Política sobre el uso aceptable de los sistemas de información

De fecha 25 de octubre de 2017

Introducción

Las tecnologías de la información ("TI") son herramientas fundamentales para el desarrollo de los negocios de Minera Agua Rica Alumbrera. y sus subsidiarias ("MARA"). Esta Política sobre el uso aceptable de los sistemas de información y diferentes medidas de seguridad son necesarias para proteger los activos, la gente, los recursos y la información de MARA. MARA requiere que todas las personas que accedan a los servicios y recursos de TI de MARA (los "Usuarios de TI") lean, reconozcan y cumplan esta política.

Esta política de TI se aplica a MARA y a todas sus subsidiarias en todo el mundo, y todas las referencias a "MARA" incluyen a sus subsidiarias.

1. Objetivo

- Protegerlo a usted, a MARA y a otros empleados.
- Ayudarlo a usted y a otros empleados a comprender los usos aceptables de TI.
- Ayudarlo a usted y a la gerencia a identificar y mitigar los riesgos de TI.
- Respaldar el Código de conducta, la Política de divulgación oportuna y confidencialidad, la Política de control corporativo y la Política de derechos humanos.
- Ofrecer un ambiente de TI confiable y efectivo para MARA y sus empleados.

2. Aplicación

Esta política se aplica a todas las personas que acceden o usan dispositivos y servicios de TI provistos por MARA. Esto incluye empleados, contratistas, proveedores de servicios, etc. que usan cualquier recurso y servicio de tecnología de la información de MARA.

Tecnología de la información incluye, sin carácter restrictivo,

- sistemas de computación, incluyendo computadoras de escritorio, computadoras portátiles, tablets y teléfonos celulares,
- correo electrónico y sistemas de colaboración,
- todo los programas instalados y equipos,
- servicios de programas, también conocidos como "aplicaciones en la nube",
- redes de MARA y conexiones a internet,

- todos los datos almacenados electrónicamente (incluyendo correo de voz, correo electrónico y SMS), etc.

3. Documentos de referencia

- Código de conducta,
- Política de divulgación oportuna y confidencialidad
- Política de control corporativo
- Política de derechos humanos

4. Uso aceptable

Esta sección describe el uso aceptable de TI. El uso adecuado y responsable para fines de negocios pretende mitigar los riesgos asociados con:

- Virus, programas maliciosos, mensajes electrónicos fraudulentos (phishing) y otras formas de ciberataques
- Una violación a la seguridad que comprometa las redes y sistemas de MARA
- Otorgar inadvertidamente acceso al sistema a partes no autorizadas
- Actividad inadecuada e ilegal

4.1 Confidencialidad y Código de conducta

El Código de conducta, la Política de divulgación oportuna y confidencialidad, la Política de control corporativo y la Política de derechos humanos se aplican al uso de TI.

Los equipos, programas informáticos y servicios de propiedad de la empresa están destinados para ser utilizados para actividades de la empresa y no se deberá pretender que exista privacidad al usarlos. El uso personal incidental está permitido en tanto sea mínimo, no interfiera con las responsabilidades laborales del empleado y cumpla con esta política.

Los siguientes usos están prohibidos:

- Enviar mensajes amenazantes, acosadores u ofensivos que no cumplan con el Código de conducta, la Política de comunicación de empleados y la Política de derechos humanos.
- Configurar las TI de MARA para permitir intencionalmente el acceso a usuarios no autorizados.
- El uso de TI para beneficio personal o para hacer conocer opiniones personales; promover cualquier emprendimiento comercial o campaña privada, con excepción de eventos benéficos.

- Todo uso contrario a las leyes aplicables, incluyendo cualquier actividad que pudiera resultar en reclamos de violación de derechos de propiedad intelectual o copyright.
- Ver, publicar, bajar, imprimir o distribuir información o materiales que pudieran ser considerados razonablemente obscenos, profanos, abusivos o de otra manera ofensivos, como pornografía y sitios o materiales que instigan el odio.
- Apostar en línea.
- Bajar, instalar o activar aplicaciones de piratería informática o "hacking" o aplicaciones troyanas para escanear puertos, crackear contraseñas, realizar espionaje electrónico u otro tipo de actividad de piratería.

