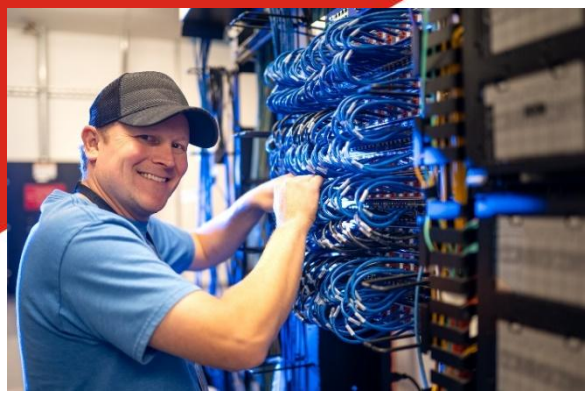
DOC2133

W. L. GORE & ASSOCIATES

POLÍTICA DE USO ACEPTABLE

Para Gore Partners



Introducción

Los activos de Gore nos permiten hacer negocios tanto con nuestros clientes y partners como entre nosotros. En Gore, creemos que los Asociados y partners actúan de manera responsable y prestan debida atención a la protección de nuestros activos en sus actividades de negocio. Esta Política de uso aceptable y la determinación de cumplir con sus requisitos resultan esenciales para nuestro éxito como empresa.

Objetivo

El objetivo de esta Política de Uso Aceptable ("Política") es establecer las responsabilidades de los Gore Partners que acceden o utilizan los activos de W. L. Gore & Associates ("Gore" o "la Empresa"). A presente Política se ha establecido para proteger los Recursos de Información de Gore y orientar a los Gore Partners en el uso apropiado de dichos recursos.

La presente Política anula y reemplaza la Política de uso aceptable anterior. Los Gore Parners firmarán esta Política para reconocer que han leído, comprendido y aceptado cumplir el contenido expuesto en este documento.

Ámbito de aplicación

Esta Política se aplica a todos los Gore Partners que utilicen los activos de Gore.

Todo uso de los Recursos de Información de Gore o acceso a información de Gore, ya sea en hardware emitido por la Empresa, en un dispositivo gestionado de propiedad personal o en un dispositivo no gestionado de propiedad personal (sujeto a aprobación) está sujeto a esta política.

La exclusión de esta Política no constituye necesariamente un permiso. Si tiene alguna pregunta sobre un área no cubierta por esta Política o sobre un posible conflicto, póngase en contacto con su Guía Gore o con ITAC.

Definiciones

A continuación se incluyen las definiciones relativas a esta política. Consulte el Glosario de informática de Gore para obtener definiciones adicionales.

Herramientas de IA: aplicaciones de software que se sirven de la inteligencia artificial para realizar tareas específicas y resolver problemas. En esta categoría se incluyen:

- Las *herramientas de aprendizaje automático (AA)*, que analizan los datos para identificar patrones y realizar predicciones, lo que ayuda a Gore en tareas como la previsión de la demanda, la segmentación de clientes y la detección de fraudes.
- Las *herramientas de procesamiento de lenguaje natural (PLN)*, que procesan y analizan el lenguaje humano y posibilitan el funcionamiento de los chatbots, el análisis de sentimiento y la automatización del servicio de atención al cliente.
- Las *herramientas de visión informática*, que permiten que los ordenadores interpreten los datos visuales y tomen decisiones basándose en ellos. Resultan útiles en ámbitos como el control de calidad, el reconocimiento facial y la inspección automatizada.
- Las *herramientas de automatización robótica de procesos (RPA, por sus siglas en inglés)*, que automatizan las tareas repetitivas como el registro de datos y el procesamiento de facturas.

- Las *herramientas de análisis predictivo*, que se basan en algoritmos estadísticos y técnicas de aprendizaje automático para predecir los resultados en función de los datos históricos disponibles, lo que ayuda en la toma de decisiones.
- La *IA generativa, como los grandes modelos de lenguaje (LLM, por sus siglas en inglés)*, que genera texto, imágenes o código basándose en los datos introducidos. Se puede emplear en la creación de contenido, las tareas de marketing y mucho más.
- Las aplicaciones con *generación aumentada de recuperación (RAG, por sus siglas en inglés)*, que generan contenido con datos personales que no provienen del modelo de IA en sí, sino de la información que introducen los Asociados, o bien de otras fuentes de datos.
- Los *sistemas de gestión de traducciones (TMS, por sus siglas en inglés)*, que se sirven de algunas características de la automatización y pueden incluir elementos de IA para mejorar el proceso de traducción, como la consulta de traducciones anteriores y la incorporación de nuevos contenidos en la maquetación del documento.

