguridad de las operaciones de la empresa.

Las empresas grandes, complejas y dinámicas, comprensiblemente luchan contra los desafíos de administrar entornos intrincados y cambiantes. Sin embargo, los atacantes han demostrado que tienen la habilidad, paciencia, y la voluntad de "Inventariar y Controlar" los activos de nuestra empresa a gran escala para apoyar sus oportunidades.

Otro desafío es que los dispositivos portátiles de un usuario final que periódicamente se unen a la red y luego desaparecen, haciendo que el inventario de activos disponible sea muy dinámico. Del mismo modo, los entornos de nube y máquinas virtuales pueden ser difíciles de rastrear en los inventarios cuando se apagan o interrumpen.

Otro beneficio de una gestión completa de los activos empresariales es el apoyo en la respuesta a incidentes, tanto cuando se investiga el origen del tráfico de una red de un activo en la red como cuando se identifican todos los activos potencialmente vulnerables, o impactados, de tipo o ubicación similar durante un incidente.

Procedimientos y Herramientas

Estos Controles CIS requieren acciones técnicas y procedimentales, unidas a un proceso que registre, y gestione el inventario de activos de la empresa y todos los datos asociados de su ciclo de vida. También se enlaza a la gobernanza empresarial a través del establecimiento de propietario de datos/activos que son responsables de cada componente de un proceso de la empresa. Las empresas pueden utilizar productos integrales empresariales de gran escala para mantener los inventarios de TI. Las empresas más pequeñas pueden aprovechar herramientas de seguridad ya instaladas en los activos empresariales o utilizadas en la red para recopilar estos datos. Esto incluye tareas de escaneo de descubrimiento en la red con un escáner de vulnerabilidades; revisar registros de anti malware, revisar registros de clientes de las soluciones de seguridad, registros de red de switches, o registros de autenticación, y la gestión de resultados una planilla o bases de datos.

Mantener una visión actual y precisa de los activos de la empresa es un proceso dinámico. Incluso para empresas, raramente existe una única fuente fiable. La realidad es que hay una variedad de fuentes que necesitan ser “Múltiples fuentes” para determinar un recuento de alta confianza de los activos de la empresa. Las empresas pueden escanear activamente de forma regular, enviando una variedad de diferentes tipos de paquetes para identificar los activos conectados a la red. Además de las fuentes de activos mencionados anteriormente para las pequeñas empresas, las empresas más grandes pueden recopilar datos de portales en la nube y registros de plataformas como: Directorio Activo (AD), Inicio de sesión único (SSO), Múltiple Factor de Autenticación (MFA), Redes Privadas Virtuales (VPN), Sistemas de Detección de Intrusos (IDS) o Inspección Profunda de Paquetes (DPI), Administración de Dispositivos Móviles (MDM), y escáneres de vulnerabilidades. Las bases de datos de propiedades, el seguimiento de pedidos de compras y listas de inventario local son otras fuentes de datos para determinar otras fuentes de datos para determinar qué dispositivos están conectados. Existen herramientas y métodos para normalizar estos datos para identificar dispositivos únicos entre estas fuentes.

- ➔ Para obtener orientación específica sobre la nube, consulte la Guía complementaria de la nube de los Controles CIS: <https://www.cisecurity.org/controls/v8/>
- ➔ Para obtener orientación para tabletas y teléfonos inteligentes, consulte la guía complementaria de los Controles CIS: <https://www.cisecurity.org/controls/v8/>
- ➔ Para obtener orientación sobre IoT, consulte la Guía complementaria de los Controles CIS de Internet de las Cosas: <https://www.cisecurity.org/controls/v8/>
- ➔ Para obtener una orientación sobre sistemas de control industrial (ICS), consulte la Guía de implementación de ICS de Controles CIS: <https://www.cisecurity.org/controls/v8/>

Salvaguardas

SALVAGUARDA	TÍTULO DE SALVAGUARDA/ DESCRIPCIÓN DE SALVAGUARDA	TIPO DE ACTIVO	FUNCIÓN DE SEGURIDAD	IG1	IG2	IG3
1.1	Establecer y Mantener un Detallado Inventario de Activos Empresariales Establecer y mantener un inventario preciso, detallado y actualizado de todos los activos de la empresa con el potencial de almacenar o procesar datos, para incluir: dispositivos de usuarios finales (incluidos portátiles y móviles), dispositivos de red, no informáticos IoT y servidores. Asegúrese de que el inventario registre la dirección de red (si es estática), la dirección de la máquina, el propietario del activo de datos, el departamento de cada activo y si el activo ha sido aprobado para conectarse a la red. Para los dispositivos móviles de usuario final, las herramientas tipo MDM pueden admitir este proceso, cuando corresponda. Este inventario incluye activos conectados a la infraestructura física, virtual, remotamente y aquellos de entornos de la nube. Adicionalmente, incluye activos que están conectados regularmente a la infraestructura de red de la empresa, incluso si no están bajo el control de la empresa. Revisar y actualizar el inventario de todos los activos de la empresa cada dos años o con mayor frecuencia.	Dispositivos	Identificar			
1.2	Gestionar Activos no Autorizados Asegúrese de que exista un proceso para abordar los activos no autorizados semanalmente. La empresa puede optar por eliminar el activo de la red, negar que el activo se conecte de forma remota a la red o poner en cuarentena el activo.	Dispositivos	Responder			

SALVAGUARDA	TÍTULO DE SALVAGUARDA/ DESCRIPCIÓN DE SALVAGUARDA	TIPO DE ACTIVO	FUNCIÓN DE SEGURIDAD	IG1	IG2	IG3
1.3	Utilice una herramienta de descubrimiento activo Utilice una herramienta de descubrimiento activa para identificar activos conectados a la red empresarial. Configure la herramienta de descubrimiento activo para ejecutar diariamente o con más frecuencia.	Dispositivos	<div> <div>Detectar</div> </div>			
1.4	Utilice el registro de la configuración de dinámica de host (DHCP) para actualizar el inventario de activos Utilice el registro DHCP en todos los servidores o las herramientas de administración de direcciones de protocolo de internet (IP) para actualizar el inventario de activos de la empresa. Revise y use los registros para actualizar semanalmente el inventario de activos de la empresa o con mayor frecuencia.	Dispositivos	<div> <div>Identificar</div> </div>			
1.5	Utilice una herramienta de descubrimiento de activos pasivo Utilice una herramienta de descubrimiento pasivo para identificar activos conectados a la red empresarial. Revise y utilice escaneos para actualizar el inventario de activos de la empresa al menos semanalmente o con más frecuencia.	Dispositivos	<div> <div>Detectar</div> </div>			

RESUMEN

Gestione activamente (inventario, seguimiento y corrección) todo el software (sistemas operativos y aplicaciones) dentro de la red. Únicamente el software autorizado debe ser instalado y ejecutado, y aquellos software no autorizados ni gestionados que se encuentren se impida la instalación y/o ejecución.

¿Por qué es Crítico este Control?

Un inventario de software completo es una base fundamental para prevenir ataques. Los atacantes escanean continuamente las empresas en busca de versiones vulnerables de software que puedan explotarse de forma remota. Por ejemplo, si un usuario abre un sitio malicioso o un adjunto a través de un navegador vulnerable, un atacante podría instalar un programa de puerta trasera. Los atacantes podrían utilizar este acceso para realizar movimiento lateral por la red. Una de las claves para defenderse de los atacantes es mantener actualizado y parcheado el software. Sin embargo, sin un inventario completo de activos de software, una empresa podría determinar si posee algún software vulnerable o si existen posibles infracciones de licencias.

Incluso si un parche aún no está disponible, una lista completa de inventario de software permite a la empresa protegerse contra ataques conocidos hasta que se publique el parche. Algunos atacantes sofisticados utilizan “exploits de día cero”, que se aprovechan de vulnerabilidades previamente desconocidas que aún no han recibido un parche del fabricante del software. Dependiendo de la gravedad del exploit, una empresa puede implementar medidas de mitigación temporales para protegerse contra ataques hasta que se libere el parche.

La gestión de los activos de software también es importante para identificar riesgos de seguridad innecesarios. Una empresa debe verificar su inventario de software para identificar cualquier activo que se encuentre ejecutando software que no sea necesario para el propósito de la empresa. Supongamos, que un activo de la empresa venga instalado con un software predeterminado que crea un riesgo de seguridad potencial esto no proporciona ningún beneficio para la empresa. Es fundamental inventariar, comprender, evaluar y administrar todo el software conectado a la infraestructura de la empresa.

Procedimientos y Herramientas

Implemente una lista de software permitido mediante una combinación de herramientas comerciales permitidas, políticas o herramientas de ejecución de aplicaciones que vienen embebidos en las suites anti-malware y sistemas operativos populares. Las herramientas de inventario de software comercial están ampliamente disponibles y se utilizan en muchas empresas de la actualidad. La mejor de esas herramientas proporciona una verificación de inventario de varios cientos de software de uso general en las empresas. Estas herramientas extraen la información sobre el nivel de parche de cada programa instalado para asegurarse de que sea la última versión y emplean el nombre de las aplicaciones de forma estandarizada, como los que se encuentran en la enumeración de plataforma común (CPE). Un ejemplo de un método que podría ser utilizado es el Protocolo de Automatización de Contenido de Seguridad (SCAP). Información adicional sobre SCAP se puede encontrar aquí:

→ <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-126r3.pdf>

Características sobre la implementación de listas permitidas se incluyen en muchas suites modernas de seguridad e incluso de forma nativa en ciertas versiones de los principales sistemas operativos. Además, las soluciones comerciales están incrementando la agrupación de anti-malware, anti-spyware, firewall individual, y IDS basado en equipo e IPS, junto a listas de permitir o bloquear aplicaciones. En particular, la mayoría de las soluciones de seguridad para equipos pueden observar el nombre, la ubicación del sistema de archivos y/o el hash criptográfico de un ejecutable particular para determinar si se debe permitir que la aplicación se ejecute en la máquina protegida. Las más efectivas de estas herramientas ofrecen listas de aplicaciones permitidas personalizables basadas en rutas ejecutables, hash o coincidencia de expresiones regulares. Algunas inclusive incorporan funciones de aplicaciones no maliciosas, pero no aprobadas, que permite a los administrados definir reglas para la ejecución de software específico para ciertos usuarios y en ciertas horas del día.

- Para obtener orientación específica sobre la nube, consulte la **Guía complementaria de la nube de los Controles CIS**: <https://www.cisecurity.org/controls/v8/>.
- Para obtener orientación para tabletas y teléfonos inteligentes, consulte la **guía complementaria de los Controles CIS**: <https://www.cisecurity.org/controls/v8/>.
- Para obtener orientación sobre IoT, consulte la **Guía complementaria de los Controles CIS de Internet de las Cosas**: <https://www.cisecurity.org/controls/v8/>.
- Para obtener una orientación sobre sistemas de control industrial (ICS), consulte la **Guía de implementación de ICS de Controles CIS**: <https://www.cisecurity.org/controls/v8/>.

Salvaguardas

SALVAGUARDA	TÍTULO DE SALVAGUARDA/ DESCRIPCIÓN DE SALVAGUARDA	TIPO DE ACTIVO	FUNCIÓN DE SEGURIDAD	IG1	IG2	IG3
2.1	Elaborar y Mantener actualizado el inventario de software Elabore y mantenga un inventario detallado de todas las licencias de software instalados en los activos de la empresa. El inventario de software debe documentar el título, el fabricante, la fecha de instalación inicial y el propósito para cada activo, cuando corresponda, incluya la dirección URL, las tiendas de aplicaciones, versiones, mecanismo de implementación y fecha de retirada.	Aplicaciones	Identificar	●	●	●
2.2	Asegurarse de que el software autorizado cuente con soporte Asegúrese de que únicamente el software con soporte actual del fabricante esté designado como autorizado en el inventario de software de activos empresariales. Si el software ya no se encuentra soportado por el fabricante, pero es necesario para el cumplimiento de la misión de la empresa, documente una excepción que detalle los controles de mitigación y la aceptación del riesgo residual. Para cualquier software sin soporte, sin una documentación de excepción, identificarla como no autorizada. Revise la lista de software para comprobar el soporte del software por lo menos una vez al mes o con más frecuencia.	Aplicaciones	Identificar	●	●	●
2.3	Tratamiento del Software no Autorizado Asegúrese de que el software no autorizado sea removido de los activos de la empresa o ante evidencias de instalaciones no autorizadas el evento cuente con una excepción documentada. Realice este paso mensualmente o con más frecuencia.	Aplicaciones	Responder	●	●	●
2.4	Utilice herramientas automatizadas de inventario de software Utilizar herramientas de inventario de software, cuando sea posible, en toda la empresa para automatizar la detección y documentación del software instalado.	Aplicaciones	Detectar		●	●
2.5	Use Lista de permitidos Para Software Autorizados Utilice controles técnicos, como lista de aplicaciones permitidas, para asegurarse de que solo se pueda ejecutar o acceder al software autorizado. Reevaluar semestralmente o con más frecuencia.	Aplicaciones	Proteger		●	●
2.6	Lista de Librerías Autorizadas Utilice controles técnicos para garantizar que solo las bibliotecas de software actual. Bloquee la carga de bibliotecas no autorizadas en los procesos del sistema. Reevalúe semestralmente o con más frecuencia.	Aplicaciones	Proteger		●	●
2.7	Use Lista de permitidos Para secuencias de comandos Autorizados Utilice controles técnicos, como firmas digitales y control de versiones, para asegurarse de que los scripts autorizados, específicos como los .ps1, .py, etc., archivos, estén permitidos para ejecutarse. Bloquear los scripts no autorizados para ejecutarse. Reevalúe semestralmente o con más frecuencia.	Aplicaciones	Proteger			●

RESUMEN

Desarrollar procesos y controles técnicos para identificar, clasificar, manejar, retener y eliminar de forma segura los datos.

¿Por qué es Crítico este Control?

Los datos ya no se encuentran únicamente dentro de las empresas, están en la nube, en dispositivos portátiles de usuarios finales donde los usuarios trabajan desde casa, y frecuentemente se comparte con socios o servicios en línea que pueden tenerlo en cualquier parte del mundo. Además de los datos sensibles que una empresa posee que se encuentran relacionados con las finanzas, la propiedad intelectual y los datos de los clientes, también puede haber numerosas regulaciones internacionales para la protección de datos personales. La privacidad de los datos se ha vuelto cada vez más importante y las empresas están aprendiendo que la privacidad se trata del uso y la gestión adecuada de los datos, no solo del cifrado. Los datos deben ser manipulados adecuadamente durante todo su ciclo de vida. Estas reglas de privacidad pueden ser complicadas para empresas multinacionales de cualquier tamaño; sin embargo, hay fundamentos que pueden aplicarse a todos.

Una vez que los atacantes han penetrado en la infraestructura de una empresa, una de las primeras tareas es encontrar y exfiltrar datos. Es posible que las empresas no se den cuenta de que los datos confidenciales abandonan su entorno porque no están supervisando las salidas de datos.

Mientras muchos ataques ocurren en la red, otros involucran el robo físico de dispositivos portátiles de los usuarios finales, ataques a proveedores de servicios u otros socios que tienen datos confidenciales. Otros activos empresariales sensibles también pueden incluir dispositivos no informáticos que proporcionan administración y control de sistemas físicos, como sistemas Supervisión, Control y Adquisición de datos (SCADA).

La pérdida de control de la empresa sobre los datos confidenciales o protegidos genera un impacto comercial grave, y a menudo notificable. Si bien algunos datos se ven comprometidos o se pierden como resultado de robo o espionaje, la gran mayoría son el resultado de reglas de administración de datos mal entendidas y errores de los usuarios. La adopción del cifrado de datos, tanto en tránsito como en reposo, puede proporcionar una mitigación contra el compromiso de los datos, y lo que es más importante es un requisito reglamentario para la mayoría de los datos controlados.

Procedimientos y Herramientas

Es importante que una empresa desarrolle un proceso de administración de datos que incluya un marco de administración de datos, pautas de clasificación de datos y requisitos para la protección, manejo, retención y eliminación de datos. También debe haber un proceso de violación de datos que se incluya al plan de respuesta a incidentes y a los planes de cumplimiento y comunicación. Para obtener niveles de sensibilidad de los datos, las empresas deben catalogar sus tipos de datos clave y la criticidad general (impacto de su pérdida o compromiso) para la empresa. Este análisis debe ser utilizado para crear un esquema general de clasificación de datos para la empresa. Las empresas deben utilizar etiquetas, como "Sensible", "Confidencial" y "Público" y clasificar sus datos de acuerdo a esas etiquetas.

Una vez definida la sensibilidad de los datos, se debe desarrollar un inventario o mapeo de datos que identifique el software que accede a los datos en varios niveles de sensibilidad y los activos de la empresa que albergan esas aplicaciones. Idealmente, la red debería estar separada de modo que los activos empresariales del mismo nivel de sensibilidad se encuentren en la misma red y separados de los activos empresariales con diferentes niveles de sensibilidad. Si es posible, los firewalls deben controlar el acceso a cada segmento de red, y tener reglas de acceso aplicadas a los usuarios para permitir que solo aquellos con una necesidad empresarial accedan a los datos.

Para un mejor entendimiento de este tema, sugerimos los siguientes recursos para ayudar a la empresa con la protección de los datos:

- **NIST® SP 800-88r1 Guides for Media Sanitization:** <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf>
- **NIST® FIPS 140-2:** <https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.140-2.pdf>
- **NIST® FIPS 140-3:** <https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.140-3.pdf>
- **Para obtener guías específicas sobre la guía para el entorno de la nube, consulte la guía complementaria de la nube de los Controles CIS:** <https://www.cisecurity.org/controls/v8/>.
- **Para obtener orientación para tabletas y teléfonos inteligentes, consulte la guía complementaria de los Controles CIS:** <https://www.cisecurity.org/controls/v8/>.

Salvaguardas

SALVAGUARDA	TÍTULO DE SALVAGUARDA/ DESCRIPCIÓN DE SALVAGUARDA	TIPO DE ACTIVO	FUNCIÓN DE SEGURIDAD	IG1	IG2	IG3
3.1	Establecer y mantener un proceso de gestión de datos Establecer y mantener un proceso de gestión de datos. Durante el proceso, Ubicación de los datos sensibles, propietario de los datos, Tratamiento de los datos, límites de la retención de datos, y requisitos de eliminación, basados en la sensibilidad y estándares de retención para la empresa. Revise y actualice la documentación anualmente, o cuando ocurran cambios significativos en la empresa que pudieran impactar en esta salvaguarda.	Datos	Identificar	●	●	●
3.2	Establecer y Mantener un inventario de Datos Establecer y mantener un inventario de datos, basados en el proceso de gestión de datos de la empresa. Inventario de datos sensibles, como mínimo. Revise y actualice el inventario anualmente, como mínimo, con prioridad sobre los datos sensibles.	Datos	Identificar	●	●	●
3.3	Configure listas de control de acceso a datos Configurar listas de control de acceso a datos en función de la necesidad de conocimiento de un usuario. Aplicar listas de control de acceso a datos, también conocidas como permisos de acceso, a sistemas de archivos, bases de datos y aplicaciones locales y remotas.	Datos	Proteger	●	●	●
3.4	Aplicar retención de datos Retener los datos de acuerdo con el proceso de gestión de datos de la empresa. La retención de datos debe incluir plazos mínimos y máximos.	Datos	Proteger	●	●	●
3.5	Eliminar de forma segura los datos Elimine de forma segura como se describe en el proceso de gestión de datos empresariales. Asegúrese de que el proceso y el método de eliminación sean acordes con la confidencialidad de los datos.	Datos	Proteger	●	●	●
3.6	Cifrar datos en dispositivos de usuarios Encriptar los datos en los dispositivos de los usuarios que contienen datos sensibles. Un ejemplo de implementación puede incluir: Windows BitLocker®, Apple FileVault®, Linux® dm-crypt.	Dispositivos	Proteger	●	●	●
3.7	Establecer y mantener un esquema de clasificación de datos Establecer y mantener un esquema general de clasificación de datos para la empresa. En las empresas pueden usar etiquetas, como "sensible," "Confidencial," y "Público," y clasificar sus datos de acuerdo a esas etiquetas. Revise y actualice el esquema de clasificación anualmente, o cuando suceda algún cambio significativo en la empresa que pueda tener impacto sobre esta Salvaguarda.	Datos	Identificar		●	●
3.8	Documentar el Flujo de datos Documente el flujo de datos. La documentación del flujo de datos incluye los flujos de datos del proveedor de servicios y debe basarse en el proceso de gestión de datos de la empresa. Revise y actualice la documentación anualmente, o cuando ocurran cambios significativos en la empresa que puedan impactar esta Salvaguarda.	Datos	Identificar		●	●

SALVAGUARDA	TÍTULO DE SALVAGUARDA/ DESCRIPCIÓN DE SALVAGUARDA	TIPO DE ACTIVO	FUNCIÓN DE SEGURIDAD	IG1	IG2	IG3
3.9	Cifrar datos en medios extraíbles Cifre los datos en los dispositivos extraíbles.	Datos	Proteger			
3.10	Cifre los datos confidenciales en tránsito Cifre los datos confidenciales en tránsito. Ejemplos de implementación incluyen: Transport Layer Security (TLS) y Open Secure Shell (OpenSSH).	Datos	Proteger			
3.11	Cifrar los datos confidenciales en reposo Cifre los datos confidenciales que se encuentran en reposo en servidores, aplicaciones y bases de datos que contengan datos confidenciales. El cifrado de la capa de almacenamiento, también conocido como cifrado del lado del servidor, cumple con el requisito mínimo de esta Salvaguardia. Métodos de cifrado adicionales pueden incluir el cifrado del lado del cliente, también conocido como cifrado del lado del cliente, donde el acceso a los dispositivos de almacenamiento de datos no permite el acceso a los datos de texto sin formato.	Datos	Proteger			
3.12	Segmentar el procesamiento y almacenamiento de datos en función de la sensibilidad Segmentar el procesamiento y almacenamiento de datos en función de la sensibilidad. No procesar datos confidenciales en activos empresariales destinados a datos de menor sensibilidad.	Red	Proteger			
3.13	Desplegar una solución de Prevención de Pérdida de Datos Implemente una herramienta automatizada, como una herramienta de prevención de pérdida de datos (DLP) basada en host para identificar todos los datos confidenciales almacenados, procesados, transmitidos a través de los activos de la empresa, incluidos lo que se encuentran en el sitio o en un proveedor de servicios remoto, y actualizar el inventario de datos confidenciales de la empresa.	Datos	Proteger			
3.14	Registre de acceso a datos confidenciales Registre el acceso a los datos, incluidos modificación y eliminación.	Datos	Detectar			

Configuración Segura de Activos y Software Empresarial

SALVAGUARDAS

12

IG1

7/12

IG2

11/12

IG3

12/12

RESUMEN

Establecer y mantener la configuración segura de los activos empresariales (Dispositivos de usuarios, incluidos portátiles y móviles; dispositivos de red; dispositivos no informáticos/IoT; y servidores) y software (Sistemas operativos y aplicaciones).

¿Por qué es Crítico este Control?

Tal como se entregan desde fabricantes y revendedores, las configuraciones predeterminadas para los activos y el software de la empresa normalmente están orientadas hacia la facilidad de implementación y la facilidad de uso en lugar de la seguridad. Los controles Básicos, servicios, puertos abiertos, las cuentas o contraseñas predeterminadas, configuración del sistema de nombre de dominio (DNS) preconfigurada, los protocolos antiguos (vulnerables) y la preinstalación de software innecesario pueden ser aprovechadas si se dejan en su estado predeterminado. Además, estas actualizaciones de configuración de seguridad deben administrarse y mantenerse durante el ciclo de vida de los activos y el software de la empresa. Las actualizaciones de configuración deben ser rastreables y aprobadas a través del proceso de flujo de trabajo administración de la configuración para mantener un registro que se pueda revisar para verificar el cumplimiento, aprovecharse para la respuesta a incidentes y admitir auditorías. Este Control CIS es importante para los dispositivos locales, así como para los dispositivos remotos, los dispositivos de red y los entornos en la nube.

Los proveedores de servicios juegan un papel clave en las infraestructuras modernas, especialmente para las empresas más pequeñas. A menudo, no están configurados de forma predeterminada en la configuración más segura para brindar flexibilidad a sus clientes para que apliquen sus propias políticas de seguridad. Por lo tanto, la presencia de cuentas o contraseñas predeterminadas, acceso excesivo o servicios innecesarios son comunes en las configuraciones predeterminadas. Estos podrían introducir debilidades que están bajo la responsabilidad de la empresa que está utilizando el software, en lugar del proveedor de servicios. Esto se extiende a la administración y las actualizaciones continuas, ya que algunas plataformas como servicio (PaaS) solo se extienden al sistema operativo, por lo que la aplicación de parches y actualización de las aplicaciones alojadas están bajo la responsabilidad de la empresa.

Incluso después de que se desarrolle y aplique una configuración inicial sólida, debe administrarse continuamente para evitar la degradación de la seguridad a medida que se actualiza parchea el software, se notifican nuevas vulnerabilidades de seguridad y se "ajustan" las configuraciones para permitir la instalación de un nuevo software o para dar soporte a nuevos requisitos operativos.

Procedimientos y Herramientas

Hay muchas bases de referencia de seguridad disponibles para cada sistema. Las empresas deben comenzar con estos puntos de referencia de seguridad, guías de seguridad o listas de verificación desarrollados, examinados y respaldados públicamente. Algunos recursos incluyen:

- **The CIS Benchmarks™ Program:** <http://www.cisecurity.org/cis-benchmarks/>
- **The National Institute of Standards and Technology (NIST®) National Checklist Program Repository:** <https://nvd.nist.gov/ncp/repository>

Las empresas deben aumentar o ajustar estas bases de referencia para satisfacer las políticas de seguridad empresarial y los requisitos normativos de la industria y gobierno.

