PROCEDIMIENTO DEL GRUPO

GLENCORE

# Procedimiento de servicios de TI para usuarios finales

# Procedimiento de servicios de TI para usuarios finales

## Contenido

# 1 Propósito

De acuerdo con nuestra Política de gobernanza de la información y el Marco para la seguridad de la información de Glencore, este Procedimiento de servicios de TI para usuarios finales (el Procedimiento) establece las expectativas de seguridad cuando se accede a los Servicios de tecnología de la información (TI) de la empresa y a la Información de la empresa, y abarca:

- el tratamiento seguro de la Información de la empresa, ya sea electrónica o física;
- el uso aceptable e inaceptable de los Servicios de TI de la empresa; y
- los requisitos para supervisar los Servicios de TI de la empresa.

La información de Glencore (Información de la empresa) es fundamental para nuestro éxito, y nuestro enfoque de seguridad se basa en tres principios sencillos:

- La Información de la empresa debe estar protegida;
- La seguridad de la información debe ser adecuada a los riesgos; y
- Esperamos que nuestro personal utilice los Servicios de TI de la empresa con responsabilidad.

# 2 Ámbito

Este Procedimiento se aplica a todos los empleados, directores y gerentes, así como a los contratistas bajo la supervisión directa de Glencore, que trabajan para una oficina o un activo industrial de Glencore directa o indirectamente controlado u operado por Glencore Plc en cualquier lugar del mundo, con acceso a los Servicios de TI de la empresa o a la Información de la empresa (Usuarios finales).

Hacemos valer nuestra influencia sobre las empresas conjuntas que no controlamos para incentivarlas a actuar de forma coherente con la intención de este Procedimiento.

# 3 Términos clave

**Información de la empresa:** cualquier información que Glencore cree, recopile o reciba, incluidos los conjuntos de datos que abarcan las actividades comerciales, financieras, mineras y técnicas, pero excluida la Información privada. La Información de la empresa puede tener distintos niveles de sensibilidad e importancia para la empresa.

**Equipo de TI de la empresa:** equipo de TI proporcionado y mantenido por Glencore, que puede incluir computadoras, servidores, dispositivos de mano y periféricos como teclados, ratones y unidades de almacenamiento.

**Servicios de TI de la empresa:** una serie de servicios de TI prestados por Glencore, que incluyen sistemas/aplicaciones empresariales, correo electrónico, Internet, servicios en la nube aprobados y Equipos de TI de la empresa.

**Propietario del servicio de TI:** el custodio de un Servicio de TI de la empresa específico, que a menudo participa en los derechos de acceso o en las decisiones de seguridad relacionados con el Servicio de TI de la empresa.

**Equipo de TI ajeno a la empresa:** cualquier equipo de TI que no sea Equipo de TI de la empresa (es decir, privado o de terceros), de modo que no es gestionado por Glencore.

**Datos personales:** cualquier información relacionada directa o indirectamente con empleados, contratistas, socios comerciales y otras partes interesadas de Glencore identificados o identificables, en particular relativa a identificadores como nombres, números de teléfono, direcciones de correo electrónico y datos de localización. La Información privada y la Información de la empresa pueden contener Datos personales.

**Información privada:** datos o comunicaciones no laborales de los Usuarios finales que pueden ser personalmente sensibles (por ejemplo, fotos familiares, extractos bancarios, comunicaciones privadas) y que no son Información de la empresa.

**Uso privado:** uso de Equipos de TI de la empresa y de Servicios de TI de la empresa para fines no laborales (por ejemplo, reservas de vuelos en vacaciones, compras personales, operaciones bancarias personales).

# 4 Requisitos

En las siguientes secciones se detallan los requisitos de seguridad para el uso correcto de los Servicios de TI de la empresa, los Equipos de TI de la empresa y la Información de la empresa.

## 4.1 Acceso a la Información de la empresa

### 4.1.1 Autorización de acceso a los Servicios de TI de la empresa

Concedemos derechos de acceso a los Servicios de TI de la empresa principalmente según las funciones definidas. Si necesita derechos de acceso adicionales (por ejemplo, para obtener un privilegio mayor o para el uso de *software* adicional), debe obtener la autorización formal de un director apropiado o, cuando sea pertinente, del Propietario del servicio de TI. Debe presentar las solicitudes de acceso a través de su Servicio de soporte técnico local para que pueda hacerse un seguimiento de las aprobaciones y finalizaciones.

