#	Objetivo a cumplir
	Mantener un inventario detallado de activos
1.1	Desarrollar y mantener un inventario completo y preciso de los activos de TI de la organización. Los cuales puede incluir: dispositivos de usuario final (portátiles y móviles), dispositivos de red, no informáticos/IoT dispositivos y servidores.
	Propiedad y responsabilidad de los activos
1.2	Identificar y asignar responsabilidades a los propietarios de activos de TI de la organización, asegurándose de que exista un proceso para abordar los activos no autorizados
	Mantener un inventario de software autorizado
2.1	Establezca y mantenga un inventario detallado de todo el software con licencia instalado en los activos de la empresa. El inventario de software debe documentar el título, el editor, la fecha de instalación/uso inicial y el propósito comercial de cada entrada; cuando corresponda, incluya el Localizador Uniforme de Recursos (URL), la(s) tienda(s) de aplicaciones, la(s) versión(es), el mecanismo de implementación y la fecha de retiro. Revise y actualice el inventario de software dos veces al año o con mayor frecuencia.
	Validación de software
2.2	Asegúrese de que solo el software compatible actualmente se designe como autorizado en el inventario de software para activos empresariales. Si el software no tiene soporte, 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 no compatible sin una documentación de excepción, designe como no autorizado. Revise la lista de software para verificar el soporte de software al menos una vez al mes o con mayor frecuencia.
	Eliminación de software no atorizado

2.3	Asegúrese de que el software no autorizado se elimine del uso en los activos de la empresa o reciba una excepción documentada. Revisar mensualmente, o con mayor frecuencia.

Gestión de datos

3.1	Establecer y mantener un proceso de gestión de datos. En el proceso, aborde la confidencialidad de los datos, el propietario de los datos, el manejo de los datos, los límites de retención de datos y los requisitos de eliminación, según los estándares de confidencialidad y retención para la empresa. Revise y actualice la documentación anualmente, o cuando ocurran cambios importantes en la empresa que puedan afectar esta Protección.

Inventario de datos

3.2	Establecer y mantener un inventario de datos, basado en el proceso de gestión de datos de la empresa. Inventario de datos confidenciales, como mínimo. Revise y actualice el inventario anualmente, como mínimo, con prioridad en los datos confidenciales.

Aplicar controles de acceso a datos

3.3	Configure listas de control de acceso a datos según la necesidad de saber del usuario. Aplique listas de control de acceso a datos, también conocidas como permisos de acceso, a aplicaciones, bases de datos y sistemas de archivos locales y remotos.

Retención de datos

3.4	Retenga los datos de acuerdo con el proceso de gestión de datos de la empresa. La retención de datos debe incluir plazos mínimos y máximos.

Eliminación segura de datos

3.5	Deseche los datos de forma segura como se describe en el proceso de gestión de datos de la empresa. Asegúrese de que el proceso y el método de eliminación sean acordes con la sensibilidad de los datos.

Cifrado de datos

3.6	Cifre los datos en los dispositivos de los usuarios finales que contienen datos confidenciales. Las implementaciones de ejemplo pueden incluir: Windows BitLocker®, Apple FileVault®, linux®dm-cripta.

Mantener configuraciones seguras documentadas

4.1	Establezca y mantenga un proceso de configuración seguro para los activos empresariales (dispositivos de usuario final, incluidos dispositivos y servidores portátiles y móviles, no informáticos/IoT) y software (sistemas operativos y aplicaciones). Revise y actualice la documentación anualmente, o cuando ocurran cambios importantes en la empresa que puedan afectar esta Protección.

Aplicar configuraciones seguras en sistemas/dispositivos nuevos

4.2 Establezca y mantenga un proceso de configuración seguro para los dispositivos de red. Revise y actualice la documentación anualmente, o cuando ocurran cambios importantes en la empresa que puedan afectar esta Protección.

Bloqueo automático de dispositivos

4.3 Configure el bloqueo de sesión automático en los activos de la empresa después de un período definido de inactividad. Para 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.

Implementación y configuración de firewall

4.4 Implemente y administre un firewall en los servidores, donde sea compatible. Las implementaciones de ejemplo incluyen un cortafuegos virtual, un cortafuegos del sistema operativo o un agente de cortafuegos de terceros.

Soluciones de protección a usuarios finales

4.5	Implemente y administre un firewall basado en host o una herramienta de filtrado de puertos en los dispositivos de los usuarios finales, con una regla de denegación predeterminada que elimina todo el tráfico excepto aquellos servicios y puertos que están explícitamente permitidos.

Configuración segura de infraestructura

4.6	Gestione de forma segura los activos y el software de la empresa. Las implementaciones de ejemplo incluyen la gestión de la configuración a través de una infraestructura como código controlada por versión y el acceso a interfaces administrativas a través de protocolos de red seguros, como Secure Shell (SSH) y Hypertext Transfer Protocol Secure (HTTPS). No utilice protocolos de gestión inseguros, como Telnet (Teletype Network) y HTTP, a menos que sea esencial desde el punto de vista operativo.

Validación de cuentas

4.7	Administre cuentas predeterminadas en activos y software de la empresa, como raíz, administrador y otras cuentas de proveedores preconfiguradas. Las implementaciones de ejemplo pueden incluir: deshabilitar cuentas predeterminadas o hacerlas inutilizables.

Control de inventario de cuentas

5.1 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 cronograma recurrente como mínimo trimestralmente o con mayor frecuencia.

Gestión de contraseñas

5.2 Utilice contraseñas únicas para todos los activos de la empresa. La implementación de mejores prácticas incluye, como mínimo, una contraseña de 8 caracteres para cuentas que usan MFA y una contraseña de 14 caracteres para cuentas que no usan MFA.

Gestión de cuentas inactivas

5.3 Elimine o deshabilite cualquier cuenta inactiva después de un período de 45 días de inactividad, donde sea posible.

Principio de privilegio mínimo

5.4 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.

Proceso de altas, bajas y cambios

6.1 Establezca y siga un proceso, preferiblemente automatizado, para otorgar acceso a los activos de la empresa en caso de nueva contratación, concesión de derechos o cambio de función de un usuario.