Para una empresa más grande o más compleja, habrá varias configuraciones de bases de referencia de seguridad basadas en los requisitos de seguridad o la clasificación de los datos en el activo de la empresa. A continuación, se muestra un ejemplo de los pasos para crear una imagen de referencia:

- 01 Determinar la clasificación de riesgo de los datos manejados/almacenados en el activo empresarial (por ejemplo, Alto, moderado, riesgo bajo).
- 02 Cree un script de configuración de seguridad que establezca la configuración del sistema para cumplir con los requisitos para proteger los datos utilizados en el activo empresarial. Utilice benchmarks, como los descritos anteriormente en esta sección.
- 03 Instale el software del sistema operativo base.
- 04 Aplicar apropiadamente parches de seguridad y del sistema operativo.
- 05 Instalar paquetes de software de aplicación, herramientas y utilidades adecuadas.
- 06 Aplicar las actualizaciones adecuadas al software instalado en el paso 4
- 07 Instale scripts a esta imagen local para su personalización.
- 08 Ejecute el script de seguridad creado en el Paso 2 para establecer un nivel de seguridad adecuado.
- 09 Ejecute una herramienta compatible con SCAP para registrar/puntuar la configuración del sistema de la imagen de referencia.
- 10 Realice una prueba de la garantía de la calidad de la seguridad.
- 11 Guardar esta imagen en un lugar seguro.

Herramientas de gestión de configuración comerciales y/o gratuitas, como la herramienta de evaluación de configuración CIS(CIS-CAT®) <https://learn.cisecurity.org/cis-cat-lite>, pueden ser desplegadas para medir la configuración de los sistemas operativos y aplicaciones de máquinas administradas para buscar desviaciones en las configuraciones de imagen estándar. Herramientas comerciales de gestión a veces se utilizan con una combinación de un agente instalado en cada sistema administrado, o también se realizan inspecciones en los sistemas sin agentes a través del registro remoto en cada activo de la empresa utilizando las credenciales de administrador. Además, a veces se utiliza un enfoque híbrido mediante el cual se inicia sesión remota, se despliega un agente temporal dinámico en el sistema de destino para el análisis y, a continuación, se elimina el agente.

Salvaguardas

SALVAGUARDA	TÍTULO DE SALVAGUARDA/ DESCRIPCIÓN DE SALVAGUARDA	TIPO DE ACTIVO	FUNCIÓN DE SEGURIDAD	IG1	IG2	IG3
4.1	Establecer y Mantener un Proceso de configuración seguro Establecer y mantener un proceso seguro de la configuración para los activos de la empresa (dispositivos de usuarios, incluidos portátiles y móviles; dispositivos no informáticos/IoT; and servers) y software (Sistemas operativos y aplicaciones). Revise y actualice la documentación anualmente, o cuando ocurran cambios significativos en la empresa que puedan causar un impacto a esta salvaguarda.	Aplicaciones	Proteger			
4.2	Establecer y mantener un proceso de configuración seguro para la infraestructura de red Establecer y mantener un proceso de configuración seguro para dispositivos de red. Revisar y actualizar la documentación anualmente, o cuando ocurran cambios importantes en la empresa que puedan afectar esta salvaguarda.	Red	Proteger			
4.3	Configurar el bloqueo automático de sesiones en activos empresariales Configurar el bloqueo automático de sesiones en los activos de la empresa después de un período definido de inactividad. Para los sistemas operativos de propósito general, el período no debe exceder los 15 minutos. Para dispositivos móviles de usuario final, el período no debe exceder los 2 minutos.	Usuario	Proteger			
4.4	Implementar y administrar un firewall en servidores Implemente y administre un firewall en los servidores donde sea compatible. Como ejemplo de implementación se incluyen un firewall virtual, un firewall del sistema operativo o un agente de firewall de terceros.	Dispositivos	Proteger			
4.5	Implementar y Administrar un Firewall en los dispositivos de usuario Implementar y administrar un firewall basado en host o una herramienta de filtrado de puertos en los dispositivos del usuario final, con una regla de denegación predeterminada que descarta todo el tráfico, excepto los servicios y puertos que están explícitamente permitidos.	Dispositivos	Proteger			
4.6	Gestione de forma segura los activos y el software de la empresa Gestione de forma segura los activos y el software de la empresa. Por ejemplo las implementaciones incluyen la gestión de la configuración a través de una infraestructura controlada por versiones como código y el acceso a interfaces administrativas a través de protocolos de red seguro, como Secure Shell (SSH) and Hypertext Transfer Protocol Secure (HTTPS). No utilice protocolos de administración inseguros, como Telnet (Teletype Network) y HTTP, a menos que sea operacionalmente esencial.	Red	Proteger			
4.7	Administrar cuentas predeterminadas en activos y software empresariales Administre cuentas predeterminadas en activos y software de la empresa, como root, administrador y otras cuentas de proveedores preconfiguradas. Las implementaciones de ejemplo pueden incluir: deshabilitar cuentas predeterminadas o inutilizarlas.	Usuario	Proteger			
4.8	Desinstalar o deshabilitar servicios innecesarios en activos y software empresariales Desinstale o deshabilite los servicios innecesarios en los activos y el software de la empresa, como un servicio de uso compartido de archivos, un módulo de aplicación web o una función de servicio.	Dispositivos	Proteger			
4.9	Configurar servidores DNS confiables en activos empresariales Configurar servidores DNS confiables en activos empresariales. Las implementaciones de ejemplo incluyen: configurar activos para usar servidores DNS controlados por la empresa y/o servidores DNS acreditados externamente.	Dispositivos	Proteger			
4.10	Aplicar el bloqueo automático de dispositivos en portátiles y dispositivos móviles Aplicar el bloqueo automático de dispositivos después de un umbral predeterminado de intentos de autenticación fallidos locales en dispositivos portátiles de usuario final, donde sea compatible. En el caso de las computadoras portátiles, no permite más de 20 intentos fallidos de autenticación; para tabletas y teléfonos inteligentes, no más de 10 intentos de autenticación fallidos. Las implementaciones de ejemplo incluyen Microsoft® InTune Device Lock y Apple® Intentos fallidos de mac de perfil de configuración.	Dispositivos	Responder			
4.11	Aplicar la capacidad de borrado remoto en dispositivos portátiles de usuario final Borre de forma remota los datos empresariales de los dispositivos portátiles de usuario final de propiedad de la empresa cuando se considere apropiado, como dispositivos perdidos o robados, o cuando una persona deja la empresa.	Dispositivos	Proteger			
4.12	Espacios de trabajo empresariales independientes en dispositivos móviles de usuario final Asegúrese de que se utilicen espacios de trabajo empresariales independientes en los dispositivos móviles de los usuarios finales, cuando sean compatibles. Las implementaciones de ejemplo incluyen el uso de un perfil de configuración de Apple® o un perfil de trabajo de Android™ para separar las aplicaciones y los datos empresariales de las aplicaciones y los datos personales.	Dispositivos	Proteger			

RESUMEN

Utilice procesos y herramientas para asignar y administrar la autorización de las credenciales de las cuentas de usuario, incluidas las cuentas de administrador, así como las cuentas de servicio, para los activos y el software empresarial.

¿Por qué es Crítico este Control?

Es más fácil para un actor de amenazas externo o interno obtener acceso no autorizado a los activos o datos de la empresa mediante el uso de credenciales de usuario válidas que mediante el "hacking" del entorno. Hay muchas formas de obtener acceso de forma encubierta a las cuentas de usuario, que incluyen: contraseñas débiles, cuentas que siguen siendo válidas después de que un usuario abandona la empresa, cuentas de prueba inactivas o persistentes, cuentas compartidas que no se han cambiado en meses o años, cuentas de servicio integradas en aplicaciones para scripts, un usuario que tiene la misma contraseña que el que usa para una cuenta en línea que ha sido comprometida (en un volcado de contraseña público), ingeniería social de un usuario para dar su contraseña o usar malware para capturar contraseñas o tokens en la memoria o más la red.

Las cuentas administrativas o con muchos privilegios son un objetivo particular, porque permiten a los atacantes agregar otras cuentas o realizar cambios en los activos que podrían hacerlos más vulnerables a otros ataques. Las cuentas de servicio también son confidenciales, ya que a menudo se comparten entre equipos, internos y externos a la empresa, y a veces no se conocen, solo para ser reveladas en auditorías estándar de administración de cuentas.

Por último, el registro y la supervisión de cuentas es un componente fundamental de las operaciones de seguridad. Si bien el registro y la supervisión de cuentas se tratan en los Controles CIS 8 (Gestión de Registros de Auditoría), es importante en el desarrollo de un programa de gestión integral de identidades y accesos (IAM).

Procedimientos y Herramientas

Las credenciales son activos que se deben inventariar y rastrear, cómo los activos y el software de la empresa, ya que son el punto de entrada principal a la empresa. Se deben desarrollar políticas de contraseñas adecuadas y directrices para no reutilizar contraseñas. Para obtener guía sobre la creación y el uso de contraseñas, consulte la Guía de políticas de contraseñas de CIS - <https://www.cisecurity.org/white-papers/cis-password-policy-guide/>.

También se debe realizar un seguimiento de las cuentas; cualquier cuenta que esté inactiva debe deshabilitarse y eventualmente eliminarse del sistema. Debe haber auditorías periódicas para garantizar que todas las cuentas activas se remontan a los usuarios autorizados del activo empresarial. Busque nuevas cuentas agregadas desde la revisión anterior, especialmente cuentas de administrador y de servicio. Se debe prestar mucha atención para identificar y rastrear cuentas administrativas o con altos privilegios y cuentas de servicio.

Los usuarios con acceso de administrador u otros privilegios deben tener cuentas independientes para esas tareas de autoridad superior. Estas cuentas solo se usarían al realizar esas tareas o acceder a datos especialmente confidenciales, para reducir el riesgo en caso de que su cuenta de usuario normal se vea comprometida. Para los usuarios con varias cuentas, su cuenta de usuario base, utilizada día a día para tareas no administrativas, no debe tener ningún privilegio elevado.

Inicio de Sesión Único por su abreviatura (SSO) es conveniente y seguro cuando una empresa tiene muchas aplicaciones, incluidas aplicaciones en la nube, lo que ayuda a reducir la cantidad de contraseñas que un usuario debe administrar. Se recomienda a los usuarios que utilicen aplicaciones de administración de contraseñas para almacenar de forma segura sus contraseñas y se les debe indicar que no las guarden en hojas de cálculo o archivos de texto en sus computadoras. Se recomienda MFA para acceso remoto.

Los usuarios también deben cerrar sesión automáticamente en el sistema después de un período de inactividad y estar capacitados para bloquear su pantalla cuando abandonan su dispositivo para minimizar la posibilidad de que alguien más en proximidad física alrededor del usuario acceda a su sistema, aplicaciones o datos.

→ Un recurso excelente es el NIST® Guía de Identidad Digital: <https://pages.nist.gov/800-63-3/>.

Salvaguardas

SALVAGUARDA	TÍTULO DE SALVAGUARDA/ DESCRIPCIÓN DE SALVAGUARDA	TIPO DE ACTIVO	FUNCIÓN DE SEGURIDAD	IG1	IG2	IG3
5.1	Establecer y mantener un inventario de cuentas Establecer y mantener un inventario de todas las cuentas administradas en la empresa. El inventario debe incluir cuentas de usuario y de administrador. El inventario, como mínimo, debe contener el nombre de la persona, el nombre de usuario, las fechas de inicio / finalización y el departamento. Valide que todas las cuentas activas estén autorizadas, en un horario recurrente, como mínimo trimestralmente o con mayor frecuencia.	Usuario	Identificar	●	●	●
5.2	Utilice contraseñas únicas Utilice contraseñas únicas para todos los activos de la empresa. La implementación de prácticas recomendadas incluye, como mínimo, una contraseña de 8 caracteres para las cuentas que usan MFA y una contraseña de 14 caracteres para las cuentas que no usan MFA.	Usuario	Proteger	●	●	●
5.3	Deshabilitar cuentas inactivas Elimine o deshabilite las cuentas inactivas después de un período de 45 días de inactividad, cuando sea posible.	Usuario	Responder	●	●	●
5.4	Restringir privilegios de administrador a cuentas de administrador dedicadas Restrinja los privilegios de administrador a las cuentas de administrador dedicadas en los activos de la empresa. Llevar a cabo actividades informáticas generales, como la navegación por Internet, el correo electrónico y el uso de la suite de productividad, desde la cuenta principal sin privilegios del usuario.	Usuario	Proteger	●	●	●
5.5	Establecer y mantener un inventario de cuentas de servicio Establezca y mantenga un inventario de las cuentas de servicio. El inventario, como mínimo, debe contener el propietario del departamento, la fecha de revisión y el propósito. Realizar revisiones de cuentas de servicio para validar que todas las cuentas activas están autorizadas, en una programación periódica como mínimo trimestralmente, o con más frecuencia	Usuario	Identificar		●	●
5.6	Centralizar la gestión de cuentas Centralice la gestión de cuentas a través de un directorio o servicio de identidad.	Usuario	Proteger		●	●

RESUMEN

Usar procesos y herramientas para crear, asignar, administrar y revocar credenciales y privilegios de acceso para cuentas de usuario, administrador y servicio para activos empresariales y software.

¿Por qué es Crítico este Control?

Donde el Control CIS 5 se ocupa específicamente de la administración de cuentas, el Control CIS 6 se enfoca en administrar el acceso que tienen estas cuentas, asegurando que los usuarios solo tengan acceso a los datos o activos empresariales apropiados para su función, y asegurarse que exista una autenticación sólida para los datos o funciones empresariales críticas o sensibles. Las cuentas solo deben tener la autorización mínima necesaria para el rol. Desarrollar derechos de acceso coherentes para cada rol y asignar roles a los usuarios es una práctica recomendada. También es importante desarrollar un programa para completar el acceso de aprovisionamiento y des aprovisionamiento. Centralizar esta función es ideal.

Hay algunas actividades de usuario que suponen un mayor riesgo para una empresa, ya sea porque se accede a ellas desde redes que no son de confianza o porque se realizan funciones de administrador que permiten agregar, cambiar o quitar otras cuentas, o realizar cambios de configuración en sistemas operativos o aplicaciones para que sean menos seguras. Esto también refuerza la importancia de usar MFA y herramientas de Administración de acceso con privilegios (PAM).

Algunos usuarios tienen acceso a activos o datos empresariales que no necesitan para su función; esto puede deberse a un proceso inmaduro que otorga a todos los usuarios acceso total, o un acceso prolongado a medida que los usuarios cambian de roles dentro de la empresa a lo largo del tiempo. Los privilegios de administrador local para las computadoras portátiles de los usuarios también son un problema, ya que cualquier código malicioso instalado o descargado por el usuario puede tener un mayor impacto en el activo empresarial que se ejecuta como administrador. El acceso de usuario, administrador y cuenta de servicio debe basarse en la función y la necesidad de la empresa.

Procedimientos y herramientas

Debe haber un proceso en el que se concedan y revoquen privilegios para las cuentas de usuario. Idealmente, esto se basa en el rol y la necesidad de la empresa a través del acceso basado en roles. El acceso basado en roles es una técnica para definir y administrar los requisitos de acceso para cada cuenta en función de: necesidad de saber, privilegio mínimo, requisitos de privacidad y / o separación de funciones. Existen herramientas tecnológicas para ayudar a gestionar este proceso. Sin embargo, puede haber un acceso más granular o temporal según las circunstancias.

MFA debe ser universal para todas las cuentas con privilegios o de administrador. Hay muchas herramientas que tienen aplicaciones de teléfonos inteligentes para realizar esta función, y son fáciles de implementar. El uso de la función de generador de números es más seguro que simplemente enviar un mensaje de servicio de mensajería corta (SMS) con un código de un solo uso, o solicitar una alerta "push" para que el usuario acepte. Sin embargo, no se recomienda ninguno de los dos para MFA de cuenta con privilegios. Las herramientas PAM están disponibles para el control de cuentas con privilegios y proporcionan una

contraseña de un solo uso que se debe desproteger para cada uso. Para mayor seguridad en la administración del sistema, se recomienda utilizar “jump-boxes” o conexiones de terminal fuera de banda (OOB).

El desaprovisionamiento integral de la cuenta es importante. Muchas empresas tienen procesos consistentes repetibles para eliminar el acceso cuando los empleados dejan la empresa. Sin embargo, ese proceso no siempre es consistente para los contratistas y debe incluirse en el proceso estándar de desaprovisionamiento. Las empresas también deben inventariar y rastrear las cuentas de servicio, ya que un error común es dejar tokens o contraseñas de texto sin cifrar en el código y publicar en repositorios de código basados en la nube pública.

Las cuentas con muchos privilegios no deben utilizarse para el uso diario, como la navegación web y la lectura de correo electrónico. Los administradores deben tener cuentas separadas que no tengan privilegios elevados para el uso diario de la oficina, y deben iniciar sesión en las cuentas de administrador solo cuando realicen funciones de administrador que requieran ese nivel de autorización. El personal de seguridad debe recopilar periódicamente una lista de los procesos en ejecución para determinar si algún navegador o lector de correo electrónico se está ejecutando con privilegios elevados.

→ Un recurso excelente es el NIST® Guía de Identidad Digital: <https://pages.nist.gov/800-63-3/>.

Salvaguardas

SALVAGUARDA	TÍTULO DE SALVAGUARDA/ DESCRIPCIÓN DE SALVAGUARDA	TIPO DE ACTIVO	FUNCIÓN DE SEGURIDAD	IG1	IG2	IG3
6.1	Establecer un proceso para conceder accesos Establecer y seguir un proceso, preferiblemente automatizado, para otorgar acceso a los activos de la empresa tras una nueva contratación, concesión de derechos o cambio de rol de un usuario.	Usuario	Proteger	●	●	●
6.2	Establecer un proceso de revocación de acceso Establecer y seguir un proceso, preferiblemente automatizado, para revocar el acceso a los activos de la empresa, mediante la desactivación de cuentas inmediatamente después de la terminación, revocación de derechos o cambio de rol de un usuario. Es posible que sea necesario deshabilitar cuentas, en lugar de eliminarlas, para conservar las pistas de auditoría.	Usuario	Proteger	●	●	●
6.3	Exigir MFA para aplicaciones expuestas externamente Exija que todas las aplicaciones empresariales o de terceros expuestas externamente apliquen MFA, donde sea compatible. Hacer cumplir MFA a través de un servicio de directorio o un proveedor de SSO es una implementación satisfactoria de esta salvaguarda.	Usuario	Proteger	●	●	●
6.4	Exigir MFA para el acceso remoto a la red Exigir MFA para el acceso remoto a la red.	Usuario	Proteger	●	●	●
6.5	Exigir MFA para el acceso administrativo Requerir MFA para todas las cuentas de acceso administrativo, donde sea compatible, en todos los activos de la empresa, ya sea administrado en el sitio o a través de un proveedor externo.	Usuario	Proteger	●	●	●
6.6	Establecer y mantener un inventario de sistemas de autenticación y autorización Establecer y mantener un inventario de los sistemas de autenticación y autorización de la empresa, incluidos los alojados en el sitio o en un proveedor de servicios remoto. Revisar y actualizar el inventario, como mínimo, anualmente o con mayor frecuencia.	Usuario	Identificar		●	●
6.7	Control de Acceso Centralizado Centralice el control de acceso para todos los activos de la empresa a través de un servicio de directorio o un proveedor de SSO, donde sea compatible.	Usuario	Proteger		●	●
6.8	Definir y mantener el control de acceso basado en roles Definir y mantener el control de acceso basado en roles, a través de la determinación y documentación de los derechos de acceso necesarios para que cada rol dentro de la empresa lleve a cabo con éxito las tareas asignadas. Realice revisiones de control de acceso de los activos de la empresa para validar que todos los privilegios estén autorizados, de forma periódica, como mínimo una vez al año, o con mayor frecuencia.	Datos	Proteger			●

RESUMEN

Desarrollar un plan para evaluar y dar seguimiento continuo a las vulnerabilidades en todos los activos dentro de la infraestructura de la empresa, con el fin de remediar y reducir la ventana de oportunidad para los atacantes. Monitorear las fuentes de la industria pública y privada en busca de nueva información sobre amenazas y vulnerabilidades.

¿Por qué este Control es Crítico?

Los defensores cibernéticos están siendo constantemente desafiados por los atacantes que buscan vulnerabilidades dentro de su infraestructura para explotar y obtener acceso. Los defensores deben tener información oportuna sobre amenazas disponibles para ellos sobre: actualizaciones de software, parches, avisos de seguridad, boletines de amenazas, etc., y deben revisar regularmente su entorno para identificar estas vulnerabilidades antes de que lo hagan los atacantes. Comprender y gestionar las vulnerabilidades es una actividad continua que requiere un enfoque de tiempo, atención y recursos.

Los atacantes tienen acceso a la misma información y a menudo pueden aprovechar las vulnerabilidades más rápidamente de lo que una empresa puede corregir. Si bien hay una brecha en el tiempo desde que se conoce una vulnerabilidad hasta cuándo se parchea, los defensores pueden priorizar qué vulnerabilidades son las que tienen más impacto para la empresa, o es probable que se exploten primero debido a la facilidad de uso. Por ejemplo, cuando los investigadores o la comunidad informan sobre nuevas vulnerabilidades, los proveedores deben desarrollar e implementar parches, indicadores de compromiso (IOC) y actualizaciones. Los defensores deben evaluar el riesgo de la nueva vulnerabilidad para la empresa, regresión de pruebas para parches, e instalar los parches.

En este proceso no existe la perfección. Los atacantes podrían estar usando un exploit a una vulnerabilidad que no se conoce en la comunidad de seguridad. Es posible que hayan desarrollado un exploit para esta vulnerabilidad, lo que se conoce como un exploit de "día cero". Una vez que se conoce la vulnerabilidad en la comunidad, se inicia el proceso mencionado anteriormente. Por lo tanto, los defensores deben tener en cuenta que ya puede existir un exploit cuando la vulnerabilidad está ampliamente socializada. A veces se pueden conocer vulnerabilidades dentro de una comunidad cerrada (por ejemplo, el proveedor aún está desarrollando una solución) durante semanas, meses o años antes de que se divulgue públicamente. Los defensores deben ser conscientes de que siempre puede haber vulnerabilidades que no puedan remediar y, por lo tanto, deben utilizar otros controles para mitigarlas.

Las empresas que no evalúan su infraestructura en busca de vulnerabilidades y abordan proactivamente las fallas descubiertas se enfrentan a una probabilidad significativa de que sus activos empresariales se vean comprometidos. Los defensores enfrentan desafíos particulares para escalar la remediación en toda la empresa y priorizar acciones con prioridades en conflicto, sin afectar el negocio o la misión de la empresa.

Procedimientos y Herramientas

Hay disponibles un gran número de herramientas de análisis de vulnerabilidades para evaluar la configuración de seguridad de los activos de la empresa. Algunas empresas también han descubierto que los servicios comerciales que utilizan dispositivos de análisis gestionados de forma remota son eficaces. Para ayudar a estandarizar las definiciones de vulnerabilidades descubiertas en una empresa, es preferible utilizar herramientas de escaneo de vulnerabilidades que mapean las vulnerabilidades a uno o más de los siguientes esquemas e idiomas de vulnerabilidad, configuración y clasificación de plataforma reconocidos por la industria: Vulnerabilidades y Exposiciones Comunes (CVE®), Enumeración de Configuración Común (CCE), Lenguaje Abierto de Evaluación y Vulnerabilidades (OVAL®), Plataforma de Enumeración Común (CPE), Sistema de Puntuación de Vulnerabilidades Común (CVSS), y/o Formato de Descripción de Lista de Verificación de Configuración Extensible (XCCDF). Estos esquemas y lenguajes son componentes de SCAP. Más información sobre SCAP se puede encontrar aquí: <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-126r3.pdf>

La frecuencia de las actividades de escaneo debe aumentar a medida que aumenta la diversidad de los activos de una empresa para tener en cuenta los ciclos de parches variables de cada proveedor. Las herramientas avanzadas de escaneo de vulnerabilidades se pueden configurar con credenciales de usuario para autenticarse en los activos de la empresa y realizar evaluaciones más completas. Estos se denominan “análisis autenticados”.

Además de las herramientas de escaneo que buscan vulnerabilidades y configuraciones erróneas en la red, varias herramientas gratuitas y comerciales pueden evaluar los ajustes de seguridad y las configuraciones de los activos de la empresa. Estas herramientas pueden proporcionar información detallada sobre los cambios no autorizados en la configuración o la introducción inadvertida de debilidades de seguridad por parte de los administradores.

Las empresas eficaces vinculan sus escáneres de vulnerabilidades con sistemas de identificación de problemas que rastrean e informan el progreso en la reparación de vulnerabilidades. Esto puede ayudar a resaltar las vulnerabilidades críticas no mitigadas por la alta dirección para garantizar que se resuelvan. Las empresas también pueden realizar un seguimiento de cuánto tiempo se tardó en remediar una vulnerabilidad, después de que se identificó o se emitió un parche. Estos pueden respaldar los requisitos de cumplimiento internos o de la industria. Algunas empresas maduras revisarán estos informes en las reuniones del comité directivo de seguridad de TI, que reúnen a los líderes de TI y del negocio para priorizar los esfuerzos de corrección en función del impacto en el negocio.