### 4.1.2 Acceso a los Servicios de TI de la empresa

Para obtener acceso a los Servicios de TI de la empresa necesitará su identificación de usuario y la contraseña asociada. En algunos casos, es posible que se le conceda el acceso automáticamente (por ejemplo, inicio de sesión único (SSO)). Los sistemas más sensibles y el acceso remoto pueden requerir métodos de autenticación adicionales (por ejemplo, tokens, certificados digitales, aplicaciones de autenticación de mano, tokens SMS). Debe asegurarse de que su identificación de usuario sea de su propiedad y de no compartir sus métodos de autenticación con otras personas [1].

- Gestión de contraseñas

  Debe mantener contraseñas fuertes y secretas para proteger los Servicios de TI de la empresa. Asegúrese de que las contraseñas:

  - Se cambien de inmediato con el primer uso, para que sean secretas y propias.
  - En el caso de computadoras y aplicaciones, tengan una longitud mínima de ocho caracteres, con una mezcla de letras mayúsculas y minúsculas, números y/o caracteres especiales.
  - En el caso de dispositivos de mano, tengan una longitud mínima de seis caracteres y utilicen caracteres/números no secuenciales y no adivinables.
  - Se elaboren con una buena estrategia (por ejemplo, que usted pueda recordarlas pero que no sean obvias ni fáciles de adivinar[2]).

  Además, para proteger su cuenta de forma continua, asegúrese de que sus contraseñas:

[1] En casos especiales, puede obtener autorización para cuentas compartidas (por ejemplo, sistemas industriales), pero estas deben tener un solo propietario de la empresa identificado. Las contraseñas de las cuentas compartidas deben mantenerse en secreto dentro de su grupo cerrado.
[2] Véase: la Guía de contraseñas seguras.

- Nunca se guarden en lugares obvios (por ejemplo, una nota adhesiva en su pantalla), ni se almacenen en archivos electrónicos a menos que sea de forma segura y cifrada (por ejemplo, una aplicación de gestión de contraseñas proporcionada por Glencore).
- Se introduzcan de forma segura para garantizar que no se revelen a otras personas (por ejemplo, si alguien mira por encima del hombro).
- Nunca se vuelvan a usar en servicios de TI no conectados (no SSO), y especialmente en los sistemas más sensibles de la empresa (por ejemplo, los sistemas de RR. HH.), o en las cuentas privadas de Internet.
- Se cambien con regularidad, idealmente todos los años, o de inmediato si sospecha o le notifican que su contraseña se dio a conocer.

Nota: Algunas o todas las reglas anteriores pueden ser aplicadas automáticamente por los Servicios de TI de la empresa.

### 4.1.3 Acceso físico a las instalaciones e información de Glencore

Para evitar el acceso físico no autorizado a las instalaciones de Glencore, usted debe:

- Asegurarse de que sus visitantes/consultores estén acompañados y lleven distintivos de visitante siempre que sea posible.
- Denunciar a cualquier persona que se encuentre en las instalaciones de Glencore y que parezca no estar autorizada o actúe de forma sospechosa.

Para protegerse del acceso físico inapropiado a la Información de la empresa, usted debe:

- Bloquear siempre su dispositivo de TI (por ejemplo, su computadora o dispositivo de mano) cuando se aleje, aunque solo sea por un momento.
- Guardar los documentos confidenciales (por ejemplo, información sobre transacciones comerciales, registros personales) de forma segura, en cajones o armarios con cerradura, cuando se aleje de su escritorio durante períodos prolongados.
- Asegurar cualquier activo de TI portátil valioso (por ejemplo, portátiles, dispositivos de mano, unidades de almacenamiento) cuando no lo utilice.
- Proteger sus tokens físicos de acceso al trabajo (por ejemplo, llaves, tarjetas de acceso, llaveros) y no compartirlos nunca con otras personas sin aprobación.
- Cuando sea necesario, cerrar con llave todas las puertas, ventanas, almacenamiento de escritorios, etc., cuando se retire al final del día o cuando se ausente de su oficina durante períodos prolongados.

Por último, no eluda nunca los controles de acceso físico existentes, y notifique de inmediato cualquier infracción, pérdida o robo de Información o Equipos de TI de la empresa a su director y al Servicio de soporte técnico local.

