2025

DEPARTMENT OF ECONOMIC DEVELOPMENT AND COMMERCE
GOVERNMENT OF PUERTO RICO

CMMC Nivel 1 Requisitos, Procedimientos y Ejemplos

FeCC FEDERAL CONTRACTING CENTER
AN APEX ACCELERATOR

APEX ACCELERATORS

CMMC Nivel 1 – Requisitos, Procedimientos y Ejemplos
Última actualización: 17 de marzo de 2025

Índice

I. Aviso Legal

Esta guía cubre los requisitos del Nivel 1 del **Modelo de Certificación de Madurez en Ciberseguridad (CMMC)**. El CMMC tiene tres niveles, cada uno con requisitos adicionales de ciberseguridad. Aunque esta guía ofrece una base para prácticas básicas, las organizaciones deben considerar sus objetivos a largo plazo y futuras oportunidades de contratos. Si planifica participar en contratos que requieran CMMC Nivel 2 o superior, **se recomienda** implementar desde el inicio una infraestructura y controles de seguridad alineados con esos niveles.

- **Información provista tal cual:** El contenido de esta guía se ofrece únicamente con propósitos de informar y no debe considerarse asesoramiento profesional. **El Centro de Contratación Federal de Puerto Rico (FeCC)**, un **Acelerador APEX**, no garantiza, ya sea de forma expresa o implícita, la precisión, integridad o efectividad de la información contenida en este documento.
- **Sin garantía ni respaldo**: El **FeCC** no garantiza que la información, métodos o procesos descritos en esta guía no infrinjan derechos de propiedad intelectual ni evitarán daños derivados de su uso. La mención de productos específicos o nombres comerciales no constituye un respaldo por parte del FeCC.
- **Los recursos principales**: Usted es responsable de consultar el sitio web oficial del DoD CMMC, la cláusula FAR 52.204-21, y la última Guía de Evaluación del CMMC para conocer los requisitos actualizados del Nivel 1 de CMMC. Aunque esta guía refleja la orientación actual del **DoD**, los requisitos de CMMC están sujetos a cambios. Por lo tanto, revise periódicamente el sitio web oficial del **DoD CMMC** y la última **Guía de Evaluación del CMMC** para mantenerse en cumplimiento.
- **Alcance limitado y Desarrollo**: Esta guía fue producida por el **FeCC** con la asistencia de la inteligencia artificial y no ha sido revisada por expertos en ciberseguridad.
- **Requisitos de transferencia**: Las cláusulas de la **Regulación Federal de Adquisiciones (FAR)** y el **Suplemento de Regulación Federal de Adquisiciones del Departamento de Defensa (DFARS)**, incluyendo **FAR 52.204-21, DFARS 252.204-7012**, y **DFARS 252.204-7021**, generalmente requieren que los contratistas principales **transfieran** los requisitos de ciberseguridad a sus subcontratistas. Esto significa que, en la mayoría de los casos, los subcontratistas también deben cumplir con los estándares de ciberseguridad aplicables.

II. Introducción

Las pequeñas empresas que trabajan o planifican trabajar con el gobierno federal, en especial con el DoD, deben cumplir con estándares específicos de ciberseguridad. Esta guía simplifica los fundamentos del CMMC Nivel 1 en pasos fáciles de entender, cubriendo prácticas esenciales para proteger la Información de Contratos Federales (FCI). Los requisitos completos están en la Guía de Evaluación del CMMC Nivel 1 (Versión 2.13 | Septiembre 2024)

Aunque esta guía cubre el **Nivel** 1, es importante saber que el programa CMMC incluye tres niveles. Estos niveles son:

Nivel 1: Autoevaluación (Información de Contratos Federales – FCI)

Este nivel requiere una autoevaluación para garantizar la seguridad de la Información de Contratos Federales (FCI) que se procesa, almacena o transmite durante la ejecución del contrato.

- El contratista debe cumplir con los 15 requisitos de seguridad establecidos en la cláusula FAR 52.204-21.
- Todos los requisitos deben cumplirse en su totalidad—no se permiten excepciones.

Nivel 2: Autoevaluación (Información No Clasificada Controlada – CUI)

Este nivel requiere una autoevaluación para garantizar la seguridad de la Información No Clasificada Controlada (CUI) que se procesa, almacena o transmite durante la ejecución del contrato.

- El contratista debe cumplir con los 110 requisitos de seguridad del Nivel 2, basados en el estándar NIST SP 800-171.

Nivel 2: Evaluación por C3PAO (Cumplimiento Verificado por Terceros)

Este nivel difiere al Nivel 2 (Autoevaluación) en el método de verificación de cumplimiento.

- Las empresas deben contratar a una Organización de Evaluación del CMMC de Tercera Parte (C3PAO) para llevar a cabo la evaluación.

Nivel 3: Evaluación por DIBCAC (Requisitos Avanzados)

Este nivel implica una evaluación realizada directamente por el gobierno e incluye 24 requisitos adicionales, basados en el estándar NIST SP 800-172.

III. ¿Qué es la Información de Contratos Federales (FCI)?

Entender la FCI es crucial para garantizar su adecuada protección. La FCI incluye una amplia variedad de datos generados o intercambiados durante un contrato con el gobierno federal. En esencia, es cualquier información que no esté disponible al público y que sea creada o proporcionada a un contratista en apoyo a un contrato federal. Para calificar como FCI, la información debe:

- Ser generada para o proporcionada al contratista específicamente para el contrato.
- **No estar disponible públicamente**.
- Apoyar directamente el cumplimiento del contrato.

Ejemplos de FCI incluyen:

Documentos contractuales:

- Términos y condiciones del contrato
- Declaraciones de trabajo
- Avisos de adjudicación de contrato

Datos Técnicos:

- Planos de ingeniería y esquemas
- Código fuente de software
- Informes de investigación y desarrollo

Datos financieros:

- Propuestas e informes de costos
- Datos de desempeño financiero

Información sobre el personal:

- Roles y responsabilidades dentro del contrato
- Autorizaciones y credenciales de seguridad

IV. La importancia del CMMC

El aumento de la sofisticación de los ciberataques representa riesgos significativos para la seguridad nacional y la integridad de los programas del DoD. El CMMC es clave para asegurar que los contratistas que gestionan información sensible cuenten con las medidas de ciberseguridad adecuadas.

Toda empresa con un contrato federal activo debe verificar si la cláusula **FAR 52.204-21** está incluida en su contrato. Si lo está, es importante saber que, al firmarlo, usted está certificando que cumple con todos los requisitos. *No cumplir con esta cláusula puede constituir un* ***incumplimiento de contrato*** y, en algunos casos, generar responsabilidad legal bajo la ***Ley de Reclamaciones Falsas (False Claims Act).*** El incumplimiento de los requisitos del **CMMC**, cuando son obligatorios pueden resultar en rechazo de la oferta del contrato, suspensión del contrato, o terminación del contrato, potencialmente afectando tanto los ingresos como la reputación de la empresa.

Por ello, se recomienda que las empresas con contratos federales, o aquellas que buscan oportunidades de negocio con el gobierno, tomen las medidas necesarias para cumplir con todos los requisitos de esta cláusula.

V. Identificando el Alcance de la Evaluación CMMC – Primer Paso

El **primer paso** para cumplir con los requisitos del **Nivel 1 del CMMC** es definir el **alcance (scoping)**. Este paso te ayuda a identificar cuáles de sus sistemas informáticos incluyendo aquellos administrados por **Proveedores de Servicios Externos (ESPs)** manejan **Información de Contratos Federales (FCI)**.

El **alcance** determina qué sistemas y equipos deben cumplir con los **requisitos de seguridad del Nivel 1 del CMMC**. En términos simples, cualquier sistema que maneje FCI de alguna manera se considera “dentro del alcance” (In Scope) para su autoevaluación del Nivel 1.

¿Cuándo un Sistema está Dentro del Alcance?

Un Sistema está dentro del alcance si:

- **Procesa FCI**: El sistema **utiliza** FCI, es decir, accede, ingresa, edita, genera, manipula o imprime información de contratos federales. Ejemplos: Una computadora utilizada para crear facturas con números de contrato, una impresora que imprime documentos contractuales o una aplicación de software que gestiona datos de contratos.
- **Almacena FCI:** La FCI se encuentra **guardada** en el sistema, ya sea en medios electrónicos (disco duro, almacenamiento en la nube) o en formato físico (documentos

impresos). Ejemplos: Un servidor que almacena archivos de contratos, una computadora con especificaciones de contratos, un archivo con copias físicas de contrato o un dispositivo USB utilizado para respaldar datos de contratos.