Al seleccionar qué vulnerabilidades corregir o parches aplicar, una empresa debe aumentar NIST®s Sistema de Puntuación de Vulnerabilidades Común (CVSS) con datos sobre la probabilidad de que un actor de amenazas utilice una vulnerabilidad o el impacto potencial de un exploit en la empresa. La información sobre la probabilidad de explotación también debe actualizarse periódicamente en función de la información sobre amenazas más actuales. Por ejemplo, el lanzamiento de un nuevo exploit, o nueva inteligencia relacionada con la explotación de la vulnerabilidad, debería cambiar la prioridad a través de la cual se debería considerar la vulnerabilidad para parchear. Hay varios sistemas comerciales disponibles para permitir que una empresa automatice y mantenga este proceso de manera escalable.

Las herramientas de análisis de vulnerabilidades más eficaces comparan los resultados del análisis actual con los análisis anteriores para determinar cómo han cambiado las vulnerabilidades en el entorno con el tiempo. El personal de seguridad utiliza estas características para llevar a cabo tendencias de vulnerabilidad de mes a mes.

Finalmente, debe haber un proceso de aseguramiento de la calidad para verificar las actualizaciones de la configuración, o que los parches se implementen correctamente y en todos los activos relevantes de la empresa.

Salvaguardas

SALVAGUARDA	TÍTULO DE SALVAGUARDA/ DESCRIPCIÓN DE SALVAGUARDA	TIPO DE ACTIVO	FUNCIÓN DE SEGURIDAD	IG1	IG2	IG3
7.1	Establecer y mantener un proceso de gestión de vulnerabilidades Establezca y mantenga un proceso de gestión de vulnerabilidades documentado para los activos de la empresa. Revisar y actualizar la documentación anualmente, o cuando ocurran cambios importantes en la empresa que puedan afectar esta salvaguarda.	Aplicaciones	Proteger			
7.2	Establecer y mantener un proceso de remediación Establecer y mantener una estrategia de remediación basada en riesgos documentada en un proceso de remediación, con revisiones mensuales o más frecuentes.	Aplicaciones	Responder			
7.3	Realice una gestión automatizada de parches del sistema operativo Realice actualizaciones del sistema operativo en los activos de la empresa a través de la gestión automatizada de parches de forma mensual o con mayor frecuencia.	Aplicaciones	Proteger			
7.4	Realizar la administración automatizada de parches de aplicaciones Realice actualizaciones de aplicaciones en los activos de la empresa a través de la gestión automatizada de parches de forma mensual o con mayor frecuencia.	Aplicaciones	Proteger			
7.5	Realizar análisis automatizados de vulnerabilidades de activos internos de la empresa Realice escaneos automatizados de vulnerabilidades de los activos internos de la empresa de forma trimestral o con mayor frecuencia. Realice escaneos autenticados y no autenticados, utilizando una herramienta de escaneo de vulnerabilidades compatible con SCAP.	Aplicaciones	Identificar			
7.6	Realice análisis automatizados de vulnerabilidades de activos empresariales expuestos externamente Realice escaneos automatizados de vulnerabilidades de los activos empresariales expuestos externamente utilizando una herramienta de escaneo de vulnerabilidades compatible con SCAP. Realice exploraciones mensualmente o con mayor frecuencia.	Aplicaciones	Identificar			
7.7	Remediar las vulnerabilidades detectadas Repare las vulnerabilidades detectadas en el software a través de procesos y herramientas de forma mensual o más frecuente, según el proceso de corrección.	Aplicaciones	Responder			

RESUMEN

Recopilar, alertar, revisar y conservar registros de auditoría de eventos que podrían ayudar a detectar, comprender o recuperarse de un ataque.

¿Por qué es Crítico este Control?

La recopilación y el análisis de registros son fundamentales para que una empresa pueda detectar rápidamente la actividad maliciosa. A veces, los registros de auditoría son la única evidencia de un ataque exitoso. Los atacantes saben que muchas empresas mantienen registros de auditoría con fines de cumplimiento, pero rara vez los analizan. Los atacantes utilizan este conocimiento para ocultar su ubicación, software malicioso y actividades en los equipos de las víctimas. Debido a procesos de análisis de registros deficientes o inexistentes, los atacantes a veces controlan las máquinas víctimas durante meses o años sin que nadie en la empresa de destino lo sepa.

Hay dos tipos de registros que generalmente se tratan y a menudo se configuran de forma independiente: registros del sistema y registros de auditoría. Los registros del sistema generalmente proporcionan eventos a nivel del sistema que muestran varios tiempos de inicio/finalización de procesos del sistema, fallas, etc. Estos son nativos de los sistemas y requieren menos configuración para activarse. Los registros de auditoría generalmente incluyen eventos a nivel de usuario, cuando un usuario inicia sesión, accede a un archivo, etc., y su configuración requiere más planificación y esfuerzo.

Los registros también son fundamentales para la respuesta a incidentes. Una vez que se ha detectado un ataque, el análisis de registros puede ayudar a las empresas a comprender el alcance de un ataque. Los registros de registro completos pueden mostrar, por ejemplo, cuándo y cómo ocurrió el ataque, a qué información se accedió y si se extrajeron los datos. La conservación de los registros también es fundamental en caso de que se requiera una investigación de seguimiento o si un ataque no se detecta durante un largo período de tiempo.

Procedimientos y Herramientas

La mayoría de los activos y software empresariales ofrecen capacidades de registro. Este registro debe activarse y los registros se envían a servidores de registro centralizados. Los firewalls, proxies y sistemas de acceso remoto (red privada virtual (VPN), acceso telefónico, etc.) deben configurarse para un registro detallado cuando sea beneficioso. La retención de los datos de registro también es importante en caso de que se requiera una investigación de incidente.

Además, todos los activos de la empresa deben configurarse para crear registros de control de acceso cuando un usuario intenta acceder a los recursos sin los privilegios adecuados. Para evaluar si dicho registro está en su lugar, una empresa debe escanear periódicamente a través de sus registros y compararlos con el inventario de activos de la empresa reunido como parte del Control CIS 1, con el fin de asegurarse de que cada activo gestionado conectado activamente a la red está generando periódicamente registros.

Salvaguardas

SALVAGUARDA	TÍTULO DE SALVAGUARDA/ DESCRIPCIÓN DE SALVAGUARDA	TIPO DE ACTIVO	FUNCIÓN DE SEGURIDAD	IG1	IG2	IG3
8.1	Establecer y mantener un proceso de gestión de registros de auditoría Establezca y mantenga un proceso de gestión de registros de auditoría que defina los requisitos de registro de la empresa. Como mínimo, aborde la recopilación, revisión y retención de registros de auditoría para activos empresariales. Revisar y actualizar la documentación anualmente, o cuando ocurran cambios importantes en la empresa que puedan afectar esta salvaguarda.	Red	Proteger			
8.2	Recopilar registros de auditoría Recopile registros de auditoría. Asegúrese de que el registro, según el proceso de gestión de registros de auditoría de la empresa, se haya habilitado en todos los activos de la empresa.	Red	Detectar			
8.3	Garantizar un almacenamiento adecuado del registro de auditoría Asegúrese de que los destinos de registro mantengan un almacenamiento adecuado para cumplir con el proceso de gestión de registros de auditoría de la empresa.	Red	Proteger			
8.4	Estandarizar la sincronización de hora Estandarizar la sincronización horaria. Configurar al menos dos orígenes de hora sincronizados en los activos de la empresa, donde se admite.	Red	Proteger			
8.5	Recopilar registros de auditoría detallados Configure el registro de auditoría detallado para los activos empresariales que contienen datos confidenciales. Incluya el origen del evento, la fecha, el nombre de usuario, la marca de tiempo, las direcciones de origen, las direcciones de destino y otros elementos útiles que podrían ayudar en una investigación forense.	Red	Detectar			
8.6	Recopilar registros de auditoría de consultas de DNS Recopile registros de auditoría de consultas de DNS en activos de la empresa, cuando sea apropiado y compatible.	Red	Detectar			
8.7	Recopilar registros de auditoría de solicitudes de URL Recopile registros de auditoría de solicitudes de URL en los activos de la empresa, cuando sea apropiado y compatible.	Red	Detectar			
8.8	Recopilar registros de auditoría de la línea de comandos Recopile registros de auditoría de la línea de comandos. Las implementaciones de ejemplo incluyen la recopilación de registros de auditoría de PowerShell®, BASH™ y terminales administrativas remotas.	Dispositivos	Detectar			
8.9	Centralice Audit Logs Centralice, en la medida de lo posible, la recopilación y retención de registros de auditoría en todos los activos de la empresa.	Red	Detectar			
8.10	Conservar registros de auditoría Conservar registros de auditoría en todos los activos de la empresa durante un mínimo de 90 días.	Red	Proteger			
8.11	Realizar revisiones de registros de auditoría Realice revisiones de los registros de auditoría para detectar anomalías o eventos anormales que podrían indicar una amenaza potencial. Realizar revisiones semanalmente o con mayor frecuencia.	Red	Detectar			
8.12	Recopilar registros de auditorías para proveedores de servicios Recopile registros de proveedores de servicios, donde sea compatible. Las implementaciones de ejemplo incluyen la recopilación de eventos de autenticación y autorización, eventos de creación y eliminación de datos y eventos de gestión de usuarios.	Datos	Detectar			

Protección del Correo Electrónico y Navegador Web

SALVAGUARDAS

7

IG1

2/7

IG2

6/7

IG3

7/7

RESUMEN

Mejorar la protección y detección de amenazas del correo electrónico y vectores web, ya que estas son oportunidades para que los atacantes manipulen el comportamiento humano a través de su compromiso.

¿Por qué es Crítico este Control?

Los navegadores web y los clientes de correo electrónico son puntos de entrada muy comunes para los atacantes debido a su interacción directa con los usuarios dentro de una empresa. El contenido se puede diseñar para atraer o engañar a los usuarios para que revelen credenciales, proporcionen datos confidenciales o brinden un canal abierto para permitir que los atacantes obtengan acceso, lo que aumenta el riesgo para la empresa. Dado que el correo electrónico y la web son los principales medios de que los usuarios interactúan con usuarios y entornos externos que no fueran de confianza, estos son los principales objetivos tanto para el código malicioso como para la ingeniería social. Además, a medida que las empresas pasan al correo electrónico basado en la web o al acceso al correo electrónico móvil, los usuarios ya no utilizan los clientes de correo electrónico tradicionales con todas las funciones, que proporcionan controles de seguridad integrados como cifrado de conexión, autenticación segura y botones de informes de phishing.

Procedimientos y Herramientas

Navegador Web

Los ciberdelincuentes pueden explotar los navegadores web de múltiples maneras. Si tienen acceso a exploits de navegadores vulnerables, pueden crear páginas web maliciosas que pueden aprovechar estas vulnerabilidades cuando se navega con un navegador inseguro o sin parches. Alternativamente, pueden intentar apuntar a cualquier número de complementos de terceros de navegador web comunes que les permitan conectarse al navegador o incluso directamente al sistema operativo o la aplicación. Estos complementos, al igual que cualquier otro software dentro de un entorno, deben revisarse para detectar vulnerabilidades, mantenerse actualizados con los últimos parches o versiones y controlarse. Muchos provienen de fuentes no confiables y algunos incluso están escritos para ser maliciosos. Por lo tanto, es mejor evitar que los usuarios instalen, de forma intencionada o involuntaria, malware que pueda estar oculto en algunos de estos complementos, extensiones y complementos. Las actualizaciones de configuración simples en el navegador pueden dificultar la instalación del malware al reducir la capacidad de instalar complementos/complementos/extensiones y evitar que tipos específicos de contenido se ejecuten automáticamente.

Los navegadores más populares emplean una base de datos de sitios de phishing y/o malware para protegerse contra las amenazas más comunes. Una práctica recomendada es habilitar estos filtros de contenido y activar los bloqueadores de elementos emergentes. Las ventanas emergentes no solo son molestas; también pueden alojar malware incorporado directamente o atraer a los usuarios para que hagan clic en enlaces utilizando trucos de ingeniería social. Para ayudar a hacer cumplir el bloqueo de dominios maliciosos conocidos, también considere la posibilidad de suscribirse a 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 seres humanos trabajan con los activos de la empresa; la formación y el fomento del comportamiento correcto es tan importante como la configuración técnica. El correo electrónico es el vector de amenaza más común contra las empresas a través de tácticas como el phishing y el Compromiso del Correo electrónico Empresarial por sus siglas en inglés (BEC).

El uso de una herramienta de filtrado de correo no deseado y el análisis de malware en la puerta de enlace de correo electrónico reduce el número de correos electrónicos y archivos adjuntos malintencionados que entran en la red de la empresa. Iniciar la autenticación de mensajes basada en dominio, informes y conformidad por sus siglas en inglés (DMARC) ayuda a reducir las actividades de correo no deseado y 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 en la red. Además de bloquear en función del remitente, también vale la pena permitir solo ciertos tipos de archivos que los usuarios necesitan para sus trabajos. Esto requerirá la coordinación con diferentes unidades de negocio para comprender qué tipos de archivos reciben por correo electrónico para garantizar que no haya una interrupción en sus procesos.

Dado que las técnicas de correo electrónico de phishing están en constante evolución para superar algo que se hace pasar por correo (SPAM) reglas de filtro, es importante capacitar a los usuarios sobre cómo identificar el phishing y notificar a seguridad de TI cuando vean uno. Hay muchas plataformas que realizan pruebas de phishing contra los usuarios para ayudarlos a educarlos sobre diferentes ejemplos y realizar un seguimiento de su mejora con el tiempo. El uso colectivo de este conocimiento para notificar a los equipos de seguridad de TI sobre el phishing ayuda a mejorar las protecciones y detecciones de amenazas basadas en correo electrónico.

Salvaguardas

SALVAGUARDA	TÍTULO DE SALVAGUARDA/ DESCRIPCIÓN DE SALVAGUARDA	TIPO DE ACTIVO	FUNCIÓN DE SEGURIDAD	IG1	IG2	IG3
9.1	Garantizar el uso de solo navegadores y clientes de correo electrónico totalmente compatibles Asegúrese de que solo los navegadores y clientes de correo electrónico totalmente compatibles puedan ejecutarse en la empresa, solo utilizando la versión más reciente de los navegadores y clientes de correo electrónico proporcionados a través del proveedor.	Aplicaciones	Proteger			
9.2	Usar servicios de filtrado DNS Utilice los servicios de filtrado de DNS en todos los activos de la empresa para bloquear el acceso a dominios maliciosos conocidos	Red	Proteger			
9.3	Mantener y aplicar filtros de URL basados en la red Hacer cumplir y actualizar los filtros de URL basados en la red para limitar la conexión de un activo empresarial a sitios web potencialmente maliciosos o no aprobados. Las implementaciones de ejemplo incluyen filtrado basado en categorías, filtrado basado en reputación o mediante el uso de listas de bloqueo. Aplicar filtros para todos los activos de la empresa	Red	Proteger			
9.4	Restringir extensiones innecesarias o no autorizadas de navegador y cliente de correo electrónico Restringir, ya sea mediante la desinstalación o desactivación, cualquier navegador no autorizado o innecesario o complementos de cliente de correo electrónico, extensiones y aplicaciones complementos.	Aplicaciones	Proteger			
9.5	Implementar DMARC Para reducir la posibilidad de correos electrónicos falsificados o modificados de dominios válidos, implemente la directiva DMARC y la verificación, comenzando con la implementación del marco de políticas de remitente (SPF) y los estándares domain keys identified mail (DKIM).	Red	Proteger			
9.6	Bloquear tipos de archivos innecesarios Bloquear tipos de archivos innecesarios que intentan ingresar por la puerta de enlace de correo electrónico de la empresa.	Red	Proteger			
9.7	Implementar y mantener protecciones anti malware del servidor de correo electrónico Implementar y mantener protecciones anti malware del servidor de correo electrónico, como el análisis de archivos adjuntos y/o el espacio aislado.	Red	Proteger			

RESUMEN

Prevenir o controlar la instalación, propagación y ejecución de aplicaciones, códigos o scripts maliciosos en activos empresariales.

¿Por qué es este Control Crítico?

El software malicioso (a veces categorizado como virus o troyanos) es un aspecto integral y peligroso de las amenazas de Internet. Pueden tener muchos propósitos, desde capturar credenciales, robar datos, identificar otros objetivos dentro de la red y cifrar o destruir datos. El malware está en constante evolución y es adaptable, ya que las variantes modernas aprovechan las técnicas de aprendizaje automático.

El malware ingresa a una empresa a través de vulnerabilidades dentro de la empresa en los dispositivos del usuario final, archivos adjuntos de correo electrónico, páginas web, servicios en la nube, dispositivos móviles y medios extraíbles. El malware a menudo se basa en un comportamiento inseguro del usuario final, como hacer clic en enlaces, abrir archivos adjuntos, instalar software o perfiles, o insertar unidades flash (USB). El malware moderno está diseñado para evitar, engañar o desactivar las defensas.

Las defensas contra malware deben ser capaces de operar en este entorno dinámico a través de la automatización, la actualización oportuna y rápida, y la integración con otros procesos como la gestión de vulnerabilidades y la respuesta a incidentes. Deben implementarse en todos los puntos de entrada y activos empresariales posibles para detectar, evitar la propagación o controlar la ejecución de software o código malintencionados.

Procedimientos y Herramientas

La protección eficaz contra malware incluye conjuntos tradicionales de detección y prevención de malware para clientes. Para garantizar que los IOC de malware estén actualizados, las empresas pueden recibir actualizaciones automáticas del proveedor para enriquecer otros datos de vulnerabilidades o amenazas. Estas herramientas se gestionan mejor de forma centralizada para proporcionar coherencia en toda la infraestructura.

Ser capaz de bloquear o identificar malware es sólo una parte de este control CIS; también se centra en la recopilación centralizada de los registros para admitir alertas, identificación y respuesta a incidentes. A medida que los actores maliciosos continúan desarrollando sus metodologías, muchos están comenzando a adoptar un enfoque de "vivir de la tierra" (LotL) para minimizar la probabilidad de ser atrapados. Este enfoque se refiere al comportamiento del atacante que utiliza herramientas o funciones que ya existen en el entorno de destino. Habilitar el registro, según las Salvaguardas en Control CIS 8, hará que sea mucho más fácil para la empresa seguir los eventos para comprender qué sucedió y por qué sucedió.

Salvuardas

SALVAGUARDA	TÍTULO DE SALVAGUARDA/ DESCRIPCIÓN DE SALVAGUARDA	TIPO DE ACTIVO	FUNCIÓN DE SEGURIDAD	IG1	IG2	IG3
10.1	Implementar y mantener software anti-malware Implementar y mantener software antimalware en todos los activos de la empresa.	Dispositivos	Proteger			
10.2	Configurar actualizaciones automáticas de firmas de Antimalwares Configurar actualizaciones automáticas para archivos de firma antimalware en todos los activos de la empresa.	Dispositivos	Proteger			
10.3	Deshabilitar la ejecución automática y la reproducción automática para medios extraíbles Desactive la ejecución automática y la función de ejecución automática de reproducción automática para medios extraíbles.	Dispositivos	Proteger			
10.4	Configurar el análisis anti malware automático de medios extraíbles Configure el software anti-malware para escanear automáticamente los medios extraíbles.	Dispositivos	Detectar			
10.5	Habilitar funciones anti-explotación Habilite funciones anti-explotación en activos y software empresariales, cuando sea posible, como Microsoft® Data Execution Prevention (DEP), Windows® Defender Exploit Guard (WDEG) o Apple® System Integrity Protection (SIP) y Gatekeeper™.	Dispositivos	Proteger			
10.6	Administrar de forma centralizada el software antimalware Gestione de forma centralizada el software antimalware.	Dispositivos	Proteger			
10.7	Utilice el software anti-malware basado en el comportamiento Usar software anti malware basado en el comportamiento.	Dispositivos	Detectar			

RESUMEN

Establecer y mantener prácticas de recuperación de datos suficientes para restaurar los activos empresariales incluidos en el alcance a un estado de confianza previo al incidente.

¿Por qué es Crítico este Control?

En la tríada de ciberseguridad - Confidencialidad, Integridad y Disponibilidad (CIA) - la disponibilidad de datos es, en algunos casos, más crítica que su confidencialidad. Las empresas necesitan muchos tipos de datos para tomar decisiones comerciales y, cuando esos datos no están disponibles o no son de confianza, podrían afectar a la empresa. Un ejemplo sencillo es la información meteorológica para una empresa de transporte.

Cuando los atacantes ponen en peligro los activos, realizan cambios en las configuraciones, agregan cuentas y, a menudo, agregan software o scripts. Estos cambios no siempre son fáciles de identificar, ya que los atacantes pueden haber corrompido o reemplazado aplicaciones confiables con versiones maliciosas, o los cambios pueden parecer nombres de cuentas de aspecto estándar. Los cambios de configuración pueden incluir agregar o cambiar entradas del Registro, abrir puertos, desactivar los servicios de seguridad, eliminar registros u otras acciones malintencionadas que hacen que un sistema sea inseguro. Estas acciones no tienen que ser maliciosas; el error humano puede causar cada uno de estos también. Por lo tanto, es importante tener la capacidad de tener copias de seguridad o espejos recientes para recuperar los activos y datos de la empresa a un estado de confianza conocido.

Ha habido un aumento exponencial del ransomware en los últimos años. No es una amenaza nueva, aunque se ha vuelto más comercializada y organizada como un método confiable para que los atacantes ganen dinero. Si un atacante cifra los datos de una empresa y exige un rescate por su restauración, puede resultar útil tener una copia de seguridad reciente para recuperarla en un estado conocido y de confianza. Sin embargo, a medida que el ransomware ha evolucionado, también se ha convertido en una técnica de extorsión, en la que los datos se exfiltran antes de encriptarlos y el atacante solicita un pago para restaurar los datos de la empresa, así como para evitar que se vendan o publiciten. En este caso, la restauración sólo resolvería el problema de restaurar los sistemas a un estado confiable y continuar las operaciones. Aprovechar la guía dentro de los Controles CIS ayudará a reducir el riesgo de ransomware a través de una mejor higiene cibernética, ya que los atacantes generalmente usan exploits más antiguos o básicos en sistemas inseguros.

Procedimientos y Herramientas















Los procedimientos de recuperación de datos deben definirse en el proceso de gestión de datos descrito en el Control CIS 3, Protección de datos. Esto debe incluir procedimientos de respaldo basados en el valor, la sensibilidad o los requisitos de retención de los datos. Esto ayudará a desarrollar la frecuencia y el tipo de copia de seguridad (copia de respaldo completa frente a incremental).

Una vez por trimestre (o siempre que se introduzca un nuevo proceso o tecnología de respaldo), un equipo de pruebas debe evaluar una muestra aleatoria de respaldos e intentar restaurarlos en un entorno de banco de pruebas. Las copias de seguridad restauradas deben

verificarse para garantizar que el sistema operativo, la aplicación y los datos de la copia de seguridad estén intactos y en funcionamiento.

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

Salvaguadas

SALVAGUARDA	TÍTULO DE SALVAGUARDA/ DESCRIPCIÓN DE SALVAGUARDA	TIPO DE ACTIVO	FUNCIÓN DE SEGURIDAD	IG1	IG2	IG3
11.1	Establecer y mantener un proceso de recuperación de datos Establecer y mantener un proceso de recuperación de datos. En el proceso, aborde el alcance de las actividades de recuperación de datos, la priorización de la recuperación y la seguridad de los datos de respaldo. Revisar y actualizar la documentación anualmente, o cuando ocurran cambios importantes en la empresa que puedan afectar esta salvaguarda.	Datos	Recuperar			
11.2	Realice copias de seguridad automatizadas Realizar copias de seguridad automatizadas de activos empresariales dentro del ámbito. Ejecutar copias de seguridad semanalmente, o con más frecuencia, en función de la sensibilidad de los datos.	Datos	Recuperar			
11.3	Proteja los datos de recuperación Proteja los datos de recuperación con controles equivalentes a los datos originales. Cifrado de referencia o separación de datos, en función de los requisitos	Datos	Proteger			
11.4	Establecer y mantener una instancia aislada de datos de recuperación Establecer y mantener una instancia aislada de datos de recuperación. Entre las implementaciones de ejemplo se incluyen el control de versiones de destinos de copia de seguridad a través de sistemas o servicios sin conexión, en la nube o fuera del sitio.	Datos	Recuperar			
11.5	Prueba de recuperación de datos Pruebe la recuperación de copias de seguridad trimestralmente, o con mayor frecuencia, para obtener una muestra de los activos empresariales incluidos en el alcance.	Datos	Recuperar			

RESUMEN

Establecer, implementar y administrar activamente (rastrear, informar, corregir) dispositivos de red, con el fin de evitar que los atacantes exploten los servicios de red y los puntos de acceso vulnerables.

¿Por qué es Crítico este Control?

La infraestructura de red segura es una defensa esencial contra los ataques. Esto incluye una arquitectura de seguridad adecuada, el tratamiento de vulnerabilidades que, a menudo, se introducen con la configuración predeterminada, la supervisión de los cambios y la reevaluación de las configuraciones actuales. La infraestructura de red incluye dispositivos como puertas de enlace físicas y virtualizadas, firewalls, puntos de acceso inalámbricos, enrutadores y conmutadores.

Las configuraciones predeterminadas para dispositivos de red están orientadas a la facilidad de implementación y la facilidad de uso, no a la seguridad. Entre las posibles vulnerabilidades predeterminadas se incluyen servicios y puertos abiertos, cuentas y contraseñas predeterminadas (incluidas las cuentas de servicio), compatibilidad con protocolos vulnerables más antiguos y preinstalación de software innecesario. Los atacantes buscan configuraciones predeterminadas vulnerables, brechas o inconsistencias en conjuntos de reglas de firewall, enrutadores y conmutadores y usan esos agujeros para penetrar las defensas. Explotan fallas en estos dispositivos para obtener acceso a las redes, redirigir el tráfico en una red e interceptar datos mientras están en transmisión.