## 4.2 Uso de Equipos y Servicios de TI de la empresa

### 4.2.1 Reglas generales

Los Equipos y Servicios de TI de la empresa se proporcionan para fines laborales definidos. En consecuencia, no haga un uso indebido de ellos en ningún momento, ya sea *in situ* o cuando trabaje a distancia. Por ejemplo, no debe:

- realizar actividades que puedan infringir las leyes aplicables, ofender o dañar la reputación o las operaciones de Glencore, de sus empleados y filiales;
- instalar *software* no autorizado o modificar la configuración de seguridad de los Equipos de TI de la empresa;
- interceptar de forma inapropiada, modificar o destruir cualquier Información de la empresa; o
- llevar a cabo operaciones comerciales privadas utilizando los Equipos y Servicios de TI de la empresa.

### 4.2.2 Uso de los servicios de correo electrónico y mensajería de Glencore

Glencore puede proporcionarle una cuenta de correo electrónico y/o de mensajería de la empresa como parte de su función. Estas cuentas están destinadas a las comunicaciones de la empresa, y usted debe tener en cuenta los siguientes principios:

- Como sucede con toda la correspondencia comercial, tenga en cuenta que las palabras que elija tienen peso legal. Debe ser prudente, ya que las declaraciones indebidas pueden dar lugar a responsabilidad personal o exponer a la empresa a riesgos legales, normativos o de reputación.
- Conserve todas las comunicaciones electrónicas que contengan Información importante de la empresa o decisiones que son necesarias para el mantenimiento de registros, de conformidad con nuestras políticas, estándares y procedimientos.
- Según el grado de confidencialidad necesario, considere otros métodos de comunicación (por ejemplo, servicio de transferencia segura de archivos de Glencore, archivos adjuntos comprimidos y protegidos con contraseña, o correo postal/servicio de mensajería).

Algunas de las actividades de correo electrónico/mensajería prohibidas son:

- Compartir información confidencial o sensible recibida o generada por Glencore con partes inapropiadas o no destinatarias, o a direcciones de correo electrónico personales.
- Representar formalmente a Glencore en cualquier tipo de comunicación pública (por ejemplo, en LinkedIn), a menos que se autorice específicamente[3].
- Compartir contenido ilegal o inapropiado (por ejemplo, piratería, pornografía, bromas racistas, odiosas u ofensivas) en forma de imágenes, *software*, archivos de audio o video.
- Enviar un correo electrónico en nombre de otra persona sin su consentimiento.

[3] Consulte nuestra Guía sobre redes sociales para obtener más información.

Además, tenga en cuenta lo siguiente:

- Algunos archivos adjuntos enviados/recibidos pueden ser bloqueados o puestos en cuarentena para proteger los Servicios de TI de la empresa.
- No registre nunca su dirección de correo electrónico de Glencore en servicios externos, a menos que sea con un propósito empresarial genuino (por ejemplo, portales de proveedores, membrecías profesionales).
- Tenga cuidado con los correos electrónicos/mensajes de fuentes sospechosas, especialmente si contienen hipervínculos, archivos adjuntos o solicitudes inusuales. Estos correos electrónicos suelen utilizarse para cometer fraude, robar credenciales o distribuir *malware*[4].
- No utilice nunca cuentas de correo electrónico personales (por ejemplo, Gmail, Hotmail) con fines empresariales.
- No utilice cuentas personales de redes sociales o herramientas de comunicación electrónica no corporativas para las comunicaciones de la empresa (por ejemplo, WhatsApp, Telegram, Signal, Threema), siempre que sea posible.
    - Nota: cuando se hayan utilizado las redes sociales o las herramientas de comunicación electrónica con un socio externo para fines empresariales, copie cualquier dato o decisión relevante para el negocio al almacenamiento de Glencore, de conformidad con nuestras políticas, estándares y procedimientos.

### 4.2.3 Uso interno

De acuerdo con su función, es posible que se le conceda acceso a Internet. Si es así, tenga en cuenta lo siguiente:

- Internet es una red pública, y la información presentada o enviada a través de ella suele estar mal protegida y fuera del control de Glencore.
- Obtenga acceso solo a información, documentos o archivos de sitios web de confianza y buena reputación.
- Descargue el *software* o el código ejecutable solo después de la validación de su Servicio de soporte técnico local.
- Es posible que algunos sitios web o servicios de Internet públicos estén bloqueados adrede para proteger mejor la Información o los sistemas de la empresa.