- **Transmite FCI:** La FCI **se transfiere** de un sistema a otro, ya sea mediante métodos físicos o digitales. Ejemplos: Enviar archivos de contrato por correo electrónico, subir documentos de contrato a un portal gubernamental, transferir datos de contrato a través de una red o enviar físicamente FCI en un disco duro.

Preguntas Clave para Definir el Alcance:

- ¿Este sistema procesa, almacena o transmite FCI?
- ¿Este sistema se conecta con otros sistemas que manejan FCI?
- ¿Algún Proveedor de Servicios Externos (ESPs) administran algún sistema que maneje FCI bajo su nombre?

¿Cuándo un Sistema está Fuera del Alcance?

Los activos que no procesan, almacenan ni transmiten FCI están fuera del alcance. Sin embargo, es importante identificar todos los activos, incluso esos fuera del alcance. Además, algunos activos especializados se excluyen automáticamente de las evaluaciones de Nivel 1, incluso si pudieran manejar FCI, ya que no pueden asegurarse completamente bajo sus requisitos. Estos incluyen:

- Dispositivos IoT(Internet de las Cosas)
- Dispositivos IIoT (Internet Industrial de las Cosas)
- Sistemas de tecnología operativa
- Equipos suministrados por el gobierno
- Sistemas con acceso restringido
- Dispositivos o herramientas de prueba

Cómo determinar si un Activo Está Dentro o Fuera del Alcance

Para clasificar un activo en una de estas categorías, considere las siguientes preguntas:

- **Propiedad**: ¿Quién es el dueño del activo (empresa o personal)?
- **Uso**: ¿Se usa el activo exclusivamente para negocios, solo para uso personal, o para ambos?
- **Conexión**: ¿El activo se conecta a sistemas que contienen FCI?
- **Manejo de FCI**: ¿El activo almacena, procesa o transmite FCI?

Entornos de Uso Mixto (*Dispositivos Personales y de Trabajo*):

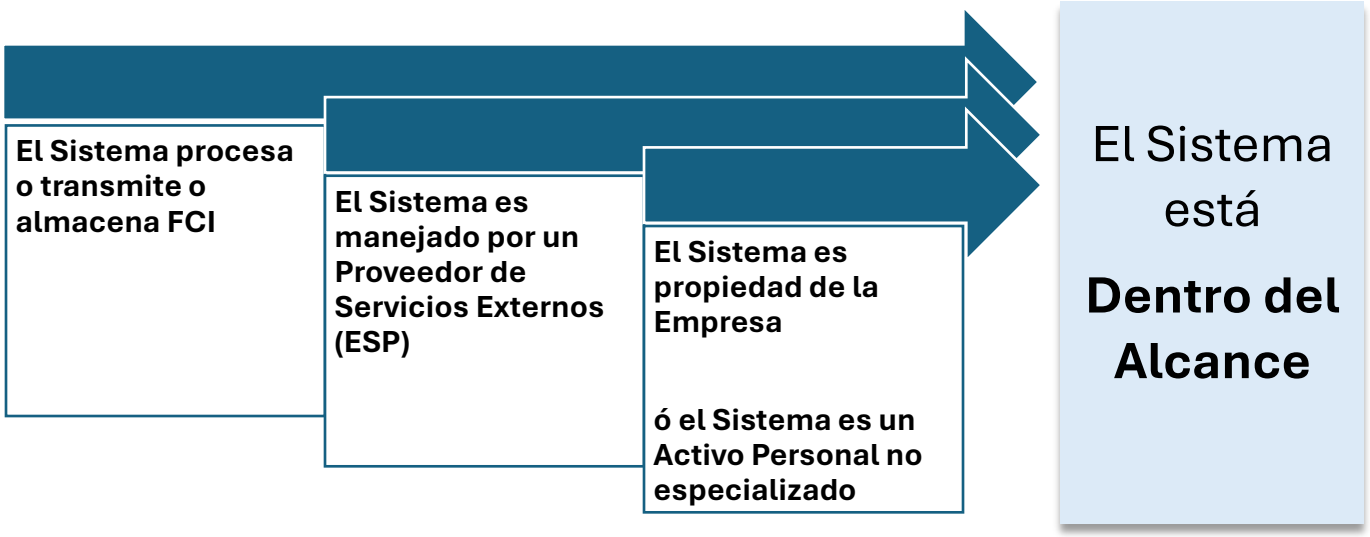
En estos casos, el *uso principal* del activo generalmente determina si está dentro o fuera del alcance.

- **Ejemplo Fuera del Alcance**: Una **laptop personal** usada principalmente para tareas personales, pero ocasionalmente utilizada para revisar correos electrónicos del trabajo (siempre que esté adecuadamente separada de la FCI y cubierta por políticas de uso).
- **Ejemplo Dentro del Alcance**: Un **dispositivo personal** que se usa regularmente para manejar FCI, como redactar o revisar documentos de contratos.

Punto Clave: Mantenga un inventario detallado de *todos los activos*. Marque claramente cada activo como "dentro del alcance" o "fuera del alcance", y documente la razón. Esta documentación es crucial para auditorías y para demostrar su comprensión sobre los límites de su CMMC.

Diagrama de Flujo de Decisión de Alcance del CMMC Nivel 1

El siguiente diagrama de flujo proporciona una representación visual de cómo determinar si un sistema está dentro del alcance para el CMMC Nivel 1.



Ejemplos de Escenarios – Evaluación de Sistemas dentro y fuera del alcance

Escenario 1: Negocio Regular (Empresa de Manufactura Pequeña)

- **Descripción del Negocio**: Una pequeña empresa de manufactura que produce piezas para una agencia federal o un contratista principal. Reciben planos, especificaciones e información de contrato de forma electrónica.
- **Sistemas y Activos:**
  - **Dentro del Alcance:**
    - Computadoras utilizadas por ingenieros para acceder y modificar planos.
    - Servidor de archivos donde se almacenan planos y datos de contratos.
    - Servidor de correo electrónico utilizado para enviar y recibir correos con FCI.
    - Routers de red y firewalls que protegen estos sistemas.
    - Servicio de almacenamiento en la nube usado para respaldar los planos.
  - **Fuera del Alcance**:
    - Computadoras utilizadas para contabilidad y recursos humanos (a menos que interactúen directamente con sistemas que manejan FCI).
    - Sitio web de la empresa (a menos que almacene o transmita FCI).
    - Impresoras utilizadas solo para documentos administrativos internos.

Escenario 2: Negocio desde el Hogar

- **Descripción del Negocio:** Un consultor independiente que ofrece servicios de redacción técnica a una agencia gubernamental. Recibe y entrega documentos con FCI de forma electrónica.
- **Sistemas y Activos:**
  - **Dentro del Alcance:**
    - Laptop personal utilizada para crear, editar y almacenar documentos con FCI.
    - Router Wi-Fi y módem del hogar.
    - Cuenta de correo electrónico personal utilizada para intercambiar FCI con la agencia.
    - Servicio de almacenamiento en la nube utilizado para respaldar documentos relacionados con FCI.

- **Fuera del Alcance:**
  - Teléfono inteligente personal utilizado para llamadas y mensajes privados (a menos que se use para acceder o almacenar FCI).

¿Por qué importa esta diferencia?

Como se puede ver, el **alcance del CMMC Nivel 1** puede variar significativamente según la naturaleza de su negocio. La empresa de manufactura tiene una infraestructura de tecnología más compleja y varios sistemas que manejan FCI, lo que amplía su alcance. El consultor independiente, que trabaja desde casa, tiene una configuración mucho más simple, lo que resulta en un alcance más reducido.

Consideraciones importantes:

- **Flujo de Datos:** Rastrear cómo circula la FCI en su empresa le ayudará a identificar todos los sistemas que la procesan, almacenan, o transmiten.
- **Proveedores de Servicios Externos (ESPs):** Si utiliza servicios externos (por ejemplo, almacenamiento en la nube, servicios de IT gestionados), debe considerar sus sistemas y prácticas de seguridad dentro del alcance.
- **Documentación:** Mantenga un registro detallado de sus decisiones de alcance. Esto será clave para su autoevaluación y posibles auditorías futuras.

La Guía de Alcance del CMMC Nivel 1 ofrece una visión completa de los requisitos y procesos de alcance.

