Política de Uso Aceptable

**Abril 2023**

**Contenido**

[**Contenido 2**](#_30j0zll)

[**Reconocimientos 3**](#_1y810tw)

[**Introducción 4**](#_1fob9te)

[Propósito 4](#_3znysh7)

[Alcance 4](#_2et92p0)

[Definición de activos empresariales 4](#_tyjcwt)

[**Temas de la política de uso aceptable 6**](#_3dy6vkm)

[**Plantilla de política de uso aceptable 9**](#_4d34og8)

[Propósito 9](#_2s8eyo1)

[Aplicabilidad 9](#_17dp8vu)

[Excepciones 9](#_3rdcrjn)

[Política 9](#_26in1rg)

[**Historial de Revisiones 12**](#_lnxbz9)

[**Apéndice A: Acrónimos y abreviaturas 13**](#_35nkun2)

[**Apéndice B: Glosario 14**](#_1ksv4uv)

[**Apéndice C: Grupos de implementación 17**](#_44sinio)

[**Apéndice D: Mapeo de Salvaguardas del CIS 18**](#_z337ya)

[**Apéndice E: Referencias y recursos 19**](#_3j2qqm3)

**Introducción**

Las políticas de uso aceptable a menudo actúan como un documento de términos y condiciones para los empleados. Son la piedra angular de un conjunto de políticas de seguridad de la información. Por lo general, se pedirá a los usuarios que lean el documento, confirmen su comprensión y firmen antes de que se les otorgue acceso a los activos, datos y otros recursos de la empresa. Por lo general, estos acuerdos de usuario están destinados a aplicarse en toda la empresa, pero a veces es necesario para que existan acuerdos específicos del proyecto y de la unidad de negocio. Las reglas definidas en este documento deben actualizarse periódicamente para satisfacer las necesidades de la empresa y aplicarse periódicamente. Las políticas de uso aceptable ayudan a reducir el riesgo y a educar a los usuarios sobre la política actual de la empresa. Por lo tanto, deben estar escritos de tal manera que sean fáciles de entender y seguir por todos los lectores, independientemente de su nivel de experiencia técnica.

**Propósito**

Los Controles de Seguridad Críticos del CIS® (CIS Controls®) recomiendan múltiples políticas que una empresa debe tener implementadas como elementos fundamentales de su programa de ciberseguridad. El Grupo de Trabajo sobre Políticas de Seguridad de la Información de los Controles del CIS trabajó en la elaboración de políticas de apoyo a los Controles del CIS. Una vez completado el alcance inicial del Grupo de Trabajo, el Grupo de Trabajo recomendó que también se creara un modelo de Política de Uso Aceptable. Esta plantilla de política existe fuera de los temas típicos tratados en los controles CIS, ya que los controles CIS no abordan el uso aceptable. Si se desea, se recomienda a las empresas que utilicen esta plantilla de política en su totalidad o parcialmente. El contenido específico de una Política de Uso Aceptable varía ampliamente. Dicho esto, a menudo se considera una buena práctica incluir lo que un usuario puede hacer con los datos de la empresa, cómo se pueden usar los activos de la empresa y cómo se pueden transmitir los datos de la empresa a otras partes.

**Alcance**

Esta plantilla de directiva está pensada para complementar los controles de CIS v8. Las declaraciones de política incluidas en este documento pueden ser utilizadas por todos los Grupos de Implementación (IGs) de la CIS, pero están específicamente orientadas a las Salvaguardias en el Grupo de Implementación 1 (IG1). [En el Apéndice D](#_2jxsxqh) se señala que hay 0 Salvaguardas CIS dentro de esta Política asignadas a los Controles CIS. Para más información sobre los Grupos de Implementación del CIS, véase el [Apéndice C](#_44sinio). Además, en el [Apéndice B se proporciona un glosario](#_1ksv4uv)  para explicar la terminología utilizada en todo el documento. Dependiendo del sector o la misión de una empresa, es posible que también sea necesario agregar o eliminar otras declaraciones de política.