La seguridad de red es un entorno en constante cambio que requiere una reevaluación regular de los diagramas de arquitectura, las configuraciones, los controles de acceso y los flujos de tráfico permitidos. Los atacantes aprovechan que las configuraciones de dispositivos de red se vuelven menos seguras con el tiempo a medida que los usuarios exigen excepciones para necesidades empresariales específicas. A veces, las excepciones se implementan, pero no se quitan cuando ya no son aplicables a las necesidades de la empresa. En algunos casos, el riesgo de seguridad de una excepción no se analiza ni se mide adecuadamente en función de la necesidad empresarial asociada y puede cambiar con el tiempo.

Procedimientos y Herramientas

Las empresas deben asegurarse de que la infraestructura de red esté completamente documentada y que los diagramas de arquitectura se mantengan actualizados. Es importante que los componentes clave de la infraestructura tengan soporte de proveedores para parches y actualizaciones de funciones. Actualice los componentes al final de su vida útil (EOL) antes de la fecha en que dejarán de ser compatibles o aplique controles de mitigación para aislarlos. Las empresas deben monitorear las versiones y configuraciones de su infraestructura en busca de vulnerabilidades que requieran que actualicen los dispositivos de red a la última versión segura y estable que no afecte la infraestructura.

Un diagrama de arquitectura de red actualizado, incluidos los diagramas de arquitectura de seguridad, son una base importante para la gestión de la infraestructura. Lo siguiente es tener una gestión de cuentas completa para el control de acceso, el registro y la supervisión. Finalmente, la administración de la infraestructura sólo debe realizarse a través de protocolos

seguros, con autenticación fuerte (MFA para PAM) y desde dispositivos administrativos dedicados o redes fuera de banda (OOB).

Las herramientas comerciales pueden ser útiles para evaluar los conjuntos de reglas de los dispositivos de filtrado de red para determinar si son consistentes o están en conflicto. Esto proporciona una verificación de salud automatizada de los filtros de red. Estas herramientas buscan errores en conjuntos de reglas o listas de controles de acceso (ACL) que pueden permitir servicios no deseados a través del dispositivo de red. Estas herramientas deben ejecutarse cada vez que se realizan cambios significativos en los conjuntos de reglas del firewall, las ACL del enrutador u otras tecnologías de filtrado.

→ Para obtener orientación sobre el teletrabajo y las oficinas pequeñas, consulte la guía de Controles CIS de teletrabajo y pequeñas oficinas: <https://www.cisecurity.org/controls/v8/>.

Salvaguardas

SALVAGUARDA	TÍTULO DE SALVAGUARDA/ DESCRIPCIÓN DE SALVAGUARDA	TIPO DE ACTIVO	FUNCIÓN DE SEGURIDAD	IG1	IG2	IG3
12.1	Asegúrese de que la infraestructura de red esté actualizada Asegúrese de que la infraestructura de red se mantenga actualizada. Entre las implementaciones de ejemplo se incluyen la ejecución de la última versión estable de software y/o el uso de servicios de red como NaaS actualmente admitidas. Revise las versiones de software mensualmente, o con más frecuencia, para verificar la compatibilidad del software.	Red	Proteger			
12.2	Establecer y mantener una arquitectura de red segura Establecer y mantener una arquitectura de red segura. Una arquitectura de red segura debe abordar la segmentación, los privilegios mínimos y la disponibilidad, como mínimo.	Red	Proteger			
12.3	Gestione de forma segura la infraestructura de red Gestione de forma segura la infraestructura de red. Las implementaciones de ejemplo incluyen infraestructura de versión controlada como código y el uso de protocolos de red seguros, como SSH y HTTPS.	Red	Proteger			
12.4	Establecer y mantener diagramas de arquitectura Establezca y mantenga los diagramas de la arquitectura y/o la documentación del sistema de red. Revise y actualice la documentación anualmente, o cuando se produzcan cambios significativos en la empresa que puedan afectar a esta salvaguarda.	Red	Identificar			
12.5	Centralice la autenticación, la autorización, y la auditoría de la red (AAA) Centralice la red AAA.	Red	Proteger			
12.6	Uso de protocolos seguros de administración de redes y comunicaciones Utilice protocolos seguros de administración de redes y comunicación (por ejemplo, 802.1X, Wi-Fi Protected Access 2 (WPA2) Enterprise o superior).	Red	Proteger			
12.7	Asegúrese de que los dispositivos remotos utilicen una VPN y se conecten a la infraestructura AAA de una empresa Requerir que los usuarios se autenticuen en los servicios de autenticación y VPN administrados por la empresa antes de acceder a los recursos de la empresa en los dispositivos de usuario final.	Dispositivos	Proteger			
12.8	Establecer y mantener recursos informáticos dedicados para todo el trabajo administrativo Establezca y mantenga recursos informáticos dedicados, ya sea física o lógicamente separados, para todas las tareas administrativas o tareas que requieran acceso administrativo. Los recursos informáticos deben segmentarse de la red principal de la empresa y no se les debe permitir el acceso a Internet.	Dispositivos	Proteger			

RESUMEN

Operar procesos y herramientas para establecer y mantener la supervisión y defensa integrales de la red contra las amenazas de seguridad en toda la infraestructura de red y la base de usuarios de la empresa.

¿Por qué es Crítico este Control?

No podemos confiar en que las defensas de la red sean perfectas. Los adversarios continúan evolucionando y madurando, a medida que comparten o venden información entre su comunidad sobre exploits y omisiones de los controles de seguridad. Incluso si las herramientas de seguridad funcionan "como se anuncia", se necesita una comprensión de la postura de riesgo empresarial para configurarlas, ajustarlas y registrarlas para que sean efectivas. A menudo, las configuraciones incorrectas debido a errores humanos o la falta de conocimiento de las capacidades de las herramientas dan a las empresas una falsa sensación de seguridad.

Las herramientas de seguridad sólo pueden ser efectivas si respaldan un proceso de monitoreo continuo que permita al personal recibir alertas y responder rápidamente a los incidentes de seguridad. Las empresas que adoptan un enfoque puramente tecnológico también experimentaron más falsos positivos, debido a su excesiva dependencia de las alertas de las herramientas. Identificar y responder a estas amenazas requiere visibilidad de todos los vectores de amenazas de la infraestructura y el aprovechamiento de personas en el proceso de detección, análisis y respuesta. Es fundamental para las empresas grandes o muy específicas tener una capacidad de operaciones de seguridad para prevenir, detectar y responder rápidamente a las amenazas cibernéticas antes de que puedan afectar a la empresa. Este proceso generará informes de actividad y métricas que ayudarán a mejorar las políticas de seguridad y respaldan el cumplimiento normativo para muchas empresas.

Como hemos visto muchas veces en la prensa, las empresas han estado comprometidas durante semanas, meses o años antes de ser descubiertas. El principal beneficio de tener una conciencia situacional integral es aumentar la velocidad de detección y respuesta. Esto es fundamental para responder rápidamente cuando se descubre malware, se roban credenciales o cuando se comprometen datos confidenciales para reducir el impacto en la empresa.

A través de un buen conocimiento de la situación (es decir, operaciones de seguridad), las empresas identifican y catalogan tácticas, técnicas y procedimientos (TTP) de los atacantes, incluidos sus IOC, que ayudarán a la empresa a ser más proactiva en la identificación de amenazas o incidentes futuros. La recuperación se puede lograr más rápidamente cuando la respuesta tiene acceso a información completa sobre el entorno y la estructura empresarial para desarrollar estrategias de respuesta eficientes.

Procedimientos y Herramientas

La mayoría de las empresas no necesitan levantar un Centro de Operaciones de Seguridad (SOC) para obtener conciencia situacional. Esto comienza con la comprensión de las funciones comerciales críticas, las arquitecturas de redes y servidores, los flujos de datos y de datos, el servicio del proveedor y la conexión de los socios comerciales, y los dispositivos

y cuentas de los usuarios finales. Esto informa el desarrollo de una arquitectura de seguridad, controles técnicos, registro, monitoreo y procedimientos de respuesta.

En el núcleo de este proceso se encuentra un equipo capacitado y organizado que implementa procesos para la detección, el análisis y la mitigación de incidentes. Estas capacidades podrían llevarse a cabo internamente, o a través de consultores o un proveedor de servicios gestionados. Las empresas deben considerar las actividades de red, activos empresariales, credenciales de usuario y acceso a datos. La tecnología jugará un papel crucial para recopilar y analizar todos los datos y monitorear las redes y los activos de la empresa interna y externamente a la empresa. Las empresas deben incluir visibilidad de las plataformas en la nube que podrían no estar en línea con la tecnología de seguridad local.

Reenviar todos los registros importantes a programas analíticos, como las soluciones de administración de eventos e información de seguridad (SIEM), puede proporcionar valor; sin embargo, no proporcionan una imagen completa. Las revisiones semanales de registros son necesarias para ajustar los umbrales e identificar eventos anormales herramientas de correlación pueden hacer que los registros de auditoría sean más útiles para la inspección manual posterior. Estas herramientas no reemplazan al personal capacitado en seguridad de la información ni a los administradores de sistemas. Incluso con herramientas automatizadas de análisis de registros, a menudo se requiere experiencia e intuición humanas para identificar y comprender los ataques.

A medida que este proceso madure, las empresas crearán, mantendrán y desarrollarán una base de conocimientos que ayudará a comprender y evaluar los riesgos empresariales, desarrollando una capacidad interna de inteligencia de amenazas. La inteligencia de amenazas es la recopilación de TTPs de incidentes y adversarios. Para lograr esto, un programa de evaluación situacional definirá y estimará qué fuentes de información son relevantes para detectar, informar y controlar ataques. La mayoría de las empresas maduras pueden evolucionar hacia la búsqueda de amenazas, donde el personal capacitado revisa manualmente los registros del sistema y de los usuarios, los flujos de datos y los patrones de tráfico para encontrar anomalías.

Salvaguardas

SALVAGUARDA	TÍTULO DE SALVAGUARDA/ DESCRIPCIÓN DE SALVAGUARDA	TIPO DE ACTIVO	FUNCIÓN DE SEGURIDAD	IG1	IG2	IG3
13.1	Centralizar alertas de eventos de seguridad Centralice las alertas de eventos de seguridad en todos los activos de la empresa para la correlación y el análisis de registros. La implementación de las mejores prácticas requiere el uso de un SIEM, que incluye alertas de correlación de eventos definidas por el proveedor. Una plataforma de análisis de registros configurada con alertas de correlación relevantes para la seguridad también satisface esta protección.	Red	Detectar			
13.2	Implemente una solución de detección de intrusiones basada en host Implementar una solución de detección de intrusiones basada en host en activos empresariales, cuando sea apropiado y/o compatible.	Dispositivos	Detectar			
13.3	Implementación de una solución de detección de intrusiones en la red Implemente una solución de detección de intrusiones en la red de activos de la empresa, cuando corresponda. Las implementaciones de ejemplo incluyen el uso de un sistema de detección de intrusiones en la red (NIDS) o un servicio equivalente de proveedor de servicios en la nube (CSP).	Red	Detectar			
13.4	Realizar filtrado de tráfico entre segmentos de red Realice un filtrado de tráfico entre los segmentos de la red, cuando corresponda.	Red	Proteger			
13.5	Gestionar el control de acceso para activos remotos Administre el control de acceso para los activos que se conectan de forma remota a los recursos de la empresa. Determine la cantidad de acceso a los recursos de la empresa en función de: el software antimalware actualizado instalado, el cumplimiento de la configuración con el proceso de configuración segura de la empresa y la garantía de que el sistema operativo y las aplicaciones estén actualizados.	Dispositivos	Proteger			
13.6	Recopilar registros de flujo de tráfico de red Recopilar registros de flujo de tráfico de red y/o tráfico de red para revisar y alertar desde dispositivos de red.	Red	Detectar			

SALVAGUARDA	TÍTULO DE SALVAGUARDA/ DESCRIPCIÓN DE SALVAGUARDA	TIPO DE ACTIVO	FUNCIÓN DE SEGURIDAD	IG1	IG2	IG3
13.7	Implementar una solución de prevención de intrusiones basada en host Implemente una solución de prevención de intrusiones basada en host en los activos de la empresa, cuando corresponda o sea compatible. Las implementaciones de ejemplo incluyen el uso de un cliente de detección y respuesta de extremo (EDR) o un agente IPS basado en host.	Dispositivos	Proteger			●
13.8	Implementar una solución de prevención de intrusiones en la red Implemente una solución de prevención de intrusiones en la red, en donde corresponda. Entre las implementaciones de ejemplo se incluye el uso de un sistema de prevención de intrusiones en la red (NIPS) o un servicio CSP equivalente.	Red	Proteger			●
13.9	Implementar el control de acceso a nivel de puerto Implementar el control de acceso a nivel de puerto. El control de acceso a nivel de puerto utiliza 802.1x o protocolos de control de acceso a la red similares, como certificados, y puede incorporar autenticación de usuario y/o dispositivo.	Dispositivos	Proteger			●
13.10	Realizar el filtrado en la capa de aplicación Realizar el filtrado de la capa de aplicación. Entre las implementaciones de ejemplo se incluyen un proxy de filtrado, un firewall de nivel de aplicación o una puerta de enlace.	Red	Proteger			●
13.11	Ajustar los umbrales de alerta de eventos de seguridad Ajustar los umbrales de alerta de eventos de seguridad mensualmente o con más frecuencia	Red	Detectar			●

Concientización en Seguridad y Formación de Habilidades

SALVAGUARDAS

9

IG1

8/9

IG2

9/9

IG3

9/9

RESUMEN

Establecer y mantener un programa de concientización sobre seguridad para influir en el comportamiento de la fuerza laboral para que sea consciente de la seguridad y esté debidamente capacitado para reducir los riesgos de ciberseguridad para la empresa.

¿Por qué es Crítico este Control?

Las acciones de las personas juegan un papel crítico en el éxito o fracaso del programa de seguridad de una empresa. Es más fácil para un atacante atraer a un usuario a hacer clic en un enlace o abrir un archivo adjunto de correo electrónico para instalar malware con el fin de entrar en una empresa, que encontrar un exploit de red para hacerlo directamente.

Los propios usuarios, tanto intencionalmente como involuntariamente, pueden causar incidentes como resultado del mal manejo de datos confidenciales, el envío de un correo electrónico con datos confidenciales al destinatario equivocado, la pérdida de un dispositivo portátil de usuario final, el uso de contraseñas débiles o el uso de la misma contraseña que utilizan en sitios públicos.

Ningún programa de seguridad puede abordar eficazmente el riesgo cibernético sin un medio para abordar esta vulnerabilidad humana fundamental. Los usuarios de todos los niveles de la empresa tienen diferentes riesgos. Por ejemplo: los ejecutivos manejan datos más sensibles; los administradores de sistemas tienen la capacidad de controlar el acceso a sistemas y aplicaciones; y los usuarios de finanzas, recursos humanos y contratos tienen acceso a diferentes tipos de datos confidenciales que pueden convertirlos en objetivos.

La formación debe actualizarse periódicamente. Esto aumentará la cultura de seguridad y desalentará las soluciones alternativas riesgosas.

Procedimientos y Herramientas

Un programa de capacitación de conciencia de seguridad efectivo no debe ser solo un video de capacitación enlatado, una vez al año, junto con pruebas regulares de phishing. Si bien se necesita capacitación anual, también debería haber mensajes y notificaciones más frecuentes y de actualidad sobre seguridad. Esto podría incluir mensajes sobre: uso seguro de contraseñas que coincide con un informe de medios de volcado de contraseñas, el aumento del phishing durante el tiempo de impuestos o una mayor conciencia de los correos electrónicos de entrega de paquetes maliciosos durante los días festivos.

La capacitación también debe considerar las diferentes posturas regulatorias y de amenaza de la empresa. Las empresas financieras pueden tener más capacitación relacionada con el cumplimiento sobre el manejo y uso de datos, las empresas de atención médica sobre el manejo de datos de atención médica y los comerciantes para datos de tarjetas de crédito.

La capacitación en ingeniería social, como las pruebas de phishing, también debe incluir el conocimiento de las tácticas que se dirigen a diferentes roles. Por ejemplo, el equipo financiero recibirá intentos de BEC haciéndose pasar por ejecutivos que piden transferir









dinero, o recibirá correos electrónicos de socios o proveedores comprometidos que piden cambiar la información de la cuenta bancaria para su próximo pago.

Para un tratamiento más completo de este tema, los siguientes recursos son útiles para crear un programa eficaz de concienciación sobre la seguridad:

- **NIST® SP 800-50 Formación de Sensibilización de Infosec:** <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-50.pdf>
- **Centro de Ciber Seguridad Nacional (UK):** <https://www.ncsc.gov.uk/guidance/10-steps-user-education-and-awareness>
- **EDUCAUSE:** <https://www.educause.edu/focus-areas-and-initiatives/policy-and-security/cybersecurity-program/awareness-campaigns>
- **Alianza Nacional de Ciber Seguridad (NCSA):** <https://staysafeonline.org/>
- **SANS:** <https://www.sans.org/security-awareness-training/resources>
- **Para obtener orientación sobre la configuración de enrutadores domésticos, consulte la Guía de seguridad de redes de oficinas pequeñas y teletrabajo de los Controles CIS:** <https://www.cisecurity.org/white-papers/cis-controls-telework-and-small-office-network-security-guide/>.

Salvaguardas

SALVAGUARDA	TÍTULO DE SALVAGUARDA/ DESCRIPCIÓN DE SALVAGUARDA	TIPO DE ACTIVO	FUNCIÓN DE SEGURIDAD	IG1	IG2	IG3
14.1	Establecer y mantener un programa de concientización sobre seguridad Establecer y mantener un programa de concientización sobre seguridad. El propósito de un programa de concientización sobre seguridad es educar a la fuerza laboral de la empresa sobre cómo interactuar con los activos y datos de la empresa de manera segura. Realice la capacitación al momento de contratar y, como mínimo, anualmente. Revisar y actualizar el contenido anualmente o cuando se produzcan cambios empresariales importantes que puedan afectar a esta salvaguarda.	N/A	Proteger			
14.2	Capacitar a los miembros de la plana laboral para que reconozcan los ataques de ingeniería social Capacite a los miembros de la fuerza laboral para que reconozcan los ataques de ingeniería social, como suplantación de identidad (phishing), pretextos y seguimiento.	N/A	Proteger			
14.3	Capacitar a los miembros de la plana laboral sobre las mejores prácticas de autenticación Capacite a los miembros de la fuerza laboral sobre las mejores prácticas de autenticación. Los temas de ejemplo incluyen MFA, composición de contraseñas y administración de credenciales.	N/A	Proteger			
14.4	Capacitar a la fuerza laboral en las mejores prácticas de manejo de datos Capacite a los miembros de la fuerza laboral sobre cómo identificar y almacenar, transferir, archivar y destruir correctamente los datos confidenciales. Esto también incluye la capacitación de los miembros de la fuerza laboral en las mejores prácticas de pantalla limpia y escritorio, cómo bloquear su pantalla cuando se alejan de su activo empresarial, borrar pizarras físicas y virtuales al final de las reuniones y almacenar datos y activos de forma segura.	N/A	Proteger			
14.5	Capacitar a los miembros de la plana laboral sobre las causas de la exposición involuntaria de datos Capacite a los miembros de la fuerza laboral para que sean conscientes de las causas de la exposición involuntaria de datos. Entre los temas de ejemplo se incluyen la entrega errónea de datos confidenciales, la pérdida de un dispositivo portátil de usuario final o la publicación de datos para audiencias no deseadas.	N/A	Proteger			
14.6	Capacitar a los miembros de la plana laboral sobre el reconocimiento y la notificación de incidentes de seguridad Capacitar a los miembros de la fuerza laboral para que puedan reconocer un incidente potencial y puedan reportar dicho incidente.	N/A	Proteger			

SALVAGUARDA	TÍTULO DE SALVAGUARDA/ DESCRIPCIÓN DE SALVAGUARDA	TIPO DE ACTIVO	FUNCIÓN DE SEGURIDAD	IG1	IG2	IG3
14.7	Capacitar al personal sobre cómo identificar e informar si sus activos empresariales carecen de actualizaciones de seguridad Capacite al personal para que comprenda cómo verificar e informar sobre parches de software desactualizados o cualquier falla en los procesos y herramientas automatizados. Parte de esta capacitación debe incluir notificar al personal de TI de cualquier falla en los procesos y herramientas automatizados.	N/A	Proteger			
14.8	Capacitar a la plana laboral sobre los peligros de conectarse y transmitir datos empresariales a través de redes inseguras Capacite a los miembros de la fuerza laboral sobre los peligros de conectarse y transmitir datos a través de redes inseguras para actividades empresariales. Si la empresa tiene trabajadores remotos, la capacitación debe incluir orientación para garantizar que todos los usuarios configuren de manera segura su infraestructura de red doméstica.	N/A	Proteger			
14.9	Llevar a cabo capacitación en habilidades y concientización sobre seguridad para roles específicos Llevar a cabo capacitación en habilidades y concientización sobre seguridad para funciones específicas. Las implementaciones de ejemplo incluyen cursos de administración de sistemas seguros para profesionales de TI, capacitación en prevención y concientización de vulnerabilidades de OWASP® Top 10 para desarrolladores de aplicaciones web y capacitación avanzada en concientización sobre ingeniería social para roles de alto perfil.	N/A	Proteger			

RESUMEN

Desarrollar un proceso para evaluar a los proveedores de servicios que poseen datos confidenciales o que son responsables de las plataformas o procesos de TI críticos de una empresa, para garantizar que estos proveedores protejan esas plataformas y datos de manera adecuada.

¿Por qué es Crítico este Control?

En nuestro mundo moderno y conectado, las empresas confían en los proveedores y socios para que les ayuden a administrar sus datos o en la infraestructura de terceros para las aplicaciones o funciones principales.

Ha habido numerosos ejemplos en los que las infracciones de terceros han afectado significativamente a una empresa; por ejemplo, ya a finales de la década de 2000, las tarjetas de pago se vieron comprometidas después de que los atacantes se infiltraron en proveedores externos más pequeños de la industria minorista. Ejemplos más recientes incluyen ataques de ransomware que afectan a una empresa indirectamente, debido a que uno de sus proveedores de servicios está bloqueado, causando la interrupción del negocio. O peor aún, si se conecta directamente, un ataque de ransomware podría cifrar los datos de la empresa principal.

La mayoría de las regulaciones de seguridad y privacidad de datos requieren que su protección se extienda a proveedores de servicios externos, como con la Ley de Portabilidad y Responsabilidad de Seguros de Salud (HIPAA) Business Associate agreements in healthcare, Federal Financial Institutions Examination Council (FFIEC) Acuerdos de socios comerciales en el cuidado de la salud, Consejo Federal de Examen de Instituciones Financieras. La confianza de terceros es una función central de Cumplimiento y Riesgo de Gobernanza (GRC), ya que los riesgos que no se gestionan dentro de la empresa se transfieren a entidades externas a la empresa.

Si bien la revisión de la seguridad de terceros ha sido una tarea realizada durante décadas, no existe un estándar universal para evaluar la seguridad; y, muchos proveedores de servicios están siendo auditados por sus clientes varias veces al mes, lo que genera impactos en su propia productividad. Esto se debe a que cada empresa tiene una "lista de verificación" o un conjunto de estándares diferentes para calificar al proveedor de servicios. Hay solo unos pocos estándares de la industria, como en finanzas, con el programa de evaluaciones compartidas, o en educación superior, con su kit de herramientas de evaluación de proveedores comunitarios de educación superior (HECVAT). Las compañías de seguros que venden pólizas de ciberseguridad también tienen sus propias medidas.

Si bien una empresa puede someter a un gran escrutinio a las grandes empresas de alojamiento de aplicaciones o en la nube porque alojan su correo electrónico o aplicaciones comerciales críticas, las empresas más pequeñas suelen tener un riesgo mayor. A menudo, un proveedor de servicios de terceros contrata a terceros para proporcionar otros complementos o servicios, como cuando un tercero utiliza una plataforma o producto de terceros para respaldar a la empresa principal.

Procedimientos y Herramientas

La mayoría de las empresas han utilizado tradicionalmente listas de verificación estándar, como las de ISO 27001 o los Controles CIS. A menudo, este proceso se gestiona mediante hojas de cálculo; sin embargo, ahora existen plataformas en línea que permiten la gestión centralizada de este proceso. El enfoque de este CIS Control, aunque no está en la lista de verificación; en cambio, se basa en los fundamentos del programa. Asegúrese de volver a visitarlo anualmente, ya que las relaciones y los datos pueden cambiar.

Independientemente del tamaño de la empresa, debe haber una política sobre la revisión de los proveedores de servicios, un inventario de estos proveedores y una calificación de riesgo asociada con su impacto potencial en la empresa en caso de un incidente. También debe haber un lenguaje en los contratos para que rindan cuentas si hay un incidente que afecta a la empresa.

Existen plataformas de evaluación de terceros que tienen un inventario de miles de proveedores de servicios, que intentan proporcionar una visión central de la industria, para ayudar a las empresas a tomar decisiones de riesgo más informadas. Estas plataformas a menudo tienen una puntuación de riesgo dinámica para los proveedores de servicios, basada (generalmente) en evaluaciones técnicas pasivas o enriquecidas a través de evaluaciones de terceros de otras empresas.