VI. Requisitos Actuales para Contratistas y Subcontratistas – Segundo Paso

Después de identificar qué sistemas manejan Información de Contratos Federales (FCI), el siguiente paso es implementar medidas de seguridad básicas para proteger esa información y cumplir con el Nivel 1 del CMMC. Estas medidas se denominan “controles de seguridad”, y hay 15 requisitos específicos para este nivel. Estos controles están detallados en 48 CFR 52.204-21(b)(1)(i) al (xv), una publicación que explica exactamente qué debe hacer para proteger sus sistemas. Dado que las regulaciones gubernamentales pueden cambiar, es importante revisar siempre la versión más reciente de 52.204-21.

Controles de Seguridad del CMMC Nivel 1: 15 Requisitos

I. **Limitar el acceso** a los sistemas de información a usuarios, procesos y dispositivos autorizados.

II. **Restringir el acceso** a los sistemas según las transacciones y funciones permitidas a los usuarios autorizados.

III. **Verificar, controlar y limitar** las conexiones y el uso de sistemas de información externos.

IV. **Controlar la información publicada** o procesada en sistemas de información públicos.

V. **Identificar a usuarios,** procesos y dispositivos en los sistemas de información.

VI. **Autenticar las identidades** de usuarios, procesos y dispositivos antes de conceder acceso.

VII. **Limpiar o destruir** medios que contengan FCI antes de su eliminación o reutilización.

VIII. **Restringir el acceso físico** a los sistemas de información de la organización, equipos y entornos operativos a personas autorizadas.

IX. **Escoltar a los visitantes y monitorear su actividad;** mantener registros de auditoría de acceso físico; controlar y gestionar dispositivos de acceso físico.

X. **Monitorear, controlar y proteger** las comunicaciones organizacionales (es decir, la información transmitida o recibida por los sistemas de información de la organización) en los límites externos y en los puntos clave internos del sistema.

XI. **Implementar subredes** para componentes del sistema accesibles públicamente, asegurando que estén física o lógicamente separados de las redes internas.

XII. **Identificar, reportar y corregir vulnerabilidades** en los sistemas de información de manera oportuna.

XIII. **Proteger los sistemas de información contra código malicioso** en los puntos adecuados dentro de la infraestructura organizacional.

XIV. **Actualizar los mecanismos de protección** contra código malicioso cuando hayan nuevas versiones disponibles.

XV. **Realizar escaneos periódicos** del sistema de información y escaneos en tiempo real de archivos provenientes de fuentes externas al descargarlos, abrirlos o ejecutarlos.

La cláusula 52.204-21 no exime al contratista de otros requisitos de seguridad específicos impuestos por agencias o departamentos federales en relación con los sistemas de información del contratista ni de otros requisitos federales de protección para información no pública (FCI) o no clasificada controlada (CUI).

Responsabilidad del Contratista Principal

Es fundamental comprender que los contratistas principales son responsables de extender los requisitos de esta cláusula a sus subcontratistas que trabajen bajo un contrato cubierto. Esto aplica incluso para subcontratos de productos o servicios comerciales (excepto artículos comerciales disponibles comercialmente) si el sistema de información del subcontratista puede almacenar, procesar o transmitir FCI.

VII. Verificación CMMC Nivel 1 – Tercer Paso

Ahora es el momento de evaluar qué tan bien cumplen sus sistemas con las **normas de seguridad del CMMC Nivel 1** para proteger la FCI. Esto se hace a través de una "autoevaluación", donde revisa sus propios sistemas. ¡No se preocupe! Existen recursos, como Project Spectrum (PS), una plataforma gratuita de aprendizaje que ofrece una gran cantidad de herramientas, capacitación y videos para guiarlo a lo largo del proceso del CMMC. Incluso cuentan con una herramienta llamada **Cyber Readiness Assessment**, que le ayuda a identificar áreas que podrían necesitar mejoras.

Para cumplir con el CMMC Nivel 1, debe satisfacer los **15 controles de seguridad requeridos** y tener todos completamente implementados al momento de la auto-certificación. Esto significa que no puede simplemente tener un plan para corregir las fallas; todo debe estar operativo y funcionando. Sin embargo, si un requisito en particular **no aplica a su negocio** y puede demostrarlo, se considera como cumplido.

VIII. Sistema de Riesgo de Desempeño de Proveedores (SPRS) – Cuarto Paso

Una vez haya cumplido con todos los requisitos, deberá enviar los resultados de su evaluación en el Sistema de Riesgo de Desempeño de Proveedores (SPRS, por sus siglas en inglés). Para mantener el cumplimiento con los requisitos, debe realizar una autoevaluación del Nivel 1 cada año y enviar los resultados en el SPRS.

IX. Ejemplo de Documentación – Cumplimiento CMMC Nivel 1

Hemos hablado sobre los pasos claves para lograr el cumplimiento del **CMMC Nivel 1**, y ahora es el momento de ver cómo funciona en la práctica. Esta sección proporciona un ejemplo práctico sobre cómo delimitar el alcance de sus sistemas, identificar los requisitos de seguridad relevantes y realizar una autoevaluación. Para facilitar la comprensión, hemos creado una tabla que guía a través de un ejemplo de autoevaluación para los 15 requisitos.

La tabla incluye explicaciones sobre cómo se puede lograr el cumplimiento en dos escenarios comunes: **un negocio desde el hogar** y un **negocio estándar**. *Hemos incluido ambos escenarios para demostrar que los mismos objetivos de seguridad pueden alcanzarse mediante* ***diferentes enfoques y recursos.*** Piense en este ejemplo como una ilustración útil, no como una solución universal. **Cada empresa debe adaptar estos pasos en función de sus sistemas y tipos de información manejados.**

1. Ejemplo de Identificación de Sistemas para el Cumplimiento de CMMC

Definir el Alcance (Scoping):

Los siguientes activos han sido identificados como **dentro del alcance** para esta autoevaluación del **CMMC Nivel 1**.

Procesamiento:

1. Computadora 01 utilizada para crear facturas con números de contrato.
2. Computadora 02 utilizada para gestionar el contrato.
3. Impresora 02 utilizada para imprimir y escanear documentos de contrato.
4. Dispositivos móviles: Teléfono 01

Almacenamiento:

1. Servidor 01 que almacena archivos de contratos.
2. Laptop 01 que contiene especificaciones de contrato descargadas.
3. Archivador 01 con copias impresas de acuerdos de contrato.
4. Unidad USB 01 utilizada para respaldar datos del contrato.
5. Discos duros externos 01 y 02

Transmisión:

1. Plataforma de correo electrónico (Outlook, Gmail...).

2. Portal gubernamental PIEE.
3. Red(describir).
4. Envío físico de información de contrato.

Justificación para Incluir/Excluir Activos:

Computadora 01 es utilizada por el gerente de contratos para crear y editar contratos, por lo que está **dentro del alcance**. Impresora 02 solo se usa para documentos administrativos internos y nunca maneja FCI, por lo que está **fuera del alcance**.

---

2. Ejemplo en forma de Tabla: 15 Controles de Seguridad Requeridos

La siguiente tabla enumera los **15 requisitos de protección** de la cláusula FAR 52.204-21 y muestra cómo **dos tipos de negocios**– un negocio estándar con empleados e infraestructura IT formal y un negocio desde el hogar operado por una sola persona pueden cumplirlos.

La tabla incluye:

- Cada requisito con una breve descripción.
- Estado de cumplimiento.
- Ejemplos de implementación para ambos tipos de negocios.

Este análisis comparativo muestra cómo el **tamaño y la complejidad de un negocio afectan los métodos de cumplimiento**. Por ejemplo, mientras una empresa estándar puede utilizar tarjetas de acceso y registros de visitantes, un negocio desde el hogar se basa en seguridad residencial y supervisión directa. Otro caso incluye: mientras una empresa con una red grande necesita segmentación de red y dispositivos de seguridad avanzados, una sola computadora en un negocio desde el hogar depende de su firewall y software antivirus incorporado.

Conclusión Clave: Incluso las pequeñas empresas pueden cumplir con los requisitos de **FAR 52.204-21** al aplicar controles de seguridad adaptados a sus necesidades específicas.