**Definición de activos empresariales**

Hay muchos tipos de activos empresariales que pueden existir en una empresa. Muchos de ellos deberán estar cubiertos por una Política de Uso Aceptable, pero habrá situaciones en las que esto no sea posible. Por ejemplo, los usuarios fuera de la unidad de negocio de tecnología de la información (TI) rara vez necesitarán ingresar a la sala de servidores y administrar servidores, lo que significa que es posible que los servidores no necesiten estar cubiertos por la Política de uso aceptable más general. A los efectos de este documento y en los Controles® de seguridad críticos de CIS v8 (CIS Controls® v8), los activos empresariales se definen como todos los dispositivos de usuario final, dispositivos de red, dispositivos no informáticos/de Internet de las cosas (IoT) y servidores que existen en entornos virtuales, basados en la nube o físicos, incluidos aquellos a los que se puede conectar de forma remota. Los activos empresariales son activos gestionados por la empresa y tienen el potencial de almacenar, procesar o transmitir datos. Los tipos de activos empresariales incluyen:

* *Dispositivos de usuario final*, como ordenadores de sobremesa, estaciones de trabajo, portátiles, tabletas y smartphones.
* *Dispositivos de red*, como puntos de acceso inalámbricos, conmutadores, firewalls, puertas de enlace físicas/virtuales y enrutadores.
* *Dispositivos no informáticos/de Internet de las cosas (IoT),* como sistemas de control industrial (ICS), pantallas inteligentes, impresoras, sensores de seguridad física y sensores de seguridad de TI.
* *Servidores*, como servidores web, servidores de correo electrónico, servidores de aplicaciones y servidores de archivos.



*Figura 1. Activos de la empresa, tal y como se definen en CIS Controls v8*

**Temas de la política de uso aceptable**

Las plantillas de política de seguridad de la información de CIS generalmente siguen un modelo tipo ciclo de vida, pero eso no es posible dentro de esta plantilla de política. Una política de uso aceptable simplemente informa a los empleados sobre cómo se les permite utilizar los activos de tecnología de la información (TI) que su empresa les ha proporcionado para realizar su trabajo. Esencialmente, una lista de lo que se debe y no se debe hacer, o "Uso aceptable" y "Uso inaceptable". El contenido real de una política de *uso aceptable* variará, pero generalmente contiene las mejores prácticas para los siguientes temas que se tratarán:



* **Uso aceptable** : acciones que los empleados pueden realizar con los activos empresariales.
* **Uso prohibido** : acciones que los empleados no deben realizar con los activos empresariales.
* **Uso personal** : restricciones en torno al uso de los activos de la empresa para asuntos personales.
* **Expectativas de privacidad** : descripciones del nivel de privacidad que los usuarios pueden esperar al trabajar con los activos empresariales.
* **Notificación de infracciones** : métodos para notificar infracciones de la directiva de uso aceptable de la empresa y otras directivas de la empresa.
* **Trabajo remoto** : políticas para usuarios que trabajan desde sus hogares en lugar de la oficina o el lugar de destino asignado.
* **Bring Your Own Device** : declaraciones que restringen o permiten el uso de dispositivos personales para actividades laborales.

**Uso aceptable**

Esta sección debe describir la manera en que los usuarios están autorizados a usar sus activos, datos y otros recursos de la empresa. Se deben enumerar los tipos específicos de activos cubiertos por la Política de uso aceptable, como estaciones de trabajo, dispositivos móviles y computadoras portátiles. También se pueden cubrir aplicaciones específicas, especialmente navegadores, correo electrónico, contactos y calendario. Deben examinarse los métodos aceptables de tratamiento de los datos de la empresa, que deben hacer referencia específicamente a la propiedad intelectual. Por último, las políticas relacionadas con las redes sociales pueden colocarse aquí o en la sección *Uso prohibido*.

**Uso prohibido**

Las acciones que no desea que los usuarios realicen con los activos de empresa se pueden colocar dentro de esta sección. Muchos de los elementos enumerados aquí también podrían indicarse de una manera diferente dentro de la sección Uso *aceptable* . El número de declaraciones de política enumeradas en *Uso prohibido* puede ser mucho mayor que en *Uso aceptable*. Aunque cada empresa variará en cuanto a lo que específicamente debe colocarse aquí, los temas de ejemplo incluyen: uso de almacenamiento en la nube y servicios de intercambio de archivos, IT shadow, conexión de activos empresariales a otras redes que no son propiedad de la empresa y uso de activos empresariales en las redes sociales y representación de la empresa ante el público en general. En caso de duda, puede ser prudente especificar en exceso las acciones prohibidas y modificar la Política de uso aceptable con el tiempo después de adquirir experiencia. Dicho esto, los redactores de políticas no deben colocar una multitud de actividades prohibidas dentro de la Política de uso aceptable que no se aplican regularmente.

