**Política de manejo de cuentas y credenciales**

# Contenido

[**Contenido 2**](#_heading=h.gjdgxs)

[**Reconocimientos 3**](#_heading=h.2xcytpi)

[**Introducción 4**](#_heading=h.30j0zll)

[Propósito 4](#_heading=h.1fob9te)

[Tipos de cuentas y gestión de credenciales 4](#_heading=h.3znysh7)

[Tipos de credenciales 5](#_heading=h.2et92p0)

[Alcance 5](#_heading=h.tyjcwt)

[**Ciclo de vida de la administración de cuentas y credenciales 6**](#_heading=h.3dy6vkm)

[**Plantilla de política de administración de cuentas y credenciales 9**](#_heading=h.1ci93xb)

[Propósito 9](#_heading=h.4d34og8)

[Responsabilidad 9](#_heading=h.17dp8vu)

[Excepciones 9](#_heading=h.3rdcrjn)

[Política 9](#_heading=h.26in1rg)

[**Historial de revisiones 12**](#_heading=h.1ksv4uv)

[**Apéndice A: Acrónimos y abreviaturas 13**](#_heading=h.44sinio)

[**Apéndice B: Glosario 14**](#_heading=h.2jxsxqh)

[**Apéndice C: Grupos de implementación 17**](#_heading=h.z337ya)

[**Apéndice D: Mapeo de Salvaguardias del CIS 18**](#_heading=h.1y810tw)

[**Apéndice E: Referencias y recursos 20**](#_heading=h.4i7ojhp)

# Introducción

Las cuentas y credenciales, como las contraseñas, son la forma en que accedemos a teléfonos, tabletas, estaciones de trabajo y aplicaciones web. Cada una de estas cuentas se puede utilizar para obtener acceso no autorizado al jardín amurallado de una empresa para robar datos. Hay muchas formas de obtener acceso de forma encubierta a cuentas, como contraseñas débiles, cuentas antiguas de un empleado despedido o contraseñas involucradas en una violación de datos para una empresa separada que también se utilizan en sus sistemas. Hay varios tipos de cuentas que a menudo necesitan ser administradas.

## Propósito

Los controles de seguridad crítica de CIS® (controles CIS®) describen varias políticas que una empresa debe tener implementadas. Esto incluye un conjunto de políticas para cubrir cómo se administran las cuentas y las credenciales en la empresa, y otras funciones relacionadas con el control de acceso. Esta política pretende ser un "punto de partida" para las empresas que necesitan elaborar sus propias políticas. Se anima a las empresas a utilizar esta plantilla de política en su totalidad o parcialmente. Dicho esto, hay múltiples puntos de decisión y áreas que deben adaptarse a su empresa. En CIS Controls v8, los controles 5 y 6 establecen:

***Control 5 – Gestión de cuentas***

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

***Control 6 – Gestión del control de acceso***

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

Para respaldar esta protección, es importante que una empresa desarrolle políticas y procesos para controlar el acceso en la empresa. Este documento apoya el desarrollo de dichos procesos de acuerdo con los Controles CIS.

## Tipos de cuentas y gestión de credenciales

Los controles CIS cubren una amplia gama de funciones de autenticación, autorización y administración de cuentas. Existen varios tipos de cuentas y todas deben administrarse de alguna manera. Estos tipos de cuentas pueden incluir:

* Cuentas administrativas: también conocidas como cuentas de superusuario, privilegiadas o root, estas cuentas tienen amplios privilegios para controlar sistemas operativos, aplicaciones y plataformas.
* Cuentas de usuario: Estas cuentas son normalmente cuentas privilegiadas utilizadas por empleados y contratistas para realizar sus tareas laborales.
* Cuentas de proveedor: cuentas creadas por el proveedor de una tecnología, como un firewall o una plataforma en la nube. Estas cuentas pueden, o no, ser cuentas administrativas. A menudo están preinstalados y los nombres de usuario y contraseñas pueden ser ampliamente conocidos, lo que provoca una vulnerabilidad de acceso.
* Cuentas predeterminadas: Estas cuentas suelen estar preinstaladas y los nombres de usuario y contraseñas pueden ser ampliamente conocidos, lo que podría permitir el acceso no autorizado. Pueden ser cuentas de proveedor, pero también pueden ser cuentas para que cualquier usuario las aproveche.