Desvinculación o cambio de cuentas

6.2 Establezca y siga un proceso, preferiblemente automatizado, para revocar el acceso a los activos de la empresa, mediante la desactivación de cuentas inmediatamente después de la terminación, la revocación de derechos o el cambio de función de un usuario. Puede ser necesario deshabilitar cuentas, en lugar de eliminarlas, para preservar los registros de auditoría.

Protección multifactor

6.3 Requerir 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.

Protección remota de la red

6.4 Requerir MFA para el acceso remoto a la red.

Protección adicional a cuentas administradoras

6.5 Requerir MFA para todas las cuentas de acceso administrativo, donde sea compatible, en todos los activos de la empresa, ya sea que se administren en el sitio o a través de un proveedor externo.

Establecer un programa de gestión de vulnerabilidades

7.1 Establezca y mantenga un proceso documentado de gestión de vulnerabilidades para los activos de la empresa. Revise y actualice la documentación anualmente, o cuando ocurran cambios importantes en la empresa que puedan afectar esta Protección.

Realizar escaneos de vulnerabilidades y priorizar estrategias de remediación

7.2 Establezca y mantenga una estrategia de remediación basada en riesgos documentada en un proceso de remediación, con revisiones mensuales o más frecuentes.

Proceso de actualización de sistemas

7.3 Realice actualizaciones del sistema operativo en los activos de la empresa a través de la administración de parches automatizada mensualmente o con mayor frecuencia.

Proceso de actualizaciones automatizadas

7.4 Realice actualizaciones de aplicaciones en los activos de la empresa a través de la administración de parches automatizada mensualmente o con mayor frecuencia.

Proceso de registro de auditorías

8.1 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. Revise y actualice la documentación anualmente, o cuando ocurran cambios importantes en la empresa que puedan afectar esta Protección.

Habilitación de Registros Relevantes

8.2 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.

Almacenar y proteger los registros de auditoría

8.3 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.

Uso de servicios de navegación y correo electrónico seguro y actualizado

9.1 Asegúrese de que solo los navegadores y clientes de correo electrónico totalmente compatibles puedan ejecutarse en la empresa, utilizando solo la última versión de navegadores y clientes de correo electrónico proporcionados a través del proveedor.

Bloqueo de dominios maliciosos

9.2 Utilice los servicios de filtrado de DNS en todos los activos de la empresa para bloquear el acceso a dominios maliciosos conocidos.

Presencia de altimalware en todos los activos organizacionales

10.1 Implemente y mantenga software antimalware en todos los activos de la empresa.

Configuración de antimalware con actualizaciones periódicas

10.2 Configure actualizaciones automáticas para archivos de firmas antimalware en todos los activos de la empresa.

Protección de medios extraibles

10.3 Deshabilite la ejecución automática y la ejecución automática de reproducción automática para medios extraíbles.

Proceso de recuperación de datos

11.1 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. Revise y actualice la documentación anualmente, o cuando ocurran cambios importantes en la empresa que puedan afectar esta Protección.

Copias de seguridad automatizadas

11.2 Realice copias de seguridad automatizadas de los activos empresariales dentro del alcance. Ejecute copias de seguridad semanalmente o con mayor frecuencia, según la sensibilidad de los datos.

Protección de datos de recuperación

11.3 Proteja los datos de recuperación con controles equivalentes a los datos originales. Cifrado de referencia o separación de datos, en función de los requisitos.

Instancia aislada de datos de recuperación

11.4	Establezca y mantenga una instancia aislada de datos de recuperación. Las implementaciones de ejemplo incluyen destinos de respaldo de control de versiones a través de sistemas o servicios fuera de línea, en la nube o fuera del sitio.

Actualización de infraestructura de red

12.1	Asegúrese de que la infraestructura de la red se mantenga actualizada. Las implementaciones de ejemplo incluyen la ejecución de la última versión estable de software y/o el uso de ofertas de red como servicio (NaaS) compatibles actualmente. Revise las versiones de software mensualmente, o con mayor frecuencia, para verificar la compatibilidad del software.

Programa de concientización sobre habilidades de seguridad

14.1	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. Llevar a cabo la capacitación al contratar y, como mínimo, anualmente. Revise y actualice el contenido anualmente, o cuando ocurran cambios importantes en la empresa que puedan afectar esta Protección.

Capacitación constante sobre ciberseguridad

14.2 Capacite a los miembros de la fuerza laboral para que reconozcan los ataques de ingeniería social, como el phishing, los mensajes de texto previos y los seguimientos

Capacitación en prácticas de autenticación

14.3 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.

Capacitación en manejo de datos

14.4 Capacite a los miembros de la fuerza laboral sobre cómo identificar y almacenar, transferir, archivar y destruir datos confidenciales de manera adecuada. Esto también incluye capacitar a los miembros de la fuerza laboral sobre las mejores prácticas de pantalla clara y escritorio, como 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.

Capacitación sobre exposición de datos

14.5 Capacite a los miembros de la fuerza laboral para que sean conscientes de las causas de la exposición no intencional de los datos. Los temas de ejemplo incluyen la entrega incorrecta de datos confidenciales, la pérdida de un dispositivo portátil de usuario final o la publicación de datos para audiencias no deseadas.

Identificación de incidentes y comunicación

14.6 Capacite a los miembros de la fuerza laboral para que puedan reconocer un incidente potencial y puedan informar dicho incidente.

Capacitación de actualizaciones de sistemas

14.7 Capacitar a la fuerza laboral para que comprenda cómo verificar e informar parches de software desactualizados o cualquier falla en los procesos y herramientas automatizados. Parte de esta capacitación debe incluir la notificación al personal de TI de cualquier falla en los procesos y herramientas automatizados.

Capacitación de riesgos laborales

14.8

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.

Proceso de inventarios de proovedores de servicio

15.1 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. Revise y actualice el inventario anualmente, o cuando ocurran cambios importantes en la empresa que puedan afectar esta salvaguarda.

Designar responsables de incidentes

17.1 Designe una persona clave, y al menos un respaldo, que administrará el proceso de manejo de incidentes de la empresa. El personal de gestión 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. Revisar anualmente, o cuando ocurran cambios importantes en la empresa que puedan afectar esta Salvaguarda.