Activos: hardware o software (propios de Gore o que este gestiona), u otros componentes del entorno de Gore que respaldan las operaciones de la empresa y que Gore posee, utiliza u opera, o bien para los que emite licencias.

- *Hardware*, en el que se incluyen ordenadores, portátiles, tabletas, discos duros, equipamiento de red, memorias USB y otros dispositivos de almacenamiento, estaciones de trabajo, teléfonos, dispositivos móviles, herramientas para videoconferencias, impresoras, escáneres o cualquier otra tecnología tangible que se utiliza en las operaciones empresariales.
- *Software*, en el que se incluyen sistemas operativos, software de red, aplicaciones de mensajería, proveedores de correo electrónico, aplicaciones de mensajería de voz, herramientas colaborativas, procesadores de texto, hojas de cálculo y otras aplicaciones de datos, bases de datos, aplicaciones web o cualquier otro programa, aplicación o plataforma de software.

Contenido: datos, información o registros que poseen cierto valor para la empresa en función de sus necesidades operativas, legales o regulatorias.

Datos: contenido que constituye una representación simbólica de algo y cuyo significado depende en parte de sus metadatos. Los datos son un conjunto de hechos, como números, palabras, medidas, observaciones o descripciones de cosas.

Delegado de protección de datos: el Reglamento general de protección de datos (RGPD) ha establecido el concepto de delegado de protección de datos (DPD) en Europa. La función de un DPD consiste en garantizar el cumplimiento de todas las leyes de protección de datos aplicables al supervisar procesos específicos y colaborar con las autoridades correspondientes.

Cuenta de correo electrónico de Gore: una cuenta de usuario (incluido el software, el hardware y el almacenamiento) asociada a un dominio que le permite enviar y recibir correos electrónicos.

Información: contenido con valor para la empresa a corto plazo. La información son datos en contexto.

Acceso a internet: todos los recursos que posibilitan la comunicación digital, especialmente la recuperación de datos de internet, incluidos el hardware y el software relacionados.

Intranet: todos los recursos que proporciona Gore para la comunicación digital en la red **interna** de Gore, así como el hardware y el software relacionados.

Registros: contenido que refleja las acciones, decisiones y transacciones de la empresa. Los registros son conjuntos de información completa y definitiva en cualquier formato (físico o digital) que deben conservarse durante períodos de tiempo especificados en función de los requisitos legales, normativos u operativos.

Dispositivos gestionados: dispositivos móviles personales que se utilizan para acceder al contenido de Gore o a su red, y que cuentan con el software de gestión de dispositivos de Gore y lo tienen activado.

- Consulte las directrices sobre el uso de dispositivos móviles

Partners: contratistas, terceros, etc.

Uso de los activos de Gore

La actividad empresarial de Gore debe llevarse a cabo mediante aplicaciones o dispositivos gestionados autorizados. De lo contrario, surge el riesgo de que el contenido de Gore no se preserve correctamente ni cuente con la protección necesaria.

Es responsabilidad de cada Gore Partner de mantener seguro el contenido de Gore y no permitir el acceso a ningún activo a menos que sea un Asociado o Partner autorizado.

Acceso

Los Gore Partners sólo deben utilizar aquellos activos a los que se les haya concedido acceso.

Los Gore Partners tomarán las siguientes medidas cuando accedan o concedan acceso a los activos de Gore:

- Los Gore Partners deben acceder o conceder acceso a los activos de Gore siguiendo el principio de "necesidad de conocer".
- Los Gore de Partners deben conceder acceso a los activos de Gore sólo durante el tiempo que sea necesario y revocar el acceso cuando se hayan cumplido los requisitos empresariales o haya un cambio en el compromiso.
- Cuando sea necesario, los Gore Parners deberán solicitar el acceso a través de los canales adecuados (propietario de la aplicación, seguridad de la información, etc.).
- El acceso remoto a la red de Gore se permite únicamente a través de métodos y dispositivos autorizados.

Gestión

Los Gore Partners deben gestionar los activos de Gore de forma segura mediante el cumplimiento de las directrices proporcionadas en la Política de Clasificación de Seguridad y la Política de Gestión de Registros e Información.