## Tipos de credenciales

* Contraseñas: Texto memorizado que puede incluir números, caracteres especiales y letras mayúsculas. Para este documento, los números de identificación personal (PIN), las contraseñas y las frases de acceso se clasifican como "contraseñas".
* Autenticador de software: Esta contraseña o PIN se utilizará una sola vez y puede enviarse a través de un servicio de mensajes cortos (SMS) o compartirse dentro de una aplicación. Además, este método de autenticación puede requerir simplemente una interacción entre el usuario y su dispositivo, como seleccionar "Sí, este soy yo" dentro de una aplicación móvil. Hay muchos tipos diferentes de autenticadores de software y esto continúa evolucionando a medida que cambia la tecnología.
* Credencial física de un solo uso: son dispositivos físicos que a menudo proporcionan a los usuarios un PIN rotativo. El ejemplo más común es un token RSA.
* Insignia física: Estas insignias se usan a menudo y se usan para entrar y salir de los edificios. La credencial puede proporcionar una imagen del empleado, también ser capaz de comunicarse de forma inalámbrica con un sistema de control de acceso físico o puede contener credenciales adicionales para un usuario, como una clave criptográfica.
* Biometría: Los dispositivos móviles hacen que el aprovechamiento de las credenciales biométricas, como la cara, la retina o la huella dactilar, esté mucho más disponible.

## 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 (GI) del CIS, pero están específicamente orientadas hacia las Salvaguardias en el Grupo de Implementación 1 (IG1). En  [el Apéndice D](#_heading=h.1y810tw), las medidas de seguridad exclusivas de IG1 se destacan específicamente para facilitar su uso. Para más información sobre los Grupos de Implementación de la CIS, véase el [Apéndice C](#_heading=h.z337ya). Además, en el [Apéndice B se proporciona un glosario](#_heading=h.2jxsxqh)  para orientar la terminología utilizada en todo el documento. Es posible que las versiones futuras de esta plantilla amplíen el alcance a las dos salvaguardias del Grupo de Implementación 2 (IG2). Las empresas IG2 e IG3 pueden sentir la necesidad de agregar secciones que vayan más allá de IG1, y son bienvenidas a hacerlo. Dependiendo del sector o la misión de una empresa, es posible que también sea necesario agregar o eliminar otras declaraciones de política. Esto se fomenta, ya que esta política debe moldearse y ajustarse a las necesidades de la empresa.

# Ciclo de vida de la administración de cuentas y credenciales

Al igual que los activos, se debe realizar un seguimiento de las cuentas y las credenciales para garantizar que se utilicen de manera adecuada y autorizada. Esto se debe al hecho de que son el principal punto de entrada a la red empresarial. Además, las cuentas y credenciales deben crearse y aprovisionarse de forma segura para los usuarios de la empresa. Las credenciales deben ser de cierta solidez para ser realistas y seguras en el entorno de amenazas actual, ya que las credenciales antiguas, débiles o incluso olvidadas son un candidato principal como medio para el acceso no autorizado. La figura 1 muestra el ciclo de vida general de cómo se crean, usan y, en última instancia, revocan las cuentas y las credenciales.



*Figura 1. Diagrama del ciclo de vida de la administración de cuentas y credenciales*