Requisitos	Descripción	Estado de Cumplimiento	Explicación de Cumplimiento (Implementación de un negocio estándar)	Explicación de Cumplimiento (Implementación de un negocio desde el hogar)
(i) Limitar el acceso a los sistemas de información a usuarios, procesos y dispositivos autorizados.	Limitar el acceso a los sistemas de información a usuarios, procesos, y dispositivos autorizados.	Cumple	El acceso a los sistemas está controlado mediante cuentas de usuario únicas con contraseñas seguras. El acceso se concede según el principio de mínimo privilegio. Se revisan periódicamente las cuentas para asegurar que solo el personal autorizado tenga acceso.	El acceso está limitado al usuario (propietario) a través de una cuenta protegida por contraseña en la computadora. Ningún otro usuario, proceso ni dispositivo accede al sistema directamente.
(ii) Restringir el acceso a los sistemas según las transacciones y funciones permitidas a los usuarios autorizados.	Limitar el acceso a transacciones y funciones autorizadas.	Cumple	Los permisos de usuario se configuran según su rol y responsabilidades. Los usuarios solo tienen acceso a aplicaciones y datos específicos necesarios para su trabajo. Se realizan revisiones periódicas de roles y permisos de usuarios.	El único usuario (propietario) tiene acceso administrativo a la computadora y todo el software. Esto está inherentemente limitado por el software instalado y las necesidades operativas del usuario. Se utilizan controles estándar de cuentas de usuario.
(iii) Verificar, controlar y limitar las conexiones y el uso de sistemas de información externos.	Controlar las conexiones a los sistemas externos	Cumple	Las conexiones a sistemas de información externos se controlan mediante un firewall y listas de control de acceso. Solo se concede acceso a sistemas externos autorizados. Se realizan revisiones periódicas de las conexiones externas.	Las conexiones salientes se gestionan a través del firewall de la computadora y la configuración del navegador de internet. El acceso a servicios externos es iniciado por el usuario (propietario).
(iv) Controlar la información publicada o procesada en sistemas de información públicos.	Controlar las conexiones a los sistemas externos	Cumple / No Aplica	Ninguna FCI se publica ni procesa en sistemas de acceso público. Se identifican las personas autorizadas para hacerlo. Existe una política que prohíbe	Si la empresa no opera sistemas públicos, esto “No Aplica”. Si se requieren, se alojan por un proveedor externo. El propietario asegura que los datos

			almacenar o procesar FCI en estos sistemas.	publicados cumplan con los requisitos aplicables.
(v) Identificar a usuarios, procesos y dispositivos en los sistemas de información.	Identificar usuarios, procesos y dispositivos.	Cumple	Se requieren cuentas únicas con contraseñas seguras para todos los usuarios. Se implementa autenticación multifactor cuando es viable. La autenticación de dispositivos se utiliza para el acceso a la red.	El único usuario es identificado por su cuenta de usuario. Los procesos son identificados por el sistema operativo. La computadora es el único dispositivo.
(vi) Autenticar las identidades de usuarios, procesos y dispositivos antes de conceder acceso.	Autenticar usuarios, procesos, o dispositivos antes de permitir acceso	Cumple	Se han establecido políticas de contraseñas fuertes, implementado firmas digitales, certificados de dispositivos y Control de Acceso a la Red. Se documentan políticas, configuraciones y se mantienen registros de auditoría, evaluando regularmente los controles de seguridad.	La autenticación de usuario se realiza mediante el inicio de sesión con contraseña en la computadora.
(vii) Limpiar o destruir medios que contengan FCI antes de su eliminación o reutilización.	Limpiar/ destruir medios de almacenamiento antes de desechar/ reutilizar.	Cumple	Los discos duros y otros medios de almacenamiento se borran de forma segura utilizando métodos aprobados antes de su eliminación o reutilización. Existe un procedimiento documentado para la sanitización de estos dispositivos.	Los datos se eliminan de forma segura utilizando herramientas de software o destrucción física del medio (por ejemplo, trituración del disco duro) antes de su eliminación o reutilización.
(viii) Restringir el acceso físico a los sistemas de información de la organización, equipos y entornos operativos a personas autorizadas.	Restringir el acceso físico a los sistemas, equipos y entornos.	Cumple	El acceso físico a las salas de servidores y otras áreas sensibles está controlado mediante puertas con cerradura y sistemas de control de acceso. El acceso de visitantes se registra y monitorea.	El acceso físico a la computadora está controlado mediante medidas de seguridad residencial estándar dentro de la vivienda privada.
(ix) Escoltar a los visitantes y monitorear su actividad; mantener registros de auditoría de	Escoltar visitantes, monitorear actividad,		Todas las visitas deben registrarse al entrar y salir y ser acompañadas	Como negocio basado en el hogar, el acceso está controlado mediante medidas

acceso físico; controlar y gestionar dispositivos de acceso físico.	mantener registros de acceso físico, y controlar/ gestionar dispositivos de acceso físico.	Cumple / No Aplica	mientras estén en las instalaciones. Los registros se conservan durante un año según la política de la empresa. Se usa acceso mediante tarjeta de identificación para gestionar el acceso físico a las áreas restringidas.	de seguridad residencial. No se mantienen registros formales de visitantes. Los visitantes relacionados con el negocio son acompañados y supervisados. El acceso a la computadora está protegido mediante contraseñas.
(x) Monitorear, controlar y proteger las comunicaciones organizacionales (es decir, la información transmitida o recibida por los sistemas de información de la organización) en los límites externos y en los puntos clave internos del sistema.	Monitorear, controlar y proteger las Comunicaciones en los límites externos y puntos claves internos.	Cumple / No Aplica	Se implementaron firewalls, IDS/IPS y filtrado de contenido en los límites de la red. Se aseguraron configuraciones de dispositivos, se monitorean registros de tráfico y se realizan escaneos de vulnerabilidades y pruebas de penetración regularmente.	Como configuración de una sola computadora, no existen límites de red internos. La protección externa se logra mediante el firewall integrado y el software antivirus. Todas las comunicaciones se consideran externas.
(xi) Implementar subredes para componentes del sistema accesibles públicamente, asegurando que estén física o lógicamente separados de las redes internas.	Implementar subredes(por ejemplo, DMZ) para separar los sistemas públicos de las redes internas.	Cumple / No Aplica	Se ha creado una zona Desmilitarizada (DMZ) para alojar servidores y servicios de acceso público. Se han implementado reglas de firewall para restringir el tráfico entre la DMZ y las redes internas. Evaluamos periódicamente las reglas de firewall y la segmentación de la red.	Al ser una configuración de una sola computadora, no hay sistemas separados que requieran un DMZ o subredes. Si se requieren servicios de acceso público, estos son alojados por un proveedor de tercera parte.
(xii) Identificar, reportar y corregir vulnerabilidades en los sistemas de información de manera oportuna.	Identificar, reportar y corregir vulnerabilidades en los sistemas..	Cumple	Se ha establecido un proceso de escaneo de vulnerabilidades. Las vulnerabilidades identificadas se reportan y remedian de manera oportuna según su nivel de riesgo.	El usuario (propietario) es responsable de mantener el sistema operativo y el software actualizados con los parches de seguridad. Las actualizaciones automáticas se activan mientras sea posible.
(xiii) Proteger los sistemas de información contra código malicioso en los puntos adecuados dentro de la infraestructura organizacional.	Proteger contra código malicioso.	Cumple	El software antimalware está instalado y en ejecución activa en todos los sistemas dentro del alcance. Se realizan escaneos periódicos y las actualizaciones se aplican automáticamente.	El software antivirus/antimalware está instalado y se mantiene actualizado.

(xiv) Actualizar los mecanismos de protección contra código malicioso cuando hayan nuevas versiones disponibles.	Actualizar la protección contra código malicioso.	Cumple	El software antimalware está configurado para recibir e instalar actualizaciones automáticamente. Se realizan verificaciones periódicas para asegurar que las actualizaciones se estén aplicando.	El software antivirus/antimalware está configurado para actualizarse automáticamente.
(xv) Realizar escaneos periódicos del sistema de información y escaneos en tiempo real de archivos provenientes de fuentes externas al descargarlos, abrirlos o ejecutarlos.	Realizar escaneos periódicos en tiempo real.	Cumple	Se realizan escaneos completos del sistema de forma periódica en todos los sistemas dentro del alcance. El escaneo en tiempo real está habilitado para todas las descargas, aperturas y ejecuciones de archivos.	El software antivirus/antimalware realiza escaneos en tiempo real de archivos y escaneos completos del sistema de forma periódica.

3. Declaración de Autoevaluación:

Se realizó una autoevaluación en [Fecha] utilizando [Método utilizado, e.g., NIST Handbook 162, Project Spectrum's Cyber Readiness Assessment Tool] para verificar el cumplimiento de los 15 requisitos de seguridad. Los resultados de la evaluación confirmaron que se cumplieron todos los requisitos. Consulte la tabla anterior para los hallazgos.

4. Envío a SPRS:

Los resultados de esta autoevaluación de CMMC Nivel 1 han sido sometidos al Supplier Performance Risk System (SPRS) en [Fecha]. Use este enlace para obtener un conjunto completo de instrucciones sobre cómo subir la autoevaluación en SPRS.