Directorio de responsable tras algún incidente de seguridad

17.2 Establezca y mantenga información de contacto para las partes que necesitan estar informadas sobre 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 Análisis e Intercambio de Información (ISAC) u otras partes interesadas. Verifique los contactos anualmente para asegurarse de que la información esté actualizada.

Plan de revisión y evaluación de cumplimiento Cib

Estructura de posible evidencia para cumplimiento

Control #1: Inventari

-Inventario de activos: Un archivo (Excel, base de datos, CMDB) donde estén listados todos los dispositivos de TI (laptops, móviles, servidores, redes, IoT).
-Capturas de pantalla de herramientas: Imágenes de sistemas que manejan inventarios, como ServiceNow, Lansweeper, GLPI, etc.

-Listado de activos con responsables asignados Inventario donde cada activo tenga asignado un "dueño" o responsable (nombre, área, contacto).

CIS Control #2: Inventario y C

-Archivo o sistema donde se liste:
+Nombre del software, Fabricante/Desarrollador, Fecha de instalación, Propósito al interior de la secretaría o entidad, versión, URL o tienda de descarga, método de instalación, fecha de retiro (cuando aplique).
-Actas, correos o registros que demuestren que el inventario se revisa y actualiza al menos una vez al año.

-Listado donde se indique claramente qué software está autorizado (compatible) y qué software está no autorizado (no compatible).
-Documento que establezca que solo se permite software soportado y qué hacer si se detecta software obsoleto.
-Documentos de excepción para software no soportado: Formularios o registros que documenten cuándo un software sin soporte sigue usándose, junto con controles de mitigación (por ejemplo: aislamiento de red, acceso restringido) y aceptación del riesgo por parte de responsables.
-Evidencia de que se revisa el inventario de software al menos una vez al mes o al año (pueden ser registros de tickets, actas de reunión, correos de confirmación de revisión).

-Documento o sistema donde se indique qué software está autorizado, no autorizado, y si hay

-Documento o sistema donde se indique qué software está autorizado, no autorizado, y si hay excepciones documentadas.
-Registro de eliminación de software no autorizado: Bitácoras, reportes o tickets que evidencien que el software no autorizado fue desinstalado de los activos.
-Documentos de excepción aprobados: Formularios o registros donde se documente qué software no compatible sigue en uso y bajo qué controles de mitigación.
-Documento o manual interno que explique los pasos para identificar, validar y eliminar software prohibido.
-Evidencia de que se realiza una revisión mensual para identificar y eliminar software no autorizado (pueden ser actas de reunión, reportes automáticos de escaneo, correos).
-políticas de configuración segura que impida la instalación de software no autorizado

CIS Control #3: Pr

-Procedimiento de gestión de datos: Documento sencillo que explique cómo se identifican, clasifican, almacenan, retienen y eliminan los datos.
-Matriz de clasificación de datos: Archivo donde se clasifiquen datos (Ej: Confidencial, Interno, Público) y quién es el propietario responsable de cada tipo.
-Documento que diga cuánto tiempo se conserva la información y cómo se elimina (papel triturado, borrado seguro, baja de sistemas).

´-Documento o archivo que contenga qué tipos de datos maneja la organización, su nivel de confidencialidad, ubicación (física o digital), responsable y sistemas donde residen.
-Documento sencillo donde se indique que el inventario de datos debe actualizarse mínimo una vez al año o cuando haya cambios importantes.
-Registro que evidencie que el inventario de datos fue revisado (acta, minuta o correo firmado).

´-Documento que explique que los accesos a datos se otorgan solo si el usuario realmente los necesita ("necesidad de saber").
-Imágenes de configuraciones de permisos en carpetas compartidas, bases de datos o aplicaciones (mostrando que los accesos están restringidos por usuario o rol).
-Archivo que muestre qué roles existen y qué tipo de acceso tienen a datos confidenciales (por ejemplo: lectura, edición, eliminación).
-Actas, correos o minutas de revisiones periódicas de accesos a datos (idealmente semestrales o anuales).

´-Documento que indique los plazos mínimos y máximos de conservación de datos según su tipo y confidencialidad.
-Matriz de tiempos de retención de datos: Tabla que relacione tipo de dato, tiempo de conservación mínimo y máximo, responsable, y método de eliminación.
-Bitácoras o actas donde conste que se eliminaron datos conforme al tiempo de retención establecido.
-Evidencia de que áreas operativas aplican los tiempos de retención (por ejemplo: baja de expedientes físicos, eliminación de archivos electrónicos antiguos).

´-Documento donde se explique cómo eliminar datos de acuerdo a su sensibilidad: borrado seguro, destrucción física, formateo, etc.
-Actas, bitácoras o reportes donde conste que los datos fueron destruidos o eliminados conforme al procedimiento.
-Capturas o constancias de herramientas de borrado seguro (ej: uso de software como Eraser, DBAN para discos, o destrucción de papel con trituradoras).
-Registro de activos que contenían datos (computadoras, discos duros, USBs) que fueron desechados correctamente.
-Constancia de capacitación básica en eliminación segura: Registro de que el personal conoce el procedimiento (puede ser un taller interno, acta de capacitación o circular de conocimiento).

´-Documento que establezca que los dispositivos que almacenan datos confidenciales deben estar cifrados.
-Evidencia visual de que los dispositivos tienen activado el cifrado (por ejemplo, capturas de BitLocker activo en Windows, FileVault activo en Mac).
-Archivo o tabla que indique qué dispositivos tienen cifrado activo, qué método de cifrado utilizan y responsable asignado.
-Reporte interno que evidencie revisiones periódicas para verificar que el cifrado sigue activo.
-Documento o guía que indique qué hacer si se detecta un equipo que no tiene cifrado (ej: activar BitLocker, restringir su uso, solicitar regularización).
Recomendación de herramienta gratuita para cifrado de datos: VeraCrypt

CIS Control #4: Mantener configu

´-Documento que describa cómo configurar de forma segura dispositivos (PCs, móviles, servidores, IoT) y software (Sistemas Operativos y aplicaciones).
-Archivo donde se documenten configuraciones base recomendadas: desactivar servicios innecesarios, configuración de firewalls, actualizaciones automáticas, etc.
-Imágenes que muestren ejemplos de configuraciones aplicadas (por ejemplo: bloqueo de pantalla, cifrado habilitado, servicios desactivados, contraseñas de arranque).
-Acta, minuta o correo que evidencie que se revisan al menos una vez al año las configuraciones seguras (y si es necesario, se actualizan).

