GLENCORE

ESTÁNDAR DEL GRUPO

Estándar de Seguridad de la Información

Departamento de Tecnología de la Información del Grupo

Estándar

ESTÁNDAR DE SEGURIDAD DE LA INFORMACIÓN

Contenido

1 Propósito

Este Estándar de Seguridad de la Información (Estándar) apoya la Política de gobernanza de la información y el Marco de seguridad de Glencore, que es utilizado por los empleados responsables de implementar los controles de seguridad necesarios. Los objetivos de este documento son presentar:

- la postura de Glencore respecto a la seguridad de la información;
- los conocimientos sobre los riesgos cibernéticos a los que nos enfrentamos; y
- el enfoque de Glencore para proteger la información de la compañía.

2 Ámbito

Este Estándar es aplicable 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 controlado u operado directa o indirectamente por Glencore Plc en cualquier lugar del mundo, y que disponen de acceso a los Servicios de TI de la compañía o a la Información de esta (Usuarios).

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

3 Términos clave

Información de la compañía: cualquier información que Glencore cree, recopile o reciba, incluidos los conjuntos de datos que abarcan las actividades comerciales, financieras, mineras y técnicas, pero excluyendo la Información privada (por ejemplo, datos no laborales o comunicaciones privadas de los usuarios). La información de la compañía puede tener distintos niveles de sensibilidad e importancia para la compañía.

Servicios de TI de la compañía: 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 compañía.

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.

4 El panorama de la seguridad de la información

4.1 Información y seguridad de la información

Toda la información generada o intercambiada durante la realización de los negocios de Glencore, o que haya sido almacenada, procesada o transmitida mediante los sistemas de Glencore, se considera Información de la compañía y está sometida a este Estándar. Glencore reconoce que la Información de la compañía:

- varía en cuanto a su importancia y sensibilidad para la empresa; y
- existe en formato electrónico, en papel y de forma oral.

Por lo tanto, la Seguridad de la información también es importante para Glencore; abarca las prácticas para gestionar los riesgos de la información de nuestra compañía y garantiza que la información de la compañía se valore, se proteja y se ponga a disposición de las personas adecuadas en el momento oportuno.

4.2 El compromiso de Glencore

Glencore reconoce la importancia de la seguridad de la información mediante:

- el cumplimiento de todas las leyes y reglamentos aplicables;
- la capacitación de los equipos de TI para que sean facilitadores de la seguridad de la información; y
- proporcionando a los usuarios de Glencore los recursos para que trabajen de forma segura.

Este Estándar garantiza que todos seamos conscientes de los amplios riesgos para la información corporativa de Glencore, que comprendamos el enfoque de Glencore respecto a la seguridad de la información y las consecuencias del incumplimiento.

4.3 El panorama de las amenazas

Las tendencias de las tecnologías de la información están cambiando nuestra forma de operar y aumentando el volumen y el valor de la información de nuestra compañía. Por ejemplo:

- **mayor conectividad**: entre nuestros sistemas, empleados y socios de servicios externos;
- **movilidad de los trabajadores**: dispositivos informáticos portátiles más inteligentes, que transforman cómo y dónde trabajamos; y
- **complejidad creciente**: con soluciones transformadoras para las operaciones industriales y comerciales.

Reconocemos que nuestro sector es propenso a sufrir una serie de amenazas, y nuestro perfil nos convierte en un objetivo más allá de las fronteras geopolíticas. A medida que aprovechamos las tecnologías de la información para nuestro negocio y nos conectamos con nuestros socios globales, tenemos que estar atentos a los posibles orígenes de las amenazas a la seguridad.

