Bolivia abre planta de litio; busca liderar el mercado

El país sudamericano pretende producir hasta 2025-2026 unas 100 toneladas de carbono de litio en Oruro y Potosí

EFE
BOLIVIA

El Gobierno de Bolivia puso en marcha un complejo industrial que producirá 15.000 toneladas métricas de carbonato de litio por año en el suroeste del país, esto para cumplir con la meta de convertirse en uno de los "productores más importantes" del elemento en el mundo.

La primera planta industrial boliviana de carbonato de litio fue emplazada en la localidad de Llipi, en el municipio de Colcha K, al borde del salar de Uyuni, donde se encuentra la principal reserva del país, en la región andina de Potosí.

El evento fue liderado por el presidente de Bolivia, Luis Arce, y su ministro de Hidrocarburos y Energías, Franklin Molina, junto a funcionarios de la estatal Yacimientos de Litio Bolivianos (YLB) y pobladores de Colcha K y el municipio vecino de Uyuni, entre otros. En su discurso, Arce destacó que "hoy es un día histórico", pues además de inaugurar las actividades del complejo industrial, el país da "un paso trascendental" en su vida económica" al "entrar de plano al proceso industrializador" del litio.

"Contra todos y contra todo hemos concluido el trabajo y empieza a producir nuestra planta de litio, porque el pueblo lo que necesita son este tipo de obras", expresó.

El mandatario indicó que inicialmente se calculó un presupuesto de 669 millones de bolivianos (unos 96 millones de dólares) para la planta, pero se superó "con creces esta inversión para hacerla funcional".

Según Arce, "esto es clave" porque el complejo es administrado por YLB y lo que se quiere es que la estatal "compita con esa tecnología con las empresas extranjeras que han decidido" invertir en la producción del litio boliviano.

Luis Gandarillas | EFE

Yacimiento de litio en Bolivia.

Se eleva el costo de la vulneración de datos

Solo en el 2023, el costo de una filtración de datos en América Latina alcanzó los $2,46 millones, es decir, un aumento del 76% desde 2020

Mirta Rodríguez
mrodriguez@laestrella.com.pa
PANAMÁ

El informe sobre vulneración de información titulado "Cost of a Data Breach" revela que en 2023, el costo promedio de una filtración de datos en América Latina alcanzó un máximo histórico de 2,46 millones de dólares.

La cifra anterior representa un aumento del 76% desde 2020, arroja el estudio que recoge las experiencias de más de 550 organizaciones afectadas por una vulneración de datos. En los resultados, la infiltración malintencionada lidera el ranking de costos, con ataques de "insiders" maliciosos alcanzando los 2,59 millones de dólares.

A estos les siguen de cerca los ataques con credenciales robadas o comprometidas (2,56 millones de dólares.), mientras que la pérdida accidental o robo de datos y dispositivos se posiciona en tercer lugar, con un costo aproximado de 2,51 millones de dólares.

De acuerdo con el estudio, realizado por Ponemon Institute y analizado por IBM Security, los costos asociados con la detección y el escalamiento se han duplicado en el período, representando la porción más significativa de los gastos en las filtraciones.

Indica que este cambio sugiere una evolución hacia investigaciones más complejas y la necesidad de estrategias de seguridad más avanzadas.

En conclusión, es fundamental considerar estrategias avanzadas de ciberseguridad, con el objetivo de reducir estos riesgos. El costo medio mundial de una vulneración de datos en 2023 fue de 4,45 millones de dólares, un aumento del 15% en 3 años.

"La identificación y contención de las filtraciones de datos tardaron en promedio 339 días, destacando la importancia de mejorar la velocidad de respuesta para minimizar el impacto financiero y reputacional. Con el uso de inteligencia artificial, podemos reducir ese tiempo a 245 días", dijo Diana Robles, líder de IBM Security para el norte de Suramérica.

Entre los principales resultados de la investigación se determinó cómo se identifican las vulneraciones: por parte del propio equipo de seguridad de una organización, un tercero benigno como fuerzas policiales o el atacante, cómo la automatización y la Inteligencia Artificial (IA) en torno a la seguridad reducen los costos y los tiempos de respuesta; el impacto financiero y temporal de la participación de las fuerzas policiales en la respuesta a un ataque de ransomware; y los efectos sobre el costo y el tiempo de los recursos, incluida la información de seguridad y la supervisión de sucesos, la gestión de la superficie de ataque y la inteligencia de amenazas.