Además, no debe:

- Revelar de forma inapropiada Información confidencial o sensible de la empresa, o publicar contenido difamatorio sobre Glencore o sus empleados (por ejemplo, en foros o sitios de redes sociales).
- Utilizar servicios en la nube no autorizados o personales para cargar o compartir información corporativa confidencial o sensible (por ejemplo, Dropbox, WeTransfer). Póngase en contacto con su Servicio de soporte técnico local para recibir soluciones aprobadas.

[4] Consulte nuestra Guía de seguridad de correo electrónico para obtener más información.

- Obtener acceso a sitios web que podrían aumentar los riesgos de *malware* (por ejemplo, sitios de torrents, uso compartido de archivos ilegales, pornografía).
- Obtener acceso o transmitir contenido ilegal o inapropiado (por ejemplo, piratería, pornografía, bromas racistas, odiosas u ofensivas) en forma de imágenes, *software*, archivos de audio o video.

### 4.2.4 Conexión de Equipos de TI ajenos a la empresa a Servicios de TI de la empresa

Para proteger mejor los Servicios de TI de la empresa, se le aconseja no conectar Equipos de TI ajenos a la empresa no autorizados a ningún sistema, computadora o infraestructura de red de Glencore. Tenga en cuenta que:

- La conexión de periféricos de TI privados o de terceros (por ejemplo, dispositivos de juegos, paneles táctiles, cámaras) podría provocar fallos técnicos o afectar la integridad de los Servicios de TI de la empresa.
- Los dispositivos multimedia privados (por ejemplo, teléfonos móviles, reproductores de música o video) solo deben conectarse con fines de carga. Toda sincronización de datos puede conducir a la copia, el almacenamiento o la distribución inapropiados de contenido protegido por derechos de autor a través de los Servicios de TI de la empresa.
- Los dispositivos de almacenamiento portátiles ajenos a la empresa (por ejemplo, unidades USB) no deben utilizarse[5] a menos que sea para fines empresariales aprobados, luego cualquier dato sensible debe copiarse localmente en recursos compartidos de red y la unidad debe borrarse. Los dispositivos de almacenamiento no fiables podrían filtrar datos de Glencore o propagar *malware*.

Nota: Los Equipos de TI ajenos a la empresa pueden obtener acceso al servicio de Internet local y, si es necesario, a servicios de acceso remoto. Póngase en contacto con su Servicio de soporte técnico local para obtener autorización cuando sea necesario, o si tiene dudas sobre alguno de los requisitos anteriores.

## 4.3 Trabajo a distancia seguro

De acuerdo con su función, es posible que reciba un Equipo de TI de la empresa portátil, como una computadora portátil de Glencore y/o un dispositivo de mano de Glencore. Si no, puede obtener permiso para conectarse a las puertas de enlace de acceso remoto de Glencore utilizando Equipos de TI ajenos a la empresa. En todos los casos se aplican los siguientes requisitos de seguridad:

- Tenga cuidado al utilizar redes inalámbricas públicas y procure utilizar solamente proveedores de confianza.
- Los datos de trabajo no deben copiarse a su dispositivo o a cuentas ajenas a la empresa. No eluda ese requisito reenviando o guardando información de trabajo en el correo electrónico personal o en servicios de almacenamiento de datos personales.
- Proteja su cuenta y las credenciales por múltiples factores asociadas, como tokens, aplicaciones de autenticación, SMS o mensajes de voz. Estas son sus claves secretas para conectarse a los Servicios y Equipos de TI de nuestra empresa.

[5] Véase también la sección 4.5.2

- Asegúrese de que la información confidencial y sensible de Glencore no se dé a conocer a otras personas en lugares públicos (por ejemplo, que otras personas miren por encima del hombro en una cafetería).

En esta sección se detallan los controles específicos adicionales que se establecen más adelante, y que deben considerarse cuando se trabaja a distancia. Sin embargo, debe tener en cuenta que los controles indicados en este documento, incluida la supervisión, también se aplican cuando se trabaja a distancia.