Usos prohibidos

Los Gore Partners no deben:

- Hacer uso ilegal o malintencionado de los activos de Gore, especialmente si puede dañar su reputación, conllevar acciones legales o perjudicar a la empresa.
- Acceder a materiales que puedan considerarse obscenos, racistas, sexistas, peligrosos, ofensivos, discriminatorios o abusivos, ni tampoco descargarlos, exhibirlos ni difundirlos.
- Utilizar lenguaje o contenido de carácter amenazador, acosador o abusivo.
- Exhibir contenido que podría considerarse inapropiado en el entorno laboral.
- Tratar de soslayar los mecanismos de seguridad establecidos por el Equipo de seguridad de la información o el Equipo de seguridad física de Gore.
- Utilizar las credenciales de inicio de sesión de otro Asociado o partner.
- Conectarse a la red de Gore a través de un dispositivo personal no gestionado.
- Configurar una red inalámbrica no autorizada en las instalaciones de Gore, conectarla a la red de la empresa ni acceder a una red de este tipo desde las instalaciones de Gore.
- Instalar o modificar los activos existentes ni realizar de forma intencionada acciones que provoquen averías o fallos en los activos de Gore o los pongan en peligro.
- Manipular o desactivar el software antivirus de Gore o las funciones de cifrado.
- Instalar software personal o inhabitual en un activo de Gore (excepto las aplicaciones personales en smartphones o tabletas).

- Almacenar datos o información de Gore en un dispositivo de propiedad personal (ordenador, teléfono, almacenamiento en la nube, etc.) a menos que el dispositivo disponga de software de Gore para gestionar la información que se almacena en dicho dispositivo (consulte los Términos y condiciones del programa de uso de dispositivos propios) o en una nube o red que no haya sido evaluada por Gore Information Security.

Supervisión

A menos que lo prohíba la ley, Gore se reserva el derecho de consultar, interceptar, bloquear, registrar la actividad o investigar («supervisar») de otra forma el uso de los activos de Gore por parte de Asociados o partners para garantizar el cumplimiento de las políticas y normas de Gore. Estas medidas pueden tomarse sin previo aviso.

Gore tomará todas las medidas posibles para cumplir con la legislación específica de cada país en el proceso de supervisión y garantizar que los datos personales se utilicen únicamente con fines establecidos.

Siempre que sea posible, la supervisión se realizará de forma automatizada. Durante el proceso de supervisión se recogerán algunos datos. Los tipos de información que podrían recopilarse, en ciertas circunstancias y con fines específicos, se pueden consultar en el Anexo B adjunto.

Si no constituye una vulneración de la legislación local aplicable, Gore puede supervisar el uso de algunos tipos de información confidencial (p. ej., exportación controlada, datos personales, tecnología confidencial de Gore, etc.) para cumplir las normativas, o bien para proteger la reputación de la marca Gore y la ventaja competitiva de la empresa.

Pueden aplicarse otros procedimientos regionales o normativas locales a este proceso de supervisión. El Anexo A incluye más información acerca de cómo se lleva a cabo el proceso de supervisión para los Asociados.

En la medida en que lo permita la legislación aplicable, Gore podrá intentar identificar a un Socio de Gore si tiene motivos para creer que está infringiendo esta Política u otras políticas relacionadas. Podrá, previa consulta con el Delegado de Protección de Datos correspondiente, llevar a cabo un seguimiento específico.

En el caso de que, a través del proceso de supervisión, Gore sospeche que se ha vulnerado la presente Política:

- Gore se reserva el derecho de eliminar el acceso de los Gore Partners a los activos de Gore. Cuando proceda, Gore también eliminará o bloqueará el acceso a cualquier información de la Empresa en dispositivos personales (consulte los Términos y condiciones del programa de uso de dispositivos propios).
- De conformidad a la legislación aplicable, Gore puede almacenar copias de cualquier contenido capturado a través de actividades de supervisión que reflejen el uso inapropiado de los activos de Gore por parte de un Socio de Gore. Gore también podrá revelar copias de dicho contenido o un dispositivo que contenga dicho contenido, según sea necesario en caso de litigio o investigación.

Dispositivos personales

Gore puede permitir que los Gore Partners utilicen dispositivos de propiedad personal, como teléfonos inteligentes o tabletas, para llevar a cabo actividades relacionadas con Gore. En esos casos:

- Los Gore Partners deben firmar un acuerdo de usuario a través del proceso de solicitud de ITAC y permitir que el departamento de informática de Gore instale el software de gestión de dispositivos móviles. El software de Gestión de Dispositivos Móviles permite al departamento de informática de Gore controlar el contenido y las aplicaciones de Gore en el dispositivo, o
- De forma limitada, se puede conceder acceso según el proceso de excepción que se describe a continuación.