5. Resumen de la Implementación del Cumplimiento de CMMC Nivel 1

[Nombre de la empresa] ha implementado exitosamente los requisitos de seguridad necesarios para proteger la Información de Contratos Federales (FCI) y cumplir con los requisitos CMMC Nivel 1. Esta documentación sirve como evidencia de nuestro compromiso con la ciberseguridad y el cumplimiento de las regulaciones federales.

X. Ejemplos de Políticas y Procesos

Ahora, revisemos ejemplos de políticas y procedimientos para cumplir con **CMMC Nivel 1**. Las políticas son clave para cualquier negocio, ya sea grande o pequeño, en oficina u hogar. Estas establecen reglas claras para manejar datos sensibles y evitar errores de seguridad.

Esta sección incluye ejemplos, uno diseñado para un negocio basado en el hogar, para brindarle una mejor comprensión de cómo podrían estructurarse estas políticas. Estos ejemplos fueron **creados utilizando IA**, y son solo para fines ilustrativos. *No fueron creados con el propósito de ser copiados directamente.*

Ya que cada negocio es único, será necesario adaptar las políticas a su situación específica. Trabajar con un **experto en ciberseguridad** es la mejor manera de garantizar que sus políticas sean efectivas y cumplan completamente con los requisitos de **CMMC**.

1. Política de Control de Acceso
2. Política de Identificación y Autenticación

3. Política de Protección de Medios
4. Política de Protección Física
5. Política de Protección del Sistema y Comunicaciones
6. Política de Seguridad de la Información para Negocios Basados en el Hogar

1. Política de Control de Acceso (Ejemplo)

Propósito:

Esta Política de Control de Acceso establece los procedimientos y controles para limitar el acceso a los sistemas de información y datos de [Nombre de la Organización], incluyendo la Información de Contratos Federales (FCI), únicamente a usuarios, procesos y dispositivos autorizados. Esta política está alineada con los requisitos de Certificación de Modelo de Madurez en Ciberseguridad (CMMC) Nivel 1.

Alcance:

Esta política se aplica a todos los empleados, contratistas y usuarios externos que tengan acceso a los sistemas de información y datos de [Nombre de la Organización].

Declaración de Política:

[Nombre de la Organización] está comprometida con la protección de la confidencialidad, integridad y disponibilidad de sus sistemas de información y datos. El acceso a estos recursos será otorgado únicamente a individuos autorizados, de acuerdo con sus responsabilidades laborales y bajo el principio del mínimo privilegio. Se pueden emplear mecanismos de control de acceso a nivel de aplicación y servicio para mejorar la seguridad de la información.

Medidas de Control de Acceso:

1. **Identificación y Autenticación:**
    - **Nombres de usuario y contraseñas únicas:** Todos los usuarios deben contar con nombres de usuarios únicos y contraseñas seguras y complejas.
    - **Autenticación multifactor (MFA):** Se debe implementar MFA para todas las cuentas de usuario, incluidas las cuentas administrativas.
    - **Cambio regular de contraseñas:** Se exigirá el cambio periódico de contraseñas para todos los usuarios.
2. **Listas de Control de Acceso (ACLs):**
    - Implementar ACLs en todos los dispositivos de red y sistemas para restringir el acceso únicamente a usuarios y dispositivos autorizados.
    - Revisar y actualizar regularmente las ACLs para reflejar cambios en los roles y responsabilidades de los usuarios.

3. **Mínimo Privilegio:**
    - Conceder a los usuarios solo el nivel de acceso mínimo necesario para realizar sus funciones laborales.
    - Revisar periódicamente los derechos de acceso y eliminar privilegios innecesarios o software no autorizado.
4. **Gestión de Cuentas:**
    - Desactivar o eliminar las cuentas de usuario inactivas de manera inmediata.
    - Implementar procedimientos para gestionar cuentas privilegiadas, incluyendo revisiones periódicas y rotación de contraseñas.
5. **Control de Acceso Físico:**
    - Limitar el acceso físico a centros de datos, salas de servidores y otras áreas que contengan información sensible.
    - Implementar medidas de seguridad física, como cerraduras, cámaras de seguridad y credenciales de acceso.
6. **Clasificación de Datos:**
    - Clasificar los datos según su sensibilidad y valor.
    - Aplicar controles de acceso adecuados según el nivel de clasificación de los datos.
7. **Integridad del Sistema y la Información:**
    - Implementar controles de seguridad para proteger la integridad de los sistemas de información y datos.
    - Monitorear regularmente los sistemas para detectar accesos no autorizados y actividades maliciosas.
8. **Control de Información en Sistemas Públicamente Accesibles:**
    - **Depuración de datos:** Asegurar que cualquier FCI u otros datos sensibles publicados o procesados en sistemas de acceso público estén anonimizados o eliminados correctamente.
    - **Orientación a Usuarios:** Proporcionar una guía clara a los empleados sobre qué información puede y no se puede publicar en sistemas de acceso público.
    - **Monitoreo:** Supervisar regularmente los sistemas accesibles al público para detectar cualquier divulgación no autorizada de información sensible.
    - **Publicación:** Garantizar que solo personas autorizadas publiquen información en sistemas de acceso público y que el contenido sea revisado antes de su publicación para evitar la divulgación de datos no públicos.
9. **Verificación y Control de Conexiones a Sistemas Externos:**

- **Conexiones Autorizadas:** Solo se permitirán conexiones a sistemas externos autorizados, las cuales deberán estar documentadas y aprobadas por [Autoridad o Rol Designado].
- **Métodos de Conexión:** Controlar los métodos utilizados para conectarse a sistemas externos, como VPNs, protocolos de transferencia segura de archivos (SFTP) u otros canales de comunicación seguros.
- **Restricciones de Transferencia de Datos:** Implementar controles para limitar el tipo y la cantidad de datos que pueden transferirse a sistemas externos. Prohibir la transferencia de FCI sin autorización explícita.
- **Revisión Periódica:** Auditar regularmente las conexiones a sistemas externos para garantizar el cumplimiento de esta política.
- **Prohibición de Dispositivos no Autorizados:** Prohibir la conexión de dispositivos personales no autorizados a la red de la organización si aprobación explícita de [Autoridad o Rol Designado].

Aplicación de la Política:

- Las violaciones de esta política estarán sujetas a acciones disciplinarias, que pueden incluir la terminación del empleo.
- Se realizarán auditoría y evaluaciones regulares para garantizar el cumplimiento de esta política.

Capacitación y Concienciación:

- Todos los empleados y contratistas recibirán capacitación sobre esta política y sus responsabilidades en la protección en la protección de los sistemas de información y datos.
- Se ofrecerán sesiones regulares de concienciación en seguridad para todos los usuarios.

Revisión y Actualización:

- Esta política será revisada y actualizada al menos una vez al año o cuando sea necesario debido a cambios en la tecnología, amenazas o requisitos normativos.

Información de Contacto:

Si tiene dudas o alguna inquietud sobre esta política, favor de comunicarse con [Persona de Contacto] a través de [Información de Contacto].

Nota: Esta es una política de control de acceso de ejemplo y deberá adaptarse a las necesidades específicas de su organización. Se recomienda consultar con un profesional de ciberseguridad cualificado para garantizar el cumplimiento de CMMC Nivel 1 y otras regulaciones aplicables.

2. Política de Identificación y Autenticación (Ejemplo)

Propósito:

Esta política define los requisitos para la identificación y autenticación de usuarios, procesos que actúan en nombre de usuarios y dispositivos que buscan acceder a los sistemas de información de [Nombre de la Organización]. Esta política está diseñada para cumplir con los requisitos de Certificación de Modelo de Madurez en Ciberseguridad (CMMC) Nivel 1.

Alcance:

Esta política se aplica a todos los empleados, contratistas, usuarios externos y dispositivos que acceden a los sistemas de información de [Nombre de la Organización], incluyendo aquellos que contienen Información de Contratos Federales (FCI).

Declaración de Política:

[Nombre de la Organización] se compromete a garantizar que solo los usuarios, procesos y dispositivos autorizados tengan acceso a sus sistemas de información. Esto se logra mediante mecanismos sólidos de identificación y autenticación.