### 4.3.1 Protección de los Equipos de TI de la empresa portátiles

Cuando se facilitan, las portátiles de Glencore ofrecen un acceso seguro a los Servicios de TI de la empresa a través de una red privada virtual (VPN)[6] y la posibilidad de copiar archivos localmente para poder trabajar sin conexión (por ejemplo, en viajes en avión sin Internet).

Los dispositivos de mano de Glencore también pueden venir con planes móviles de voz y datos. Cuando se le entregue un dispositivo de mano de Glencore, tenga en cuenta su plan de datos móviles y los costos de itinerancia. Cuando viaje, utilice redes inalámbricas de confianza y limite las actividades de gran ancho de banda (por ejemplo, transmisión de video, videollamadas, descargas de *software*) en redes de operadores extranjeros.

Además, cuando lleve Equipos de TI de la empresa, como portátiles, dispositivos de mano, etc., fuera de las instalaciones, debe tener cuidado de protegerlos de robos, riesgos o daños, y considerar lo siguiente:

- Mantenga los Equipos de TI de la empresa bloqueados o asegurados cuando no se utilicen o no estén vigilados. Nunca los deje en lugares públicos o visibles, como por ejemplo en el asiento de un coche estacionado.
- En viajes aéreos, lleve siempre a bordo los Equipos de TI de la empresa para minimizar el riesgo de daños o pérdidas.
- Nunca permita que otras personas (incluidos familiares o amigos) manipulen o inicien sesión en sus Equipos de TI de la empresa.
    - Nota: Cuando viaja al extranjero, y si las autoridades gubernamentales (por ejemplo, aduana o policía) solicitan formalmente el acceso a los Equipos de TI de la empresa, debe cooperar y cumplir con cualquier solicitud e informar a su director local y al Servicio de soporte técnico lo más pronto posible después de producido el hecho.

Por último, comunique siempre de inmediato todo daño o pérdida de cualquier Equipo de TI de la empresa a su Servicio de soporte técnico local y al director.

### 4.3.2 Servicios de acceso remoto – dispositivos de PC ajenos a la empresa

De acuerdo con su función, es posible que lo autoricen a tener acceso remoto a los Servicios de TI de la empresa a través de un dispositivo informático ajeno a la empresa (por ejemplo, conectándose a una

[6] Una VPN protege su identidad y navegación aprovechando un túnel virtual cifrado desde su dispositivo hasta los servicios de TI de destino.

solución de escritorio remoto a través de una portátil personal). Si se le autoriza al acceso remoto, tenga en cuenta lo siguiente:

- Es posible que deba instalar un *software* para conectarse al servicio, por ejemplo, con Citrix.
- Asegúrese de que su dispositivo de PC ajeno a la empresa esté en buen estado de funcionamiento, cuente con *software* actualizado/revisado y utilice servicios antivirus eficaces.
- Salga de sus sesiones de trabajo y cierre el navegador web cuando haya terminado.
    - Nota: Si utiliza una computadora pública (por ejemplo, en un hotel o quiosco de Internet), también debe borrar el historial o la caché de Internet cuando sea posible.

Otras buenas prácticas de seguridad específicas relativas al trabajo desde casa, o durante viajes, también están disponibles en guías separadas[7].

### 4.3.3 Servicios de acceso remoto – dispositivos de mano ajenos a la empresa

De acuerdo con su función, es posible que se le conceda acceso a los Servicios de TI de la empresa a través de un dispositivo móvil no corporativo (por ejemplo, conectándose a los servicios de correo electrónico de la empresa a través de un teléfono o una tableta personal). Si obtiene autorización, tenga en cuenta los siguientes requisitos:

- Deberá instalar/modificar *software* (por ejemplo, aplicaciones móviles) en su dispositivo para poder obtener acceso a los Servicios de TI de la empresa.
- Asegúrese de que su dispositivo esté en buen estado de funcionamiento, tenga una contraseña del dispositivo, no esté descodificado o en peligro, y cuente con *software* actualizado/revisado.
- Notifique de inmediato a su Servicio de soporte técnico local si las aplicaciones de Glencore no funcionan correctamente, si aparece *software* malicioso en el dispositivo o si pierde o roban su dispositivo.