* **Incorporación** : este proceso atrae a nuevos usuarios a la empresa. Su identidad se verifica para garantizar que son quienes dicen ser.
* **Creación de cuenta** : una vez que se considera que un nuevo usuario se unirá a la empresa, se deben crear cuentas para ellos. Estas cuentas pueden almacenarse en Active Directory, pero también pueden ser necesarias cuentas adicionales para aplicaciones y servicios específicos. Estas cuentas tendrán permisos asignados en función de su rol.
* **Creación y emisión de credenciales** : las contraseñas, las insignias y cualquier otra credencial necesaria para que un usuario aproveche sus cuentas en el lugar de trabajo deben crearse y proporcionarse al usuario.
* **Uso de cuentas y credenciales** : los usuarios aprovecharán sus cuentas y credenciales para acceder a los recursos de trabajo y realizar sus tareas laborales.
* **Monitorear** : las cuentas también deben ser rastreadas y monitoreadas para asegurarse de que se están utilizando adecuadamente.
* **Modificar el acceso** : las personas pueden dejar la empresa, tomar una licencia médica prolongada o simplemente cambiar de trabajo dentro de la empresa. Los permisos otorgados a una cuenta cuando un usuario comienza con la empresa rara vez son el conjunto exacto de permisos que tienen cuando abandonan la empresa.
* **Terminación de la cuenta**: cuando los empleados abandonan la empresa, sus credenciales deben ser revocadas y ya no deben tener acceso a sus cuentas.

**Incorporación**

Una identidad se puede considerar como un conjunto de atributos que describen de forma única a una persona, dispositivo u otra entidad dentro de un contexto determinado. En el caso de la incorporación, la creación de una cuenta para una persona es la forma en que se crean las identidades para los nuevos usuarios y contratistas. Sin embargo, es importante asegurarse de que las personas sean realmente quienes dicen ser antes de que se les dé acceso a la empresa. Dicho más sucintamente; Las empresas deben verificar a los usuarios antes de que sean empleados. Las instituciones públicas, como las agencias gubernamentales federales y estatales, locales, tribales y territoriales (SLTT, por sus siglas en inglés) en los Estados Unidos, a menudo verifican los registros biométricos y de otro tipo con las fuerzas del orden y otras bases de datos gubernamentales. Es común que los empleadores privados realicen verificaciones de antecedentes crediticios, penales y de otro tipo para verificar la identidad.

**Creación de cuenta**

Una vez que se han verificado las identidades de los nuevos usuarios, se crean cuentas para ellos. Las cuentas actúan esencialmente como la  *"identidad" de facto dentro de* la empresa y, a menudo, se almacenan en servicios de directorio, como Microsoft Active Directory. Sin embargo, es poco común que Active Directory pueda admitir todas las cuentas que se necesiten. La mayoría de las empresas aprovechan las aplicaciones de terceros que pueden o no integrarse con Active Directory. Además, las aplicaciones en la nube a menudo requieren cuentas y, a menudo, son cuentas separadas y no están necesariamente asociadas con cuentas creadas y utilizadas dentro de la empresa. Algunos servicios y plataformas de terceros admitirán la federación de identidades, lo que significa que no será necesario crear nuevas cuentas.

Una vez que se crean cuentas para cualquier plataforma, deben colocarse en el inventario de la cuenta. Este inventario es un registro de todas las cuentas en uso para todo el software y otras aplicaciones utilizadas en toda la empresa. Aunque esto puede ser difícil, este inventario debe mantenerse actualizado. Este inventario se utilizará como base para administrar la identidad de un usuario en toda la empresa, desde la obtención de nuevos privilegios hasta la retirada o eliminación. Sin este inventario, es mucho más fácil que las cuentas se olviden y queden activas. Un método común utilizado para que los actores de amenazas obtengan acceso a una empresa es a través de la suplantación de identidad, utilizando cuentas creadas legítimamente.

**Creación y emisión de credenciales**

El propósito de las credenciales es validar una identidad. Se pueden encontrar ejemplos de credenciales en *Tipos de credenciales dentro de* este documento. Tenga en cuenta que la seguridad de las credenciales no es igual. Algunas credenciales son más sólidas o más confiables que otras. Las empresas deben tomar una decisión temprana sobre qué credenciales emitirán a los usuarios. Además, las combinaciones de diferentes tipos de credenciales permiten la autenticación multifactor, que debería ser el método predeterminado de autenticación en muchas aplicaciones empresariales.

Las contraseñas son omnipresentes en la sociedad moderna y, a menudo, son la forma más común de credencial utilizada por una empresa. Si tiene una cuenta en un sistema informático, es probable que haya al menos una contraseña que deberá administrarse. CIS proporciona una guía de política de contraseñas separada que puede ayudar a las empresas a tomar decisiones acertadas sobre la seguridad y el uso de contraseñas.