Comunicación digital

El sistema de correo electrónico de Gore y otros servicios de mensajería, como Teams u otras herramientas de mensajería instantánea («IM», por sus siglas en inglés) que gestiona Gore, junto con toda la información que contienen, es propiedad expresa de Gore, a menos que una ley o normativa local establezca lo contrario. Las cuentas de correo electrónico y de mensajería instantánea deben utilizarse con fines comerciales. Es obligatorio garantizar la confidencialidad de la información sensible y los datos personales (normalmente, mediante el cifrado) en todas las comunicaciones digitales, de conformidad con nuestro Estándar de clasificación de seguridad.

Aplicaciones de mensajería

En Gore, reconocemos que a menudo resulta necesario comunicarse mediante aplicaciones de mensajería instantánea o comunicación a nivel tanto interno como externo. Recomendamos encarecidamente utilizar aplicaciones, plataformas o herramientas que proporciona y mantiene Gore en un dispositivo autorizado cuando sea posible.

Si resulta necesario comunicarse a través de aplicaciones de mensajería externas, como WhatsApp, no se debe compartir información confidencial o delicada, incluidos los datos personales y la propiedad intelectual.

La comunicación por estos medios debe tener un carácter logístico. No almacene registros comerciales de Gore en ninguna aplicación de mensajería tanto convencional como instantánea. Todos los registros comerciales, como las aprobaciones y la documentación de apoyo para las transacciones, deben preservarse de acuerdo con los procesos establecidos.

Grabación

Los Gore Partners puede utilizar herramientas (como Microsoft Teams u otro software) para grabar o transcribir reuniones e interacciones. Los Gore Partners deben informar a los participantes sobre la grabación o transcripción antes del comienzo de la reunión, preferiblemente en la invitación a la reunión, y permitir que los participantes opten por abstenerse de participar si así lo desean. Si una herramienta de grabación no muestra un indicador claro a lo largo de la reunión, el organizador debe notificar a los participantes que se incorporen con retraso que la reunión se está grabando. En las reuniones híbridas y con grabación automática, el anfitrión deberá informar a todos los participantes de la grabación en la invitación a la reunión o en el chat. Las grabaciones deben interrumpirse durante las pausas o las conversaciones de carácter personal. Las reuniones en las que se mencione información personal sensible o temas de este tipo no deben grabarse. Algunos ejemplos son: datos de pacientes, discusiones sobre contribuciones o compensaciones, tecnología Gore confidencial, etc.

Herramientas de IA de Gore

Animamos a los Gore Partners a utilizar las herramientas de IA de Gore **proporcionadas por Gore** para mejorar la productividad, agilizar los flujos de trabajo y apoyar los procesos de toma de decisiones. A la hora de introducir datos personales o comerciales en las herramientas de IA de Gore, los Gore Partners deben asegurarse de que los datos son precisos, pertinentes y cumplen los protocolos de seguridad y privacidad de datos. Los Gore Partners no deben cargar ni compartir datos en herramientas de IA no proporcionadas por Gore que sean confidenciales, sensibles, de propiedad o protegidos por normativas, a menos que lo autorice explícitamente el líder y lo evalúe el Departamento de Seguridad de la Información. Además, los Gore Partners deben tener en cuenta que los resultados generados por la IA a veces pueden ser engañosos o incorrectos. Por lo tanto, es esencial verificar la exactitud y fiabilidad de los resultados de la IA antes de tomar decisiones o emprender acciones basadas en ellos. Los Gore Partners son responsables de los resultados generados por las herramientas de IA y deben estar preparados para explicar y justificar dichos resultados. El uso indebido de las herramientas de IA, como la generación de información engañosa, la violación de los derechos de propiedad intelectual o la automatización de tareas sin la debida supervisión, está estrictamente prohibido y puede dar lugar a medidas disciplinarias, incluido el despido.

Cumplimiento y presentación de informes

- Los Gore Partners deberán completar toda la formación asociada a esta Política, incluida la formación obligatoria

sobre Privacidad y Seguridad de la Información.