## 4.4 Uso privado

A menos que las normas locales determinen lo contrario, usted puede hacer un uso privado limitado de los Equipos de TI y de los servicios de TI de la empresa cuando, en la opinión razonable de Glencore:

- no interfieran con su trabajo;
- no expongan la Información de la empresa o a los empleados a posible responsabilidad o a reclamaciones; o
- no desacrediten a Glencore y a sus empleados.

El uso privado de los Equipos y Servicios de TI de la empresa está sujeto a los requisitos establecidos en este documento, y usted debe comprender que el uso privado es un privilegio a discreción de Glencore.

[7] Consulte nuestras Guías para trabajo en casa y de seguridad en viajes para obtener más información.

### 4.4.1 Datos privados sobre los servicios de TI de la empresa

Debe tener en cuenta que todo uso privado de los Servicios de TI de la empresa (por ejemplo, correos electrónicos, almacenamiento en PC o en red, uso de Internet) desde cualquier dispositivo puede supervisarse. Sin embargo, algunas opciones de dispositivos pueden ofrecer una mayor privacidad:

- **PC y portátiles de Glencore:** debido a que estos dispositivos se conectan directamente con la red de Glencore, las opciones de uso privado están restringidas (por ejemplo, categorías de Internet restringidas, puertos USB bloqueados) para evitar riesgos de *malware* o pérdida de datos. Glencore recomienda no utilizar estos dispositivos para uso privado; sin embargo, si lo hace, le recomendamos que no almacene datos privados localmente ni etiquete registros privados (entre otros: correos electrónicos, archivos, entradas de calendario, contactos), por ejemplo, incluyendo «PRIVADO» en los nombres de las carpetas, los asuntos de los correos electrónicos o utilizando las características de etiquetado integradas. Etiquetar claramente sus datos privados ayuda a identificarlos y puede ayudar a excluirlos de la supervisión, las investigaciones, etc., cuando sea posible.
- **Dispositivos de mano de Glencore y ajenos a la empresa:** nuestra configuración de los Servicios de TI en los dispositivos de mano de Glencore o ajenos a la empresa crea «espacios de trabajo» separados de los personales, por lo cual estos dispositivos son más adecuados para el uso privado. Esta configuración le permite instalar aplicaciones privadas y evita que Glencore supervise, obtenga acceso o realice copias de seguridad de cualquier dato almacenado fuera del espacio de trabajo de los Servicios de TI de la empresa (por ejemplo, fotos, videos, documentos o archivos de música privados almacenados localmente en el dispositivo o dentro de aplicaciones privadas).
- **Dispositivos informáticos ajenos a la empresa:** estos dispositivos se conectan a soluciones de escritorio remoto y ofrecen una separación completa para cualquier dato y aplicación que resida en el dispositivo. Es decir que los datos y las aplicaciones de trabajo permanecen en la sesión de trabajo, mientras que los datos y las aplicaciones privados permanecen en su dispositivo privado.

Tenga en cuenta en todos los casos:

- Usted es responsable de hacer copias de seguridad de sus datos privados en sus propios repositorios o servicios de gestión privada (por ejemplo, iCloud).
- Glencore puede comprobar el tipo, el sistema operativo y el estado de seguridad de su dispositivo privado como parte de cualquier conexión a los Servicios de TI de la empresa.
- Toda actualización o cambio en su dispositivo privado fuera de las versiones admitidas (por ejemplo, sistemas operativos beta u obsoletos) puede provocar problemas de servicio o su revocación.
- Glencore no acepta la responsabilidad de cualquier impacto en el rendimiento o pérdida de datos derivados de la implementación de los Servicios de TI de la empresa en cualquier Equipo de TI ajeno a la empresa.

## 4.5 Tratamiento de la Información de la empresa

### 4.5.1 Clasificación de la información

Debe comprender las clasificaciones de seguridad de la información de Glencore, que se enumeran a continuación:

- **Restringida:** incluye nuestra información más sensible, como la Información interna de la empresa o los Datos personales sensibles, cuya divulgación puede tener un impacto negativo sobre Glencore o sobre la privacidad de los empleados.
- **Confidencial:** información que se comparte dentro de los equipos o departamentos para cumplir con las tareas habituales. Esta categoría abarca la mayor parte de nuestra información, que debe protegerse y no divulgarse innecesariamente (por ejemplo, memorandos internos de los departamentos, documentos de proyectos, reportes de estado operativo).
- **Interna:** abarca la información que se comparte ampliamente entre los equipos y divisiones de Glencore, pero no externamente (por ejemplo, contenido de la intranet, boletines de noticias de los equipos, directorios de personal).
- **Pública:** información que se ha hecho pública a través de los equipos y canales de comunicación oficiales (por ejemplo, nuestro informe anual de sostenibilidad, el informe anual, los informes de producción trimestrales).