Por último, la forma en que se aprovisionan las credenciales a los usuarios marca la diferencia en su seguridad. El aprovisionamiento de credenciales a los usuarios físicamente en persona tiene un impacto positivo en su confiabilidad, lo que significa que dar credenciales a los usuarios en persona generalmente se considera más seguro. A veces es necesario proporcionar credenciales a los usuarios de forma remota, como con usuarios remotos a tiempo completo o proporcionar credenciales a través del dispositivo móvil de un usuario. Una vez hecho esto, se deben tomar las precauciones de seguridad adecuadas (por ejemplo, cifrado) para proteger la credencial en tránsito.

**Uso de cuentas y credenciales**

El proceso de autenticación utiliza identidades y credenciales para verificar las notificaciones de identidad de un usuario. Los protocolos se utilizan para realizar el proceso de autenticación con redes y computadoras. Algunos protocolos son más fuertes que otros y se deben usar protocolos modernos y seguros siempre que sea posible. Una vez que la autenticación se realiza correctamente, se proporcionan a un usuario derechos y privilegios para los recursos de la empresa. La autenticación remota, como la autenticación a través de credenciales empresariales a través de una red, generalmente requiere tipos de autenticación más seguros. En estos casos se debe utilizar la autenticación multifactor.

**Monitor**

A medida que los usuarios llegan y salen de la empresa, es mejor comprobar periódicamente el estado de las cuentas de usuario en el inventario de la cuenta. Algunas cuentas pasarán desapercibidas y conservarán los derechos y permisos de los datos confidenciales mucho después de que el usuario se haya ido. Las cuentas inactivas y olvidadas son los principales objetivos que los atacantes deben encontrar y utilizar para violar una red empresarial.

Las cuentas administrativas son un subconjunto importante de cuentas en las que centrarse y protegerse. Estas cuentas tienen la capacidad de apagar completamente la red de una empresa si se hace un mal uso. Por lo tanto, su actividad y uso deben ser monitoreados y cuando un administrador deja la empresa, estas cuentas deben ser rápidamente desactivadas o eliminadas. Además, es importante asegurarse de que los permisos de administrador no se proporcionen a la cuenta de usuario normal de un administrador. Esto puede causar incidentes y accidentes relevantes para la seguridad en los que el sistema de un administrador está infectado con malware y, a continuación, el malware se ejecuta con privilegios de superusuario.

**Modificar el acceso**

Los empleados pueden dejar la empresa, tomar una licencia médica prolongada o simplemente cambiar de trabajo dentro de la empresa. Los permisos otorgados a una cuenta cuando un usuario comienza con la empresa rara vez son el conjunto exacto de permisos que tienen cuando se van. A medida que los usuarios aprovechan sus cuentas, a menudo necesitarán nuevos permisos para acceder a nuevos recursos para nuevos proyectos y para acceder a nuevas tecnologías y aplicaciones que la empresa comience a usar. Los usuarios cambian de rol o se agregan a nuevos proyectos con bastante frecuencia, por lo que este puede ser un proceso grande y continuo.

**Cancelación de la cuenta**

Cuando los usuarios abandonan la empresa, sus credenciales deben ser revocadas y ya no deben tener acceso a sus cuentas. Esto debe suceder tan pronto como sea posible después de que abandonen la empresa para que el usuario no pueda abusar de su acceso. Algunas empresas incluso revocan el acceso antes de que se termine a un usuario, por lo que no hay oportunidad de que ocurra un abuso. Es importante tener un proceso escrito para la revocación de cuentas y credenciales para que, cuando surja la situación, los administradores y otro personal relevante sepan qué hacer en el momento. Es habitual que las cuentas se deshabiliten en lugar de eliminarse para conservar un registro de auditoría. La eliminación directa de las cuentas puede crear partes ilegibles en los archivos de registro y otras partes de la pista de auditoría.

## Propósito

La administración de cuentas y credenciales es el proceso de creación, aprovisionamiento, uso y finalización de cuentas y credenciales en la empresa. La *política de administración de cuentas y credenciales* proporciona los procesos y procedimientos para gobernar las cuentas y las credenciales.