Al realizar revisiones, céntrese en los servicios o departamentos del proveedor que apoyan a la empresa. Un tercero que tenga un contrato de servicio de seguridad administrado, o un anticipo, y tenga un seguro de ciberseguridad, también puede ayudar con la reducción de riesgos.

También es importante dar de baja de forma segura a los proveedores de servicios cuando los contratos se completan o rescinden. Las actividades de retirada pueden incluir la desactivación de cuentas de usuario y servicio, la terminación de flujos de datos y la eliminación segura de datos empresariales dentro de los sistemas de proveedores de servicios.

→ **Referencia a NIST® 800-88r1 – Directrices para la desinfección de medios, según corresponda:** <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf>.

Salvaguardas

SALVAGUARDA	TÍTULO DE SALVAGUARDA/ DESCRIPCIÓN DE SALVAGUARDA	TIPO DE ACTIVO	FUNCIÓN DE SEGURIDAD	IG1	IG2	IG3
15.1	Establecer y mantener un inventario de proveedores de servicios Establecer y mantener un inventario de proveedores de servicios. El inventario debe enumerar todos los proveedores de servicios conocidos, incluir clasificaciones y designar un contacto empresarial para cada proveedor de servicios. Revisar y actualizar el inventario anualmente o cuando ocurran cambios importantes en la empresa que puedan afectar esta Salvaguarda.	N/A	Identificar			
15.2	Establecer y mantener una política de gestión de proveedores de servicios Establecer y mantener una política de gestión de proveedores de servicios. Asegúrese de que la política aborde la clasificación, el inventario, la evaluación, el seguimiento y el desmantelamiento de los proveedores de servicios. Revisar y actualizar la política anualmente, o cuando ocurran cambios importantes en la empresa que puedan afectar esta Salvaguarda.	N/A	Identificar			
15.3	Clasificar proveedores de servicios Clasificar a los proveedores de servicios. La consideración de la clasificación puede incluir una o más características, como la sensibilidad de los datos, el volumen de datos, los requisitos de disponibilidad, las regulaciones aplicables, el riesgo inherente y el riesgo mitigado. Actualizar y revisar las clasificaciones anualmente, o cuando se produzcan cambios significativos en la empresa que puedan afectar a esta Salvaguarda.	N/A	Identificar			

SALVAGUARDA	TÍTULO DE SALVAGUARDA/ DESCRIPCIÓN DE SALVAGUARDA	TIPO DE ACTIVO	FUNCIÓN DE SEGURIDAD	IG1	IG2	IG3
15.4	Asegúrese de que los contratos de los proveedores de servicios incluyan requisitos de seguridad Asegúrese de que los contratos del proveedor de servicios incluyan requisitos de seguridad. Los requisitos de ejemplo pueden incluir requisitos mínimos del programa de seguridad, notificación y respuesta de incidentes de seguridad y/o violación de datos, requisitos de cifrado de datos y compromisos de eliminación de datos. Estos requisitos de seguridad deben ser coherentes con la directiva de administración del proveedor de servicios de la empresa. Revisar los contratos de los proveedores de servicios anualmente para asegurarse de que los contratos no faltan requisitos de seguridad.	N/A	Proteger			
15.5	Evaluar proveedores de servicios Evaluar a los proveedores de servicios de acuerdo con la política de gestión de proveedores de servicios de la empresa. El alcance de la evaluación puede variar según la (s) clasificación (es) y puede incluir la revisión de informes de evaluación estandarizados, como el Control de la organización de servicio 2 (SOC 2) y la Certificación de cumplimiento (AoC) de la industria de tarjetas de pago (PCI), cuestionarios personalizados u otros procesos rigurosos. Reevaluar a los proveedores de servicios anualmente, como mínimo, o con contratos nuevos y renovados.	N/A	Identificar			
15.6	Supervisar proveedores de servicios Supervise a los proveedores de servicios de forma coherente con la directiva de administración de proveedores de servicios de la empresa. El monitoreo puede incluir reevaluación periódica del cumplimiento del proveedor de servicios, monitoreo de notas de la versión del proveedor de servicios y monitoreo de la web oscura.	Datos	Detectar			
15.7	Dar de baja de forma segura a los proveedores de servicios Desmantele de forma segura a los proveedores de servicios. Entre las consideraciones de ejemplo se incluyen la desactivación de cuentas de usuario y servicio, la terminación de flujos de datos y la eliminación segura de datos empresariales dentro de los sistemas de proveedores de servicios.	Datos	Proteger			

RESUMEN

Administrar el ciclo de vida de seguridad del software desarrollado, alojado o adquirido internamente para prevenir, detectar y corregir las debilidades de seguridad antes de que puedan afectar a la empresa.

¿Por qué es Crítico este Control?

Las aplicaciones proporcionan una interfaz amigable para los humanos que permite a los usuarios acceder y administrar los datos de una manera alineada con las funciones comerciales. También minimizan la necesidad de que los usuarios se ocupen directamente de funciones del sistema complejas (y potencialmente propensas a errores), cómo iniciar sesión en una base de datos para insertar o modificar archivos. Las empresas utilizan aplicaciones para administrar sus datos más confidenciales y controlar el acceso a los recursos del sistema. Por lo tanto, un atacante puede usar la aplicación en sí para comprometer los datos, en lugar de una elaborada secuencia de intrusión en el sistema y la red, intentando eludir los controles y sensores de seguridad de la red. Esta es la razón por la que proteger las credenciales de usuario (específicamente las credenciales de la aplicación) definidas en el Control CIS 6 son muy importantes.

Al carecer de credenciales, los defectos en las aplicaciones son el vector de ataque preferido. Sin embargo, las aplicaciones actuales se desarrollan, operan y mantienen en un entorno altamente complejo, diverso y dinámico. Las aplicaciones se ejecutan en múltiples plataformas: web, móvil, nube, etc., con arquitecturas de aplicaciones que son más complejas que las estructuras heredadas cliente-servidor o base de datos-servidor web. Los ciclos de vida de desarrollo se han acortado, pasando de meses o años en metodologías de cascada larga, a ciclos de DevOps con actualizaciones frecuentes de código. Además, las aplicaciones rara vez se crean desde cero y, a menudo, se “ensamblan” a partir de una combinación compleja de marcos de desarrollo, bibliotecas, código existente y código nuevo. También existen normativas de protección de datos modernas y en evolución que se ocupan de la privacidad del usuario. Estas pueden requerir el cumplimiento de los requisitos de protección de datos regionales o sectoriales específicos.

Estos factores hacen que los enfoques tradicionales de seguridad, como el control (de procesos, fuentes de código, entorno de tiempo de ejecución, etc.), la inspección y las pruebas, sean mucho más desafiantes. Además, es posible que no se comprenda el riesgo de que introduzca una vulnerabilidad de la aplicación, excepto en un contexto o entorno operativo específico.

Las vulnerabilidades de las aplicaciones pueden estar presentes por muchas razones: diseño inseguro, infraestructura insegura, errores de codificación, autenticación débil y falla al probar condiciones inusuales o inesperadas. Los atacantes pueden explotar vulnerabilidades específicas, que incluyen desbordamientos de búfer, exposición a inyección de lenguaje de consulta estructurado (SQL), secuencias de comandos entre sitios, falsificación de solicitudes entre sitios y clics de código para obtener acceso a datos confidenciales o tomar el control de activos vulnerables. dentro de la infraestructura como punto de lanzamiento para nuevos ataques.

Las aplicaciones y los sitios web también se pueden usar para recopilar credenciales, datos o intentar instalar malware en los usuarios que acceden a ellos.

Finalmente, ahora es más común adquirir plataformas de software como servicio (SaaS), donde el software se desarrolla y administra en su totalidad a través de un tercero. Estos pueden estar alojados en cualquier parte del mundo. Esto plantea desafíos a las empresas que necesitan saber qué riesgos están aceptando con el uso de estas plataformas; y, a menudo, no tienen visibilidad del desarrollo y las prácticas de seguridad de las aplicaciones de estas plataformas. Algunas de estas plataformas SaaS permiten personalizar sus interfaces y bases de datos. Las empresas que difunden el uso de soluciones de seguridad basadas en SaaS deben seguir este Control CIS, similar a si estuvieran haciendo un desarrollo de clientes desde cero.

Procedimientos y Herramientas

Para la versión 8, CIS se asoció con SAFECode para ayudar a desarrollar los procedimientos y las salvaguardas para este control de seguridad actualizado del software de la aplicación. Sin embargo, la seguridad del software de aplicación es un tema importante en sí mismo y, por lo tanto, (de acuerdo con los principios de los controles CIS generales), nos centramos aquí en las salvaguardas más críticas. Estos se derivaron de un documento complementario sobre la seguridad del software de aplicaciones que SAFECode desarrolló (al que se hace referencia a continuación), que proporciona un tratamiento más profundo del tema, y es consistente con el cuerpo de contenido existente de SAFECode.

SAFECode desarrolló un enfoque de tres niveles para ayudar a los lectores a identificar en qué Grupo de Desarrollo (DG) encajan como una escala de madurez para los programas de desarrollo. Los tres niveles de CIS IG utilizados en las Salvaguardas inspiraron su enfoque para las DG siguientes:

- **Grupo de Desarrollo 1:** La empresa depende en gran medida de software y paquetes listos para usar o de código abierto (OSS) con solo la adición ocasional de pequeñas aplicaciones o codificación de sitios web. La empresa es capaz de aplicar las mejores prácticas operativas y de procedimiento básicas y de administrar la seguridad de su software proporcionado por el proveedor como resultado de seguir la guía de los Controles CIS.
- **Grupo de Desarrollo 2:** La empresa se basa en algunas aplicaciones de código web y/o nativo personalizadas (desarrolladas por el contratista o desarrolladas por el contratista) integradas con componentes de terceros y se ejecuta en las instalaciones o en la nube. La empresa cuenta con un personal de desarrollo que aplica las mejores prácticas de desarrollo de software.
- **Grupo de Desarrollo 3:** La empresa realiza una importante inversión en software personalizado que requiere para ejecutar su negocio y servir a sus clientes. Puede alojar software en su propia infraestructura, en la nube o en ambos, y puede integrar una amplia gama de componentes de software comercial y de código abierto de terceros. Los proveedores de software y las empresas que ofrecen SaaS deben considerar el Grupo de Desarrollo 3 como un conjunto mínimo de requisitos.

El primer paso en el desarrollo de un programa de seguridad de aplicaciones es la implementación de un proceso de gestión de vulnerabilidades. Este proceso debe integrarse en el ciclo de vida de desarrollo y debe ser ligero para insertarlo en el progreso estándar de corrección de errores. El proceso debe incluir un análisis de la causa raíz para corregir fallas subyacentes a fin de reducir futuras vulnerabilidades, y una calificación de gravedad para priorizar los esfuerzos de remediación.

Los desarrolladores deben estar capacitados en conceptos de seguridad de aplicaciones y prácticas de codificación segura. Esto incluye un proceso para adquirir o evaluar software, módulos y bibliotecas de terceros utilizados en la aplicación para garantizar que no introduzcan fallas de seguridad. Se debe enseñar a los desarrolladores qué tipos de módulos

pueden usar de forma segura, dónde pueden adquirirse de manera segura y qué componentes pueden o no deben desarrollar ellos mismos (por ejemplo, cifrado).

Las debilidades en la infraestructura que soporta estas aplicaciones pueden presentar riesgos. Los controles CIS y el concepto de minimizar la superficie de ataque pueden ayudar a proteger las redes, los sistemas y las cuentas que se utilizan dentro de la aplicación. Puede encontrar orientación específica en los Controles CIS 1-7, 12 y 13.

El programa de seguridad de aplicaciones ideal es aquel que introduce la seguridad tan pronto como sea posible en el ciclo de vida del desarrollo de software. La gestión de los problemas de seguridad debe ser coherente e integrada con la gestión de errores y fallos de software estándar, en lugar de un proceso independiente que compita por los recursos de desarrollo. Los equipos de desarrollo más grandes o más maduros deben considerar la práctica del modelado de amenazas en la fase de diseño. Las vulnerabilidades de nivel de diseño son menos comunes que las vulnerabilidades de nivel de código; sin embargo, a menudo son muy graves y mucho más difíciles de solucionar rápidamente. El modelado de amenazas es el proceso de identificar y abordar las fallas de diseño de seguridad de las aplicaciones antes de que se cree el código. El modelado de amenazas requiere capacitación, conocimientos técnicos y comerciales específicos. Se lleva a cabo mejor a través de "campeones de seguridad" internos en cada equipo de desarrollo, para liderar las prácticas de modelado de amenazas para el software de ese equipo. También proporciona un contexto valioso para las actividades posteriores, como el análisis de la causa raíz y las pruebas de seguridad.

Los equipos de desarrollo más grandes o comerciales también pueden considerar un programa de recompensas por errores en el que se paga a las personas por encontrar fallas en sus aplicaciones. Un programa de este tipo se utiliza mejor para complementar un proceso de desarrollo seguro interno y puede proporcionar un mecanismo eficiente para identificar las clases de vulnerabilidades en las que el proceso debe centrarse.

Finalmente, en 2020, NIST® publicó su Marco de desarrollo de software seguro (SSDF), que reunió lo que la industria ha aprendido sobre la seguridad del software en las últimas dos décadas y creó un marco de desarrollo de software seguro para planificar, evaluar y comunicar sobre las actividades de seguridad del software. Las empresas que adquieren software o servicios pueden utilizar este marco para desarrollar sus requisitos de seguridad y comprender si el proceso de desarrollo de un proveedor de software sigue las mejores prácticas.

These are some application security resources:

- **SAFECode Application Security Addendum:** <https://safecode.org/cis-controls/>
- **NIST® SSDF:** <https://csrc.nist.gov/News/2020/mitigating-risk-of-software-vulns-ssdf>
- **The Software Alliance:** <https://www.bsa.org/reports/updated-bsa-framework-for-secure-software>
- **OWASP®:** <https://owasp.org/>

Salvaguardas

SALVAGUARDA	TÍTULO DE SALVAGUARDA/ DESCRIPCIÓN DE SALVAGUARDA	TIPO DE ACTIVO	FUNCIÓN DE SEGURIDAD	IG1	IG2	IG3
16.1	Establecer y mantener un proceso de desarrollo de aplicaciones seguro Establecer y mantener un proceso de desarrollo de aplicaciones seguro. En el proceso, aborde elementos tales como: estándares de diseño de aplicaciones seguras, prácticas de codificación segura, capacitación de desarrolladores, gestión de vulnerabilidades, seguridad de código de terceros y procedimientos de prueba de seguridad de aplicaciones. Revisar y actualizar la documentación anualmente, o cuando ocurran cambios importantes en la empresa que puedan afectar esta Salvaguarda.	Aplicaciones	Proteger		●	●
16.2	Establecer y mantener un proceso para aceptar y abordar las vulnerabilidades del software Establecer y mantener un proceso para aceptar y abordar los informes de vulnerabilidades de software, incluido el suministro de un medio para que las entidades externas informen. El proceso debe incluir elementos tales como: una política de manejo de vulnerabilidades que identifique el proceso de notificación, la parte responsable de manejar los informes de vulnerabilidad y un proceso de admisión, asignación, remediación y pruebas de remediación. Como parte del proceso, utilice un sistema de seguimiento de vulnerabilidades que incluya calificaciones de gravedad y métricas para medir el tiempo de identificación, análisis y corrección de vulnerabilidades. Revisar y actualizar la documentación anualmente, o cuando ocurran cambios importantes en la empresa que puedan afectar esta Salvaguarda. Los desarrolladores de aplicaciones de terceros deben considerar esta una política orientada externamente que ayuda a establecer expectativas para las partes interesadas externas	Aplicaciones	Proteger		●	●
16.3	Realice un análisis de la causa raíz de las vulnerabilidades de seguridad Realizar análisis de causa raíz sobre vulnerabilidades de seguridad. Al revisar las vulnerabilidades, el análisis de la causa raíz es la tarea de evaluar los problemas subyacentes que crean vulnerabilidades en el código y permite a los equipos de desarrollo ir más allá de simplemente corregir las vulnerabilidades individuales a medida que surgen.	Aplicaciones	Proteger		●	●
16.4	Establecer y administrar un inventario de componentes de software de terceros Establezca y administre un inventario actualizado de los componentes de terceros utilizados en el desarrollo, a menudo conocido como una "lista de materiales", así como los componentes programados para su uso futuro. Este inventario debe incluir cualquier riesgo que cada componente de terceros pueda plantear. Evalúe la lista al menos una vez al mes para identificar cualquier cambio o actualización de estos componentes y validar que el componente sigue siendo compatible	Aplicaciones	Proteger		●	●
16.5	Utilice componentes de software de terceros actualizados y confiables Utilice componentes de software de terceros actualizados y confiables. Cuando sea posible, elija marcos y bibliotecas establecidos y probados que brinden la seguridad adecuada. Acquire these components from trusted sources or evaluate the software for vulnerabilities before use.	Aplicaciones	Proteger		●	●
16.6	Establecer y mantener un sistema y proceso de clasificación de gravedad para las vulnerabilidades de las aplicaciones Establecer y mantener un sistema de clasificación de gravedad y un proceso para las vulnerabilidades de las aplicaciones que facilite la priorización del orden en que se corrigen las vulnerabilidades detectadas. Este proceso incluye establecer un nivel mínimo de aceptabilidad de seguridad para liberar código o aplicaciones. Las clasificaciones de gravedad aportan una forma sistemática de evaluar las vulnerabilidades que mejora la gestión de riesgos y ayuda a garantizar que los errores más graves se solucionen primero. Revisar y actualizar el sistema y el proceso anualmente.	Aplicaciones	Proteger		●	●
16.7	Usar plantillas de configuración de protección estándar para la infraestructura de aplicaciones Utilice plantillas de configuración de protección estándar recomendadas por la industria para los componentes de la infraestructura de aplicaciones. Esto incluye servidores subyacentes, bases de datos y servidores web, y se aplica a contenedores en la nube, componentes de plataforma como servicio (PaaS) y componentes SaaS. No permita que el software desarrollado internamente debilite el endurecimiento de la configuración.	Aplicaciones	Proteger		●	●
16.8	Sistemas de producción separados y sistemas de no producción Mantener entornos separados para sistemas de producción y no de producción.	Aplicaciones	Proteger		●	●
16.9	Capacitar a los desarrolladores en conceptos de seguridad de aplicaciones y codificación segura Asegúrese de que todo el personal de desarrollo de software reciba capacitación en la escritura de código seguro para su entorno de desarrollo y responsabilidades específicas. La capacitación puede incluir principios generales de seguridad y prácticas estándar de seguridad de aplicaciones. Realizar capacitaciones al menos una vez al año y diseñar de manera que se promueva la seguridad dentro del equipo de desarrollo y crear una cultura de seguridad entre los desarrolladores.	Aplicaciones	Proteger		●	●

SALVAGUARDA	TÍTULO DE SALVAGUARDA/ DESCRIPCIÓN DE SALVAGUARDA	TIPO DE ACTIVO	FUNCIÓN DE SEGURIDAD	IG1	IG2	IG3
16.10	Aplicar principios de diseño seguro en arquitecturas de aplicaciones Aplicar principios de diseño seguro en arquitecturas de aplicaciones. Los principios de diseño seguro incluyen el concepto de privilegio mínimo y la aplicación de la mediación para validar cada operación que realiza el usuario, promoviendo el concepto de "nunca confiar en la entrada del usuario". Los ejemplos incluyen asegurarse de que se realice y documente la verificación explícita de errores para todas las entradas, incluido el tamaño, el tipo de datos y los rangos o formatos aceptables. El diseño seguro también significa minimizar la superficie de ataque de la infraestructura de la aplicación, como apagar los puertos y servicios desprotegidos, eliminar programas y archivos innecesarios y cambiar el nombre o eliminar las cuentas predeterminadas.	Aplicaciones	Proteger			
16.11	Aprovechar los módulos o servicios examinados para los componentes de seguridad de las aplicaciones Aproveche los módulos o servicios examinados para los componentes de seguridad de las aplicaciones, como la administración de identidades, el cifrado y la auditoría y el registro.	Aplicaciones	Proteger			
16.12	Implementar verificaciones de seguridad a nivel de código Aplique herramientas de análisis estático y dinámico dentro del ciclo de vida de la aplicación para comprobar que se siguen las prácticas de codificación seguras.	Aplicaciones	Proteger			
16.13	Realizar pruebas de penetración de aplicaciones Realice pruebas de penetración de aplicaciones. Para aplicaciones críticas, las pruebas de penetración autenticadas son más adecuadas para encontrar vulnerabilidades de lógica empresarial que el escaneo de código y las pruebas de seguridad automatizadas. Las pruebas de penetración se basan en la habilidad del evaluador para manipular manualmente una aplicación como un usuario autenticado y no autenticado.	Aplicaciones	Proteger			
16.14	Realizar modelado de amenazas Realice modelos de amenazas. El modelado de amenazas es el proceso de identificar y abordar las fallas de diseño de seguridad de las aplicaciones dentro de un diseño, antes de que se cree el código. Se lleva a cabo a través de personas especialmente capacitadas que evalúan el diseño de la aplicación y miden los riesgos de seguridad para cada punto de entrada y nivel de acceso. El objetivo es mapear la aplicación, la arquitectura y la infraestructura de una manera estructurada para comprender sus debilidades.	Aplicaciones	Proteger			

RESUMEN

Establecer un programa para desarrollar y mantener una capacidad de respuesta a incidentes (por ejemplo, políticas, planes, procedimientos, roles definidos, capacitación y comunicaciones) para preparar, detectar y responder rápidamente a un ataque.

¿Por qué es Crítico este Control?

Un programa integral de ciberseguridad incluye capacidades de protección, detección, respuesta y recuperación. A menudo, los dos últimos se pasan por alto en empresas inmaduras, o la técnica de respuesta a los sistemas comprometidos es simplemente volver a crear una imagen de ellos a su estado original y seguir adelante. El objetivo principal de la respuesta a incidentes es identificar las amenazas en la empresa, responder a ellas antes de que se propaguen y remediarlas antes de que puedan causar daños. Sin comprender el alcance total de un incidente, cómo sucedió y qué se puede hacer para evitar que vuelva a suceder, los defensores estarán en un patrón perpetuo de "golpee al topo".

No podemos esperar que nuestras protecciones sean efectivas el 100% del tiempo. Cuando ocurre un incidente, si una empresa no tiene un plan documentado, incluso con buenas personas, es casi imposible conocer los procedimientos de investigación, informes, recopilación de datos, responsabilidad de gestión, protocolos legales y estrategia de comunicaciones correctas que permitirán a la empresa comprender, gestionar y recuperar con éxito.

Junto con la detección, la contención y la erradicación, la comunicación con las partes interesadas es clave. Si queremos reducir la probabilidad de impacto material debido a un evento cibernético, el liderazgo de la empresa debe saber qué impacto potencial podría haber, para que puedan ayudar a priorizar las decisiones de remediación o restauración que mejor apoyen a la empresa. Estas decisiones de negocios podrían basarse en el cumplimiento de normas, las reglas de divulgación, los acuerdos de nivel de servicio con socios o clientes, los ingresos o los impactos de la misión.

El tiempo de permanencia desde que ocurre un ataque hasta que se identifica puede ser de días, semanas o meses. Cuanto más tiempo esté el atacante en la infraestructura de la empresa, más integrado estará y desarrollará más formas de mantener el acceso persistente para cuando finalmente se lo descubra. Con el auge del ransomware, que es un generador de dinero estable para los atacantes, este tiempo de permanencia es crítico, especialmente con las tácticas modernas de robar datos antes de cifrarlos para obtener un rescate.

Procedimientos y Herramientas

Incluso si una empresa no tiene recursos para llevar a cabo la respuesta a incidentes dentro de una empresa, sigue siendo fundamental tener un plan. Esto incluiría las fuentes de protección y detecciones, una lista de a quién recurrir para obtener asistencia y planes de comunicación sobre cómo transmitir información a los líderes, empleados, reguladores, socios y clientes.

Después de definir los procedimientos de respuesta a incidentes, el equipo de respuesta a incidentes, o un tercero, debe participar en una capacitación periódica basada en escenarios, trabajando a través de una serie de escenarios de ataque ajustados a las amenazas y los

impactos potenciales que enfrenta la empresa. Estos escenarios ayudan a garantizar que los miembros del equipo técnico y de liderazgo empresarial comprendan su papel en el proceso de respuesta a incidentes para ayudarles a prepararse para controlar los incidentes. Es inevitable que los escenarios de ejercicio y entrenamiento identifiquen brechas en los planes y procesos, y dependencias inesperadas, que luego se pueden actualizar en el plan.

Las empresas más maduras deben incluir inteligencia de amenazas y/o búsqueda de amenazas en su proceso de respuesta a incidentes. Esto ayudará al equipo a ser más proactivo, identificando a los atacantes clave o principales de su empresa o industria para monitorear o buscar sus TTPs. Esto ayudará a enfocar las detecciones y definir procedimientos de respuesta para identificar y corregir más rápidamente.