Cuando sea posible, los propietarios y creadores de información restringida (electrónica o física) deben etiquetar el contenido correspondiente (por ejemplo, insertar la clasificación en el pie de página de un documento) para asegurarse de que otras personas sean conscientes de su sensibilidad y gestionen esta información con otras consideraciones de seguridad, por ejemplo, uso compartido restringido, prevención de pérdida de datos o controles de acceso más seguros.

### 4.5.2 Compartir Información de la empresa con terceros

Es posible que deba compartir Información de la empresa con terceros. En la mayoría de los casos, puede utilizar el correo electrónico de la empresa o las herramientas de colaboración de la empresa (por ejemplo, MS Teams), que son adecuadas para compartir Información de la empresa sin restricciones. Sin embargo, si tiene requisitos adicionales (por ejemplo, compartir información de Datos Personales sensibles o archivos de gran tamaño) debe considerar otras opciones, por ejemplo:

- Enviar información sensible como archivos adjuntos cifrados (por ejemplo, archivos ZIP).
- Utilizar un servicio de uso compartido de archivos aprobado por Glencore (por ejemplo, CORE Drive), para archivos sensibles o de gran tamaño.
- En caso de que se apruebe, utilizar las unidades USB proporcionadas por Glencore que aprovechan el cifrado.
    - Nota: Cuando reciba archivos de los socios en unidades USB, especialmente sin cifrar, copie los datos necesarios en el almacenamiento en red de Glencore y elimine o borre la unidad de forma segura.

Cuando sea necesario, póngase en contacto con su Servicio de soporte técnico local para obtener orientación.

### 4.5.3 Conservación de Información de la empresa

Para garantizar la correcta conservación de la Información de la empresa, usted:

- Debe almacenar la Información de la empresa en recursos compartidos de la red personal o del departamento, o en sistemas de gestión de datos aprobados, antes que en unidades locales de las que no se realizan copias de seguridad.
- No debe almacenar datos privados o no comerciales (por ejemplo, fotos privadas, cartas) en los Equipos de TI de la empresa o en los recursos compartidos de la red, a menos que sea con el entendimiento y consentimiento de que dichos archivos estarán sujetos a las prácticas internas de TI de Glencore (por ejemplo, copias de seguridad, conservación y supervisión).
- Debe tener en cuenta los límites locales establecidos en los recursos compartidos de la red u otros Servicios de TI de la empresa (por ejemplo, carpetas de correo electrónico). Usted es responsable del mantenimiento interno para asegurarse de que cumple con las obligaciones de conservación.

Para más información, consulte las políticas, estándares y procedimientos relevantes o póngase en contacto con su Servicio de soporte técnico local.

### 4.5.4 Devolución y eliminación de dispositivos de almacenamiento portátiles e información en papel

Debe eliminar cualquier dispositivo de almacenamiento de datos portátil (por ejemplo, DVD, unidades USB y otros soportes físicos) y toda información en papel de acuerdo con los procedimientos locales de conservación y destrucción, y tener en cuenta específicamente que:

- Los documentos sensibles deben destruirse con las trituradoras disponibles en su oficina.
- Los documentos no sensibles pueden eliminarse a través de las recolecciones locales de reciclaje de papel.
- Los dispositivos de almacenamiento portátiles o los Equipos de TI de la empresa que no se utilicen o sean redundantes deben devolverse a su Servicio de soporte técnico local para su limpieza y/o eliminación segura.

### 4.5.5 Respeto de los derechos de propiedad intelectual

El acceder, copiar, instalar, almacenar y distribuir contenido protegido por derechos de autor o patentado (por ejemplo, *software*, juegos, multimedia, documentos, imágenes) sin licencia puede ser ilegal y dar lugar a responsabilidad de la empresa o personal. No debe descargar ningún contenido en los Equipos de TI de la empresa que suponga una infracción de los derechos de autor o de la propiedad intelectual. Además:

- No debe hacer o tomar copias privadas ilegítimas de ningún *software* proporcionado por Glencore.
- No debe consultar, reproducir, almacenar o distribuir ilegalmente material protegido por derechos de autor (por ejemplo, textos, imágenes, audio, video) descargado o recibido, en la Información de la empresa y en los Servicios de TI de la empresa.