## Responsabilidad

* La unidad de negocio de TI es responsable de todas las funciones de gestión de cuentas y credenciales. Esta información se transmite a otras unidades de negocio dentro de la empresa, como finanzas, contabilidad y ciberseguridad, según sea necesario o necesario. El departamento de TI es responsable de informar a todos los usuarios de sus responsabilidades en el uso de las cuentas y credenciales que se les asignen.
* Los usuarios son responsables de usar sus cuentas de manera coherente con la política de la empresa.

## Excepciones

Es probable que se produzcan excepciones a esta política. 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.

## Política

**Incorporación**

1. El departamento de TI debe mantener procedimientos para modificar el acceso, los permisos y las funciones de las cuentas de usuario.
2. Las cuentas recién creadas deben estar representadas dentro de este proceso.
3. El cambio de roles de usuario debe incluirse en este proceso.
4. El proceso de concesión de permisos debe aplicar el principio de privilegios mínimos.
5. Las cuentas predeterminadas o genéricas innecesarias deben cambiarse antes de que se implemente un nuevo sistema en la empresa.

**Creación de cuenta**

1. El departamento de TI debe desarrollar procedimientos para crear cuentas y asignar privilegios.
2. Los privilegios de administrador solo se deben proporcionar a las cuentas administrativas.
	1. Las cuentas de administrador y con privilegios solo deben usarse para las tareas de instalación y mantenimiento adecuadas; No es de uso diario.
	2. Las cuentas de administrador deben ser únicas y asignadas a una persona específica, a menos que estén técnicamente limitadas por un sistema o una aplicación.
3. Es responsabilidad de TI mantener un inventario de cuentas.
4. Como mínimo, el inventario de la cuenta debe contener los siguientes datos para cada cuenta:
5. Nombre de la persona
6. Nombre de la cuenta
7. Fecha de inicio y finalización del empleo
8. Unidad de negocio
9. Estado de la cuenta (es decir, habilitado, deshabilitado)
10. Todas las cuentas habilitadas dentro del inventario deben validarse regularmente una vez al trimestre, o con mayor frecuencia

**Creación y emisión de credenciales**

1. Todas las contraseñas deben ser únicas.
2. Las contraseñas creadas por los usuarios no deben utilizarse también para cuentas personales.
3. Las contraseñas no deben ser compartidas por los usuarios.
4. Las contraseñas creadas para su uso con autenticación multifactor deben tener un mínimo de 8 caracteres.
5. Las contraseñas creadas para su uso sin autenticación multifactor deben tener un mínimo de 14 caracteres.

**Uso de cuentas y credenciales**

1. Todos los usuarios deben utilizar la autenticación multifactor para acceder a las aplicaciones externas.
2. Todos los usuarios deben utilizar la autenticación multifactor para acceder a las aplicaciones alojadas por un proveedor de servicios externo, cuando sea compatible.
3. Todos los usuarios remotos deben utilizar la autenticación multifactor para acceder a los sistemas y aplicaciones internos.
4. La autenticación multifactor es necesaria para todas las cuentas administrativas de todos los activos de la empresa, ya sea que se administren en el sitio o a través de un proveedor externo.
5. Todas las contraseñas de usuario predeterminadas deben cambiarse en el primer inicio de sesión.

**Monitor**

No hay ninguna protección IG1 que admita esta parte del proceso de administración de cuentas y credenciales.

**Modificar el acceso**

1. Todas las cuentas de usuario a las que no se haya accedido dentro de los 45 días posteriores a la creación deben deshabilitarse.
2. Las cuentas de las personas con licencia prolongada, según la definición de recursos humanos, deben estar deshabilitadas.
3. Los procedimientos de Creación y Cancelación de Cuenta deben incluir la capacidad de cambiar el rol de un usuario.

**Cancelación de la cuenta**

1. El departamento de TI debe desarrollar procedimientos para revocar el acceso a la cuenta.
	1. El despido de los empleados debe incluirse en este proceso.
2. Todas las credenciales de usuario deben ser revocadas inmediatamente después de la separación del empleado.
	1. Los mecanismos de autoservicio de contraseñas para los usuarios no deben permitirles volver a habilitar su propia cuenta.