4.2 Correo electrónico e internet

4.2.1 Correo electrónico

El correo electrónico es un servicio de TI que debe usarse de manera razonable y respetuosa para comunicaciones de negocios. Los mensajes de correo electrónico deben ser profesionales tanto en cuanto al lenguaje como al tono. Todos los empleados de MARA deben enviar y recibir correos electrónicos relacionados con el negocio usando una cuenta de correo electrónico autorizado por la empresa, salvo en situaciones particulares en las que los servicios de correo electrónico de la empresa no están disponibles. Las cuentas de correo electrónico personales como hotmail, yahoo mail, etc. no deben ser utilizadas para enviar y recibir información relacionada con la empresa. En circunstancias particulares en las que no se puede acceder al sistema de correo electrónico de MARA debido a desperfectos en la red, internet o de otro tipo, podrá utilizar su correo electrónico personal, pero deberá **copiar todos los mensajes a su dirección de correo electrónico de MARA**.

Debe hacer todos los intentos razonables para usar el correo electrónico de MARA para fines laborales.

4.2.2 Internet

Los servicios de internet ofrecidos por MARA deben ser utilizados de manera razonable y respetuosa para fines de negocios. El tráfico de internet puede estar restringido y/o monitoreado por razones de seguridad o relacionadas con el trabajo.

Los empleados pueden usar acceso a internet no provisto por la empresa en áreas como su casa, aeropuertos, hoteles, wifi, etc. Esta política recomienda ser cauteloso al acceder a internet. Cerciórese de que todas las conexiones sean seguras y no lo expongan a usted, su información o su dispositivo a un acceso no deseado y a amenazas. Si no está seguro sobre un servicio de internet, comuníquese con el soporte de TI local.

4.3 Instalar programas y equipos

Todo programa y equipo de TI debe ser utilizado de conformidad con las licencias y términos correspondientes y todas las leyes aplicables.

Instalar programas o equipos en un dispositivo puede resultar en un dispositivo inestable o un comportamiento de sistema inestable. Se recomienda encarecidamente que solicite a la persona de soporte de TI local que lo asista a instalar programas o equipos.

TI se reserva el derecho de desinstalar cualquier programa o equipo que provoque el malfuncionamiento del dispositivo, comprometa la seguridad de TI o no cumpla con los términos de esta política. La instalación de aplicaciones para uso personal no será permitido.

Todo el programa desarrollado por empleados o terceros usando los recursos de TI de MARA o mientras estén contratados por MARA constituirán propiedad intelectual de MARA (salvo que MARA haya acordado lo contrario por escrito) y el desarrollador no tendrá derecho a vender o distribuir el software a otras personas o empresas sin el consentimiento escrito de MARA.

4.4 Almacenamiento de datos

Toda la información de MARA, incluyendo, sin carácter restrictivo, archivos, correos electrónicos, documentos, etc., deberán ser almacenados en la red de MARA, en dispositivos de almacenamiento aprobados por TI o en un proveedor de servicios aprobado por TI. Los datos deben estar almacenados de modo tal que, si fuera necesario, la administración de TI pueda obtenerlos para fines de recuperación y asuntos relacionados con la seguridad.

El almacenamiento de datos también está sujeto a todas las políticas de gestión de la información y retención de documentos que implemente MARA de tanto en tanto.

Los dispositivos de almacenamiento externo como discos duros externos, llaves USB, DVD, CD, etc. pueden introducir programas maliciosos como virus, spyware, troyanos, etc. que pueden dañar la integridad de la red y los datos de la empresa. Se recomienda encarecidamente verificar la presencia de virus antes de acceder a cualquier información en estos dispositivos. Es responsabilidad de cada persona asegurarse que el uso de tales dispositivos cumpla con esta política.

4.5 Uso de dispositivos móviles personales para el trabajo

TI permite a los empleados usar dispositivos personales como teléfonos celulares y tablets para acceder a su cuenta de correo electrónico de MARA. Los empleados **NO** están obligados a usar sus dispositivos personales para estos fines. Deben tener en cuenta que vincular una cuenta de correo electrónico de MARA a su dispositivo personal le permite a TI iniciar políticas de seguridad y procedimientos de seguridad que pueden afectar el comportamiento y el estado de su dispositivo y datos. Una vez terminado el

vínculo laboral con MARA, usted deberá borrar toda cuenta de correo electrónico de MARA vinculada con sus dispositivos móviles. TI se reserva el derecho de borrar todos los datos en los dispositivos que tienen cuentas de correo electrónico de MARA cuando se informe su pérdida, robo o uso no autorizado.