Las acciones en el ControloCIS 17 proporcionan pasos específicos de alta prioridad que pueden mejorar la seguridad empresarial y deben ser parte de cualquier plan integral de respuesta e incidentes. Además, recomendamos el siguiente recurso dedicado a este tema:

→ **Consejo de Probadores de Seguridad Registrados (CREST) Guía de respuesta a incidentes de seguridad cibernética:** CREST proporciona guías, estándares y conocimientos sobre una amplia variedad de temas de defensa cibernética. <https://www.crest-approved.org/wp-content/uploads/2014/11/CSIR-Procurement-Guide.pdf>

Salvaguardas

SALVAGUARDA	TÍTULO DE SALVAGUARDA/ DESCRIPCIÓN DE SALVAGUARDA	TIPO DE ACTIVO	FUNCIÓN DE SEGURIDAD	IG1	IG2	IG3
17.1	Designar personal para administrar el manejo de incidentes Diseñe una persona clave, y al menos una persona como respaldo, que gestionará el proceso de gestión de incidentes de la empresa. El personal de administración es responsable de la coordinación y documentación de la respuesta a incidentes y los esfuerzos de recuperación y puede consistir en empleados internos de la empresa, proveedores externos o un enfoque híbrido. Si utiliza un proveedor externo, designe al menos una persona interna de la empresa para supervisar cualquier trabajo de terceros. Revise anualmente o cuando ocurran cambios importantes en la empresa que puedan afectar esta protección.	N/A	Responder	●	●	●
17.2	Establecer y mantener información de contacto para informar incidentes de seguridad Establecer y mantener la información de contacto de las partes que necesitan ser informadas de incidentes de seguridad. Los contactos pueden incluir personal interno, proveedores externos, fuerzas del orden, proveedores de seguros cibernéticos, agencias gubernamentales relevantes, socios del Centro de Intercambio y Análisis de Información (ISAC) u otras partes interesadas. Verificar los contactos anualmente para asegurarse de que la información está actualizada.	N/A	Responder	●	●	●
17.3	Establecer y mantener un proceso empresarial para informar de incidentes Establezca y mantenga un proceso de la empresa para que la plana laboral informe de incidentes de seguridad. El proceso incluye el plazo de presentación de informes, el personal al que informar, el mecanismo de presentación de informes y la información mínima que se debe informar. Asegúrese de que el proceso esté disponible públicamente para toda la plana laboral. Revisar esta salvaguarda anualmente, o cuando se produzcan cambios significativos en la empresa que puedan afectar a esta Salvaguarda.	N/A	Responder	●	●	●
17.4	Establecer y mantener un proceso de respuesta a incidentes Establezca y mantenga un proceso de respuesta a incidentes que aborde los roles y responsabilidades, los requisitos de cumplimiento y un plan de comunicación. Revise anualmente o cuando ocurran cambios importantes en la empresa que puedan afectar esta salvaguarda.	N/A	Responder		●	●
17.5	Asignar Roles Claves y Responsabilidades Asigne roles claves y responsabilidades responder a incidentes, incluido el personal de legal, TI, seguridad de la información, instalaciones, relaciones públicas, recursos humanos, personal de respuesta a incidentes y analistas, según corresponda. Revise esta salvaguarda anualmente o cuando ocurran cambios importantes en la empresa que puedan afectar esta protección.	N/A	Responder		●	●
17.6	Definir mecanismos de comunicación durante la respuesta a incidentes Determine qué mecanismos principales y secundarios se usarán para comunicarse e informar durante un incidente de seguridad. Los mecanismos pueden incluir llamadas telefónicas, correos electrónicos o cartas. Tenga en cuenta que ciertos mecanismos, como los correos electrónicos, pueden verse afectados durante un incidente de seguridad. Revisar anualmente, o cuando se produzcan cambios significativos en la empresa que puedan afectar a esta Salvaguarda.	N/A	Responder		●	●

SALVAGUARDA	TÍTULO DE SALVAGUARDA/ DESCRIPCIÓN DE SALVAGUARDA	TIPO DE ACTIVO	FUNCIÓN DE SEGURIDAD	IG1	IG2	IG3
17.7	Realizar ejercicios rutinarios de respuesta a incidentes Planifique y lleve a cabo ejercicios y escenarios de respuesta a incidentes de rutina para el personal clave involucrado en el proceso de respuesta a incidentes a fin de prepararse para responder a incidentes del mundo real. Los ejercicios deben probar los canales de comunicación, la toma de decisiones y los flujos de trabajo. Realice pruebas anualmente, como mínimo.	N/A	Recuperar			
17.8	Realizar revisiones posteriores a un incidente Realice revisiones posteriores al incidente. Las revisiones posteriores al incidente ayudan a prevenir la repetición del incidente mediante la identificación de lecciones aprendidas y acciones de seguimiento.	N/A	Recuperar			
17.9	Establecer y mantener umbrales de incidentes de seguridad Establezca y mantenga umbrales de incidentes de seguridad, incluyendo, como mínimo, la diferenciación entre un incidente y un evento. Los ejemplos pueden incluir: actividad anormal, vulnerabilidad de seguridad, debilidad de seguridad, violación de datos, incidente de privacidad, etc. Revisar anualmente, o cuando se produzcan cambios significativos en la empresa que puedan afectar a esta Salvaguardia.	N/A	Recuperar			

RESUMEN

Pruebe la eficacia y la resistencia de los activos empresariales mediante la identificación y explotación de debilidades en los controles (personas, procesos y tecnología) y la simulación de los objetivos y acciones de un atacante.

¿Por qué es Crítico este Control?

Una postura defensiva exitosa requiere un programa integral de políticas y gobernanza efectivas, defensas técnicas sólidas, combinadas con una acción apropiada de las personas. Sin embargo, rara vez es perfecto. En un entorno complejo donde la tecnología está en constante evolución y aparecen regularmente atacantes que realizan nuevos tipos de ataques, las empresas deben probar periódicamente sus controles para identificar brechas y evaluar su capacidad de recuperación. Esta prueba puede ser desde la perspectiva de una red externa, una red interna, una aplicación, un sistema o un dispositivo. Puede incluir ingeniería social de usuarios o derivaciones de control de acceso físico. A menudo, las pruebas de penetración se realizan con fines específicos.:

- Como una demostración “dramática” de un ataque, generalmente para convencer a los responsables de toma de decisiones de las debilidades de su empresa
- Como medio para probar el correcto funcionamiento de las defensas empresariales (“verificación”)
- Para probar que la empresa ha construido las defensas adecuadas en primer lugar (“validación”)

Las pruebas de penetración independientes pueden proporcionar información valiosa y objetiva sobre la existencia de vulnerabilidades en los activos de la empresa y los seres humanos, y la eficacia de las defensas y los controles de mitigación para proteger contra los impactos adversos a la empresa. Forman parte de un programa integral y continuo de gestión y mejora de la seguridad. También pueden revelar debilidades del proceso, como una administración de configuración incompleta o inconsistente, o capacitación del usuario final

Las pruebas de penetración difieren de las pruebas de vulnerabilidad, descritas en los Controles CIS v7. Las pruebas de vulnerabilidad sólo comprueban la presencia de activos empresariales conocidos e inseguros, y se detienen allí. Las pruebas de penetración van más allá para explotar esas debilidades para ver hasta dónde puede llegar un atacante y qué proceso de negocio o datos podrían verse afectados por la explotación de esa vulnerabilidad. Este es un detalle importante, y a menudo las pruebas de penetración y las pruebas de vulnerabilidad se usan de forma incorrecta indistintamente. Las pruebas de vulnerabilidad son exclusivamente escaneo automatizado con validación a veces manual de falsos positivos, mientras que las pruebas de penetración requieren más participación y análisis humanos, a veces apoyados por el uso de herramientas o scripts personalizados. Sin embargo, las pruebas de vulnerabilidad suelen ser un punto de partida para una prueba de penetración.

Otro término común son los ejercicios de Equipo Rojo “Red Team”. Son similares a las pruebas de penetración en el sentido de que se explotan las vulnerabilidades; sin embargo, la diferencia es el enfoque. Los Red Teams simulan tácticas, técnicas y procedimientos de atacantes específicos para evaluar cómo el entorno de una empresa resistiría un ataque de un adversario específico o una categoría de adversarios.

Procedimientos y Herramientas

Las pruebas de penetración comienzan con el reconocimiento de la empresa y el entorno, y el escaneo para identificar las vulnerabilidades que se pueden usar como entradas a la empresa. Es importante asegurarse de que se descubran todos los activos de la empresa que están dentro del alcance, y no solo depender de una lista estática, que puede estar desactualizada o incompleta. A continuación, se identificarán las vulnerabilidades en estos objetivos. Los exploits de estas vulnerabilidades se ejecutan para demostrar específicamente cómo un adversario puede perturbar los objetivos de seguridad de la empresa (p. Ej., La protección de datos confidenciales específicos) o lograr objetivos adversarios específicos (p. Ej., El establecimiento de una infraestructura encubierta de Comando y Control (C2)). Los resultados proporcionan una visión más profunda, a través de la demostración, de los riesgos comerciales de varias vulnerabilidades. Estos pueden ser probados contra los controles de acceso físico, la red, el sistema o las capas de aplicación y, a menudo, incluye componentes de ingeniería social.

Las pruebas de penetración son caras, complejas y potencialmente presentan sus propios riesgos. Las personas con experiencia de ser proveedores de buena reputación deben llevarlos a cabo. Algunos riesgos incluyen el apagado inesperado de sistemas que podrían ser inestables, exploits que podrían eliminar o dañar datos o configuraciones, y la salida de un informe de prueba que debe protegerse, ya que brinda instrucciones paso a paso sobre cómo ingresar la empresa para apuntar a activos o datos críticos.

Cada empresa debe definir un alcance claro y reglas de compromiso para las pruebas de penetración. El alcance de estos proyectos debe incluir, como mínimo, activos empresariales con la información de mayor valor y funcionalidad de procesamiento de producción. Otros sistemas de menor valor también se pueden probar para ver si se pueden utilizar como puntos de apoyo para comprometer objetivos de mayor valor. Las reglas de compromiso para los análisis de pruebas de penetración deben describir, como mínimo, las horas del día para las pruebas, la duración de las pruebas y el enfoque general de la prueba. Sólo unas pocas personas en la empresa deben saber cuándo se realiza una prueba de penetración, y se debe designar un punto de contacto principal en la empresa si se producen problemas. Recientemente, es cada vez más popular realizar pruebas de penetración a través de un asesor legal externo para proteger el informe de la prueba de penetración de la divulgación.

Las Salvaguardas en este Control CIS proporcionan pasos específicos de alta prioridad que pueden mejorar la seguridad empresarial y deben ser parte de cualquier prueba de penetración. Además, recomendamos el uso de algunos de los excelentes recursos integrales dedicados a este tema para respaldar la planificación, la gestión y la generación de informes de las 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

Salvaguardas

SALVAGUARDA	TÍTULO DE SALVAGUARDA/ DESCRIPCIÓN DE SALVAGUARDA	TIPO DE ACTIVO	FUNCIÓN DE SEGURIDAD	IG1	IG2	IG3
18.1	Establecer y mantener un programa de pruebas de penetración Establezca y mantenga un programa de pruebas de penetración adecuado al tamaño, complejidad y madurez de la empresa. Las características del programa de pruebas de penetración incluyen el alcance, como la red, la aplicación web, la interfaz de programación de aplicaciones (API), los servicios alojados y los controles de las instalaciones físicas; frecuencia; limitaciones, como horas aceptables y tipos de ataques excluidos; información del punto de contacto; remediación, como la forma en que los hallazgos se enrutarán internamente; y requisitos retrospectivos.	N/A	Identificar			
18.2	Realizar pruebas periódicas de penetración externa Realice pruebas de penetración externas periódicas basadas en los requisitos del programa, no menos de una vez al año. Las pruebas de penetración externas deben incluir reconocimiento empresarial y ambiental para detectar información explotable. Las pruebas de penetración requieren habilidades y experiencia especializadas y deben realizarse a través de una organización calificada. La prueba puede ser caja blanca o caja gris.	Red	Identificar			
18.3	Corregir los resultados de la prueba de penetración Repare los hallazgos de las pruebas de penetración según la política de la empresa para el alcance y la priorización de la remediación.	Red	Proteger			
18.4	Valide las medidas de seguridad Valide las medidas de seguridad después de cada prueba de penetración. Si lo considera necesario, modifique los conjuntos de reglas y las capacidades para detectar las técnicas utilizadas durante las pruebas.	Red	Proteger			
18.5	Realice pruebas periódicas de penetración interna Realice pruebas de penetración internas periódicas basadas en los requisitos del programa, no menos de una vez al año. La prueba puede ser caja blanca o caja gris.	N/A	Identificar			

Recursos y Referencias

CIS Benchmarks™ Program: <http://www.cisecurity.org/cis-benchmarks/>

CIS Controls Cloud Companion Guide: <https://www.cisecurity.org/controls/v8/>

CIS Community Defense Model (CDM): <https://www.cisecurity.org/controls/v8/>

CIS Configuration Assessment Tool (CIS-CAT®): <https://learn.cisecurity.org/cis-cat-lite>

CIS Controls Assessment Specification: <https://controls-assessment-specification.readthedocs.io/en/latest/>

CIS Controls Implementation Groups: <https://www.cisecurity.org/controls/v8/>

CIS Controls Industrial Control Systems Implementation Guide: <https://www.cisecurity.org/controls/v8/>

CIS Controls Internet of Things Companion Guide: <https://www.cisecurity.org/controls/v8/>

CIS Controls Mobile Companion Guide: <https://www.cisecurity.org/controls/v8/>

CIS Risk Assessment Method (RAM): <https://www.cisecurity.org/controls/v8/>

CIS Controls Self Assessment Tool (CSAT): <https://www.cisecurity.org/blog/cis-csat-free-tool-assessing-implementation-of-cis-controls/>

CIS Controls Telework and Small Office Network Security Guide: <https://www.cisecurity.org/controls/v8/>

CIS Password Policy Guide: <https://www.cisecurity.org/white-papers/cis-password-policy-guide/>

Cloud Security Alliance (CSA): <https://cloudsecurityalliance.org/>

Council of Registered Security Testers (CREST) Cyber Security Incident Response Guide - CREST provides guidance, standards, and knowledge on a wide variety of cyber defense topics: <https://www.crest-approved.org/wp-content/uploads/2014/11/CSIR-Procurement-Guide.pdf>

EDUCAUSE: <https://www.educause.edu/focus-areas-and-initiatives/policy-and-security/cybersecurity-program/awareness-campaigns>

International Organization for Standardization: <https://www.iso.org/home.html>

National Cyber Security Centre (U.K.): <https://www.ncsc.gov.uk/guidance/10-steps-user-education-and-awareness>

National Institute of Standards and Technology (NIST®): <https://www.nist.gov/>

National Institute of Standards and Technology (NIST®) SSDF: <https://csrc.nist.gov/News/2020/mitigating-risk-of-software-vulns-ssdf>

National Institute of Standards and Technology (NIST®) National Checklist Program Repository: <https://nvd.nist.gov/ncp/repository>

National Institute of Standards and Technology (NIST®) Digital Identity Guidelines: <https://pages.nist.gov/800-63-3/>

National Institute of Standards and Technology (NIST®) FIPS 140-2: <https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.140-2.pdf>

National Institute of Standards and Technology (NIST®) FIPS 140-3: <https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.140-3.pdf>

National Institute of Standards and Technology (NIST®) SP 800-50 Infosec Awareness Training: <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-50.pdf>

National Institute of Standards and Technology (NIST®) SP 800-88r1 - Guidelines for Media Sanitization: <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf>

National Cyber Security Alliance (NCSA): <https://staysafeonline.org/>

OWASP®: <https://owasp.org/>

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

SANS: <https://www.sans.org/security-awareness-training/resources>

SAFECode Application Security Addendum: <https://safecode.org/cis-controls/>

National Institute of Standards and Technology (NIST®) SP 800-126r3 The Technical Specification for the Security Content Automation Protocol (SCAP): <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-126r3.pdf>

The Software Alliance: <https://www.bsa.org/reports/updated-bsa-framework-for-secure-software>

Verizon Data Breach Investigations Report: <https://enterprise.verizon.com/resources/reports/2020-data-breach-investigations-report.pdf>

Controles y Salvaguarda

CONTROL 01 / SALVAGUARDA 1.1 — CONTROL 02

CONTROL	TÍTULO DE CONTROL	TÍTULO DE SALVAGUARDA/ DESCRIPCIÓN DE SALVAGUARDA	TIPO DE ACTIVO	FUNCIÓN DE SEGURIDAD	IG1	IG2	IG3
01	Inventario y Control de los Activos Empresariales						
	1.1	Establecer y Mantener un Detallado Inventario de Activos Empresariales	Dispositivos	Identificar	●	●	●
		Establecer y mantener un inventario preciso, detallado y actualizado de todos los activos de la empresa con el potencial de almacenar o procesar datos, para incluir: dispositivos de usuarios finales (incluidos portátiles y móviles), dispositivos de red, no informáticos IoT y servidores. Asegúrese de que el inventario registre la dirección de red (si es estática), la dirección de la máquina, el propietario del activo de datos, el departamento de cada activo y si el activo ha sido aprobado para conectarse a la red. Para los dispositivos móviles de usuario final, las herramientas tipo MDM pueden admitir este proceso, cuando corresponda. Este inventario incluye activos conectados a la infraestructura física, virtual, remotamente y aquellos de entornos de la nube. Adicionalmente, incluye activos que están conectados regularmente a la infraestructura de red de la empresa, incluso si no están bajo el control de la empresa. Revisar y actualizar el inventario de todos los activos de la empresa cada dos años o con mayor frecuencia.					
	1.2	Gestionar Activos no Autorizados	Dispositivos	Responder	●	●	●
		Asegúrese de que exista un proceso para abordar los activos no autorizados semanalmente. La empresa puede optar por eliminar el activo de la red, negar que el activo se conecte de forma remota a la red o poner en cuarentena el activo.					
02	1.3	Utilice una herramienta de descubrimiento activo	Dispositivos	Detectar		●	●
		Utilice una herramienta de descubrimiento activa para identificar activos conectados a la red empresarial. Configure la herramienta de descubrimiento activo para ejecutar diariamente o con más frecuencia.					
	1.4	Utilice el registro de la configuración de dinámica de host (DHCP) para actualizar el inventario de activos	Dispositivos	Identificar		●	●
		Utilice el registro DHCP en todos los servidores o las herramientas de administración de direcciones de protocolo de internet (IP) para actualizar el inventario de activos de la empresa. Revise y use los registros para actualizar semanalmente el inventario de activos de la empresa o con mayor frecuencia.					
	1.5	Utilice una herramienta de descubrimiento de activos pasivo	Dispositivos	Detectar			●
		Utilice una herramienta de descubrimiento pasivo para identificar activos conectados a la red empresarial. Revise y utilice escaneos para actualizar el inventario de activos de la empresa al menos semanalmente o con más frecuencia.					
	Inventario y Control de Activos de Software						
	2.1	Elaborar y Mantener actualizado el inventario de software	Aplicaciones	Identificar	●	●	●
		Elabore y mantenga un inventario detallado de todas las licencias de software instalados en los activos de la empresa. El inventario de software debe documentar el título, el fabricante, la fecha de instalación inicial y el propósito para cada activo, cuando corresponda, incluya la dirección URL, las tiendas de aplicaciones, versiones, mecanismo de implementación y fecha de retirada.					
	2.2	Asegurarse de que el software autorizado cuente con soporte	Aplicaciones	Identificar	●	●	●
		Asegúrese de que únicamente el software con soporte actual del fabricante esté designado como autorizado en el inventario de software de activos empresariales. Si el software ya no se encuentra soportado por el fabricante, pero es necesario para el cumplimiento de la misión de la empresa, documente una excepción que detalle los controles de mitigación y la aceptación del riesgo residual. Para cualquier software sin soporte, sin una documentación de excepción, identificarla como no autorizada. Revise la lista de software para comprobar el soporte del software por lo menos una vez al mes o con más frecuencia.					
	2.3	Tratamiento del Software no Autorizado	Aplicaciones	Responder	●	●	●
		Asegúrese de que el software no autorizado sea removido de los activos de la empresa o ante evidencias de instalaciones no autorizadas el evento cuente con una excepción documentada. Realice este paso mensualmente o con más frecuencia.					

CONTROL	TÍTULO DE CONTROL	TÍTULO DE SALVAGUARDA/ DESCRIPCIÓN DE SALVAGUARDA	TIPO DE ACTIVO	FUNCIÓN DE SEGURIDAD	IG1	IG2	IG3
2.4	Utilice herramientas automatizadas de inventario de software	Utilizar herramientas de inventario de software, cuando sea posible, en toda la empresa para automatizar la detección y documentación del software instalado.	Aplicaciones	Detectar			
2.5	Use Lista de permitidos Para Software Autorizados	Utilice controles técnicos, como lista de aplicaciones permitidas, para asegurarse de que solo se pueda ejecutar o acceder al software autorizado. Reevaluar semestralmente o con más frecuencia.	Aplicaciones	Proteger			
2.6	Lista de Librerías Autorizadas	Utilice controles técnicos para garantizar que solo las bibliotecas de software actual. Bloquee la carga de bibliotecas no autorizadas en los procesos del sistema. Reevalúe semestralmente o con más frecuencia.	Aplicaciones	Proteger			
2.7	Use Lista de permitidos Para secuencias de comandos Autorizados	Utilice controles técnicos, como firmas digitales y control de versiones, para asegurarse de que los scripts autorizados, específicos como los .ps1, .py, etc., archivos, estén permitidos para ejecutarse. Bloquear los scripts no autorizados para ejecutarse. Reevalúe semestralmente o con más frecuencia.	Aplicaciones	Proteger			

03 Protección de los Datos

Desarrollar procesos y controles técnicos para identificar, clasificar, manejar, retener y eliminar de forma segura los datos.

3.1	Establecer y mantener un proceso de gestión de datos	Establecer y mantener un proceso de gestión de datos. Durante el proceso, Ubicación de los datos sensibles, propietario de los datos, Tratamiento de los datos, límites de la retención de datos, y requisitos de eliminación, basados en la sensibilidad y estándares de retención para la empresa. Revise y actualice la documentación anualmente, o cuando ocurran cambios significativos en la empresa que pudieran impactar en esta salvaguardia.	Datos	Identificar			
3.2	Establecer y Mantener un inventario de Datos	Establecer y mantener un inventario de datos, basados en el proceso de gestión de datos de la empresa. Inventario de datos sensibles, como mínimo. Revise y actualice el inventario anualmente, como mínimo, con prioridad sobre los datos sensibles.	Datos	Identificar			
3.3	Configure listas de control de acceso a datos	Configurar listas de control de acceso a datos en función de la necesidad de conocimiento de un usuario. Aplicar listas de control de acceso a datos, también conocidas como permisos de acceso, a sistemas de archivos, bases de datos y aplicaciones locales y remotas.	Datos	Proteger			
3.4	Aplicar retención de datos	Retener los datos de acuerdo con el proceso de gestión de datos de la empresa. La retención de datos debe incluir plazos mínimos y máximos.	Datos	Proteger			
3.5	Eliminar de forma segura los datos	Elimine de forma segura como se describe en el proceso de gestión de datos empresariales. Asegúrese de que el proceso y el método de eliminación sean acordes con la confidencialidad de los datos.	Datos	Proteger			
3.6	Cifrar datos en dispositivos de usuarios	Encriptar los datos en los dispositivos de los usuarios que contienen datos sensibles. Un ejemplo de implementación puede incluir: Windows BitLocker®, Apple FileVault®, Linux® dm-crypt.	Dispositivos	Proteger			
3.7	Establecer y mantener un esquema de clasificación de datos	Establecer y mantener un esquema general de clasificación de datos para la empresa. En las empresas pueden usar etiquetas, como "sensible," "Confidencial," y "Público," y clasificar sus datos de acuerdo a esas etiquetas. Revise y actualice el esquema de clasificación anualmente, o cuando suceda algún cambio significativo en la empresa que pueda tener impacto sobre esta Salvaguardia.	Datos	Identificar			
3.8	Documentar el Flujo de datos	Documente el flujo de datos. La documentación del flujo de datos incluye los flujos de datos del proveedor de servicios y debe basarse en el proceso de gestión de datos de la empresa. Revise y actualice la documentación anualmente, o cuando ocurran cambios significativos en la empresa que puedan impactar esta Salvaguardia.	Datos	Identificar			
3.9	Cifrar datos en medios extraíbles	Cifre los datos en los dispositivos extraíbles.	Datos	Proteger			
3.10	Cifre los datos confidenciales en tránsito	Cifre los datos confidenciales en tránsito. Ejemplos de implementación incluyen: Transport Layer Security (TLS) y Open Secure Shell (OpenSSH).	Datos	Proteger			

CONTROL	TÍTULO DE CONTROL	TÍTULO DE SALVAGUARDA/ DESCRIPCIÓN DE SALVAGUARDA	TIPO DE ACTIVO	FUNCIÓN DE SEGURIDAD	IG1	IG2	IG3
3.11	Cifrar los datos confidenciales en reposo	Cifre los datos confidenciales que se encuentran en reposo en servidores, aplicaciones y bases de datos que contengan datos confidenciales. El cifrado de la capa de almacenamiento, también conocido como cifrado del lado del servidor, cumple con el requisito mínimo de esta Salvaguardia. Métodos de cifrado adicionales pueden incluir el cifrado del lado del cliente, también conocido como cifrado del lado del cliente, donde el acceso a los dispositivos de almacenamiento de datos no permite el acceso a los datos de texto sin formato.	Datos	Proteger			
3.12	Segmentar el procesamiento y almacenamiento de datos en función de la sensibilidad	Segmentar el procesamiento y almacenamiento de datos en función de la sensibilidad. No procesar datos confidenciales en activos empresariales destinados a datos de menor sensibilidad.	Red	Proteger			
3.13	Desplegar una solución de Prevención de Pérdida de Datos	Implemente una herramienta automatizada, como una herramienta de prevención de pérdida de datos (DLP) basada en host para identificar todos los datos confidenciales almacenados, procesados, transmitidos a través de los activos de la empresa, incluidos lo que se encuentran en el sitio o en un proveedor de servicios remoto, y actualizar el inventario de datos confidenciales de la empresa.	Datos	Proteger			
3.14	Registre de acceso a datos confidenciales	Registre el acceso a los datos, incluidos modificación y eliminación.	Datos	Detectar			

04 Configuración Segura de Activos y Software Empresarial

Establecer y mantener la configuración segura de los activos empresariales (Dispositivos de usuarios, incluidos portátiles y móviles; dispositivos de red; dispositivos no informáticos/IoT; y servidores) y software (Sistemas operativos y aplicaciones).