´-Documento que describa cómo deben configurarse de manera segura routers, switches,

firewalls, access points, etc.
-Tabla o documento donde se indique configuraciones aplicadas: cambios de contraseñas predeterminadas, desactivación de servicios innecesarios, actualizaciones de firmware, listas de control de acceso (ACLs), etc.
-Evidencias visuales de configuraciones seguras o respaldos de configuraciones guardadas en archivo.
-Actas, minutas o correos donde se registre que las configuraciones fueron revisadas (y actualizadas si es necesario).
-Manual o instructivo para que cada nuevo dispositivo de red que se instale siga las configuraciones seguras definidas.

´- Documento que establezca que los dispositivos deben bloquearse automáticamente tras un periodo de inactividad (15 min para PCs/servidores, 2 min para móviles).
-Evidencia visual de la configuración de bloqueo automático en sistemas operativos (Windows, Linux, Mac) y dispositivos móviles (Android, iOS).
-Registro o tabla donde se indique qué dispositivos tienen habilitado el bloqueo automático y qué configuración tienen.
-Reportes donde se evidencie que se revisa periódicamente que los tiempos de bloqueo estén configurados adecuadamente.
- Evidencia de políticas de grupo (GPOs) en Active Directory que obliguen el bloqueo automático de PCs de usuarios.

´- Documento que establezca que todos los servidores deben tener un firewall habilitado y administrado (puede ser el propio sistema operativo o un firewall de red virtual).
-Evidencia visual de firewalls activos, por ejemplo: Windows Firewall configurado en servidores Windows, iptables o firewalld en Linux.
-Registro que indique qué servidores tienen firewall activo, tipo de firewall usado (integrado o de terceros) y reglas básicas aplicadas.
-Evidencia de que periódicamente se revisan las reglas y el estado del firewall en los servidores.
-Documento que indique cómo se debe instalar y configurar el firewall en nuevos servidores antes de ponerlos en producción.

´-Documento que establezca que los equipos de usuario final deben tener firewall activado, con regla por defecto de denegar todo tráfico salvo el permitido explícitamente.
-Evidencia visual del firewall activo en computadoras de escritorio, laptops o dispositivos móviles. Ejemplo: Windows Firewall configurado, firewalld/iptables en Linux.
-Registro de PCs, laptops o móviles indicando que tienen firewall habilitado, reglas aplicadas y responsables asignados.
-Checklists o actas donde se registre la revisión de estado y configuración de los firewalls en los dispositivos.
-Evidencia de políticas de grupo (GPOs) aplicadas en caso de tener Active Directory, donde se gestione de forma centralizada el firewall en PCs.

´-Documento que establezca que todo acceso administrativo debe ser realizado por protocolos seguros (SSH, HTTPS, RDP con TLS, etc.) y que se prohíbe el uso de Telnet o HTTP sin protección.
-Evidencia visual de que los dispositivos de red, servidores, y sistemas administran conexiones usando protocolos seguros. Ejemplos: acceso a switches por SSH, a servidores por HTTPS, no habilitar HTTP abierto.
-Registro donde se documente qué servicios/protocolos están activos en servidores y dispositivos (y evidenciar que son seguros).
-Actas o checklists donde se revise periódicamente que no se estén utilizando protocolos inseguros en los activos.
-(Opcional si hay infraestructura más madura) Evidencia de que configuraciones se administran mediante control de versiones (puede ser en Git, aunque sea local).

´-Documento que establezca que todas las cuentas predeterminadas (ej. root, admin, guest, administrator) deben ser deshabilitadas, eliminadas o cambiadas de nombre/contraseña, según corresponda.
-Registro que muestre qué dispositivos o sistemas tenían cuentas predeterminadas y qué acciones se tomaron (deshabilitar, renombrar, fortalecer).
-Evidencia visual de que las cuentas predeterminadas fueron deshabilitadas o modificadas (capturas del panel de usuarios en Windows, Linux, dispositivos de red, etc.).
-Checklist o acta donde se evidencie que periódicamente se revisan los activos para asegurar que no existan cuentas predeterminadas activas o sin control.
-Documento que indique que cada vez que se implementa un nuevo dispositivo o sistema, se debe revisar y gestionar cualquier cuenta predeterminada.

´-Archivo o sistema donde se registren todas las cuentas de usuario y administrador, incluyendo: nombre de la persona, nombre de usuario, fecha de alta, fecha de baja (si aplica) y departamento.
-Documento que explique cómo se crean, modifican, eliminan y revisan las cuentas de usuario y administrador.
-Evidencias visuales de listados de usuarios de los principales sistemas (Active Directory, servidores, sistemas de gestión, bases de datos).
-Checklists, actas o correos que evidencien que se realiza revisión periódica para validar que las cuentas activas estén autorizadas y actualizadas.
-Bitácora o reporte que evidencie que cuentas de usuarios inactivos o no autorizados fueron dadas de baja o deshabilitadas.

´-Documento que establezca que todas las cuentas deben usar contraseñas únicas, y que indique los requisitos mínimos de longitud (8 caracteres con MFA, 14 caracteres sin MFA).
-Capturas o reportes de políticas de contraseñas aplicadas en sistemas principales: Active Directory, servidores Linux, bases de datos, aplicaciones críticas.
-Reportes o registros donde se valide que las cuentas no usan contraseñas duplicadas o débiles (por ejemplo, mediante auditorías internas de TI).
-Documento que describa qué hacer si se detecta una contraseña comprometida o débil.
-Evidencia de que se capacitó a los usuarios en el uso de contraseñas seguras y únicas.

´- Documento que establezca que toda cuenta de usuario o administrador que esté inactiva por más de 45 días debe ser deshabilitada o eliminada.
-Evidencia de listados de cuentas con fechas de último inicio de sesión, mostrando cuáles llevan más de 45 días sin actividad.
-Registro donde conste que se deshabilitaron o eliminaron las cuentas detectadas como inactivas.
-Checklists o actas donde conste que se realiza la revisión de cuentas inactivas, idealmente mensual o trimestral.
-Evidencia visual de que se aplicaron las acciones en los sistemas (por ejemplo, en Active Directory, consola de usuarios Linux, etc.).