**Uso personal de los activos de la empresa**

El uso personal de los activos de la empresa puede ser un tema desafiante. Es fácil imaginar un espectro de uso personal, desde "no uso personal de los activos de la empresa" hasta "los usuarios pueden hacer lo que quieran con los activos de la empresa". La mayoría de las empresas se encuentran en algún lugar en el medio de ese espectro. Una política clara y bien redactada puede ayudar a los usuarios a comprender qué es y qué no es apropiado con las diferentes clases de activos empresariales. Por ejemplo, los usuarios pueden recibir teléfonos empresariales y pueden realizar una variedad de tareas personales en esos dispositivos, pero es posible que se aplique un conjunto diferente de reglas a las computadoras portátiles. El uso personal de los activos de la empresa no es el único tema que debe tenerse en cuenta. La forma en que los usuarios acceden a los recursos empresariales y manejan los datos empresariales en dispositivos personales puede tener un impacto masivo en la seguridad de la empresa en general. En parte debido a este hecho, Bring Your Own Device (BYOD) se divide en un área temática separada dentro de esta plantilla de directiva.

Como mínimo, las declaraciones de política de *uso personal* deben cubrir las reglas para los usuarios que visitan sitios web y que revisan cuentas de correo electrónico personales en los activos de la empresa. Una frase común que se encuentra en muchas políticas de uso aceptable es "uso personal limitado". No existe una definición 100% consensuada de este término, y las empresas deben trabajar para definir lo que significa para ellas el uso personal limitado si se va a utilizar. Dado que es muy probable que los usuarios revisen su correo electrónico y visiten sitios personales utilizando activos de la empresa, independientemente de la política de la empresa, se necesita una definición realista. Otros temas incluyen el uso de cuentas personales en todo un dispositivo, el almacenamiento de datos empresariales en plataformas personales en la nube. También se debe tener en cuenta la sincronización del navegador y los perfiles del navegador, ya que los sitios web y las aplicaciones no seguros que el usuario visita en su tiempo personal en dispositivos personales pueden propagarse a los activos de la empresa. También se puede discutir el uso de administradores de contraseñas, especialmente si la empresa no proporciona un administrador de contraseñas autorizado por la empresa.

**Expectativas de privacidad**

Los usuarios deben tener en cuenta que en los activos de la empresa, los usuarios no deben esperar ningún grado de privacidad personal. Esto significa que todos los datos almacenados y todas las comunicaciones que se originan en los activos de la empresa son propiedad de la empresa y pueden ser monitoreados y

revisados. Si bien la mejor práctica es mantener los datos personales o las comunicaciones en dispositivos personales y fuera de la red empresarial, algunas empresas pueden permitir el uso compartido de los activos empresariales y BYOD.

**Denuncia de infracciones**

Las empresas deben definir claramente cómo los usuarios pueden denunciar infracciones de la política de uso aceptable, otras políticas empresariales y cualquier signo potencial de una violación de datos dentro de la empresa. Esto debe incorporarse en el Programa de Capacitación en Conciencia de Ciberseguridad de la empresa. Se debe informar a los usuarios de que las infracciones autoinformadas no tendrán repercusiones para garantizar que esta información esté disponible para la empresa.