Requisitos de Identificación y Autenticación:

1. **Identificación Única de Usuarios:**
    - Cada usuario que acceda a los sistemas de información de la organización tendrá un identificador único (nombre de usuario o cuenta).
    - Se prohíben las cuentas genéricas o compartidas, excepto en casos documentados y aprobados (por ejemplo, acceso a Wi-Fi para invitados con privilegios limitados).
    - Los identificadores de usuario serán administrados mediante un proceso formal de gestión de cuentas, que incluirá la creación, modificación, suspensión y eliminación de cuentas.
2. **Mecanismos de Autenticación:**
    - **Contraseñas:** Deben cumplir con los siguientes requisitos mínimos:
        - Longitud mínima de 12 caracteres.
        - Combinación de letras mayúsculas, minúsculas, números y símbolos.
        - No deben basarse en información personal (por ejemplo, nombres o fechas de nacimiento).
        - No deben reutilizarse.
    - **Autenticación Multifactor (MFA):** MFA es obligatoria para todas las cuentas de usuario, especialmente para cuentas privilegiadas (administradores). Métodos aceptables de MFA incluyen:

        - Contraseñas de un solo uso basadas en tiempo (TOTP, como Google Authenticator o Authy).
        - Tokens de hardware.
    - **Autenticación de Dispositivos:** Los dispositivos que se conecten a la red de la organización serán identificados y auten
        - MAC address filtering.
        - Network Access Control (NAC).
        - Device certificates.
3. **Gestión de la Autenticación:**
    - **Cambios de contraseñas:** Los usuarios deberán cambiar sus contraseñas al menos cada 90 días o según lo determine [Autoridad/Rol Designado].
    - **Bloqueo de cuentas:** Para prevenir ataques de fuerza bruta, se implementará un bloqueo de cuenta después de un número definido de intentos fallidos (por ejemplo, 5). El bloqueo durará un período determinado (por ejemplo, 30 minutos) o requerirá intervención del administrador.
    - **Gestión de sesiones:** Las sesiones de usuario inactivas se cerrarán automáticamente después de un período definido de inactividad (por ejemplo, 15 minutos).
4. **Procesos que Actúan en Nombre de los Usuarios:**
    - Los procesos automatizados que requieren acceso a los sistemas de información deberán utilizar cuentas de servicio únicas con los privilegios adecuados.
    - Estas cuentas de servicio estarán sujetas a las mismas políticas de autenticación y control de acceso que las cuentas de usuario.
5. **Acceso a Invitados:**
    - El acceso de invitados a los recursos de la organización será limitado y controlado.
    - Las cuentas de invitados serán temporales y otorgadas únicamente para propósitos específicos.
    - Siempre que sea posible, el acceso de invitados se proporcionará en un segmento de red separado para aislarlo de los recursos internos.
6. **Identificación y Autenticación para el Acceso Inalámbrico:**
    - Todo acceso a la red inalámbrica deberá requerir autenticación utilizando protocolos de cifrado robustos (por ejemplo, WPA2/3-Enterprise) y credenciales únicas.

Aplicación de la Política:

- El incumplimiento de esta política puede dar lugar a medidas disciplinarias, incluyendo la terminación del contrato laboral o de servicios.

Capacitación y Concienciación:

- Todos los usuarios recibirán capacitación sobre esta política y sus responsabilidades para mantener contraseñas seguras y proteger sus credenciales.

Revisión y Actualización:

- Esta política será revisada y actualizada al menos una vez al año o cuando sea necesario debido a cambios en la tecnología, amenazas o requisitos normativos.

Información de Contacto:

Para preguntas o inquietudes sobre esta política, comuníquese con [Persona de Contacto] a través de [Información de Contacto].

Nota: Esta es una política de identificación y autenticación de ejemplo y deberá adaptarse a las necesidades específicas de su organización. Se recomienda consultar con un profesional de ciberseguridad calificado para garantizar el cumplimiento de CMMC Nivel 1 y otras regulaciones aplicables.

3. Política de Protección (Ejemplo)

Propósito:

Esta política establece los requisitos para la protección, manipulación y eliminación de medios de almacenamiento de sistemas de información que contengan Información de Contratos Federales (FCI) dentro de [Nombre de la Organización]. Está diseñada para cumplir con los requisitos de Certificación de Modelo de Madurez en Ciberseguridad (CMMC) Nivel 1.

Alcance:

Esta política se aplica a todos los empleados, contratistas y terceros que manejen, almacenen o eliminen medios de almacenamiento de información, tanto digitales como no digitales, que contengan FCI. Esto incluye, pero no se limita a:

- Discos duros de computadoras (HDD)
- Unidades de estado sólido (SSD)
- Dispositivos USB
- Dispositivos ópticos (CDs, DVDs, Blu-rays)
- Cintas magnéticas
- Documentos en papel
- Impresoras y dispositivos multifunción con almacenamiento integrado

Declaración de Política:

[Nombre de la Organización] se compromete a proteger la FCI durante todo su ciclo de vida, incluyendo la eliminación y reutilización segura de los medios de almacenamiento. Todos los medios que contengan FCI deben ser saneados o destruidos antes de su eliminación o reutilización para evitar su divulgación no autorizada.

Manejo y Almacenamiento de Medios:

1. **Almacenamiento:** Los medios que contengan FCI deben guardarse en ubicaciones seguras, con controles de acceso físico adecuados (por ejemplo, gabinetes con llave o salas seguras).
2. **Etiquetado:** Los medios que contengan FCI deben estar claramente etiquetados para indicar su nivel de sensibilidad.
3. **Transporte:** Durante el transporte de medios con FCI, deben tomarse medidas de seguridad para evitar pérdidas o robos (por ejemplo, el uso de mensajeros seguros o cifrado de datos).

Saneamiento y Destrucción de Medios:

1. **Saneamiento:** El saneamiento consiste en eliminar datos de un medio de forma que no puedan ser recuperados mediante técnicas forenses. Métodos aceptables incluyen:
    - **Limpieza (Clearing):** Sobrescribir los datos con patrones aleatorios (ceros, unos, caracteres aleatorios). Adecuado para algunos medios magnéticos, pero no es efectivo para SSDs.
    - **Purgado (Purging):** Uso de software o hardware especializado para sobrescribir los datos varias veces con patrones complejos, haciendo los datos irrecuperables. Adecuado para la mayoría de los medios magnéticos y algunos SSDs.
    - **Desmagnetización (Degaussing):** Uso de un campo magnético fuerte para borrar datos en medios magnéticos, dejándolos inservibles.
    - **Borrado Criptográfico:** Eliminación de la clave de cifrado en discos auto-cifrados (SEDs), lo que hace que los datos sean inaccesibles de manera rápida y efectiva.
2. **Destrucción:** La destrucción física de los medios los deja completamente inutilizables. Métodos aceptables incluyen:
    - **Trituración:** Uso de una trituradora de corte cruzado para documentos en papel.
    - **Pulverización:** Reducción de medios a partículas pequeñas.
    - **Incineración:** Quema de medios hasta convertirlos en cenizas.
    - **Perforación o Aplastamiento:** Dañar físicamente los medios para inhabilitarlos.
3. **Procedimientos de Saneamiento y Destrucción:**
    - Todas las actividades de saneamiento y destrucción deben documentarse, incluyendo la fecha, método utilizado, persona responsable y número de serie del medio (si aplica).
    - Un individuo designado será responsable de supervisar el proceso de saneamiento y destrucción.
    - Si un medio no puede ser saneado o destruido internamente, se debe contratar a un proveedor certificado en destrucción de datos. Se debe obtener un Certificado de Destrucción para todos los medios eliminados por terceros.
4. **Métodos de Saneamiento para Tipos Específicos de Medios:**
    - **Documentos en papel:** Trituración con trituradora de corte cruzado, incineración o pulpeo.

- **Discos duros (HDDs):** Purgado con software especializado o desmagnetización. Destrucción física (trituración, perforación, pulverización) como método alternativo.
- **Unidades de estado sólido (SSDs):** Borrado criptográfico (si está soportado), purgando con software especializado para SSDs o destrucción física. La sobrescritura no es confiable para SSDs.
- **Discos ópticos (CDs, DVDs, Blu-rays):** Trituración o pulverización.
- **Dispositivos USB:** Purgado con software especializado o destrucción física.s

Reutilización de Medios:

Los medios saneados mediante métodos aprobados pueden reutilizarse dentro de la organización, donarse o venderse. Sin embargo, los medios que han sido destruidos físicamente no pueden reutilizarse.

Aplicación de la Política:

El incumplimiento de esta política puede dar lugar a medidas disciplinarias, incluyendo terminación del contrato laboral o de servicios.

Capacitación y Concienciación:

Todos los usuarios que manejen medios que contengan FCI recibirán capacitación sobre esta política, incluyendo procedimientos de manejo, saneamiento y destrucción.

Revisión y Actualización:

Esta política será revisada y actualizada al menos una vez al año o cuando sea necesario debido a cambios tecnológicos, amenazas o regulaciones.