4.6 Compartir documentos e información electrónica

Al compartir, transmitir o transferir archivos electrónicos a terceros o cuando estos se los transmitan, transfieran o compartan, usted será responsable de la integridad y la seguridad de los datos. Todos los métodos para compartir, transmitir y transferir datos deben cumplir con esta política. Introducir datos de terceros sin los controles adecuados puede resultar en la pérdida de datos, corrupción de archivos, ingreso de programas maliciosos y problemas de cumplimiento.

5. Seguridad

La ciberseguridad evoluciona rápidamente. La cantidad y el tipo de amenazas están en aumento. Este aumento en actividad delictiva está relacionado con nuestra mayor dependencia en la tecnología y la rentabilidad de los delitos informáticos.

Es importante tener en cuenta que en la mayoría de los casos el delito informático inicialmente no perturba y a menudo es difícil de detectar. Los delincuentes informáticos ya dejaron de simplemente querer perturbar los sistemas; están en busca de información personal, confidencial o de otro tipo. No quieren que usted sepa que entraron a un sistema y hacen todo lo posible para permanecer desapercibidos.

Para ayudar a MARA y a usted, es importante que lea esta sección atentamente. Para obtener mayor información o en caso de dudas, comuníquese con el personal de soporte de TI local.

- No debe desactivar, evadir, manipular o de otra manera interferir con el funcionamiento de configuraciones de seguridad, programas de seguridad, u otras características o funciones de seguridad implementadas en cualquier recurso de TI de MARA.
- Debe acceder a los dispositivos y servicios de TI con métodos seguros proporcionados o aprobados por TI.
- Debe proteger la confidencialidad de su contraseña de red y no debe permitir que sea utilizada por otra persona.
- Debe denunciar cualquier actividad de ciberseguridad sospechosa al personal de soporte de TI local.

5.1 Dispositivos aprobados para usar en el trabajo

Los empleados deben usar los dispositivos aprobados por TI de MARA al conectarse a la red de MARA. Ello incluye computadoras, tablets, teléfonos celulares, teléfonos normales, componentes industriales como sensores, microcontroladores, etc. Su dispositivo debe ser controlado por TI para verificar que cuenta con todos los controles y programas de seguridad

adecuados y que cumple con las normas de MARA. TI se reserva el derecho de negarse a certificar sus dispositivos personales que funcional o técnicamente no son adecuados para ser utilizados para el trabajo y a desconectar dispositivos personales que no cumplen con los términos de esta póliza, y podrá abstenerse de ofrecer soporte técnico para tales dispositivos.

5.2 Control de acceso

TI o un delegado aprobado debe administrar el acceso y el otorgamiento de acceso a todos los sistemas de TI. La administración de TI debe conservar los privilegios de acceso a todos los sistemas de TI de MARA a los fines de asegurar la continuidad de las actividades comerciales, la seguridad y la integridad. El propietario del sistema o un representante de RR. HH. debe aprobar el acceso a los sistemas de TI específicos y TI deberá mantener un registro de solicitudes y aprobaciones.

5.3 Supervisión

MARA conserva el derecho de supervisar todo el tráfico de red, correos electrónicos y el uso de internet para asegurar tanto el desempeño técnico de los sistemas como el cumplimiento de esta política. MARA se reserva el derecho, cuando corresponda y sujeto a las leyes aplicables, a revisar el contenido de los correos electrónicos o archivos (por ejemplo, cuando existe una sospecha más que razonable que existe actividad inadecuada) sujeto a la aprobación del Vicepresidente Senior, el Asesor General y el Secretario Corporativo o un funcionario equivalente. Como regla general, ningún empleado debe esperar tener privacidad en el uso del correo electrónico e internet en relación con los recursos y la información de TI de MARA.