´-Documento que establezca que: 1) las cuentas administrativas deben ser cuentas separadas de las cuentas de usuario común, y 2) que las tareas normales (navegar, correo, documentos) se hagan desde una cuenta sin privilegios.
-Inventario donde se documente qué cuentas son de administrador, cuáles son de uso diario, y quién es responsable de cada cuenta.
-Evidencias visuales donde se vea la separación entre cuentas administrativas y cuentas de usuario común en sistemas principales (AD, Linux, bases de datos).
- Actas, checklists o correos que evidencien que se revisan las cuentas para validar que no se usan cuentas con privilegios de más para tareas diarias.
-Documento breve que oriente al personal sobre el uso correcto de cuentas (cuándo usar cuenta administrativa, cuándo usar cuenta normal).

´-Documento que defina cómo se deben solicitar, aprobar, otorgar y registrar accesos en caso de: nueva contratación, cambio de puesto o necesidad de nuevos permisos.
-Formato sencillo que debe llenarse y aprobarse para cada nueva solicitud o modificación de permisos.
-Bitácora donde se guarden todas las solicitudes aprobadas o rechazadas, con fecha, área solicitante, responsable de autorización y fecha de aplicación.
-Capturas o reportes que evidencien los accesos dados conforme a las solicitudes aprobadas (por ejemplo: nuevo usuario creado en Active Directory, cambios de permisos en carpetas, sistemas, bases de datos, etc.).
-Checklists o actas de revisión donde se valide que los accesos otorgados correspondan a solicitudes autorizadas.

´-Documento que explique el proceso para desactivar o revocar accesos inmediatamente tras la baja de personal, cambio de funciones o revocación de derechos.
-Formato sencillo que Recursos Humanos o el área responsable debe enviar a TI cuando se detecta una baja o cambio de puesto.
- Bitácora donde se documente cada cuenta desactivada o permisos revocados, con fecha, motivo y responsable que autorizó la acción.
-Checklists o actas que evidencien que periódicamente se revisa si las bajas de personal/cambios de puesto corresponden a revocaciones correctas de accesos.

´-Documento que establezca que toda aplicación organizacional o de terceros expuesta a internet debe usar MFA, donde sea posible.
-Inventario de aplicaciones que están accesibles desde fuera de la red y evidencia de que tienen MFA habilitado.
-Evidencias visuales de la configuración de MFA en cada aplicación (ej: portal web, VPN, correo institucional, servicios en la nube).
-Actas o checklists donde se revise periódicamente que MFA sigue activo en las aplicaciones expuestas.
-Evidencia de que, si se usa un directorio o proveedor de Single Sign-On (SSO), éste aplica MFA para los accesos.
´-Documento que establezca que todo acceso remoto (VPN, escritorio remoto, acceso por navegador, etc.) debe requerir autenticación multifactor (MFA).
-Capturas de pantalla o reportes que muestren que la VPN, el acceso remoto (RDP Gateway, Citrix, etc.) o cualquier solución similar tiene MFA activo.
-Inventario de todas las plataformas o servicios de acceso remoto indicando qué método de MFA usan.
-Evidencia de pruebas internas que demuestren que el acceso remoto requiere MFA (capturas de inicio de sesión mostrando doble factor).

´-Documento que establezca que todas las cuentas administrativas (locales, en servidores,

en dispositivos de red, en aplicaciones críticas) deben usar MFA, ya sea en sitio o con proveedores externos.
-Capturas o reportes donde se evidencie que MFA está activo para cuentas administrativas (por ejemplo: en Active Directory, plataformas en la nube, consolas de servidores, administración de bases de datos).
-Inventario donde se liste cada cuenta administrativa y se indique si tiene MFA habilitado, qué tipo de MFA usa, y en qué sistema o plataforma.
-Actas o checklists de revisión donde se verifique que todas las cuentas administrativas activas tienen MFA habilitado.
-Capturas o registros de prueba donde se vea que MFA funciona en los accesos administrativos (ejemplo: al ingresar a consola de administración de un firewall, un servidor, un portal en la nube, etc.).

CIS Control #7: Gestión co

´-Documento que defina el proceso de identificación, análisis, priorización, corrección y validación de vulnerabilidades en sistemas y dispositivos.
-Excel o documento donde se registren vulnerabilidades detectadas, fecha de detección, criticidad, responsable asignado, fecha de remediación o mitigación.
-Reportes de herramientas de escaneo (pueden ser gratuitos como OpenVAS, Nessus Essentials, Nmap, Lynis) donde se muestren vulnerabilidades detectadas.
-Documentos, tickets, o registros donde se evidencie que se tomaron acciones correctivas sobre vulnerabilidades detectadas.
-Documento que evidencie que el procedimiento de gestión de vulnerabilidades se revisa al menos una vez al año o cuando haya cambios relevantes (nueva tecnología, cambio de responsables, reorganización).
´-Documento que establezca cómo priorizar la atención de vulnerabilidades basándose en el nivel de riesgo (crítico, alto, medio, bajo) y defina los tiempos de respuesta máximos para cada nivel.
-Documento que explique el paso a paso: detección, análisis de criticidad, asignación a responsables, remediación, verificación.
-Bitácora donde se registren las vulnerabilidades detectadas, su criticidad, la fecha de detección, la fecha de cierre y acciones tomadas.
-Actas, minutas o reportes que evidencien que mensualmente se revisan vulnerabilidades abiertas, priorizaciones y avances de remediaciones.
-Capturas, reportes o registros que muestren que realmente se corrigieron las vulnerabilidades según su prioridad (parches aplicados, configuraciones modificadas, servicios reforzados).

´-Documento que describa cómo se aplican parches y actualizaciones de sistemas operativos en los activos de TI, al menos mensualmente o más frecuentemente si es necesario.
-Capturas de pantalla o reportes donde se evidencie que los equipos tienen configuradas actualizaciones automáticas (por ejemplo: Windows Update activo, actualizaciones automáticas en Linux o Mac).
-Inventario donde se documente qué equipos tienen actualizaciones al día, fecha de última actualización y responsable.
-Evidencias de ejecución de parches aplicados (bitácoras de actualización, reportes de sistemas, capturas de Windows Update History, registros de yum update en Linux, etc.).
-Actas o checklists donde se evidencie que se revisó el estado de actualizaciones de los sistemas, idealmente cada mes.