**Bring Your Own Device (BYOD)**

BYOD es la práctica de los usuarios empresariales que aprovechan sus dispositivos personales para tareas empresariales. Por lo general, estos dispositivos son teléfonos inteligentes o computadoras portátiles. Hay varias formas de implementar BYOD, como colocar el dispositivo completamente bajo el control de la administración de la empresa, usar una red privada virtual (VPN) para obtener una dirección de protocolo de Internet (IP) interna, aislar los dispositivos BYOD en redes restringidas o simplemente permitir que un dispositivo se conecte a los servicios en la nube de la empresa a través de una aplicación en el dispositivo. Las empresas deben trabajar para proteger su información en dispositivos personales y asegurarse de que otras aplicaciones no accedan a material sensible o confidencial. Tenga en cuenta que esta política de uso aceptable por sí sola no es suficiente para crear una política de BYOD y se alienta a las empresas a desarrollar sus propias políticas de BYOD sólidas para cubrir situaciones y amenazas únicas para ellas. Las empresas más avanzadas, como las que se autoclasifican como CIS Implementation Group (IG) IG2 e IG3, deben utilizar herramientas de gestión de dispositivos móviles y de gestión de la movilidad empresarial para habilitar BYOD. Para obtener instrucciones adicionales sobre el uso de los controles CIS para dispositivos móviles, consulte la [Guía complementaria móvil de CIS Controls](https://www.cisecurity.org/insights/white-papers/cis-controls-mobile-companion-guide-2).

**Trabajo remoto**

El trabajo remoto se produce cuando los usuarios de la empresa trabajan desde una ubicación fuera de las instalaciones de la empresa, accediendo a la información, ya sea en papel o electrónicamente, a través de equipos de la empresa. Los entornos de trabajo a distancia incluyen los denominados "teletrabajo", "telecommuting", "lugar de trabajo flexible", "entornos de trabajo virtuales" y "remote maintenance". La empresa debe informar a los usuarios que, independientemente de dónde estén trabajando, se aplica esta Política de uso aceptable. Las empresas deben alentar a los usuarios a tomar precauciones de seguridad adicionales cuando trabajen de forma remota, incluido permitir que otras personas ingresen a la ubicación de trabajo remoto para tener acceso o ver los datos de la empresa. Tenga en cuenta que esta política de uso aceptable por sí sola es insuficiente para crear una política integral de trabajo remoto y se alienta a las empresas a desarrollar programas sólidos de trabajo remoto.

**Política de uso aceptable**

**Propósito**

Esta *Política de Uso Aceptable* actúa como un acuerdo entre la empresa y el usuario que recibe los activos de Tecnología de la Información (TI). Los activos se definen como cualquier cosa que tenga valor para una organización, incluidos, pero no limitado a, otra organización, persona, dispositivo informático, sistema de TI, red de TI, software (tanto una instancia instalada como una instancia física), plataforma de computación virtual (común en la nube y la computación virtualizada) y hardware relacionado (por ejemplo, cerraduras, gabinetes, teclados). Esta *política de uso aceptable* define el uso permitido de estos activos, así como las acciones restringidas que los usuarios no deben realizar para reducir el riesgo para la empresa.

**Aplicabilidad**

Esta política está pensada para aplicarse a todos los usuarios de la empresa que reciben y utilizan activos de la empresa, lo que incluye a todos los miembros de la plantilla (tanto in situ como a distancia), proveedores externos, contratistas, proveedores de servicios, consultores o cualquier otra persona que opere un activo de la empresa. Es responsabilidad del usuario leer y comprender esta política y llevar a cabo sus actividades de acuerdo con sus términos. Además, los usuarios deben leer y comprender la Política de seguridad de la información de la empresa y sus estándares asociados. Se recomienda a los usuarios que consideren que las declaraciones de política de este documento no son claras que se pongan en contacto con el departamento de TI para aclarar las ambigüedades restantes.

**Excepciones**

Es probable que se produzcan excepciones a esta política. Las solicitudes de excepción pueden ocurrir por una variedad de razones, pero en general los empleados deberán usar los activos de TI de la empresa de una manera que sea incoherente con la política. Por ejemplo, es común tener que conectar un dispositivo personal a la red de la empresa o poner los datos de la empresa en posesión de un contratista externo. Todas las solicitudes de excepción deben hacerse por escrito y deben contener:

* El motivo de la solicitud,
* Riesgo para la empresa de no seguir la política escrita,
* Mitigaciones específicas que no se implementarán,
* Dificultades técnicas y de otro tipo, y
* Fecha de revisión.

Todas las excepciones deben ser aprobadas por un administrador autorizado para aprobar la excepción.