4.1	Establecer y Mantener un Proceso de configuración seguro	Establecer y mantener un proceso seguro de la configuración para los activos de la empresa (dispositivos de usuarios, incluidos portátiles y móviles; dispositivos no informáticos/IoT; and servers) y software (Sistemas operativos y aplicaciones). Revise y actualice la documentación anualmente, o cuando ocurran cambios significativos en la empresa que puedan causar un impacto a esta salvaguardia.	Aplicaciones	Proteger			
4.2	Establecer y mantener un proceso de configuración seguro para la infraestructura de red	Establecer y mantener un proceso de configuración seguro para dispositivos de red. Revisar y actualizar la documentación anualmente, o cuando ocurran cambios importantes en la empresa que puedan afectar esta salvaguardia.	Red	Proteger			
4.3	Configurar el bloqueo automático de sesiones en activos empresariales	Configurar el bloqueo automático de sesiones en los activos de la empresa después de un período definido de inactividad. Para los sistemas operativos de propósito general, el período no debe exceder los 15 minutos. Para dispositivos móviles de usuario final, el período no debe exceder los 2 minutos.	Usuario	Proteger			
4.4	Implementar y administrar un firewall en servidores	Implemente y administre un firewall en los servidores donde sea compatible. Como ejemplo de implementación se incluyen un firewall virtual, un firewall del sistema operativo o un agente de firewall de terceros.	Dispositivos	Proteger			
4.5	Implementar y Administrar un Firewall en los dispositivos de usuario	Implementar y administrar un firewall basado en host o una herramienta de filtrado de puertos en los dispositivos del usuario final, con una regla de denegación predeterminada que descarta todo el tráfico, excepto los servicios y puertos que están explícitamente permitidos.	Dispositivos	Proteger			
4.6	Gestione de forma segura los activos y el software de la empresa	Gestione de forma segura los activos y el software de la empresa. Por ejemplo las implementaciones incluyen la gestión de la configuración a través de una infraestructura controlada por versiones como código y el acceso a interfaces administrativas a través de protocolos de red seguro, como Secure Shell (SSH) and Hypertext Transfer Protocol Secure (HTTPS). No utilice protocolos de administración inseguros, como Telnet (Teletype Network) y HTTP, a menos que sea operacionalmente esencial.	Red	Proteger			
4.7	Administrar cuentas predeterminadas en activos y software empresariales	Administre cuentas predeterminadas en activos y software de la empresa, como root, administrador y otras cuentas de proveedores preconfiguradas. Las implementaciones de ejemplo pueden incluir: deshabilitar cuentas predeterminadas o inutilizarlas.	Usuario	Proteger			
4.8	Desinstalar o deshabilitar servicios innecesarios en activos y software empresariales	Desinstale o deshabilite los servicios innecesarios en los activos y el software de la empresa, como un servicio de uso compartido de archivos, un módulo de aplicación web o una función de servicio.	Dispositivos	Proteger			

CONTROL	TÍTULO DE CONTROL	TÍTULO DE SALVAGUARDA / DESCRIPCIÓN DE SALVAGUARDA	TIPO DE ACTIVO	FUNCIÓN DE SEGURIDAD	IG1	IG2	IG3
4.9	Configurar servidores DNS confiables en activos empresariales	Configurar servidores DNS confiables en activos empresariales. Las implementaciones de ejemplo incluyen: configurar activos para usar servidores DNS controlados por la empresa y/o servidores DNS acreditados externamente.	Dispositivos	Proteger			
4.10	Aplicar el bloqueo automático de dispositivos en portátiles y dispositivos móviles	Aplicar el bloqueo automático de dispositivos después de un umbral predeterminado de intentos de autenticación fallidos locales en dispositivos portátiles de usuario final, donde sea compatible. En el caso de las computadoras portátiles, no permite más de 20 intentos fallidos de autenticación; para tabletas y teléfonos inteligentes, no más de 10 intentos de autenticación fallidos. Las implementaciones de ejemplo incluyen Microsoft® InTune Device Lock y Apple® Intentos fallidos de mac de perfil de configuración.	Dispositivos	Responder			
4.11	Aplicar la capacidad de borrado remoto en dispositivos portátiles de usuario final	Borre de forma remota los datos empresariales de los dispositivos portátiles de usuario final de propiedad de la empresa cuando se considere apropiado, como dispositivos perdidos o robados, o cuando una persona deja la empresa.	Dispositivos	Proteger			
4.12	Espacios de trabajo empresariales independientes en dispositivos móviles de usuario final	Asegúrese de que se utilicen espacios de trabajo empresariales independientes en los dispositivos móviles de los usuarios finales, cuando sean compatibles. Las implementaciones de ejemplo incluyen el uso de un perfil de configuración de Apple® o un perfil de trabajo de Android™ para separar las aplicaciones y los datos empresariales de las aplicaciones y los datos personales.	Dispositivos	Proteger			

05 Administración de Cuentas

Utilice procesos y herramientas para asignar y administrar la autorización de las credenciales de las cuentas de usuario, incluidas las cuentas de administrador, así como las cuentas de servicio, para los activos y el software empresarial.

5.1	Establecer y mantener un inventario de cuentas	Establecer y mantener un inventario de todas las cuentas administradas en la empresa. El inventario debe incluir cuentas de usuario y de administrador. El inventario, como mínimo, debe contener el nombre de la persona, el nombre de usuario, las fechas de inicio / finalización y el departamento. Valide que todas las cuentas activas estén autorizadas, en un horario recurrente, como mínimo trimestralmente o con mayor frecuencia.	Usuario	Identificar			
5.2	Utilice contraseñas únicas	Utilice contraseñas únicas para todos los activos de la empresa. La implementación de prácticas recomendadas incluye, como mínimo, una contraseña de 8 caracteres para las cuentas que usan MFA y una contraseña de 14 caracteres para las cuentas que no usan MFA.	Usuario	Proteger			
5.3	Deshabilitar cuentas inactivas	Elimine o deshabilite las cuentas inactivas después de un período de 45 días de inactividad, cuando sea posible.	Usuario	Responder			
5.4	Restringir privilegios de administrador a cuentas de administrador dedicadas	Restrinja los privilegios de administrador a las cuentas de administrador dedicadas en los activos de la empresa. Llevar a cabo actividades informáticas generales, como la navegación por Internet, el correo electrónico y el uso de la suite de productividad, desde la cuenta principal sin privilegios del usuario.	Usuario	Proteger			
5.5	Establecer y mantener un inventario de cuentas de servicio	Establezca y mantenga un inventario de las cuentas de servicio. El inventario, como mínimo, debe contener el propietario del departamento, la fecha de revisión y el propósito. Realizar revisiones de cuentas de servicio para validar que todas las cuentas activas están autorizadas, en una programación periódica como mínimo trimestralmente, o con más frecuencia	Usuario	Identificar			
5.6	Centralizar la gestión de cuentas	Centralice la gestión de cuentas a través de un directorio o servicio de identidad.	Usuario	Proteger			

CONTROL	TÍTULO DE CONTROL	TÍTULO DE SALVAGUARDA/ DESCRIPCIÓN DE SALVAGUARDA	TIPO DE ACTIVO	FUNCIÓN DE SEGURIDAD	IG1	IG2	IG3
---------	-------------------	--	----------------	----------------------	-----	-----	-----

06 Gestión de Control de Accesos

Usar procesos y herramientas para crear, asignar, administrar y revocar credenciales y privilegios de acceso para cuentas de usuario, administrador y servicio para activos empresariales y software.

6.1	Establecer un proceso para conceder accesos	Usuario	Proteger			
	Establecer y seguir un proceso, preferiblemente automatizado, para otorgar acceso a los activos de la empresa tras una nueva contratación, concesión de derechos o cambio de rol de un usuario.					
6.2	Establecer un proceso de revocación de acceso	Usuario	Proteger			
	Establecer y seguir un proceso, preferiblemente automatizado, para revocar el acceso a los activos de la empresa, mediante la desactivación de cuentas inmediatamente después de la terminación, revocación de derechos o cambio de rol de un usuario. Es posible que sea necesario deshabilitar cuentas, en lugar de eliminarlas, para conservar las pistas de auditoría.					
6.3	Exigir MFA para aplicaciones expuestas externamente	Usuario	Proteger			
	Exija que todas las aplicaciones empresariales o de terceros expuestas externamente apliquen MFA, donde sea compatible. Hacer cumplir MFA a través de un servicio de directorio o un proveedor de SSO es una implementación satisfactoria de esta salvaguarda.					
6.4	Exigir MFA para el acceso remoto a la red	Usuario	Proteger			
	Exigir MFA para el acceso remoto a la red.					
6.5	Exigir MFA para el acceso administrativo	Usuario	Proteger			
	Requerir MFA para todas las cuentas de acceso administrativo, donde sea compatible, en todos los activos de la empresa, ya sea administrado en el sitio o a través de un proveedor externo.					
6.6	Establecer y mantener un inventario de sistemas de autenticación y autorización	Usuario	Identificar			
	Establecer y mantener un inventario de los sistemas de autenticación y autorización de la empresa, incluidos los alojados en el sitio o en un proveedor de servicios remoto. Revisar y actualizar el inventario, como mínimo, anualmente o con mayor frecuencia.					
6.7	Control de Acceso Centralizado	Usuario	Proteger			
	Centralice el control de acceso para todos los activos de la empresa a través de un servicio de directorio o un proveedor de SSO, donde sea compatible.					
6.8	Definir y mantener el control de acceso basado en roles	Datos	Proteger			
	Definir y mantener el control de acceso basado en roles, a través de la determinación y documentación de los derechos de acceso necesarios para que cada rol dentro de la empresa lleve a cabo con éxito las tareas asignadas. Realice revisiones de control de acceso de los activos de la empresa para validar que todos los privilegios estén autorizados, de forma periódica, como mínimo una vez al año, o con mayor frecuencia.					

07 Gestión Continua de Vulnerabilidades

Desarrollar un plan para evaluar y dar seguimiento continuo a las vulnerabilidades en todos los activos dentro de la infraestructura de la empresa, con el fin de remediar y reducir la ventana de oportunidad para los atacantes. Monitorear las fuentes de la industria pública y privada en busca de nueva información sobre amenazas y vulnerabilidades.

7.1	Establecer y mantener un proceso de gestión de vulnerabilidades	Aplicaciones	Proteger			
	Establezca y mantenga un proceso de gestión de vulnerabilidades documentado para los activos de la empresa. Revisar y actualizar la documentación anualmente, o cuando ocurran cambios importantes en la empresa que puedan afectar esta salvaguarda.					
7.2	Establecer y mantener un proceso de remediación	Aplicaciones	Responder			
	Establecer y mantener una estrategia de remediación basada en riesgos documentada en un proceso de remediación, con revisiones mensuales o más frecuentes.					
7.3	Realice una gestión automatizada de parches del sistema operativo	Aplicaciones	Proteger			
	Realice actualizaciones del sistema operativo en los activos de la empresa a través de la gestión automatizada de parches de forma mensual o con mayor frecuencia.					
7.4	Realizar la administración automatizada de parches de aplicaciones	Aplicaciones	Proteger			
	Realice actualizaciones de aplicaciones en los activos de la empresa a través de la gestión automatizada de parches de forma mensual o con mayor frecuencia.					
7.5	Realizar análisis automatizados de vulnerabilidades de activos internos de la empresa	Aplicaciones	Identificar			
	Realice escaneos automatizados de vulnerabilidades de los activos internos de la empresa de forma trimestral o con mayor frecuencia. Realice escaneos autenticados y no autenticados, utilizando una herramienta de escaneo de vulnerabilidades compatible con SCAP.					

CONTROL	TÍTULO DE CONTROL	TÍTULO DE SALVAGUARDA / DESCRIPCIÓN DE SALVAGUARDA	TIPO DE ACTIVO	FUNCIÓN DE SEGURIDAD	IG1	IG2	IG3
7.6	Realice análisis automatizados de vulnerabilidades de activos empresariales expuestos externamente	Realice escaneos automatizados de vulnerabilidades de los activos empresariales expuestos externamente utilizando una herramienta de escaneo de vulnerabilidades compatible con SCAP. Realice exploraciones mensualmente o con mayor frecuencia.	Aplicaciones	Identificar		●	●
7.7	Remediar las vulnerabilidades detectadas	Repare las vulnerabilidades detectadas en el software a través de procesos y herramientas de forma mensual o más frecuente, según el proceso de corrección.	Aplicaciones	Responder		●	●

08 Gestión de Registros de Auditoría

Recopilar, alertar, revisar y conservar registros de auditoría de eventos que podrían ayudar a detectar, comprender o recuperarse de un ataque.

8.1	Establecer y mantener un proceso de gestión de registros de auditoría	Establezca y mantenga un proceso de gestión de registros de auditoría que defina los requisitos de registro de la empresa. Como mínimo, aborde la recopilación, revisión y retención de registros de auditoría para activos empresariales. Revisar y actualizar la documentación anualmente, o cuando ocurran cambios importantes en la empresa que puedan afectar esta salvaguardia.	Red	Proteger	●	●	●
8.2	Recopilar registros de auditoría	Recopile registros de auditoría. Asegúrese de que el registro, según el proceso de gestión de registros de auditoría de la empresa, se haya habilitado en todos los activos de la empresa.	Red	Detectar	●	●	●
8.3	Garantizar un almacenamiento adecuado del registro de auditoría	Asegúrese de que los destinos de registro mantengan un almacenamiento adecuado para cumplir con el proceso de gestión de registros de auditoría de la empresa.	Red	Proteger	●	●	●
8.4	Estandarizar la sincronización de hora	Estandarizar la sincronización horaria. Configurar al menos dos orígenes de hora sincronizados en los activos de la empresa, donde se admite.	Red	Proteger		●	●
8.5	Recopilar registros de auditoría detallados	Configure el registro de auditoría detallado para los activos empresariales que contienen datos confidenciales. Incluya el origen del evento, la fecha, el nombre de usuario, la marca de tiempo, las direcciones de origen, las direcciones de destino y otros elementos útiles que podrían ayudar en una investigación forense.	Red	Detectar		●	●
8.6	Recopilar registros de auditoría de consultas de DNS	Recopile registros de auditoría de consultas de DNS en activos de la empresa, cuando sea apropiado y compatible.	Red	Detectar		●	●
8.7	Recopilar registros de auditoría de solicitudes de URL	Recopile registros de auditoría de solicitudes de URL en los activos de la empresa, cuando sea apropiado y compatible.	Red	Detectar		●	●
8.8	Recopilar registros de auditoría de la línea de comandos	Recopile registros de auditoría de la línea de comandos. Las implementaciones de ejemplo incluyen la recopilación de registros de auditoría de PowerShell®, BASH™ y terminales administrativas remotas.	Dispositivos	Detectar		●	●
8.9	Centralice Audit Logs	Centralice, en la medida de lo posible, la recopilación y retención de registros de auditoría en todos los activos de la empresa.	Red	Detectar		●	●
8.10	Conservar registros de auditoría	Conservar registros de auditoría en todos los activos de la empresa durante un mínimo de 90 días.	Red	Proteger		●	●
8.11	Realizar revisiones de registros de auditoría	Realice revisiones de los registros de auditoría para detectar anomalías o eventos anormales que podrían indicar una amenaza potencial. Realizar revisiones semanalmente o con mayor frecuencia.	Red	Detectar		●	●
8.12	Recopilar registros de auditorías para proveedores de servicios	Recopile registros de proveedores de servicios, donde sea compatible. Las implementaciones de ejemplo incluyen la recopilación de eventos de autenticación y autorización, eventos de creación y eliminación de datos y eventos de gestión de usuarios.	Datos	Detectar			●

CONTROL	TÍTULO DE CONTROL	TÍTULO DE SALVAGUARDA/ DESCRIPCIÓN DE SALVAGUARDA	TIPO DE ACTIVO	FUNCIÓN DE SEGURIDAD	IG1	IG2	IG3
---------	-------------------	---	----------------	----------------------	-----	-----	-----

09 Protección del Correo Electrónico y Navegador Web

Mejorar la protección y detección de amenazas del correo electrónico y vectores web, ya que estas son oportunidades para que los atacantes manipulen el comportamiento humano a través de su compromiso.

9.1	Garantizar el uso de solo navegadores y clientes de correo electrónico totalmente compatibles	Aplicaciones	Proteger			
Asegúrese de que solo los navegadores y clientes de correo electrónico totalmente compatibles puedan ejecutarse en la empresa, solo utilizando la versión más reciente de los navegadores y clientes de correo electrónico proporcionados a través del proveedor.						
9.2	Usar servicios de filtrado DNS	Red	Proteger			
Utilice los servicios de filtrado de DNS en todos los activos de la empresa para bloquear el acceso a dominios maliciosos conocidos						
9.3	Mantener y aplicar filtros de URL basados en la red	Red	Proteger			
Hacer cumplir y actualizar los filtros de URL basados en la red para limitar la conexión de un activo empresarial a sitios web potencialmente maliciosos o no aprobados. Las implementaciones de ejemplo incluyen filtrado basado en categorías, filtrado basado en reputación o mediante el uso de listas de bloqueo. Aplicar filtros para todos los activos de la empresa						
9.4	Restringir extensiones innecesarias o no autorizadas de navegador y cliente de correo electrónico	Aplicaciones	Proteger			
Restringir, ya sea mediante la desinstalación o desactivación, cualquier navegador no autorizado o innecesario o complementos de cliente de correo electrónico, extensiones y aplicaciones complementos.						
9.5	Implementar DMARC	Red	Proteger			
Para reducir la posibilidad de correos electrónicos falsificados o modificados de dominios válidos, implemente la directiva DMARC y la verificación, comenzando con la implementación del marco de políticas de remitente (SPF) y los estándares domain keys identified mail (DKIM).						
9.6	Bloquear tipos de archivos innecesarios	Red	Proteger			
Bloquear tipos de archivos innecesarios que intentan ingresar por la puerta de enlace de correo electrónico de la empresa.						
9.7	Implementar y mantener protecciones anti malware del servidor de correo electrónico	Red	Proteger			
Implementar y mantener protecciones anti malware del servidor de correo electrónico, como el análisis de archivos adjuntos y/o el espacio aislado.						

10 Defensas contra Malware

Prevenir o controlar la instalación, propagación y ejecución de aplicaciones, códigos o scripts maliciosos en activos empresariales.

10.1	Implementar y mantener software anti-malware	Dispositivos	Proteger			
Implementar y mantener software antimalware en todos los activos de la empresa.						
10.2	Configurar actualizaciones automáticas de firmas de Antimalwares	Dispositivos	Proteger			
Configurar actualizaciones automáticas para archivos de firma antimalware en todos los activos de la empresa.						
10.3	Deshabilitar la ejecución automática y la reproducción automática para medios extraíbles	Dispositivos	Proteger			
Desactive la ejecución automática y la función de ejecución automática de reproducción automática para medios extraíbles.						
10.4	Configurar el análisis anti malware automático de medios extraíbles	Dispositivos	Detectar			
Configure el software anti-malware para escanear automáticamente los medios extraíbles.						
10.5	Habilitar funciones anti-explotación	Dispositivos	Proteger			
Habilite funciones anti-explotación en activos y software empresariales, cuando sea posible, como Microsoft® Data Execution Prevention (DEP), Windows® Defender Exploit Guard (WDEG) o Apple® System Integrity Protection (SIP) y Gatekeeper™.						
10.6	Administrar de forma centralizada el software antimalware	Dispositivos	Proteger			
Gestione de forma centralizada el software antimalware.						
10.7	Utilice el software anti-malware basado en el comportamiento	Dispositivos	Detectar			
Usar software anti malware basado en el comportamiento.						

CONTROL	TÍTULO DE CONTROL	TÍTULO DE SALVAGUARDA / DESCRIPCIÓN DE SALVAGUARDA	TIPO DE ACTIVO	FUNCIÓN DE SEGURIDAD	IG1	IG2	IG3
11	Recuperación de Datos	Establecer y mantener prácticas de recuperación de datos suficientes para restaurar los activos empresariales incluidos en el alcance a un estado de confianza previo al incidente.					
11.1	Establecer y mantener un proceso de recuperación de datos	Datos	Recuperar				
	Establecer y mantener un proceso de recuperación de datos. En el proceso, aborde el alcance de las actividades de recuperación de datos, la priorización de la recuperación y la seguridad de los datos de respaldo. Revisar y actualizar la documentación anualmente, o cuando ocurran cambios importantes en la empresa que puedan afectar esta salvaguarda.						
11.2	Realice copias de seguridad automatizadas	Datos	Recuperar				
	Realizar copias de seguridad automatizadas de activos empresariales dentro del ámbito. Ejecutar copias de seguridad semanalmente, o con más frecuencia, en función de la sensibilidad de los datos.						
11.3	Proteja los datos de recuperación	Datos	Proteger				
	Proteja los datos de recuperación con controles equivalentes a los datos originales. Cifrado de referencia o separación de datos, en función de los requisitos						
11.4	Establecer y mantener una instancia aislada de datos de recuperación	Datos	Recuperar				
	Establecer y mantener una instancia aislada de datos de recuperación. Entre las implementaciones de ejemplo se incluyen el control de versiones de destinos de copia de seguridad a través de sistemas o servicios sin conexión, en la nube o fuera del sitio.						
11.5	Prueba de recuperación de datos	Datos	Recuperar				
	Pruebe la recuperación de copias de seguridad trimestralmente, o con mayor frecuencia, para obtener una muestra de los activos empresariales incluidos en el alcance.						
12	Gestión de la Infraestructura de Red	Establecer, implementar y administrar activamente (rastrear, informar, corregir) dispositivos de red, con el fin de evitar que los atacantes exploten los servicios de red y los puntos de acceso vulnerables.					
12.1	Asegúrese de que la infraestructura de red esté actualizada	Red	Proteger				
	Asegúrese de que la infraestructura de red se mantenga actualizada. Entre las implementaciones de ejemplo se incluyen la ejecución de la última versión estable de software y/o el uso de servicios de red como NaaS actualmente admitidas. Revise las versiones de software mensualmente, o con más frecuencia, para verificar la compatibilidad del software.						
12.2	Establecer y mantener una arquitectura de red segura	Red	Proteger				
	Establecer y mantener una arquitectura de red segura. Una arquitectura de red segura debe abordar la segmentación, los privilegios mínimos y la disponibilidad, como mínimo.						
12.3	Gestione de forma segura la infraestructura de red	Red	Proteger				
	Gestione de forma segura la infraestructura de red. Las implementaciones de ejemplo incluyen infraestructura de versión controlada como código y el uso de protocolos de red seguros, como SSH y HTTPS.						
12.4	Establecer y mantener diagramas de arquitectura	Red	Identificar				
	Establezca y mantenga los diagramas de la arquitectura y/o la documentación del sistema de red. Revise y actualice la documentación anualmente, o cuando se produzcan cambios significativos en la empresa que puedan afectar a esta salvaguarda.						
12.5	Centralice la autenticación, la autorización, y la auditoría de la red (AAA)	Red	Proteger				
	Centralice la red AAA.						
12.6	Uso de protocolos seguros de administración de redes y comunicaciones	Red	Proteger				
	Utilice protocolos seguros de administración de redes y comunicación (por ejemplo, 802.1X, Wi-Fi Protected Access 2 (WPA2) Enterprise o superior).						
12.7	Asegúrese de que los dispositivos remotos utilicen una VPN y se conecten a la infraestructura AAA de una empresa	Dispositivos	Proteger				
	Requerir que los usuarios se autentiquen en los servicios de autenticación y VPN administrados por la empresa antes de acceder a los recursos de la empresa en los dispositivos de usuario final.						
12.8	Establecer y mantener recursos informáticos dedicados para todo el trabajo administrativo	Dispositivos	Proteger				
	Establezca y mantenga recursos informáticos dedicados, ya sea física o lógicamente separados, para todas las tareas administrativas o tareas que requieran acceso administrativo. Los recursos informáticos deben segmentarse de la red principal de la empresa y no se les debe permitir el acceso a Internet.						