- **Desde dentro de nuestra organización: usuarios bienintencionados** que intentan hacer su trabajo, pero no siempre de la forma más adecuada, o **personas con información privilegiada oportunistas** que abusan del acceso que se les ha concedido.
- **Desde fuera de nuestra organización: criminales cibernéticos** cada vez más **sofisticados** que se organizan mejor, utilizan mejores herramientas y buscan recompensas financieras, políticas o sociales.
- **Dependencias:** la creciente dependencia **de socios informáticos externos** que proporcionan nuestros servicios informáticos, o **eventos medioambientales** que pueden tener efectos negativos sobre nuestros centros de servicios informáticos o nuestras operaciones clave.

4.4 Proteger la información de la compañía

La seguridad de la información también consiste en identificar y proteger la información de nuestra compañía, que puede existir en diferentes formas.

- **Información electrónica***:* que puede almacenarse en sistemas de aplicación internos y externos, bases de datos y archivos apoyados por nuestras redes informáticas e infraestructuras de comunicación.
- **Documentos impresos**: frecuentemente se generan para apoyar las reuniones de negocios, la colaboración y la toma de decisiones, y pueden ser sensibles tanto por la fecha de su creación como por la información que contienen.
- **Conocimientos y experiencia***:* mantenemos conocimientos especializados en todas nuestras divisiones y operaciones, y esta experiencia empresarial (derivada de la información de nuestra compañía) debe ser protegida.

5 Nuestros mecanismos de protección

Este Estándar está en consonancia con nuestros Valores y el Código de Conducta, que siguen siendo nuestros principios básicos de buenas prácticas. Este Estándar se enmarca en la Política de gobernanza de la información, que establece requisitos más amplios de gobernanza de la información y que se apoya en otros documentos corporativos y locales, como el Estándar de protección de datos y los procedimientos locales de protección de datos, que abordan la protección de los datos y la privacidad. Los requisitos que deben cumplir los usuarios para acceder a los servicios informáticos de la compañía se recogen en los Procedimientos de servicios informáticos para usuarios finales y privilegiados.

El Marco de seguridad de Glencore (GSF) amplía el modelo de seguridad proporcionando requisitos de control detallados y conjuntos de herramientas, que ayudan a implementar los controles de seguridad de forma coherente en toda la compañía. Los emplazamientos pueden aplicar controles más estrictos para cumplir cualquier requisito legal o reglamentario local válido, con el fin de impulsar eficazmente las actividades de seguridad en toda nuestra empresa cuando sea necesario. Sin embargo, si un emplazamiento quiere relajar los controles obligatorios, el responsable local de TI debe consultar a Tecnología de la información del Grupo para que se autorice una excepción de seguridad formal.

5.1 Principios de seguridad

Nuestro enfoque se basa en tres principios sencillos.

1. **La información de la compañía tiene que estar protegida**. Nuestros conocimientos empresariales contribuyen a nuestro éxito y el acceso a ellos debe estar justificado, y deben establecerse los niveles de protección adecuados.
2. **La seguridad de la información debe ser adecuada para los riesgos**. Es necesario determinar y validar los riesgos. Los controles de seguridad deben ser apropiados y eficaces, y no deben obstaculizar nuestra actividad.
3. **Esperamos que nuestra gente actúe de forma responsable.** Apoyamos este objetivo con políticas claras, apoyo de la dirección, controles técnicos y la formación pertinente en materia de seguridad y de informática.

Aplicando estos principios de forma colectiva podemos garantizar que las herramientas y los procesos de nuestro GSF sean asumidos por todos los niveles de nuestra compañía, y se apliquen adecuadamente a los riesgos a los que nos enfrentamos.

5.2 Clases de información de Glencore

Para facilitar la protección de nuestros activos de información hemos definido las siguientes clases:

- **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).

Glencore reconoce que algunas partes de información de la empresa son más sensibles que otras, y las medidas de protección deben ser adecuadas para el riesgo. Además, nuestro enfoque de la seguridad de la información debe tener en cuenta los diferentes riesgos de seguridad a los que se enfrenta nuestro personal, ya sea la alta dirección, los usuarios finales o los socios externos.