5.4 Accesos para la administración del sistema

Los empleados de soporte de TI autorizados (las personas de TI responsables de las operaciones técnicas de equipos o programas) podrán acceder a sus archivos y datos a los fines de mantenimiento, resolución de problemas, incidentes de seguridad u otro tipo de solución de problemas. Para ello, los usuarios de TI recibirán una notificación anticipada de dicho acceso. Es posible que no se notifique con anticipación si se debe acceder por razones de seguridad, incluyendo investigaciones de una violación potencial a esta política, a otras políticas de la empresa o a condiciones de uso.

5.5 Notificaciones y cambios

Recursos Humanos deberá notificar a TI de inmediato cuando ya no se necesitan cuentas de correo electrónico/de red de empleados (renuncias, despidos). Las cuentas no serán dejadas inactivas después de que un empleado deja de trabajar en MARA salvo que así lo apruebe el Vicepresidente Senior, el Asesor General y el Secretario Corporativo o funcionario equivalente.

Debe notificar de inmediato a TI en el caso de pérdida o robo de equipos de TI para que se tomen las medidas de seguridad adecuadas.

Solo personal de TI autorizado (o las personas designadas) puede realizar cambios a la red de MARA. No se podrán instalar dispositivos de red (hubs, switches, puntos de acceso inalámbricos, etc.) o programas de cualquier tipo en la red o dispositivos de MARA sin la aprobación previa de TI.

Usted tiene la responsabilidad de denunciar acciones o comportamientos que puedan resultar en un conflicto con esta política o que no cumplan con ella. Sírvase denunciar estas situaciones al personal de soporte de TI local o a su gerente.

5.6 Adquisición y soporte de dispositivos y servicios de TI

TI tiene la responsabilidad de entregar dispositivos y servicios de TI proporcionados por la empresa y darles soporte. No son responsabilidad del departamento de TI los dispositivos personales y los servicios de software personales. No debe esperar que TI le dé soporte a sus dispositivos personales o programas personales.

Los departamentos que deseen comprar o investigar nuevas aplicaciones, bases de datos, equipos o contratar proveedores o contratistas externos deben asegurarse de que tales opciones cumplan con los términos de esta póliza.

Todos los programas, equipos y servicios de programas de TI para uso de la empresa deben ser revisados por el funcionario de seguridad de TI de MARA o quien este designe para asegurarse de que se haya evaluado adecuadamente cualquier riesgo a la seguridad de TI.

5.7 Contraseñas

En el caso de que se le solicite crear o cambiar una contraseña para un sistema interno o externo de MARA, se deben seguir las siguientes reglas:

Al elegir una contraseña **NO**:

- use su nombre
- use su número de teléfono
- use la ciudad en la que vive
- use el nombre de la empresa en la que trabaja
- use el nombre de su hijo o cónyuge
- la escriba en un lugar que sea fácil de encontrar
- la comparta con nadie
- use menos de 8 caracteres
- use solo letras o solo números
- use solo minúscula o solo mayúscula
- use letras secuenciales o números como 1234 o abcd
- use palabras comunes como "contraseña"

Suponga que cualquiera que intenta robar su contraseña o adivinarla sabe quién es usted y tiene algo de información personal.

Por ejemplo, ninguna persona en MARA debe tener la palabra “MARA” como parte de su contraseña ni "gold", "oro", "silver" o "plata" o una combinación como Gold1234. Si tiene una contraseña con estas características, cámbiela. Cuando sea posible, use una segunda capa de autenticación como un código adicional o una función biométrica.

5.8 Incidente de seguridad de TI

Si usted o cualquiera que trabaja en MARA toma conocimiento de un incidente de seguridad de TI, debe contactarse con el representante de TI local de inmediato y denunciar lo que sabe. Esta persona **NO** debe intentar investigar, resolver o mitigar el incidente sin la indicación de TI.

5.9 Actividad de ciberseguridad

Debe estar al tanto de los métodos que existen para infiltrarse y robar su información personal. Los delincuentes se hacen pasar por gente que usted conoce por correo electrónico, mensaje de chat, medios sociales y teléfono. Controle y verifique la autenticidad de todos los mensajes cuidadosamente. Si no está seguro sobre un mensaje que recibió o una llamada telefónica, comuníquese con el personal de soporte de TI de inmediato.

