LITORALPRESS

Fecha: 21-01-2025
Medio: El Mercurio
Supl. : El Mercurio - Minería y Comunidad
Tipo: Noticia general
Título: **Obligación de notificar incidentes críticos: Las dudas del sector minero**

Pág. : 4
Cm2: 1.214,0
VPE: $ 15.946.936

Tiraje: 126.654
Lectoría: 320.543
Favorabilidad: No Definida

CON LA NUEVA LEY MARCO DE CIBERSEGURIDAD

Obligación de notificar incidentes críticos: Las dudas del sector minero

Cyber Technology South America y el cuerpo Minería & Comunidad de "El Mercurio" reunieron a la autoridad y los líderes del área de las mineras más importantes del país, quienes detallan los principales desafíos e inquietudes que presenta esta nueva norma para las compañías que sean calificadas como esenciales.

ANA MARÍA PEREIRA B.

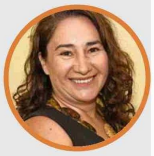
DANIEL ÁLVAREZ, *DIRECTOR, AGENCIA NACIONAL DE CIBERSEGURIDAD (ANCI)*

Primero, (la industria) debe desarrollar una cultura interna que priorice la ciberseguridad como un pilar estratégico, tal como hizo con la seguridad operacional, superando posibles resistencias internas y fortaleciendo la confianza con los diferentes grupos de interés.

Segundo, es esencial que se implementen sistemas avanzados de monitoreo y detección que les permitan prevenir, pero también identificar y reportar incidentes en tiempo real, asegurando un cumplimiento eficiente.

Finalmente, es clave asegurar la cadena de suministro, elevando los estándares de sus proveedores.

La notificación de los incidentes críticos es muy importante porque permite darles una respuesta adecuada para evitar que escalen, se propaguen y contagien al resto de la industria y las cadenas de suministro. Esta información nos permitirá como país tener más claro y actualizado el mapa de riesgos reales en materias de seguridad.



SOLEDAD BASTÍAS, *GERENTA DE CIBERSEGURIDAD IT/OT Y RIESGO TECNOLÓGICO, CODELCO*

La coordinación entre los actores clave de las industrias y la Agencia Nacional de Ciberseguridad (ANCI) es fundamental para garantizar la protección de los activos digitales y la resiliencia de los sistemas.

Uno de los principales desafíos es establecer criterios claros y unificados para las notificaciones, que respondan a preguntas como: ¿Qué tipo de incidentes se deben reportar? ¿Qué información debe incluirse? ¿Cuál es el plazo? ¿Qué acciones se desencadenan al reportar o no reportar?

Será necesario reforzar y operativizar esta línea de notificación con una estrategia que incluya capacitar a los integrantes de la Corporación con etapas como la sensibilización, el conocimiento del estándar y procedimiento, la puesta en práctica y evaluación, y la mejora continua.

FELIPE CÁCERES, *SUPERINTENDENTE DE TECNOLOGÍA, KINROSS LA COIPA*

Kinross Gold (corporativo) cuenta con una sólida estrategia de ciberseguridad y protocolos de respuesta y acción frente a ataques y amenazas cibernéticas, que se aplican en Chile. Esto incluye los protocolos de notificación y reportabilidad.

Nuestro foco y atención estarán concentrados, primero, en promover la cultura de ciberseguridad con toda la comunidad de usuarios, lo que implica seguir con los planes de entrenamiento y concientización.

Y, segundo, asegurar la protección de nuestros activos operacionales (mina y planta), lo que implica la separación de servicios, redes, equipos e infraestructura para reducir el riesgo de ataques o intervenciones no deseadas.

KATHERINA CANALES, *DIRECTORA EJECUTIVA, CORPORACIÓN DE CIBERSEGURIDAD MINERA (CCMIN)*

La obligación de notificar incidentes críticos puede generar preocupaciones sobre la exposición de información sensible y la reputación de la empresa, la que debe equilibrar la transparencia con el manejo de su imagen.

Segundo, implementar un sistema eficaz de notificación requiere invertir en tecnología y capacitación del personal: muchas compañías pueden enfrentar desafíos para adaptar sus procesos.

Por último, diversas leyes vigentes imponen la obligación de notificar incidentes a múltiples entidades gubernamentales y reguladoras. Esto puede resultar complejo si no se establece una ventanilla única de reporte por parte de la autoridad. La falta de claridad en los protocolos de comunicación puede generar incertidumbre y representar una carga excesiva para las empresas.