5.3 El marco de seguridad de Glencore (GSF)

El GSF detalla los requisitos de control de TI en todos los niveles de los servicios de TI corporativos de Glencore, por lo que solo se publica para nuestros profesionales de la seguridad con el fin de garantizar que se apliquen controles de protección coherentes y eficaces a nuestros activos de información globales. Para ello, el GSF se basa en el establecimiento de responsabilidades, tecnologías y procesos claros.

5.3.1 Responsabilidades claras

Tenemos que apoyar las siguientes funciones y responsabilidades:

- **Equipos de TI**: muchos controles del GSF están configurados en nuestros sistemas de TI y procesos de apoyo, lo que convierte a los equipos de TI en los «facilitadores» de la seguridad de la información en Glencore. El **Servicio de soporte técnico de TI** local o el **director de TI** deben ser su primer punto de contacto para cualquier problema o pregunta relacionada con la seguridad. Cuando sea necesario, **los equipos de Seguridad de la información o Seguridad técnica** pueden trabajar dentro de los equipos locales de TI como especialistas para apoyar iniciativas clave, como el desarrollo de políticas de seguridad de la información, proyectos de seguridad, formación en seguridad o investigación de incidentes.
- **Propietarios de servicios de TI**: Glencore confía en custodios de nuestros sistemas y datos clave. Estas funciones, a menudo divididas entre la empresa y los propietarios de las TI, permiten comprender los riesgos relacionados con sus sistemas y respaldar las tecnologías y los procesos necesarios para proteger sus datos.
- **Otras funciones de control interno**: **RR. HH.**, **Legal y Cumplimiento**, **Auditoría Interna y Externa** tienen conocimientos especializados y frecuentemente colaboran con los equipos de TI en proyectos, auditorías, revisiones o eventos operativos para garantizar la seguridad de la información de nuestra compañía.

Por último, como **usuarios de los servicios informáticos**, **todos** somos responsables de la seguridad de la información de la compañía a la que accedemos, especialmente si tenemos acceso privilegiado. Todos los empleados o socios externos con acceso a nuestros datos deben cumplir con nuestros **Procedimientos de servicios de TI** y nuestros **Acuerdos,** respectivamente.

5.3.2 Tecnologías y procesos

La seguridad de la información de nuestra compañía también depende de las tecnologías y los procesos. Para asegurar los servicios informáticos de nuestra compañía se necesitan sistemas y configuraciones de seguridad especializados, y la monitorización y el mantenimiento son esenciales. Todos tenemos la obligación de apoyar la implementación de nuestros controles técnicos, por ejemplo, siguiendo el Procedimiento de usuario final, para minimizar todo tipo de riesgos para la información de nuestra compañía.

Los procesos de seguridad unen a las personas y a la tecnología para implementar prácticas de seguridad coherentes y maduras en toda la empresa. Los procesos son los planes de acción por los que se guían nuestras actividades empresariales. Contar con procesos claros y eficientes puede ayudar a Glencore a mejorar la agilidad, la visibilidad y el cumplimiento, y nos proporciona una base para adaptarnos y mejorar continuamente.

6 Hablar abiertamente

Usted es responsable de garantizar el cumplimiento de los compromisos de Glencore. Glencore espera que sus empleados y contratistas hablen abiertamente y planteen sus preocupaciones sobre posibles infracciones del Código de Conducta y de esta política a su director, supervisor o a través de otros canales de comunicación de infracciones disponibles. Nuestra plataforma de comunicación de infracciones está a disposición de los empleados, los contratistas y las 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 y procedimientos, incluso si la denuncia no se confirma, siempre que el denunciante no haya presentado una denuncia falsa deliberadamente.

7 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.

8 Recursos adicionales

Nuestros Valores

Código de Conducta

Política de Gobernanza de la Información

Estándar de Protección de Datos

Procedimiento de Servicios de TI para Usuarios Finales

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