6. Medios sociales

Todos los empleados de MARA deben considerar lo siguiente al operar en línea:

- Asegurarse de que su comportamiento y el contenido de todo lo que publica es congruente con los valores de MARA y el Código de conducta, en particular al usar la infraestructura de tecnología de información de MARA – es posible que su ubicación cuando está en línea sea rastreable.
- Considerar las consecuencias de lo que planea compartir y cómo puede afectar a MARA y todos los actores interesados en MARA, incluyendo accionistas, comunidades locales, proveedores y empleados, entre otros.
- En relación con MARA o sus subsidiarias, no haga comentarios sobre actividades estratégicas, operativas o financieras; actividades de participación con la comunidad o el gobierno; acciones legales; iniciativas de desarrollo de negocios; negociaciones laborales; o tipos similares de negocios corporativos.
- Recuerde que la información confidencial e interna es propiedad de MARA y usted debe contar con el consentimiento autorizado expreso para compartirla fuera de MARA, lo que incluye publicarla o guardarla fuera de la red de MARA.
- Ofrecer información privilegiada en línea es igual que ofrecer información en persona y puede constituir una violación a reglamentaciones relevantes en materia de títulos valores.
- Al discutir información relacionada con MARA, incluyendo información públicamente disponible, debe identificar su relación con MARA, incluyendo su nombre y función en la empresa. Tenga en cuenta que, si no está autorizado a hablar en nombre de MARA, debe aclarar que las opiniones le pertenecen. Es aconsejable que incluya una declaración de

deslinde de responsabilidad como “las publicaciones en este sitio me corresponden y no representan a Minera Agua Rica Alumbrera”, según sea necesario.

- Cuando tenga dudas, no publique y pida consejo a su supervisor, el departamento de Recursos Humanos, Legal o Comunicaciones Corporativas y Relaciones con Inversionistas.
- Protéjase implementando las mejoras prácticas, como actualizar regularmente sus contraseñas, para garantizar la seguridad e integridad de sus cuentas personales.
- No deje que sus actividades en línea se interpongan en terminar con éxito sus obligaciones y responsabilidades.

6.1 Uso de los medios sociales

Salvo que se apruebe de otra manera, la presencia en línea de MARA es gestionada por el departamento de Comunicaciones Corporativas y Relaciones con Inversionistas.

Los procedimientos y protocolos de MARA que rigen su presencia en línea han sido diseñados para garantizar que exista una supervisión y controles internos adecuados para manejar eficazmente las actividades en línea de MARA.

Las comunicaciones internas oficiales de MARA, incluyendo las comunicaciones entre la gerencia y los empleados o entre grupos de empleados, solo se pueden enviar por aplicaciones de comunicaciones que TI de MARA proporciona y da soporte.

6.2 Presencia en línea oficial

A la fecha de esta política, la presencia en línea oficial de MARA incluye, sin carácter restrictivo, lo siguiente, pero podrá cambiar si la tecnología o las necesidades de MARA cambian:

Minera Agua Rica Alumbrera .

- Sitio web externo (www.yamana.com)
- Twitter (www.twitter.com/yamanagoldinc)
- Facebook (www.facebook.com/Yamana-Gold-150944298311295/)
- LinkedIn (https://www.linkedin.com/company/yamana-gold-inc-) (gestionado por Recursos Humanos)

Asimismo, las subsidiarias, operaciones o propiedades de exploración de MARA pueden establecer una presencia en los medios sociales para facilitar las actividades de relación con la comunidad. Los departamentos de Comunicaciones Corporativas y Relaciones con Inversionistas y TI deben ser consultados antes de crear nuevas cuentas vinculadas con MARA o cualquiera de sus subsidiarias, operaciones o propiedades de exploración.

7. Medidas disciplinarias

Si en algún momento usted u otra persona tiene dudas sobre la interpretación o aplicación de cualquier parte de esta política, comuníquese con TI para recibir aclaración. Usted y todos los

representantes de MARA tienen la responsabilidad de denunciar cualquier violación a su gerente u otra persona apropiada.

Cualquier violación a esta política puede resultar en medidas disciplinarias, incluso el despido.

8. Historial de revisiones

Esta política debe ser revisada cada doce (12) meses a partir de la fecha de emisión para verificar su cumplimiento y eficacia.