- Los Gore Partners que tengan conocimiento de cualquier incidente de seguridad real o presunto, o del uso o acceso no autorizado a los activos de Gore, deberán notificarlo inmediatamente a ITAC.
- La vulneración de la presente Política puede conllevar medidas disciplinarias que incluirían, si resultase necesario, el despido o acciones legales.

Anexo A: Versiones regionales

Sección 1	Supervisión de información en Italia	Establece disposiciones adicionales que conciernen a los Asociados de Italia.

Sección 1 - Información sobre el seguimiento en Italia

Gore lleva a cabo las actividades de supervisión descritas en la Política acatando los límites y las modalidades que establece la legislación sobre empleo y privacidad de Italia.

En primer lugar, de conformidad con el Artículo 4, párr. 1, de la Ley del 20 de mayo de 1970, n.º 300, Gore no lleva a cabo estas actividades con el objetivo de supervisar la actividad de los Asociados en el trabajo, excepto en lo que concierne al cumplimiento de la legislación en materia de protección de datos de Italia.

Sin embargo, Gore ha instalado algunas herramientas de seguridad que pueden conllevar la posibilidad indirecta de supervisión remota de la actividad de los Asociados.
Dicha instalación es necesaria para salvaguardar adecuadamente la organización y los activos de Gore. Como se ha indicado anteriormente, identifica y aborda la seguridad, la fuga de datos sensibles, la detección de fraudes, el cumplimiento de la legislación aplicable y el uso indebido, que crean riesgos para la organización y los activos de Gore.

Siempre que sea posible, la supervisión se realiza de forma automatizada y/o aleatoria. No obstante, Gore puede intentar identificar a un partner de Gore si tiene motivos para creer que ha cometido una conducta indebida y que dicha conducta indebida puede poner en peligro la organización, la seguridad o los activos de Gore.

Anexo B: Tipos de Información, Circunstancias y Propósitos para el Monitoreo de la Actividad de los Gore Partners en los Activos Gore.

Sección 1: La información que puede recopilarse y registrarse en el proceso de supervisión.

Actividad de red, incluidos:

- Fecha/hora
- ID de usuario, ID de dispositivo, ID de estación de trabajo, dirección IP y otros identificadores únicos
- Rutas físicas y lógicas de datos, incluidos el origen y el destino
- Volumen de los datos
- Acciones
- Palabras clave (p. ej., «confidencial», «solo para uso interno», etc.)

Actividad en internet, incluidos:

- Fecha/hora
- ID de usuario

- Dirección IP de origen
- Dirección de destino (si se permite)
- Volumen de datos transferidos

Correos electrónicos que se reciben y se envían

- Fecha/hora
- Direcciones del remitente y del destinatario
- ID de mensaje
- Tamaño de mensaje
- Asunto
- Palabras clave en los datos (p. ej., «confidencial», «solo para uso interno», etc.)
- Solo para los correos electrónicos que activan «contenido marcado»: el cuerpo del correo electrónico y los adjuntos.

Las herramientas de prevención de pérdida de datos buscan palabras clave (como "ID de paciente") y patrones en los datos para detectar posibles fugas de datos sensibles (como datos de clientes, pacientes sanitarios o datos sensibles de Gore). Estas herramientas supervisan tanto los correos electrónicos que se envían como el tráfico de salida de los portátiles, los ordenadores de sobremesa y el uso de la nube (tráfico en la web, nube, USB/CD/DVD, impresoras y unidades de red) y marcan los elementos especificados.

Los datos procesados (que pueden incluir identificadores únicos de usuario, dispositivo o ubicación) se emplean únicamente con los siguientes fines:

- Análisis y corrección de errores técnicos.
- Seguridad del sistema, incluido el mantenimiento de listas de páginas web bloqueadas («Lista de bloqueados»).
- Optimización y control del acceso a la red.
- Control de la protección de datos.

Sección 2: Ejemplos concretos de supervisión y sus propósitos.

- Protección de los activos de información de Gore frente a la divulgación, la eliminación o la alteración no autorizadas.
- Colaboración en las investigaciones y la aplicación de requisitos legales y políticas de Gore.
- Protección de los sistemas frente a virus, troyanos y otros tipos de malware.
- Protección de los sistemas y las redes frente al acceso y la manipulación no autorizados.
- Protección de los derechos legales y la seguridad tanto de Gore como de los demás.
- Cumplimiento con los requisitos de la legislación, las normativas y las órdenes judiciales, o bien con las solicitudes o los requisitos de las autoridades correspondientes o fuerzas de seguridad.