Información de Contacto:

Para preguntas o inquietudes sobre esta política, comuníquese con [Persona de Contacto] a través de [Información de Contacto].

Nota: Esta es una política de protección de medios de ejemplo y debe adaptarse a las necesidades específicas de su organización. Se recomienda consultar con un profesional de ciberseguridad calificado para garantizar el cumplimiento de CMMC Nivel 1 y otras regulaciones aplicables.

4. Política de Protección Física (Ejemplo)

Propósito:

Esta política establece los requisitos para la protección física de los sistemas de información, equipos y entornos operativos de [Nombre de la Organización] que contienen Información de Contratos Federales (FCI). Está diseñada para cumplir con los requisitos de la Certificación de Modelo de Madurez en Ciberseguridad (CMMC) Nivel 1.

Alcance:

Esta política se aplica a todas las ubicaciones físicas donde se encuentren los sistemas de información, equipos y entornos operativos de [Nombre de la Organización], incluyendo, pero no limitado a:

- Centros de datos
- Salas de servidores
- Oficinas
- Áreas de almacenamiento

Declaración de Política:

[Nombre de la Organización] se compromete a proteger sus sistemas de información y FCI mediante la implementación de medidas de seguridad física adecuadas para prevenir accesos no autorizados, daños y alteraciones.

Requisitos de Protección Física:

1. **Limitar el Acceso Físico a Personal Autorizado:**
    - El acceso a áreas donde se ubiquen sistemas de información y equipos estará restringido solo a personal autorizado.
    - El acceso se otorgará en función de las responsabilidades laborales y el principio de mínimo privilegio.
    - Se implementarán mecanismos de control de acceso, como:
        - Sistemas de acceso con tarjetas.
        - Cerraduras con combinaciones.
        - Cerraduras tradicionales con llaves.
    - Todas las entradas y puntos de acceso (puertas, ventanas, etc.) estarán asegurados.
2. **Acompañamiento y Monitoreo de Visitantes:**
    - Todos los visitantes deben registrarse al llegar y salir, proporcionando su nombre, organización, propósito de la visita y el nombre del empleado que los recibe.

- Se otorgarán credenciales de visitante, las cuales deben estar visiblemente exhibidas en todo momento.
- Los visitantes serán acompañados por personal autorizado en todo momento mientras se encuentren en áreas con sistemas de información y equipos.
- Se mantendrán registros de visitantes y se conservarán por un período definido [Especificar tiempo, por ejemplo, un año].

3. **Mantener Registros de Acceso Físico:**
   - Se mantendrán registros de auditoría de accesos físicos en áreas protegidas por sistemas electrónicos de control de acceso (ejemplo: sistemas de tarjetas de acceso).
   - Estos registros deberán incluir la fecha, hora e identidad de la persona que accedió al área protegida.
   - Los registros serán revisados regularmente y se conservarán por un período definido [Especificar tiempo, por ejemplo, un año].
   - En áreas sin control de acceso electrónico, se mantendrán registros manuales siempre que sea factible y necesario, especialmente en áreas de alta seguridad.
4. **Control y Gestión de Dispositivos de Acceso Físico:**
   - **Llaves y Tarjetas de Acceso:**
     - Un individuo designado será responsable de gestionar las llaves y tarjetas de acceso.
     - Se mantendrá un registro de las llaves y tarjetas entregadas.
     - Cualquier pérdida o robo de llaves o tarjetas debe reportarse de inmediato y dichas credenciales deberán ser desactivadas.
   - **Cerraduras y Sistemas de Control de Acceso:**
     - Las cerraduras y sistemas de control de acceso serán inspeccionados y mantenidos regularmente.
     - Cualquier cambio en los códigos de acceso o permisos de tarjetas será documentado y autorizado.
   - **Inventario Físico:** Se realizarán inventarios físicos periódicos del equipo sensible y se documentarán.
5. **Controles Ambientales:**
   - Se mantendrán controles ambientales adecuados en áreas donde se ubiquen sistemas de información y equipos para prevenir daños por temperatura, humedad y otros factores ambientales.

6. **Protección contra Desastres Naturales y Otras Amenazas:**
    - Se tomarán medidas razonables para proteger los sistemas de información y equipos contra desastres naturales (por ejemplo, incendios, inundaciones, terremotos) y otras amenazas (por ejemplo, cortes de energía o vandalismo).

Aplicación de la Política:

El incumplimiento de esta política puede resultar en medidas disciplinarias, incluyendo la terminación del contrato laboral o de servicios.

Capacitación y Concienciación:

Todos los empleados recibirán capacitación sobre esta política y sus responsabilidades en el mantenimiento de la seguridad física.

Revisión y Actualización:

Esta política será revisada y actualizada al menos una vez al año o cuando sea necesario debido a cambios tecnológicos, amenazas o regulaciones.

Información de Contacto:

Para preguntas o inquietudes sobre esta política, comuníquese con [Persona de Contacto] a través de [Información de Contacto].

Nota: Esta es una política de protección física de ejemplo y deberá adaptarse a las necesidades específicas de su organización. Se recomienda consultar con un profesional de seguridad cualificado para asegurar el cumplimiento con el Nivel 1 de CMMC y otras regulaciones aplicables.

5. Política de Protección de Sistemas y Comunicaciones (Ejemplo)

Propósito:

Esta política establece los requisitos para la protección de los sistemas de información y las comunicaciones de [Nombre de la Organización], incluyendo la Información de Contratos Federales (FCI), tanto en los límites externos como internos. Está diseñada para cumplir con los requisitos de la Certificación de Modelo de Madurez en Ciberseguridad (CMMC) Nivel 1.

Alcance:

Esta política se aplica a todos los sistemas de información propiedad, administrados o utilizados por [Nombre de la Organización], incluyendo dispositivos de red, servidores, estaciones de trabajo, dispositivos móviles y canales de comunicación relacionados.

Declaración de Política:

[Nombre de la Organización] se compromete a proteger sus sistemas de información y comunicaciones contra accesos no autorizados, uso indebido, divulgación, interrupción, modificación o destrucción.

Requisitos de Protección de Sistemas y Comunicaciones:

1. **Monitorear, Controlar y Proteger las Comunicaciones Organizacionales:**
    - El tráfico de red será monitoreado en los límites externos y en puntos clave internos mediante firewalls, sistemas de detección y prevención de intrusiones (IDS/IPS) y otras herramientas de seguridad.
    - Se implementarán reglas de firewall para controlar el tráfico de red entrante y saliente, basadas en puertos, protocolos y direcciones IP aprobadas.
    - Se utilizarán Listas de Control de Acceso (ACLs) para restringir el acceso entre segmentos de la red interna.
    - Se mantendrán registros de tráfico de red, los cuales serán revisados regularmente.
2. **Implementar Subredes para Comonentes de Sistemas de Acceso Público:**
    - Los componentes de sistemas de acceso público (por ejemplo, servidores web, servidores de correo electrónico) serán ubicados en una Zona Desmilitarizada (DMZ), una subred física o lógicamente separada de la red interna.
    - La comunicación entre la DMZ y la red interna será estrictamente controlada mediante reglas de firewall.
    - Se prohibirán las conexiones directas desde Internet a la red interna.

3. **Identificar, Reportar y Corregir Vulnerabilidades de los Sistemas de Información:**

- Se implementará un proceso de gestión de vulnerabilidades para identificar, reportar y corregir fallas en los sistemas de información de manera oportuna.
- Se realizarán escaneos de vulnerabilidades periódicos en todos los sistemas de información.
- Se aplicarán parches de seguridad y actualizaciones inmediatamente después de su lanzamiento por parte del proveedor.
- Se establecerá un proceso para reportar y rastrear incidentes de seguridad.

4. **Protección contra Código Malicioso:**
    - Se instalará software antivirus y antimalware en todas las estaciones de trabajo, servidores y dispositivos móviles.
    - Se implementará filtrado de correos electrónicos y filtrado web para bloquear correos electrónicos y sitios web maliciosos.
    - Se utilizará software de monitoreo de integridad de archivos para detectar cambios no autorizados en archivos críticos del sistema.
5. **Actualización de Mecanismos de Protección contra Código Malicioso:**
    - Las definiciones y motores de antivirus y antimalware se actualizarán automáticamente y de forma regular (por ejemplo, diariamente).
    - Los sistemas operativos y aplicaciones recibirán parches de seguridad de manera oportuna para mitigar vulnerabilidades conocidas.
6. **Realización de Escaneos Periódicos y en Tiempo Real:**
    - Se realizarán escaneos completos del sistema periódicamente en todas las estaciones de trabajo y servidores [Especificar frecuencia, por ejemplo, semanalmente].
    - Se habilitará escaneo en tiempo real de archivos provenientes de fuentes externas (descargas, adjuntos de correos electrónicos, dispositivos USB) para detectar código malicioso al acceder a los archivos.
7. **Protección de Redes Inalámbricas:**
    - Las redes inalámbricas deberán utilizar protocolos de cifrado robustos (por ejemplo, WPA2/3-Enterprise) y métodos de autenticación segura.
    - Las redes Wi-Fi para invitados estarán aisladas de la red interna.