**Política**

**Responsabilidades del usuario**

1. Los usuarios solo deben utilizar tecnología y servicios aprobados.
2. Todos los activos de la empresa se prestan a los usuarios para que se puedan realizar las funciones laborales esenciales.
3. Tras la separación de la empresa o la rescisión del contrato, el usuario debe devolver todos los activos de TI suministrados y los datos asociados.
4. Los usuarios deben proteger el entorno físico alrededor de su estación de trabajo y bloquear sus equipos cuando se alejen.
5. Los usuarios deben asegurarse de que la información de identificación personal (PII), confidencial y cualquier dato sensible que pueda estar cubierto por regulaciones

gubernamentales u otras regulaciones, no esté fácilmente disponible o accesible en sus escritorios o dentro de su espacio de trabajo.

1. Todos los usuarios deben tener el cuidado adecuado para proteger la información, los sistemas y los activos relacionados bajo su custodia o cuidado contra pérdidas, daños o perjuicios.
	1. Los equipos perdidos o dañados deben ser reportados a TI tan pronto como sea posible.
2. Los usuarios deben almacenar sus contraseñas de forma segura.
	1. Los administradores de contraseñas aprobados deben usarse para almacenar contraseñas digitalmente.
3. Las cuentas asignadas por los usuarios solo deben acceder a activos, sistemas operativos, aplicaciones, archivos y datos a los que se les haya concedido acceso. La capacidad de leer, ejecutar, modificar, eliminar o copiar datos inadvertidamente no implica permiso para hacerlo.
4. Solo los usuarios autorizados pueden publicar contenido o crear la impresión de que están representando, expresando opiniones o haciendo declaraciones en nombre de la empresa en sitios de redes sociales, blogs u otros sitios de Internet.
5. Los usuarios deben mantener la confidencialidad del conocimiento sobre la información y los sistemas de información adquiridos durante el empleo y la confidencialidad debe mantenerse después de que cese el empleo.

**Uso prohibido**

1. Solo los dispositivos aprobados y autorizados pueden conectarse a redes que sean propiedad de la empresa o estén administradas por ella. Esto incluye dispositivos portátiles de usuario final, dispositivos extraíbles (por ejemplo, memorias USB) y dispositivos de propiedad personal.
2. Los usuarios no deben compartir sus contraseñas con otras personas ni permitir el uso de su cuenta por parte de otras personas.
	1. Los usuarios son responsables de toda la actividad que se origine en sus nombres de usuario y cuentas.
3. Los usuarios no deben eludir los mecanismos de autenticación de usuarios ni la seguridad de ninguna cuenta de usuario o activo del sistema de información.
4. Los usuarios no deben instalar software, hardware ni modificar los ajustes de configuración del sistema en ningún activo de la empresa, a menos que lo permita explícitamente el rol y la responsabilidad del usuario.
5. Los usuarios no deben participar en ninguna actividad con la intención de interrumpir los activos o las redes de la empresa.
	1. Los usuarios no deben realizar ningún tipo de monitoreo de red, escaneo de puertos o escaneo de seguridad a menos que esta actividad sea parte del trabajo normal del individuo y esté formalmente autorizada.
6. Los usuarios no deben aprovechar los activos de la empresa para obtener beneficios económicos personales.
7. Los usuarios no deben utilizar la función "Recordarme" o "Recordar mi contraseña" dentro de un navegador.

**Expectativas de privacidad**

1. Al utilizar los recursos de la empresa, el usuario no tendrá ninguna expectativa de privacidad. El acceso y el uso de Internet, incluida la comunicación por correo electrónico y la mensajería instantánea y el contenido de los mismos, no son confidenciales, excepto en ciertos casos limitados reconocidos por la ley.
2. La empresa se reserva el derecho de monitorear, acceder y divulgar toda la información generada y las acciones realizadas utilizando los activos de TI de la empresa. Los archivos, los mensajes (incluidos los archivos adjuntos) y los registros pueden conservarse y utilizarse como prueba en litigios, auditorías e investigaciones.