´-Documento que establezca cómo deben mantenerse actualizadas las aplicaciones instaladas en los activos de TI, al menos una vez al mes o con mayor frecuencia si hay parches críticos.
-Capturas o reportes que evidencien que las aplicaciones principales tienen habilitada la opción de actualizaciones automáticas (ej: navegadores, suites de productividad, antivirus).
-Inventario donde se documente las aplicaciones instaladas, su versión actual y fecha de última actualización aplicada.
-Evidencia de parches instalados: logs de actualización, reportes de sistemas de TI, o capturas de versiones actualizadas de las aplicaciones críticas.
-Documentos donde conste que se hace una revisión mensual o trimestral para validar que las aplicaciones estén actualizadas.

CIS Control #8: Gestió

´-Documento que defina qué eventos deben ser registrados (inicio de sesión, errores, cambios en configuraciones críticas, accesos a información sensible), cómo se recopilan, cómo se revisan y cuánto tiempo se retienen.
-Capturas o reportes que muestren que los activos (servidores, bases de datos, dispositivos de red, sistemas críticos) generan y almacenan logs de auditoría relevantes.
-Listado donde se documente qué activos generan registros de auditoría, tipo de eventos registrados, y dónde se almacenan.
-Evidencias (actas, reportes, listas de verificación) que muestren que se revisan periódicamente los registros para detectar eventos anómalos.
-Documento o anexo donde se defina cuánto tiempo se conservan los registros (por ejemplo, 1 año, 2 años), conforme a leyes locales, regulaciones o políticas internas.

´-Documento que explique que todos los activos relevantes deben tener habilitada la

-Documento que explique que todos los activos relevantes deben tener habilitada la generación de logs, conforme al proceso de gestión de registros de auditoría establecido
-Evidencias visuales de que el registro de eventos está habilitado en: servidores, estaciones de trabajo críticas, dispositivos de red, bases de datos, aplicaciones principales.
-Listado donde se documente cada activo que tiene configurado el registro de auditoría, tipo de eventos que captura y almacenamiento de los logs.
-Checklists, actas o reportes internos donde se evidencie que periódicamente se revisa si todos los activos tienen habilitado el registro de eventos.
-Documento donde se registren casos en que se detectó que un activo no tenía logs habilitados, y las acciones correctivas aplicadas.

´-Documento que defina cómo y dónde se almacenan los registros de auditoría, asegurando que haya suficiente espacio para cumplir los periodos de retención definidos.
-Inventario donde se indique qué servidores, dispositivos o repositorios almacenan logs, su capacidad actual, y su política de retención.
-Evidencias de que el espacio en disco de los servidores de logs es suficiente (por ejemplo: capturas de espacio libre en discos, reportes de uso en servidores de almacenamiento o NAS).
-Evidencia de que se monitorea el espacio de almacenamiento para evitar saturaciones (puede ser con herramientas gratuitas o mediante scripts simples).
-Documento o plan que indique qué hacer si los sistemas de logs están cerca de llenarse (rotación de logs, depuración controlada, expansión de almacenamiento).

CIS Control #9: Protecciones de co

´-Documento que indique que solo navegadores y clientes de correo electrónico compatibles y actualizados pueden ser usados, siguiendo las versiones oficiales del proveedor.
-Inventario donde se especifiquen los navegadores (ej: Chrome, Edge, Firefox) y clientes de correo electrónico (ej: Outlook, Thunderbird) permitidos en la organización.
-Capturas de pantalla o reportes que evidencien que los navegadores y clientes de correo tienen habilitadas actualizaciones automáticas.
-Evidencia de revisiones periódicas (mensuales o trimestrales) que validen que las aplicaciones están en sus versiones más recientes.
-Bitácora donde se documente si algún navegador o cliente de correo fue encontrado desactualizado y las acciones correctivas aplicadas.

´-Documento que establezca que todos los activos deben utilizar servicios de filtrado DNS para bloquear el acceso a dominios maliciosos conocidos.
-Capturas de configuración de servidores DNS configurados para filtrar tráfico (por ejemplo: Cisco Umbrella, Cloudflare Gateway, Quad9, CleanBrowsing).
-Inventario que indique qué servicios de filtrado DNS están aplicados (nombre del servicio, IPs utilizadas, y en qué redes o activos están configurados).
-Reportes, logs o capturas de que los filtros están activos y que bloquean accesos a dominios maliciosos (por ejemplo, capturas de intentos de conexión bloqueados).
-Actas o checklists de revisión para asegurar que el servicio de filtrado está activo y actualizado.

CIS Control #10: Defe

´-Documento que establezca que todos los activos (PCs, laptops, servidores críticos) deben tener instalado y actualizado un software antimalware activo.
-Inventario donde se registre qué activos tienen antimalware instalado, versión del software y estado de actualización.
-Evidencia visual del software de protección funcionando correctamente (capturas de consola de antivirus en PCs/servidores o reportes de estado).
-Evidencias de que las definiciones de malware se actualizan automáticamente en los dispositivos protegidos.
-Actas, listas de verificación o reportes internos que demuestren que se revisa periódicamente que el antimalware esté activo y actualizado en todos los dispositivos.

´-Documento que indique que todos los activos deben tener configuradas actualizaciones automáticas de las firmas de virus/malware.
-Evidencias visuales de que en los dispositivos, el antimalware tiene habilitada la opción de actualización automática de firmas.
-Inventario donde se documente qué activos tienen la actualización automática configurada.
-Actas, listas de verificación o reportes internos que evidencien que periódicamente se revisa que las firmas de los antimalware están actualizadas.
-Bitácora donde se documenten casos en que se encontró algún activo con firmas desactualizadas y qué acciones se tomaron.

´-Documento que establezca que la ejecución automática (AutoRun) y la reproducción automática (AutoPlay) deben estar deshabilitadas en todos los activos para prevenir infecciones de malware vía USBs, CDs, DVDs, etc.
-Evidencias visuales de que AutoRun y AutoPlay están desactivadas en sistemas Windows, Linux o Mac.
-Inventario donde se registre que los activos tienen la ejecución automática de medios desactivada.
-Checklists, actas o reportes que evidencien que se revisa periódicamente que AutoRun y AutoPlay estén desactivados en todos los equipos.
-Bitácora donde se documenten casos detectados de activos con AutoRun activo, y las acciones tomadas para corregirlo.