CONTROL	TÍTULO DE CONTROL	TÍTULO DE SALVAGUARDA / DESCRIPCIÓN DE SALVAGUARDA	TIPO DE ACTIVO	FUNCIÓN DE SEGURIDAD	IG1	IG2	IG3
13	Monitoreo y Defensa de la red	Operar procesos y herramientas para establecer y mantener la supervisión y defensa integrales de la red contra las amenazas de seguridad en toda la infraestructura de red y la base de usuarios de la empresa.					
13.1	Centralizar alertas de eventos de seguridad	Centralice las alertas de eventos de seguridad en todos los activos de la empresa para la correlación y el análisis de registros. La implementación de las mejores prácticas requiere el uso de un SIEM, que incluye alertas de correlación de eventos definidas por el proveedor. Una plataforma de análisis de registros configurada con alertas de correlación relevantes para la seguridad también satisface esta protección.	Red	Detectar		●	●
13.2	Implemente una solución de detección de intrusiones basada en host	Implementar una solución de detección de intrusiones basada en host en activos empresariales, cuando sea apropiado y/o compatible.	Dispositivos	Detectar		●	●
13.3	Implementación de una solución de detección de intrusiones en la red	Implemente una solución de detección de intrusiones en la red de activos de la empresa, cuando corresponda. Las implementaciones de ejemplo incluyen el uso de un sistema de detección de intrusiones en la red (NIDS) o un servicio equivalente de proveedor de servicios en la nube (CSP).	Red	Detectar		●	●
13.4	Realizar filtrado de tráfico entre segmentos de red	Realice un filtrado de tráfico entre los segmentos de la red, cuando corresponda.	Red	Proteger		●	●
13.5	Gestionar el control de acceso para activos remotos	Administre el control de acceso para los activos que se conectan de forma remota a los recursos de la empresa. Determine la cantidad de acceso a los recursos de la empresa en función de: el software antimalware actualizado instalado, el cumplimiento de la configuración con el proceso de configuración segura de la empresa y la garantía de que el sistema operativo y las aplicaciones estén actualizados.	Dispositivos	Proteger		●	●
13.6	Recopilar registros de flujo de tráfico de red	Recopilar registros de flujo de tráfico de red y/o tráfico de red para revisar y alertar desde dispositivos de red.	Red	Detectar		●	●
13.7	Implementar una solución de prevención de intrusiones basada en host	Implemente una solución de prevención de intrusiones basada en host en los activos de la empresa, cuando corresponda o sea compatible. Las implementaciones de ejemplo incluyen el uso de un cliente de detección y respuesta de extremo (EDR) o un agente IPS basado en host.	Dispositivos	Proteger			●
13.8	Implementar una solución de prevención de intrusiones en la red	Implemente una solución de prevención de intrusiones en la red, en donde corresponda. Entre las implementaciones de ejemplo se incluye el uso de un sistema de prevención de intrusiones en la red (NIPS) o un servicio CSP equivalente.	Red	Proteger			●
13.9	Implementar el control de acceso a nivel de puerto	Implementar el control de acceso a nivel de puerto. El control de acceso a nivel de puerto utiliza 802.1x o protocolos de control de acceso a la red similares, como certificados, y puede incorporar autenticación de usuario y/o dispositivo.	Dispositivos	Proteger			●
13.10	Realizar el filtrado en la capa de aplicación	Realizar el filtrado de la capa de aplicación. Entre las implementaciones de ejemplo se incluyen un proxy de filtrado, un firewall de nivel de aplicación o una puerta de enlace.	Red	Proteger			●
13.11	Ajustar los umbrales de alerta de eventos de seguridad	Ajustar los umbrales de alerta de eventos de seguridad mensualmente o con más frecuencia	Red	Detectar			●
14	Concientización en Seguridad y Formación de Habilidades	Establecer y mantener un programa de concientización sobre seguridad para influir en el comportamiento de la fuerza laboral para que sea consciente de la seguridad y esté debidamente capacitado para reducir los riesgos de ciberseguridad para la empresa.					
14.1	Establecer y mantener un programa de concientización sobre seguridad	Establecer y mantener un programa de concientización sobre seguridad. El propósito de un programa de concientización sobre seguridad es educar a la fuerza laboral de la empresa sobre cómo interactuar con los activos y datos de la empresa de manera segura. Realice la capacitación al momento de contratar y, como mínimo, anualmente. Revisar y actualizar el contenido anualmente o cuando se produzcan cambios empresariales importantes que puedan afectar a esta salvaguarda.	N/A	Proteger	●	●	●
14.2	Capacitar a los miembros de la plana laboral para que reconozcan los ataques de ingeniería social	Capacite a los miembros de la fuerza laboral para que reconozcan los ataques de ingeniería social, como suplantación de identidad (phishing), pretextos y seguimiento.	N/A	Proteger	●	●	●

CONTROL	TÍTULO DE CONTROL	TÍTULO DE SALVAGUARDA / DESCRIPCIÓN DE SALVAGUARDA	TIPO DE ACTIVO	FUNCIÓN DE SEGURIDAD	IG1	IG2	IG3
14.3	Capacitar a los miembros de la plana laboral sobre las mejores prácticas de autenticación	Capacite a los miembros de la fuerza laboral sobre las mejores prácticas de autenticación. Los temas de ejemplo incluyen MFA, composición de contraseñas y administración de credenciales.	N/A	Proteger			
14.4	Capacitar a la fuerza laboral en las mejores prácticas de manejo de datos	Capacite a los miembros de la fuerza laboral sobre cómo identificar y almacenar, transferir, archivar y destruir correctamente los datos confidenciales. Esto también incluye la capacitación de los miembros de la fuerza laboral en las mejores prácticas de pantalla limpia y escritorio, cómo bloquear su pantalla cuando se alejan de su activo empresarial, borrar pizarras físicas y virtuales al final de las reuniones y almacenar datos y activos de forma segura.	N/A	Proteger			
14.5	Capacitar a los miembros de la plana laboral sobre las causas de la exposición involuntaria de datos	Capacite a los miembros de la fuerza laboral para que sean conscientes de las causas de la exposición involuntaria de datos. Entre los temas de ejemplo se incluyen la entrega errónea de datos confidenciales, la pérdida de un dispositivo portátil de usuario final o la publicación de datos para audiencias no deseadas.	N/A	Proteger			
14.6	Capacitar a los miembros de la plana laboral sobre el reconocimiento y la notificación de incidentes de seguridad	Capacitar a los miembros de la fuerza laboral para que puedan reconocer un incidente potencial y puedan reportar dicho incidente.	N/A	Proteger			
14.7	Capacitar al personal sobre cómo identificar e informar si sus activos empresariales carecen de actualizaciones de seguridad	Capacite al personal para que comprenda cómo verificar e informar sobre parches de software desactualizados o cualquier falla en los procesos y herramientas automatizados. Parte de esta capacitación debe incluir notificar al personal de TI de cualquier falla en los procesos y herramientas automatizados.	N/A	Proteger			
14.8	Capacitar a la plana laboral sobre los peligros de conectarse y transmitir datos empresariales a través de redes inseguras	Capacite a los miembros de la fuerza laboral sobre los peligros de conectarse y transmitir datos a través de redes inseguras para actividades empresariales. Si la empresa tiene trabajadores remotos, la capacitación debe incluir orientación para garantizar que todos los usuarios configuren de manera segura su infraestructura de red doméstica.	N/A	Proteger			
14.9	Llevar a cabo capacitación en habilidades y concientización sobre seguridad para roles específicos	Llevar a cabo capacitación en habilidades y concientización sobre seguridad para funciones específicas. Las implementaciones de ejemplo incluyen cursos de administración de sistemas seguros para profesionales de TI, capacitación en prevención y concientización de vulnerabilidades de OWASP® Top 10 para desarrolladores de aplicaciones web y capacitación avanzada en concientización sobre ingeniería social para roles de alto perfil.	N/A	Proteger			

15 Gestión de Proveedores de Servicios

Desarrollar un proceso para evaluar a los proveedores de servicios que poseen datos confidenciales o que son responsables de las plataformas o procesos de TI críticos de una empresa, para garantizar que estos proveedores protejan esas plataformas y datos de manera adecuada.

15.1	Establecer y mantener un inventario de proveedores de servicios	Establecer y mantener un inventario de proveedores de servicios. El inventario debe enumerar todos los proveedores de servicios conocidos, incluir clasificaciones y designar un contacto empresarial para cada proveedor de servicios. Revisar y actualizar el inventario anualmente o cuando ocurran cambios importantes en la empresa que puedan afectar esta Salvaguarda.	N/A	Identificar			
15.2	Establecer y mantener una política de gestión de proveedores de servicios	Establecer y mantener una política de gestión de proveedores de servicios. Asegúrese de que la política aborde la clasificación, el inventario, la evaluación, el seguimiento y el desmantelamiento de los proveedores de servicios. Revisar y actualizar la política anualmente, o cuando ocurran cambios importantes en la empresa que puedan afectar esta Salvaguarda.	N/A	Identificar			
15.3	Clasificar proveedores de servicios	Clasificar a los proveedores de servicios. La consideración de la clasificación puede incluir una o más características, como la sensibilidad de los datos, el volumen de datos, los requisitos de disponibilidad, las regulaciones aplicables, el riesgo inherente y el riesgo mitigado. Actualizar y revisar las clasificaciones anualmente, o cuando se produzcan cambios significativos en la empresa que puedan afectar a esta Salvaguarda.	N/A	Identificar			

CONTROL	TÍTULO DE CONTROL	TÍTULO DE SALVAGUARDA/ DESCRIPCIÓN DE SALVAGUARDA	TIPO DE ACTIVO	FUNCIÓN DE SEGURIDAD	IG1	IG2	IG3
15.4	Asegúrese de que los contratos de los proveedores de servicios incluyan requisitos de seguridad	Asegúrese de que los contratos del proveedor de servicios incluyan requisitos de seguridad. Los requisitos de ejemplo pueden incluir requisitos mínimos del programa de seguridad, notificación y respuesta de incidentes de seguridad y/o violación de datos, requisitos de cifrado de datos y compromisos de eliminación de datos. Estos requisitos de seguridad deben ser coherentes con la directiva de administración del proveedor de servicios de la empresa. Revisar los contratos de los proveedores de servicios anualmente para asegurarse de que los contratos no faltan requisitos de seguridad.	N/A	Proteger			
15.5	Evaluar proveedores de servicios	Evaluar a los proveedores de servicios de acuerdo con la política de gestión de proveedores de servicios de la empresa. El alcance de la evaluación puede variar según la (s) clasificación (es) y puede incluir la revisión de informes de evaluación estandarizados, como el Control de la organización de servicio 2 (SOC 2) y la Certificación de cumplimiento (AoC) de la industria de tarjetas de pago (PCI), cuestionarios personalizados u otros procesos rigurosos. Reevaluar a los proveedores de servicios anualmente, como mínimo, o con contratos nuevos y renovados.	N/A	Identificar			
15.6	Supervisar proveedores de servicios	Supervise a los proveedores de servicios de forma coherente con la directiva de administración de proveedores de servicios de la empresa. El monitoreo puede incluir reevaluación periódica del cumplimiento del proveedor de servicios, monitoreo de notas de la versión del proveedor de servicios y monitoreo de la web oscura.	Datos	Detectar			
15.7	Dar de baja de forma segura a los proveedores de servicios	Desmantele de forma segura a los proveedores de servicios. Entre las consideraciones de ejemplo se incluyen la desactivación de cuentas de usuario y servicio, la terminación de flujos de datos y la eliminación segura de datos empresariales dentro de los sistemas de proveedores de servicios.	Datos	Proteger			

16 Seguridad en el Software de Aplicación

Administrar el ciclo de vida de seguridad del software desarrollado, alojado o adquirido internamente para prevenir, detectar y corregir las debilidades de seguridad antes de que puedan afectar a la empresa.

16.1	Establecer y mantener un proceso de desarrollo de aplicaciones seguro	Establecer y mantener un proceso de desarrollo de aplicaciones seguro. En el proceso, aborde elementos tales como: estándares de diseño de aplicaciones seguras, prácticas de codificación segura, capacitación de desarrolladores, gestión de vulnerabilidades, seguridad de código de terceros y procedimientos de prueba de seguridad de aplicaciones. Revisar y actualizar la documentación anualmente, o cuando ocurran cambios importantes en la empresa que puedan afectar esta Salvaguarda.	Aplicaciones	Proteger			
16.2	Establecer y mantener un proceso para aceptar y abordar las vulnerabilidades del software	Establecer y mantener un proceso para aceptar y abordar los informes de vulnerabilidades de software, incluido el suministro de un medio para que las entidades externas informen. El proceso debe incluir elementos tales como: una política de manejo de vulnerabilidades que identifique el proceso de notificación, la parte responsable de manejar los informes de vulnerabilidad y un proceso de admisión, asignación, remediación y pruebas de remediación. Como parte del proceso, utilice un sistema de seguimiento de vulnerabilidades que incluya calificaciones de gravedad y métricas para medir el tiempo de identificación, análisis y corrección de vulnerabilidades. Revisar y actualizar la documentación anualmente, o cuando ocurran cambios importantes en la empresa que puedan afectar esta Salvaguarda. Los desarrolladores de aplicaciones de terceros deben considerar esta una política orientada externamente que ayuda a establecer expectativas para las partes interesadas externas	Aplicaciones	Proteger			
16.3	Realice un análisis de la causa raíz de las vulnerabilidades de seguridad	Realizar análisis de causa raíz sobre vulnerabilidades de seguridad. Al revisar las vulnerabilidades, el análisis de la causa raíz es la tarea de evaluar los problemas subyacentes que crean vulnerabilidades en el código y permite a los equipos de desarrollo ir más allá de simplemente corregir las vulnerabilidades individuales a medida que surgen.	Aplicaciones	Proteger			
16.4	Establecer y administrar un inventario de componentes de software de terceros	Establezca y administre un inventario actualizado de los componentes de terceros utilizados en el desarrollo, a menudo conocido como una "lista de materiales"; así como los componentes programados para su uso futuro. Este inventario debe incluir cualquier riesgo que cada componente de terceros pueda plantear. Evalúe la lista al menos una vez al mes para identificar cualquier cambio o actualización de estos componentes y validar que el componente sigue siendo compatible	Aplicaciones	Proteger			
16.5	Utilice componentes de software de terceros actualizados y confiables	Utilice componentes de software de terceros actualizados y confiables. Cuando sea posible, elija marcos y bibliotecas establecidos y probados que brinden la seguridad adecuada. Acquire these components from trusted sources or evaluate the software for vulnerabilities before use.	Aplicaciones	Proteger			

CONTROL	TÍTULO DE CONTROL	TÍTULO DE SALVAGUARDA/ DESCRIPCIÓN DE SALVAGUARDA	TIPO DE ACTIVO	FUNCIÓN DE SEGURIDAD	IG1	IG2	IG3
16.6	Establecer y mantener un sistema y proceso de clasificación de gravedad para las vulnerabilidades de las aplicaciones	Establecer y mantener un sistema de clasificación de gravedad y un proceso para las vulnerabilidades de las aplicaciones que facilite la priorización del orden en que se corrigen las vulnerabilidades detectadas. Este proceso incluye establecer un nivel mínimo de aceptabilidad de seguridad para liberar código o aplicaciones. Las clasificaciones de gravedad aportan una forma sistemática de evaluar las vulnerabilidades que mejora la gestión de riesgos y ayuda a garantizar que los errores más graves se solucionen primero. Revisar y actualizar el sistema y el proceso anualmente.	Aplicaciones	Proteger			
16.7	Usar plantillas de configuración de protección estándar para la infraestructura de aplicaciones	Utilice plantillas de configuración de protección estándar recomendadas por la industria para los componentes de la infraestructura de aplicaciones. Esto incluye servidores subyacentes, bases de datos y servidores web, y se aplica a contenedores en la nube, componentes de plataforma como servicio (PaaS) y componentes SaaS. No permita que el software desarrollado internamente debilite el endurecimiento de la configuración.	Aplicaciones	Proteger			
16.8	Sistemas de producción separados y sistemas de no producción	Mantener entornos separados para sistemas de producción y no de producción.	Aplicaciones	Proteger			
16.9	Capacitar a los desarrolladores en conceptos de seguridad de aplicaciones y codificación segura	Asegúrese de que todo el personal de desarrollo de software reciba capacitación en la escritura de código seguro para su entorno de desarrollo y responsabilidades específicas. La capacitación puede incluir principios generales de seguridad y prácticas estándar de seguridad de aplicaciones. Realizar capacitaciones al menos una vez al año y diseñar de manera que se promueva la seguridad dentro del equipo de desarrollo y crear una cultura de seguridad entre los desarrolladores.	Aplicaciones	Proteger			
16.10	Aplicar principios de diseño seguro en arquitecturas de aplicaciones	Aplicar principios de diseño seguro en arquitecturas de aplicaciones. Los principios de diseño seguro incluyen el concepto de privilegio mínimo y la aplicación de la mediación para validar cada operación que realiza el usuario, promoviendo el concepto de "nunca confiar en la entrada del usuario". Los ejemplos incluyen asegurarse de que se realice y documente la verificación explícita de errores para todas las entradas, incluido el tamaño, el tipo de datos y los rangos o formatos aceptables. El diseño seguro también significa minimizar la superficie de ataque de la infraestructura de la aplicación, como apagar los puertos y servicios desprotegidos, eliminar programas y archivos innecesarios y cambiar el nombre o eliminar las cuentas predeterminadas.	Aplicaciones	Proteger			
16.11	Aprovechar los módulos o servicios examinados para los componentes de seguridad de las aplicaciones	Aproveche los módulos o servicios examinados para los componentes de seguridad de las aplicaciones, como la administración de identidades, el cifrado y la auditoría y el registro.	Aplicaciones	Proteger			
16.12	Implementar verificaciones de seguridad a nivel de código	Aplique herramientas de análisis estático y dinámico dentro del ciclo de vida de la aplicación para comprobar que se siguen las prácticas de codificación seguras.	Aplicaciones	Proteger			
16.13	Realizar pruebas de penetración de aplicaciones	Realice pruebas de penetración de aplicaciones. Para aplicaciones críticas, las pruebas de penetración autenticadas son más adecuadas para encontrar vulnerabilidades de lógica empresarial que el escaneo de código y las pruebas de seguridad automatizadas. Las pruebas de penetración se basan en la habilidad del evaluador para manipular manualmente una aplicación como un usuario autenticado y no autenticado.	Aplicaciones	Proteger			
16.14	Realizar modelado de amenazas	Realice modelos de amenazas. El modelado de amenazas es el proceso de identificar y abordar las fallas de diseño de seguridad de las aplicaciones dentro de un diseño, antes de que se cree el código. Se lleva a cabo a través de personas especialmente capacitadas que evalúan el diseño de la aplicación y miden los riesgos de seguridad para cada punto de entrada y nivel de acceso. El objetivo es mapear la aplicación, la arquitectura y la infraestructura de una manera estructurada para comprender sus debilidades.	Aplicaciones	Proteger			

CONTROL	TÍTULO DE CONTROL	TÍTULO DE SALVAGUARDA/ DESCRIPCIÓN DE SALVAGUARDA	TIPO DE ACTIVO	FUNCIÓN DE SEGURIDAD	IG1	IG2	IG3
17	Gestión de Respuesta a Incidentes	Establecer un programa para desarrollar y mantener una capacidad de respuesta a incidentes (por ejemplo, políticas, planes, procedimientos, roles definidos, capacitación y comunicaciones) para preparar, detectar y responder rápidamente a un ataque.					
17.1	Designar personal para administrar el manejo de incidentes	Designa una persona clave, y al menos una persona como respaldo, que gestionará el proceso de gestión de incidentes de la empresa. El personal de administración es responsable de la coordinación y documentación de la respuesta a incidentes y los esfuerzos de recuperación y puede consistir en empleados internos de la empresa, proveedores externos o un enfoque híbrido. Si utiliza un proveedor externo, designe al menos una persona interna de la empresa para supervisar cualquier trabajo de terceros. Revise anualmente o cuando ocurran cambios importantes en la empresa que puedan afectar esta protección.	N/A	Responder	●	●	●
17.2	Establecer y mantener información de contacto para informar incidentes de seguridad	Establecer y mantener la información de contacto de las partes que necesitan ser informadas de incidentes de seguridad. Los contactos pueden incluir personal interno, proveedores externos, fuerzas del orden, proveedores de seguros cibernéticos, agencias gubernamentales relevantes, socios del Centro de Intercambio y Análisis de Información (ISAC) u otras partes interesadas. Verificar los contactos anualmente para asegurarse de que la información está actualizada.	N/A	Responder	●	●	●
17.3	Establecer y mantener un proceso empresarial para informar de incidentes	Establezca y mantenga un proceso de la empresa para que la plana laboral informe de incidentes de seguridad. El proceso incluye el plazo de presentación de informes, el personal al que informar, el mecanismo de presentación de informes y la información mínima que se debe informar. Asegúrese de que el proceso esté disponible públicamente para toda la plana laboral. Revisar esta salvaguarda anualmente, o cuando se produzcan cambios significativos en la empresa que puedan afectar a esta Salvaguarda.	N/A	Responder	●	●	●
17.4	Establecer y mantener un proceso de respuesta a incidentes	Establezca y mantenga un proceso de respuesta a incidentes que aborde los roles y responsabilidades, los requisitos de cumplimiento y un plan de comunicación. Revise anualmente o cuando ocurran cambios importantes en la empresa que puedan afectar esta salvaguarda.	N/A	Responder		●	●
17.5	Asignar Roles Claves y Responsabilidades	Asigne roles claves y responsabilidades responder a incidentes, incluido el personal de legal, TI, seguridad de la información, instalaciones, relaciones públicas, recursos humanos, personal de respuesta a incidentes y analistas, según corresponda. Revise esta salvaguarda anualmente o cuando ocurran cambios importantes en la empresa que puedan afectar esta protección.	N/A	Responder		●	●
17.6	Definir mecanismos de comunicación durante la respuesta a incidentes	Determine qué mecanismos principales y secundarios se usarán para comunicarse e informar durante un incidente de seguridad. Los mecanismos pueden incluir llamadas telefónicas, correos electrónicos o cartas. Tenga en cuenta que ciertos mecanismos, como los correos electrónicos, pueden verse afectados durante un incidente de seguridad. Revisar anualmente, o cuando se produzcan cambios significativos en la empresa que puedan afectar a esta Salvaguarda.	N/A	Responder		●	●
17.7	Realizar ejercicios rutinarios de respuesta a incidentes	Planifique y lleve a cabo ejercicios y escenarios de respuesta a incidentes de rutina para el personal clave involucrado en el proceso de respuesta a incidentes a fin de prepararse para responder a incidentes del mundo real. Los ejercicios deben probar los canales de comunicación, la toma de decisiones y los flujos de trabajo. Realice pruebas anualmente, como mínimo.	N/A	Recuperar		●	●
17.8	Realizar revisiones posteriores a un incidente	Realice revisiones posteriores al incidente. Las revisiones posteriores al incidente ayudan a prevenir la repetición del incidente mediante la identificación de lecciones aprendidas y acciones de seguimiento.	N/A	Recuperar		●	●
17.9	Establecer y mantener umbrales de incidentes de seguridad	Establezca y mantenga umbrales de incidentes de seguridad, incluyendo, como mínimo, la diferenciación entre un incidente y un evento. Los ejemplos pueden incluir: actividad anormal, vulnerabilidad de seguridad, debilidad de seguridad, violación de datos, incidente de privacidad, etc. Revisar anualmente, o cuando se produzcan cambios significativos en la empresa que puedan afectar a esta Salvaguarda.	N/A	Recuperar			●

CONTROL	TÍTULO DE CONTROL	TÍTULO DE SALVAGUARDA/ DESCRIPCIÓN DE SALVAGUARDA	TIPO DE ACTIVO	FUNCIÓN DE SEGURIDAD	IG1	IG2	IG3
18	Pruebas de Penetración	Pruebe la eficacia y la resistencia de los activos empresariales mediante la identificación y explotación de debilidades en los controles (personas, procesos y tecnología) y la simulación de los objetivos y acciones de un atacante.					
18.1	Establecer y mantener un programa de pruebas de penetración	Establezca y mantenga un programa de pruebas de penetración adecuado al tamaño, complejidad y madurez de la empresa. Las características del programa de pruebas de penetración incluyen el alcance, como la red, la aplicación web, la interfaz de programación de aplicaciones (API), los servicios alojados y los controles de las instalaciones físicas; frecuencia; limitaciones, como horas aceptables y tipos de ataques excluidos; información del punto de contacto; remediación, como la forma en que los hallazgos se enrutarán internamente; y requisitos retrospectivos.	N/A	Identificar			
18.2	Realizar pruebas periódicas de penetración externa	Realice pruebas de penetración externas periódicas basadas en los requisitos del programa, no menos de una vez al año. Las pruebas de penetración externas deben incluir reconocimiento empresarial y ambiental para detectar información explotable. Las pruebas de penetración requieren habilidades y experiencia especializadas y deben realizarse a través de una organización calificada. La prueba puede ser caja blanca o caja gris.	Red	Identificar			
18.3	Corregir los resultados de la prueba de penetración	Repare los hallazgos de las pruebas de penetración según la política de la empresa para el alcance y la priorización de la remediación.	Red	Proteger			
18.4	Valide las medidas de seguridad	Valide las medidas de seguridad después de cada prueba de penetración. Si lo considera necesario, modifique los conjuntos de reglas y las capacidades para detectar las técnicas utilizadas durante las pruebas.	Red	Proteger			
18.5	Realice pruebas periódicas de penetración interna	Realice pruebas de penetración internas periódicas basadas en los requisitos del programa, no menos de una vez al año. La prueba puede ser caja blanca o caja gris.	N/A	Identificar			

The Center for Internet Security, Inc. (CIS®) makes the connected world a safer place for people, businesses, and governments through our core competencies of collaboration and innovation. We are a community-driven nonprofit, responsible for the CIS Controls® and CIS Benchmarks™, globally recognized best practices for securing IT systems and data. We lead a global community of IT professionals to continuously evolve these standards and provide products and services to proactively safeguard against emerging threats.

Our CIS Hardened Images® provide secure, on-demand, scalable computing environments in the cloud. CIS is home to the Multi-State Information Sharing and Analysis Center® (MS-ISAC®), the trusted resource for cyber threat prevention, protection, response, and recovery for U.S. State, Local, Tribal, and Territorial government entities, and the Elections Infrastructure Information Sharing and Analysis Center® (EI-ISAC®), which supports the rapidly changing cybersecurity needs of U.S. elections offices. To learn more, visit www.cisecurity.org or follow us on Twitter: [@CISecurity](https://twitter.com/CISecurity).