NICOLE ALMUNA, *ABOGADA SÉNIOR, LUNDIN*

"El plazo para emitir una alerta dentro de las primeras tres horas desde que se conoce el incidente es ajustado, considerando la burocracia interna de las organizaciones (por su envergadura), y la necesidad de coordinación interna y de cumplir estándares de diligencia, lo que puede dificultar el cumplimiento oportuno de la norma. No solo se deberán crear nuevas estructuras para enfrentar ciberataques, sino también optimizar los procesos internos para responder.

También inquieta la interpretación del plazo para reportar, que comienza 'desde que se tiene conocimiento de la ocurrencia del ciberataque'. ¿Basta que cualquier trabajador detecte un posible incidente, o el plazo empieza a correr cuando es conocido por los delegados?

Otra incertidumbre es el contenido de los reportes, lo que complica la estimación de personal y tiempo necesarios para elaborarlos, y lleva a las empresas a disponer recursos no contemplados".

MANUEL DÍAZ, *HEAD OF LEGAL & COMPLIANCE, GOLD FIELDS*

En ciertos casos, es difícil medir la potencialidad de un incidente en las tres primeras horas. Esto podría acarrear una sobrerreportabilidad, desviando recursos, o una alta aplicación de sanciones por no reportar. Debiera primar un estándar técnico que minimice criterios subjetivos.

Por otra parte, la ley establece que la Agencia dictará las instrucciones para el contenido del reporte, sobre lo que aún no se tiene certeza.

Respecto a la confidencialidad, uno de los aspectos más delicados es que queda al criterio de la Agencia o el CSIRT si difunde y qué puede difundir de los casos que conozca, lo que podría ser un desincentivo, asociado a riesgos (como de reputación e incumplimiento de contratos con proveedores), que finalmente pueden ocasionar perjuicios a las compañías.

CARLOS SCHIPMANN, *GERENTE IM CHILE / IM REGIONAL, ANGLO AMERICAN*

La Ley de Ciberseguridad establece la necesidad de notificar incidentes con efectos significativos, es decir, aquellos que puedan interrumpir la continuidad de un servicio esencial.

Esperamos que en el reglamento se especifique claramente cuáles serán los criterios para determinar la relevancia de dichos incidentes, así como el procedimiento exacto para informarlos.

NESTOR STRUBE, *GERENTE GENERAL, ITQ LATAM*

Proteger su infraestructura crítica es una obligación para las mineras. No hacerlo ocasionaría grandes daños económicos, afectando la operación con millonarias pérdidas por cada hora sin operar. Además, pone en riesgo la seguridad física, pudiendo llegar a afectar vidas humanas. Las mineras deben exigir a sus proveedores planes sólidos y actualizados de ciberseguridad; si no, se convierten en una puerta de entrada a los sistemas, con las consecuencias que conlleva. Además, tener al personal capacitado en procedimientos, procesos, riesgos y políticas de ciberseguridad, independiente de su nivel o jerarquía, es clave. No estar concientizado es una de las formas más comunes de vulnerar sistemas e información crítica".

EZEQUIEL FAGETTI, *GERENTE DE CIBERSEGURIDAD, BHP MINERALS AMERICAS*

Día a día se enfrentan incidentes tecnológicos, por lo que es importante establecer claramente qué tipo de ellos hay que reportar y los tiempos de análisis, ya que se necesita un lapso para realmente entender lo que está sucediendo.

En cuanto a la confidencialidad, pese a que las autoridades tendrán medidas, al ser comunicaciones digitales, siempre existen riesgos de filtraciones, las que, en momentos no oportunos, pueden dar ventaja a los atacantes, además de daños reputacionales.

En cuanto al tiempo de reportabilidad, los procesos de respuesta y análisis de los incidentes requieren 100% de foco para expulsar a los potenciales atacantes y recuperar los sistemas con mínimo impacto, por lo que los procesos de reporte y confidencialidad deben garantizar que las empresas no pierdan el foco de la defensa por motivos de cumplimiento.

ANDRÉS PINTO, *GERENTE DE DIGITALIZACIÓN E IT, SQM*

Hemos venido robusteciendo nuestra ciberseguridad en los últimos cinco años en tres líneas: *awareness*, seguridad en los proyectos y gestión de vulnerabilidades e incidentes.

Varios de nuestros procesos críticos han sido certificados bajo estándares internacionales de ciberseguridad, como ISO 27001 y Tisax, entre otros.

La obligación de notificar incidentes es una práctica internacional que ha ido tomando fuerza y se ve, por ejemplo, en EE.UU. y Europa. Como multinacional, entendemos que adaptar e implementar las mejores prácticas y reportar a un organismo estatal es parte de ello.

Es de suma importancia también el tratamiento y uso de los datos; la colaboración absoluta con la Agencia es indispensable para así robustecer y permitirle la gestión correspondiente.