CIS Control #11: Rec

´-Documento que describa cómo recuperar datos en caso de pérdida o incidente, definiendo

´-Documento que describa cómo recuperar datos en caso de pérdida o incidente, definiendo el alcance (qué sistemas/datos cubre), la priorización (qué recuperar primero) y las medidas de seguridad de los respaldos (protección contra accesos no autorizados, cifrado, ubicación segura).
-Inventario que documente qué activos críticos están cubiertos por respaldos y cuáles son las prioridades de recuperación.
-Capturas de configuraciones donde se evidencie que los respaldos están protegidos (cifrado, acceso restringido, almacenamiento físico seguro o nube segura).
-Evidencia de que se realizan pruebas periódicas para validar que los respaldos funcionan y los datos pueden recuperarse exitosamente.
-Acta o minuta de revisión anual donde se ajuste el plan conforme a cambios organizativos o tecnológicos.

´-Documento que establezca que los activos empresariales críticos deben ser respaldados automáticamente, mínimo de forma semanal o más frecuente según la sensibilidad de los datos.
-Inventario que indique qué activos tienen respaldo activo, su frecuencia (diaria, semanal, etc.) y responsable.
-Capturas de pantallas de la programación de respaldos en herramientas de backup, sistemas operativos, scripts automatizados o servicios en la nube.
-Logs o reportes de ejecución de respaldos exitosos, generados automáticamente o recolectados manualmente.
-Actas o listas de verificación donde se evidencie que se revisa regularmente que los respaldos se están ejecutando conforme a lo programado.

´-Documento que establezca que los datos de respaldo deben tener el mismo nivel de seguridad que los datos originales: acceso controlado, cifrado, separación lógica o física si aplica.
-Capturas de pantalla o reportes que muestren que los respaldos están cifrados, ya sea en reposo (disco duro, NAS) o en tránsito (durante la transferencia al destino de respaldo).
-Evidencia de que los respaldos están separados de los datos de producción (por ejemplo, almacenados en un dispositivo distinto o en otra ubicación de red/nube).
-Listado donde se documente en qué dispositivos/medios se almacenan los respaldos y qué controles de protección tienen aplicados (cifrado, acceso restringido, ubicación segura).
-Actas o checklists donde se evidencie que periódicamente se revisa la seguridad de los respaldos (integridad, cifrado, ubicación segura).

´-Documento que establezca que los respaldos deben estar aislados del entorno de producción, usando copias fuera de línea, en nube segura, o en ubicación física separada.
-Capturas de configuración que muestren que los respaldos se almacenan en un medio separado, como discos offline, nubes independientes, o sitios fuera de las oficinas principales.
-Inventario donde se documente qué instancias o medios se usan para el respaldo aislado (identificando si son offline, fuera del sitio, en nube, etc.).
-Evidencia de que los respaldos permiten versiones múltiples (por ejemplo: versiones de archivos anteriores guardadas en servicios como OneDrive Business, Google Workspace, Azure Backup).
-Actas o listas de verificación que evidencien que se revisa regularmente que las instancias aisladas estén íntegras, actualizadas y accesibles para recuperación en caso de emergencia.

CIS Control #12: Gestión

´-Documento que establezca que routers, switches, firewalls, access points y otros dispositivos de red deben ejecutar la última versión estable compatible del firmware/software.
-Listado donde se documente cada dispositivo de red (marca, modelo, versión de firmware/software actual, fecha de última actualización).
-Evidencias visuales de los dispositivos mostrando su versión actual instalada (capturas de pantalla desde la consola o dashboard de administración).
-Actas, checklists o reportes donde se evidencie que se revisan regularmente las versiones de firmware/software y se planean actualizaciones si es necesario.
-Bitácora donde se documente cuándo y cómo se actualizó cada dispositivo o cuándo se planea actualizar si el dispositivo está próximo a ser obsoleto.

CIS Control #14: Concientización de se

´-Documento que describa el programa de capacitación en seguridad, estableciendo que debe impartirse al ingresar a la organización y, como mínimo, una vez al año.
-Presentaciones, manuales, infografías, videos o cursos que enseñen a la fuerza laboral buenas prácticas de seguridad (contraseñas seguras, phishing, manejo seguro de datos, navegación segura, etc.).
-Listado de empleados que recibieron la capacitación, fecha de capacitación, y formato de firma de participación (puede ser digital o manual).
-Bitácoras, constancias de cursos, evaluaciones o correos institucionales que documenten que se impartió capacitación al contratar y de manera anual.
-Actas o documentos que evidencien que el contenido de capacitación se revisa y actualiza anualmente o cuando cambian los riesgos o normativas.

´-Documento que establezca que los empleados deben ser capacitadas específicamente

para identificar y responder ante phishing, smishing (phishing por SMS) y vishing (phishing por llamada).
-Presentaciones, infografías, videos o manuales que expliquen los métodos de ataque comunes y cómo reconocer señales de intento de ingeniería social.
-Listado de empleados que tomaron el módulo o curso específico de ingeniería social, con fecha y firma de participación.
-Resultados de simulaciones de phishing internas o cuestionarios de evaluación de conocimientos sobre ingeniería social.
-Acta o reporte donde se evidencie que el contenido de capacitación sobre ingeniería social se revisa y actualiza anualmente.

´-Documento que establezca que todos los empleados deben ser capacitados en el uso seguro de contraseñas, MFA, y administración de credenciales.
-Presentaciones, infografías, guías o videos que expliquen temas como: qué es MFA, cómo crear contraseñas seguras, cómo administrar credenciales (no compartirlas, no guardarlas en papel, uso de gestores de contraseñas).
-Listado de empleados que tomaron la capacitación específica sobre MFA, contraseñas seguras y gestión de credenciales, incluyendo fecha y firma de participación.
-Cuestionarios o breves evaluaciones para validar que los empleados comprenden las mejores prácticas de autenticación.