Póngase en contacto con su Servicio de soporte técnico local si tiene dudas sobre los derechos de autor o la propiedad intelectual.

## 4.6 Detección del incumplimiento

### 4.6.1 Escalada de incidentes de seguridad

Entre los incidentes de seguridad pueden incluirse *malware*, comunicaciones inapropiadas o fraudulentas, daño o eliminación de Información de la empresa, o no disponibilidad de los sistemas y pérdida de Equipos de TI de la empresa o de Información de la empresa, también de documentos impresos.

Debe notificar de inmediato cualquier incidente relacionado con TI o información de Glencore a su Servicio de soporte técnico local y a su director. Si el incidente implica o afecta los Datos personales, notifique también a su contacto local de protección de datos. De esta manera, Glencore podrá reaccionar mejor y reducir el riesgo de tiempo de inactividad del sistema de TI o de divulgación de información sensible.

### 4.6.2 Supervisión

Todos los Servicios de TI de la empresa tienen la capacidad para ser supervisados a través de registros generados por el Usuario final y eventos del sistema, o por medio de los datos que contiene el sistema. La supervisión se lleva a cabo principalmente para apoyar y mantener los Servicios de TI de la empresa, pero también para garantizar el cumplimiento de las políticas, estándares y procedimientos de Glencore por parte de los Usuarios finales.

La supervisión puede identificar el uso indebido de los Servicios de TI de la empresa o de la Información de la empresa. La supervisión registra las acciones a nivel individual y puede abarcar toda la gama de Servicios de TI de nuestra empresa, entre ellos, correo electrónico, mensajería, uso de Internet, servicios en la nube, almacenamiento de archivos, uso de computadoras y dispositivos móviles, etc. y todo uso privado de los mismos.

Las actividades de supervisión pueden ser automatizadas o manuales, según el alcance, pero siempre se llevan a cabo en cumplimiento del Estándar de protección de datos de Glencore, las leyes y reglamentos aplicables, la legislación laboral, etc., y en la medida necesaria con fines empresariales y legales. Si tiene alguna pregunta, póngase en contacto con su Servicio de soporte técnico local.

# 5 Hablar abiertamente y comunicar infracciones

Cada uno de nosotros es responsable de garantizar el cumplimiento de nuestros compromisos. Esperamos que nuestros empleados y contratistas hablen abiertamente y les exigimos que nos comuniquen cualquier inquietud relacionada con infracciones del Código de Conducta, de nuestras políticas o de la ley, tanto si se refieren a ellos mismos como a otras personas. Estas inquietudes deben plantearse a los directores, supervisores, o a través de otros canales de comunicación de infracciones disponibles, entre ellos los contactos para la comunicación de infracciones en nuestras oficinas y activos industriales. Los canales de nuestro Programa de comunicación de infracciones corporativo también están a disposición de los empleados, contratistas y partes externas.

Glencore toma en serio todas las comunicaciones de infracciones y las tramita sin demora.

Glencore no tolera represalias contra ninguna persona que hable abiertamente sobre conductas que considere poco éticas, ilegales o que se opongan a nuestro Código de Conducta y a nuestras políticas, incluso si la denuncia no se confirma. No habrá consecuencias adversas para nadie que plantee una inquietud, siempre que no haya presentado una denuncia falsa deliberadamente.

# 6 Consecuencias

Nuestros procedimientos apoyan nuestros Valores y nuestro Código de Conducta, y reflejan lo que es importante para nosotros. Glencore toma en serio las infracciones de nuestros procedimientos. Dependiendo de la gravedad de la infracción, las consecuencias pueden ir desde una advertencia hasta el despido.

# 7 Recursos adicionales

Nuestros Valores

Código de Conducta

Política de gobernanza de la información

Estándar de protección de datos

Estándar de Seguridad de la Información

Guía de seguridad de correo electrónico

Guía para trabajo seguro en casa

Guía de contraseñas seguras

Guía sobre redes sociales

Guía de seguridad en viajes