**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

| CIS | Center for Internet Security (Centro para la Seguridad en Internet) |
| --- | --- |
| Controles CIS | Center for Internet Security Critical Security Controls (Centro de Controles de Seguridad Críticos de Internet) |
| COTS | Commercial-off-the-shelf (Producto Comercial listo para usar) |
| IaaS | Infrastructure as a Service (Infraestructura como servicio) |
| IG | Implementation Group (Grupo de Implementación) |
| IoT | Internet of Things (Internet de las cosas) |
| IT | Information Technology (Tecnología de la información) |
| PIN | Personal Identification Number (Número de Identificación Personal) |
| SLTT | State, Local, Tribal, and Territorial (Estatales, Locales, Tribales y Territoriales) |
| SMS | Short Message Service (Servicio de mensajes cortos) |

#

# 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 otro usuario 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 Salvaguardias del CIS

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

Esta política ayuda a reforzar las salvaguardas IG1 en *CIS Control 5: Administración de cuentas* y *CIS Control 6: Administración de control de acceso.* La Tabla 1 muestra qué Salvaguardas CIS IG1 están cubiertas por esta política tal como está redactada.

*Cuadro 1 - Salvaguardias cubiertas por el IG1*

| CIS Control | Declaración de política | Salvaguarda CIS | Descripción de la salvaguarda CIS |
| --- | --- | --- | --- |
| 5.1  | Creación de cuenta 3, 4, 5 | 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 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, de forma periódica como mínimo trimestralmente o con mayor frecuencia. |
| 5.2 | Creación y emisión de credenciales 1, 1a, 1b, 2, 3Uso de la cuenta 5  | Usar contraseñas únicas | Utilice contraseñas únicas para todos los activos de la empresa. La implementación de las prácticas recomendadas incluye, como mínimo, una contraseña de 8 caracteres para las cuentas que utilizan autenticación multifactor y una contraseña de 14 caracteres para las cuentas que no utilizan autenticación multifactor. |
| 5.3 | Modificar Acceso 6, 7Uso de la cuenta 5 | Desactivar cuentas inactivas | Elimine o deshabilite cualquier cuenta inactiva después de un período de 45 días de inactividad, cuando sea compatible. |
| 5.4 | Creación de cuenta 2, 2a, 2b | Restringir los 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. Realice 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. |
| 6.1 | Incorporación 1a, 1b, 1c, 1d Creación de cuenta 1Modificar Acceso 8 | Establecer un proceso de concesión de acceso | Establezca y siga un proceso, preferiblemente automatizado, para conceder acceso a los activos de la empresa en caso de nueva contratación, concesión de derechos o cambio de rol de un usuario. |
| 6.2 | Cancelación de cuenta 1, 1a, 2, 2aModificar Acceso 8  | Establecer un proceso de revocación de acceso | Establezca y siga un proceso, preferiblemente automatizado, para revocar el acceso a los activos de la empresa, mediante la deshabilitación de cuentas inmediatamente después de la terminación, la revocación de derechos o el cambio de rol de un usuario. Puede ser necesario deshabilitar las cuentas, en lugar de eliminarlas, para conservar los registros de auditoría. |
| 6.3 | Uso de la cuenta 1, 2 | Requerir MFA para aplicaciones expuestas externamente | Exija que todas las aplicaciones empresariales o de terceros expuestas externamente apliquen autenticación multifactor (MFA), cuando sea compatible. La aplicación de MFA a través de un servicio de directorio o un proveedor de SSO es una implementación satisfactoria de esta protección. |
| 6.4 | Uso de la cuenta 3  | Requerir MFA para el acceso remoto a la red | Requerir MFA para el acceso remoto a la red. |
| 6.5 | Uso de la cuenta 4 | Requerir MFA para el acceso administrativo | Requerir MFA para todas las cuentas de acceso administrativo, cuando se admitan, en todos los activos de la empresa, ya sea administrados in situ o a través de un proveedor externo. |

#

# Apéndice E: Referencias y recursos

Center for Internet Security®

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

CIS Critical Security Controls®

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