**Uso personal**

1. Los usuarios tienen permitido un uso personal limitado de los activos de la empresa, como visitar sitios web y consultar cuentas de correo electrónico personales.
	1. Los usuarios pueden acceder a administradores de contraseñas personales basados en la web en los activos de la empresa. La instalación local de un administrador de contraseñas debe ser aprobada por TI.
		1. Los usuarios no deben almacenar contraseñas de empresa en administradores de contraseñas personales.
	2. Los usuarios no deben utilizar la sincronización del navegador o los perfiles del navegador que mueven el historial del navegador de un usuario de un dispositivo personal a un activo de la empresa (o viceversa).
2. Los usuarios no deben usar cuentas de propiedad personal (por ejemplo, ID de Apple, cuenta de Google, cuenta de Microsoft) para cuentas de todo el dispositivo (por ejemplo, Android, iOS, Windows) en dispositivos empresariales, a menos que la empresa lo permita.
	1. Los usuarios deben trabajar con el departamento de TI para crear cuentas específicas de la empresa para los activos necesarios y los servicios de terceros, como la creación de un ID de Apple propiedad de la empresa para un dispositivo Apple.
3. Los usuarios no deben utilizar claves de licencia de empresa en dispositivos personales a menos que la empresa lo autorice.
4. Los datos empresariales no deben almacenarse en plataformas de proveedores de nube personales que no sean de empresa (por ejemplo, Google Drive, Microsoft OneDrive, Dropbox).

**Denuncia de infracciones**

1. Los usuarios que tengan conocimiento de cualquier evento que amenace la disponibilidad, integridad o confidencialidad de los datos de la empresa, o que infrinja cualquier norma, política, procedimiento o cualquier requisito asociado, o que sea contrario a la ley, debe ponerse en contacto inmediatamente con TI o con su jefe inmediato.

**Trabajo remoto**

1. Todo el trabajo de la empresa debe realizarse en activos aprobados por la empresa.
2. Todos los datos de la empresa deben almacenarse en activos empresariales aprobados.
3. Los usuarios no deben conectar activos empresariales a redes Wi-Fi abiertas y sin cifrar.
4. Los usuarios deben ser conscientes de su entorno cuando trabajen de forma remota para asegurarse de que otros no estén viendo material sensible.

**Bring Your Own Device**

1. Los dispositivos personales no deben estar conectados a la red de la empresa sin autorización formal.
2. Los datos de la empresa no deben almacenarse en dispositivos personales sin autorización formal.
3. Los usuarios que utilicen su dispositivo personal para almacenar datos empresariales pueden exponerse a un borrado completo del dispositivo. Las razones para borrar el dispositivo pueden incluir:
	1. Dispositivo perdido/robado.
	2. Terminación de la relación laboral del usuario.
	3. Cuenta o dispositivo comprometido/hackeado.

**Historial de Revisiones**
Cada vez que se actualiza este documento, se debe actualizar esta tabla.
.

| Versión | Fecha de Revisión | Descripción de la Revisión | Nombre |
| --- | --- | --- | --- |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**Apéndice A: Acrónimos y abreviaturas**

| BYOD | Bring your own device (Trae tu propio dispositivo) |
| --- | --- |
| CIS | Center for Internet Security (Centro para la Seguridad en Internet) |
| CIS Controls | Center for Internet Security Critical Security Controls (Centro de Controles de Seguridad Críticos de Internet) |
| ICS | Industrial controls systems (Sistemas de control industrial) |
| IG | Implementation Group (Grupo de Implementación)**Insertar**Traducciones de **implementación**nombre) |
| IoT | Internet of Things (Internet de las cosas) |
| IP | Internet protocol (Protocolo de Internet) |
| IT | Information Technology (Tecnologías de la información) |
| PII | Personally Identifiable Information (Información de identificación personal) |
| VPN | Virtual Private Network (Red Privada Virtual) |