Aplicación de la Política:

El incumplimiento de esta política puede resultar en acciones disciplinarias, incluyendo la terminación del contrato laboral o de servicios.

Capacitación y Concienciación:

Todos los usuarios recibirán capacitación sobre esta política y sus responsabilidades en la protección de los sistemas de información y comunicaciones.
La capacitación incluirá temas sobre identificación y reporte de correos de phishing, sitios web maliciosos y otras amenazas de seguridad.

Revisión y Actualización:

Esta política será revisada y actualizada al menos una vez al año o cuando sea necesario debido a cambios tecnológicos, amenazas o regulaciones.

Información de Contacto:

Para preguntas o inquietudes sobre esta política, comuníquese con [Persona de Contacto] a través de [Información de Contacto].

Nota: Esta es una política de protección de sistemas y comunicaciones de ejemplo y deberá adaptarse a las necesidades específicas de su organización. Se recomienda consultar con un profesional de ciberseguridad calificado para garantizar el cumplimiento de CMMC Nivel 1 y otras regulaciones aplicables.

6. Política de Seguridad de la Información para Negocios Basados en el Hogar (Ejemplo)

Declaración de Política:

Esta política establece los requisitos de seguridad para la protección de la Información de Contratos Federales (FCI) dentro de mi negocio basado en el hogar. Cubre control de acceso, identificación y autenticación, protección de medios, protección física y protección de sistemas y comunicaciones, alineándose con los requisitos de CMMC Nivel 1.

1. Política de Control de Acceso:

- Principio de Mínimo Privilegio: El acceso a los sistemas y datos que contienen FCI se concederá únicamente a personas autorizadas y solo en la medida necesaria para cumplir con sus funciones.
- Cuentas de Usuario: Cada usuario autorizado tendrá una cuenta de usuario única con una contraseña segura y compleja. No se permiten cuentas genéricas o compartidas.
- Revisión de Accesos: Los privilegios de acceso se revisarán periódicamente (al menos una vez al año) o tras la finalización de un contrato/proyecto para garantizar que sigan siendo apropiados.
- Acceso Remoto: El acceso remoto a sistemas con FCI estará protegido con métodos de autenticación robustos (ejemplo: autenticación multifactor (MFA) cuando sea posible, contraseñas seguras).

2. Política de Identificación y Autenticación:

- **Identificación de Usuario:** Cada usuario autorizado será identificado de manera única mediante un nombre de usuario u otro identificador único.
- **Requisitos de Contraseña:**
  - Debe tener al menos 12 caracteres.
  - Debe contener una combinación de letras mayúsculas, minúsculas, números y símbolos.
  - No debe basarse en información personal (ejemplo: nombre, fecha de nacimiento).
  - Debe cambiarse al menos cada 90 días.
- **Gestión de Contraseñas:** Las contraseñas no deben escribirse ni almacenarse en texto plano (se recomienda usar un gestor de contraseñas).

- **Autenticación Multifactor (MFA):** Siempre que sea posible (ejemplo: correo electrónico, almacenamiento en la nube), se habilitará MFA para proporcionar una capa adicional de seguridad.

3. Política de Protección de Medios:

- **Manejo de Medios:** Los medios que contengan FCI (ejemplo: dispositivos USB, discos duros externos, documentos impresos) deben almacenarse y protegerse físicamente cuando no estén en uso.
- **Almacenamiento de Medios:** Los medios físicos deben guardarse en un cajón o gabinete con llave cuando no estén en uso.
- **Eliminación de Medios:** Cuando los medios ya no sean necesarios, deben ser destruidos de forma segura. Los medios digitales deben ser eliminados con software especializado o destruidos físicamente. Los documentos impresos deben triturarse.
- **Medios Electrónicos:** Toda la información almacenada en medios electrónicos debe estar cifrada en reposo.

4. Política de Protección Física:

- **Seguridad en el área de trabajo:** La oficina o área de trabajo donde se procesa y almacena FCI debe permanecer asegurada para prevenir accesos no autorizados. Esto incluye cerrando las puertas con llave cuando el área quede desatendida.
- **Acceso de Visitantes:** Los visitantes serán supervisados para evitar accesos no autorizados a FCI o a los sistemas que la manejan.
- **Seguridad de los Dispositivos:** Las laptop y otros dispositivos que contengan FCI deben asegurarse físicamente cuando no estén en uso para prevenir robos.

5. Política de Protección de Sistemas y Comunicaciones:

- **Antivirus/Antimalware:** Se instalará y mantendrá actualizado el software antivirus y antimalware en todos los sistemas que manejen FCI. Se realizarán escaneos regulares del sistema.
- **Protección con Firewall:** Se habilitará un firewall en la red doméstica y en los dispositivos individuales para evitar accesos no autorizados.
- **Actualización de Software:** Los sistemas operativos y aplicaciones se mantendrán actualizados con los últimos parches de seguridad. Siempre que sea posible, se habilitarán las actualizaciones automáticas.
- **Seguridad del Correo Electrónico:** Se debe tener precaución al abrir archivos adjuntos o hacer clic en enlaces de remitentes desconocidos.

- **Seguridad de la Red Inalámbrica:** La red Wi-Fi doméstica deberá estar protegida con una contraseña segura y usar cifrado WPA2 o WPA3. Se debe cambiar la contraseña predeterminada del router.
- **Copia de Seguridad de Datos:** Se realizarán copias de seguridad regulares de los datos que contengan FCI y se almacenarán de forma segura, preferiblemente en un servicio de copia de seguridad en la nube cifrada o en un dispositivo de almacenamiento seguro y separado. Los medios de respaldo serán protegidos según la política de protección de medios.

Aplicación de la Política:

Esta política se aplica a todas las personas que acceden o manejan FCI dentro de mi negocio basado en el hogar. El incumplimiento de esta política puede dar lugar a acciones disciplinarias según corresponda.

Revisión de la Política:

Esta política será revisada y actualizada al menos una vez al año o cuando sea necesario para reflejar cambios en las operaciones del negocio, tecnología o regulaciones aplicables.

Importante:

Esta política proporciona una base inicial para la seguridad en un negocio basado en el hogar. Es fundamental revisarla y adaptarla a sus circunstancias específicas y mantenerse actualizado con las últimas directrices de CMMC.

Nota: Esta es una política genérica de ejemplo para negocios basados en el hogar. Debe adaptarse a las necesidades específicas de su organización. Se recomienda consultar con un profesional de ciberseguridad para garantizar el cumplimiento de CMMC Nivel 1 y otras regulaciones aplicables.

XI. Referencias Claves

Cláusula DFARS 252.204-7012

Cláusula DFARS 252.204-7021

Cláusula FAR 52.204-21 b.1.xv

Guía de Alcance del CMMC Nivel 1

Guía de Evaluación del CMMC Nivel 1(v2)

Página Web Oficial del DoD

Project Spectrum

Sistema de Riesgo de Desempeño de Proveedores (SPRS)

XII. Apéndice A – Acrónimos y Abreviaciones

Nota: Las siguientes siglas provienen del inglés y, en muchos casos, no tienen una traducción directa al español. Sin embargo, se proporciona una descripción en español para facilitar su comprensión.

C3PAO	Organización Certificada de Evaluación de Terceros
CMMC	Certificación del Modelo de Madurez en Ciberseguridad
CUI	Información No Clasificada Controlada
DFARS	Suplemento a la Regulación Federal de Adquisiciones de Defensa
DIBCAC	Defense Industrial Base Cybersecurity Assessment Center
DMZ	Zona Desmilitarizada
DoD	Departmentamento de Defensa
ESP	Proveedor de Servicios Externos
FAR	Regulación Federal de Adquisiciones
FCI	Información de Contratos Federales
FeCC	Centro de Contratación Federal de Puerto Rico
IP	Protocolo de Internet
NIST	Instituto Nacional de Estándares y Tecnología
SPRS	Sistema de Riesgo de Desempeño de Proveedores
TI	Tecnología de la Información
WPA	Dirección Protegida de Wi-Fi

This APEX Accelerator is funded in part through a cooperative agreement with the Department of Defense.