´-Documento que establezca que todos los empleados deben ser capacitados en identificación, almacenamiento, transferencia, archivado y destrucción segura de datos confidenciales. También debe incluir las mejores prácticas de pantalla limpia y escritorio limpio.
-Presentaciones, infografías, manuales o videos que aborden: identificación de datos confidenciales, uso seguro de medios (USB, discos duros), almacenamiento seguro, reglas de "pantalla limpia" (bloquear la pantalla al ausentarse) y "escritorio limpio" (guardar documentos físicos y electrónicos).
-Listado de participantes de la capacitación, con fecha, firma o confirmación de participación.
-Fotos, capturas de pantalla de sesiones, correos de invitación o agendas de cursos donde se aborden explícitamente temas de manejo de datos confidenciales y limpieza de espacios.

´-Documento que establezca que el personal debe ser capacitado para identificar y prevenir situaciones de exposición no intencional de datos (ej., entrega incorrecta, pérdida de dispositivos, publicación no autorizada).
-Presentaciones, infografías, guías o videos que aborden temas como: errores comunes en el manejo de datos, pérdidas de dispositivos portátiles, y consecuencias de publicaciones erróneas de datos.
-Listado de participantes de la capacitación, indicando fecha y firma de participación.
-Material de ejercicios o ejemplos que demuestren casos de exposición accidental y cómo prevenirlos (ej.: enviar un correo a destinatarios incorrectos, pérdida de USB, publicar documentos confidenciales en sitios web públicos).

´-Documento que establezca que todos los empleados deben ser capaces de identificar un incidente potencial (sospecha de malware, acceso no autorizado, fuga de información, etc.) y reportarlo de forma inmediata.
-Presentaciones, manuales, guías rápidas o infografías que enseñen: qué es un incidente, ejemplos de incidentes, y cómo reportarlos correctamente (correo, teléfono, plataforma, etc.).
-Listado de participantes de la capacitación, indicando fecha, tema y firma de participación.
-Documento o infografía accesible que explique claramente los pasos para reportar un incidente (qué datos incluir, a quién reportarlo, tiempos de respuesta).

´-Documento que indique que los empleados deben estar capacitados para identificar si el software no se actualizó correctamente o si fallaron procesos automatizados, y notificarlo a TI de inmediato.
-Presentaciones, infografías o guías rápidas que expliquen ejemplos de: software que no actualiza, errores de herramientas automáticas, alertas de sistema, o síntomas de parches fallidos.
-Listado de participantes indicando fecha, tema de capacitación y firma o confirmación de participación.
-Documento o guía que explique de forma sencilla cómo reportar al área de TI cualquier detección de software no actualizado o proceso automatizado que falle.
-Actas o reportes donde conste que el contenido de esta capacitación se revisa y actualiza anualmente.
´-Documento que indique que los empleados deben ser capacitados sobre los riesgos de

conectarse a redes Wi-Fi públicas/inseguras y la importancia de proteger su red doméstica si trabajan remotamente.
-Presentaciones, guías, infografías o videos que expliquen: los riesgos de redes abiertas, cómo conectarse de manera segura (VPN, HTTPS), y buenas prácticas para configurar redes domésticas seguras (cambio de contraseñas del router, uso de cifrado WPA2 o superior, desactivación de WPS).
-Listado de participantes indicando fecha, tema y firma o confirmación de participación.
-Documento sencillo para los empleados remotos que explique los pasos básicos para asegurar sus redes Wi-Fi caseras.
-Documento o acta que evidencie que el contenido sobre redes seguras y teletrabajo se revisa y actualiza anualmente.

CIS Control #15: Gestión d

´-Documento que establezca que se debe mantener un inventario actualizado de proveedores de servicios, con clasificación de riesgos y designación de responsables internos para cada proveedor.
-Listado donde se documenten: nombre del proveedor, servicio proporcionado, clasificación de riesgo (bajo, medio, alto), responsable interno de la relación, y estado actual del servicio.
-Documento o sección que defina los criterios para clasificar a los proveedores según el impacto en la organización (ej.: proveedores que manejan datos sensibles = alto riesgo; servicios generales = bajo riesgo).
-Acta o minuta de revisión donde se evidencie que el inventario se revisa y actualiza al menos una vez al año, o cuando cambia la relación con un proveedor.

CIS Control #17: Gestión d

´-Documento que establezca que debe designarse una persona principal y al menos un respaldo que coordinen el manejo de incidentes (interno o combinado con proveedores externos).
-Listado o acta donde se indique quién es el responsable principal del proceso de incidentes, su respaldo, y en su caso, proveedor externo involucrado (indicando el supervisor interno).
-Correo, circular o aviso institucional donde se informe al personal quién es el responsable y respaldo para incidentes de seguridad.
-Documento que indique que si se contrata a un proveedor externo para respuesta a incidentes, debe existir un supervisor interno que coordine y valide las acciones del proveedor.
-Acta de revisión anual para verificar si los responsables designados siguen vigentes o si debe actualizarse por cambios organizativos.

´-Documento que describa que debe mantenerse actualizada la información de contacto de

-Documento que describa que debe mantenerse actualizada la información de contacto de las partes que deben ser informadas en caso de incidentes (internos y externos).
-Listado que incluya: nombre de la organización/persona, rol o relación con la empresa, tipo de incidente que deben ser notificados, teléfonos, correos electrónicos, y horario de contacto preferido.
-Acta o minuta que evidencie que anualmente se revisa la información de contactos para asegurarse de que esté actualizada.
-Documento breve o guía que describa cuándo y cómo se debe notificar a cada contacto (por ejemplo: notificar a aseguradora solo si hay filtración de datos, notificar a fuerzas del orden en caso de ciberataque grave).

erHigiene 2025 - Departamento de Ciberseguridad

	Responsable de cumplimiento (Llenado por la entidad)	Evidencia Presentada
o y Control de Activos		
ontrol de Activos de Software		

otección de Datos

raciones seguras documentadas

ntinua de vulnerabilidades

ón de logs de auditoría

orreo electrónico y navegador web

ensas contra malware

cuperación de Datos

de Infraestructura de Red

eguridad y capacitación en habilidades

e proveedores de servicio

de Respuesta a Incidentes

Gobierno de Michoacán
HONESTIDAD Y TRABAJO

¿Cumple el objetivo? (Llenado por el Departamento de Ciberseguridad)