**Apéndice B: Glosario**

| Activo | Cualquier cosa que tenga valor para una organización, incluyendo, pero no limitado a, otra organización, persona, dispositivo informático, sistema de tecnología de la información (TI), red de TI, circuito de TI, software (tanto una instancia instalada como una instancia física), plataforma de computación virtual (común en la nube y la computación virtualizada) y hardware relacionado (por ejemplo, cerraduras, gabinetes, teclados).Fuente: [Activo(s) - Glosario | CSRC (nist.gov)](https://csrc.nist.gov/glossary/term/asset) |
| --- | --- |
| Inventario de activos  | Un inventario de activos es un registro, depósito o lista completa de los activos de una empresa e información específica sobre esos activos.Fuente: [Inventario de activos | TLC (dot.gov)](https://www.transit.dot.gov/TAM/resources/assetinventory) |
| Propietario del activo | El departamento, la unidad de negocio o la persona responsable de un activo de la empresa.Fuente: CIS |
| Entorno en la nube | Un entorno virtualizado que proporciona acceso de red cómodo y bajo demanda a un grupo compartido de recursos configurables, como redes, informática, almacenamiento, aplicaciones y servicios. Hay cinco características esenciales para un entorno de nube: autoservicio bajo demanda, amplio acceso a la red, agrupación de recursos, elasticidad rápida y servicio medido. Algunos servicios ofrecidos a través de entornos en la nube incluyen software como servicio (SaaS), plataforma como servicio (PaaS) e infraestructura como servicio (IaaS). |
| Activos de la empresa | Activos con potencial para 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 virtuales, basados en la nube y físicos.Fuente: CIS Controls v8  |
| Dispositivos de usuario final | 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 final incluyen dispositivos móviles y portátiles, como computadoras portátiles, teléfonos inteligentes y tabletas, así como computadoras de escritorio y estaciones de trabajo. A los efectos de este documento, los dispositivos de usuario final son un subconjunto de los activos de la empresa.Fuente: CIS Controls v8 |
| Identificador de activos empresariales  | A menudo, una pegatina o etiqueta con un número único o una cadena alfanumérica que se puede rastrear dentro de un inventario de activos empresariales.Fuente: CIS |
| Dispositivos móviles de usuario final | Pequeños dispositivos de usuario final emitidos por la empresa con capacidad inalámbrica intrínseca, como teléfonos inteligentes y tabletas. Los dispositivos móviles de usuario final son un subconjunto de dispositivos portátiles de usuario final, incluidos los portátiles, que pueden requerir hardware externo para la conectividad. A los efectos de este documento, los dispositivos móviles de usuario final son un subconjunto de los dispositivos de usuario final.Fuente: CIS Controls v8 |
| Dispositivos de red | Dispositivos electrónicos necesarios para la comunicación e interacción entre dispositivos en una red informática. Los dispositivos de red incluyen puntos de acceso inalámbricos, firewalls, puertas de enlace físicas/virtuales, enrutadores y conmutadores. Estos dispositivos constan de hardware físico, así como de dispositivos virtuales y basados en la nube. A los efectos de este documento, los dispositivos de red son un subconjunto de los activos empresariales.Fuente: CIS Controls v8 |
| Dispositivos no informáticos/de Internet de las cosas (IoT) | Dispositivos integrados con sensores, software y otras tecnologías con el fin de conectarse, 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 llevar a cabo procesos comerciales. Algunos ejemplos de estos dispositivos son las impresoras, las pantallas inteligentes, los sensores de seguridad física, los sistemas de control industrial y los sensores de tecnología de la información. A los efectos de este documento, los dispositivos no informáticos/IoT son un subconjunto de los activos empresariales.Fuente: CIS Controls v8 |  |
| Entorno físico | Partes físicas de hardware que componen una red, incluidos cables y enrutadores. El hardware es necesario para la comunicación e interacción entre dispositivos en una red.Fuente: CIS Controls v8 |
| Dispositivos portátiles para el usuario final | Dispositivos transportables para el usuario final que tienen la capacidad de conectarse de forma inalámbrica a una red. A los efectos de este documento, los dispositivos portátiles de usuario final pueden incluir computadoras portátiles y dispositivos móviles como teléfonos inteligentes y tabletas, todos los cuales son un subconjunto de los activos empresariales.Fuente: CIS Controls v8 |
| Dispositivos remotos | Cualquier activo de la empresa capaz de conectarse a una red de forma remota, normalmente desde la Internet pública. Esto puede incluir activos empresariales como dispositivos de usuario final, dispositivos de red, dispositivos no informáticos/de Internet de las cosas (IoT) y servidores.Fuente: CIS Controls v8 |
| Servidores | 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 amplia. 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.Fuente: CIS Controls v8 |
| Usuario | Empleados (tanto presenciales como remotos), proveedores externos, contratistas, proveedores de servicios, consultores o cualquier otra persona que opere un activo empresarial.Fuente: CIS |
| Entorno virtual | Simula hardware para permitir que un entorno de software se ejecute sin la necesidad de usar una gran cantidad de hardware real. Los entornos virtualizados se utilizan para hacer que un pequeño número de recursos actúe como muchos con suficiente capacidad de procesamiento, memoria, almacenamiento y red. La virtualización es una tecnología fundamental que permite que la computación en la nube funcione.Fuente: CIS Controls v8 |

**Apéndice C: Grupos de implementación**

Como parte de nuestra versión más reciente de los Controles CIS, v8, creamos Grupos de Implementación (IGs) para proporcionar granularidad y una estructura explícita a las diferentes realidades que enfrentan las empresas de diversos tamaños.

**IG1**

Una empresa IG1 es de tamaño pequeño a mediano con experiencia limitada en TI y ciberseguridad para dedicarse a proteger los activos y el personal de TI. La principal preocupación de estas empresas es mantener el negocio operativo, ya que tienen una tolerancia limitada al tiempo de inactividad. La sensibilidad de los datos que intentan proteger es baja y rodea principalmente a la información financiera y de los empleados. Las salvaguardas seleccionadas para IG1 deben poder implementarse con una experiencia limitada en ciberseguridad y tener como objetivo frustrar ataques generales no dirigidos. Estas salvaguardas también se diseñarán normalmente para funcionar en conjunto con hardware y software comercial listo para usar (COTS) de oficinas pequeñas o en el hogar.

**IG2**

Una empresa IG2 emplea a personas responsables de administrar y proteger la infraestructura de TI. Estas empresas apoyan a múltiples departamentos con diferentes perfiles de riesgo según la función y la misión del trabajo. Las unidades de pequeña empresa pueden tener cargas de cumplimiento normativo. Las empresas IG2 a menudo almacenan y procesan información confidencial de clientes o empresas, y pueden soportar breves interrupciones del servicio. Una de las principales preocupaciones es la pérdida de confianza del público si se produce una infracción. Las salvaguardas seleccionadas para IG2 ayudan a los equipos de seguridad a hacer frente a una mayor complejidad operativa. Algunas medidas de seguridad dependerán de la tecnología de nivel empresarial y de la experiencia especializada para instalarse y configurarse correctamente.

**IG3**

Una empresa IG3 emplea expertos en seguridad que se especializan en las diferentes facetas de la ciberseguridad (por ejemplo, gestión de riesgos, pruebas de penetración, seguridad de aplicaciones). Los activos y datos de IG3 contienen información o funciones confidenciales que están sujetas a supervisión regulatoria y de cumplimiento. Una empresa IG3 debe abordar la disponibilidad de los servicios y la confidencialidad e integridad de los datos confidenciales. Los ataques exitosos pueden causar un daño significativo al bienestar público. Las salvaguardas seleccionadas para IG3 deben reducir los ataques dirigidos de un adversario sofisticado y reducir el impacto de los ataques de día cero.

Si desea saber más sobre los Grupos de Implementación y cómo se relacionan con las empresas de todos los tamaños, hay muchos recursos que exploran los Grupos de Implementación y los Controles CIS en general en nuestro sitio web en <https://www.cisecurity.org/controls/cis-controls-list/>.

**Apéndice D: Mapeo de Salvaguardas del CIS**

**Controles y salvaguardas de CIS cubiertos por esta política**

Esta política no contiene ninguna asignación a los controles CIS.

*Table 1 – Salvaguardas cubiertas por IG1*

| CIS Control | Declaración de política | Salvaguarda CIS | Descripción de la salvaguarda CIS  |
| --- | --- | --- | --- |
| N/A | N/A | N/A | N/A |
| N/A | N/A | N/A | N/A |
| N/A | N/A | N/A | N/A |

**Apéndice E: Referencias y recursos**

Center for Internet Security®

<https://www.cisecurity.org/>

CIS Critical Security Controls®

<https://www.cisecurity.org/controls/>