Según el estudio, el ahorro medio para las organizaciones que utilizan ampliamente la IA y la automatización de la seguridad es de 1,76 millones de dólares en comparación con las organizaciones que no lo hacen.

Pixabay

Las empresas invierten en automatización de la seguridad $1,76 millones en comparación con las organizaciones que no lo hacen.

Se estima además que el 51% de las organizaciones tiene previsto aumentar sus inversiones en seguridad como consecuencia de una vulneración, incluyendo la planificación y las pruebas en materia de respuesta de incidencias (IR), la formación de los empleados y las herramientas de detección y respuesta a amenazas.

El análisis señala además que para abordar estos desafíos, es esencial tener en cuenta algunos retos clave:

Escasez de especialistas: la demanda de profesionales en seguridad de la información supera la oferta, subrayando la importancia de abordar la brecha de habilidades en el campo de la ciberseguridad.

Más y nuevas amenazas: la multiplicación de ciberataques en frecuencia, complejidad y finalidad destaca la necesidad de estrategias y tecnologías más avanzadas.

Infoxicación: la sobrecarga cognitiva debido a la información diversa sobre amenazas exige un enfoque claro y relevante en la seguridad operativa.

Relevancia en la seguridad operativa: centrarse en la prevención no es suficiente, tenemos que detectar, responder y recuperarnos de las amenazas.

Soluciones de seguridad insuficientes: soluciones de inteligencia actuales no abordan el riesgo empresarial, sin contexto, priorización, duración limitada y enfoque limitado.

Tecnología por si sola es insignificante: se necesitan los procesos, herramientas adecuadas, profesionales para convertir datos y novedades en inteligencia y conocimientos.

"Los cibercriminales operan sin restricciones de horario y su motivación ha evolucionado de la búsqueda de prestigio a intereses financieros, sociales y políticos. La agilidad, la organización y la cooperación entre ellos han aumentado, representando desafíos significativos para la ciberseguridad", añade Gustavo Calderón, gerente de entrega de Ciberseguridad de GBM.

Estos y otros hallazgos relacionados con ciberseguridad se dieron a conocer durante el reciente Cybe Next, un evento híbrido desarrollado por GBM, en el cual se abordaron una amplia gama de temas, desde tendencias emergentes y nuevas tecnologías hasta técnicas de mitigación de riesgos, de la mano de especialistas de empresas como GBM, IBM, Cisco y Checkmark.

Este espacio sirvió como punto de encuentro para profesionales y organizaciones de las industrias de banca y finanza, manufactura, sector público, *retail* y telecomunicaciones, entre otras.

"El GBM Cybersecurity Center cuenta con la confianza de más de 35 empresas, analizando más de 700 millones de eventos diarios desde más de 20 fuentes de inteligencia; respaldado por más de 100 especialistas de ciberseguridad en la región", destacó Alonso Ramírez, gerente regional de Ciberseguridad de GBM.

Brasil presenta al G20 su agenda económica socioambiental

Tatiana Rosito, de Finanzas del G20, explicó que la agenda **propuesta** para 2024 ha tenido "una muy buena acogida" entre los delegados

EFE
BRASIL

Brasil, que ostenta la presidencia anual del G20, terminó de presentar este viernes la agenda que le plantea al grupo de Finanzas de ese organismo, que pone un fuerte acento en la reducción de las desigualdades y la protección del planeta.

Tatiana Rosito, representante de Brasil en el grupo de trabajo de Finanzas del G20, explicó que la agenda de debates que su país propuso para 2024 ha tenido "una muy buena acogida" entre los delegados de las mayores economías del mundo y está alineada con los grandes asuntos que se discuten en la comunidad internacional.

"Son temas que expresan los principales desafíos globales", dijo Rosito en una rueda de prensa en la Cancillería brasileña, sede de estas primeras discusiones, preparatorias de una cita ministerial del G20 prevista para fines del próximo febrero en São Paulo.

Según Rosito, esos grandes asuntos pasan por promover una mayor inclusión social, combatir las desigualdades en los ámbitos internos pero también entre los países, financiar la transición energética y abordar la reforma de los organismos financieros globales a fin de dar mayor representación a las economías emergentes, entre otros puntos.

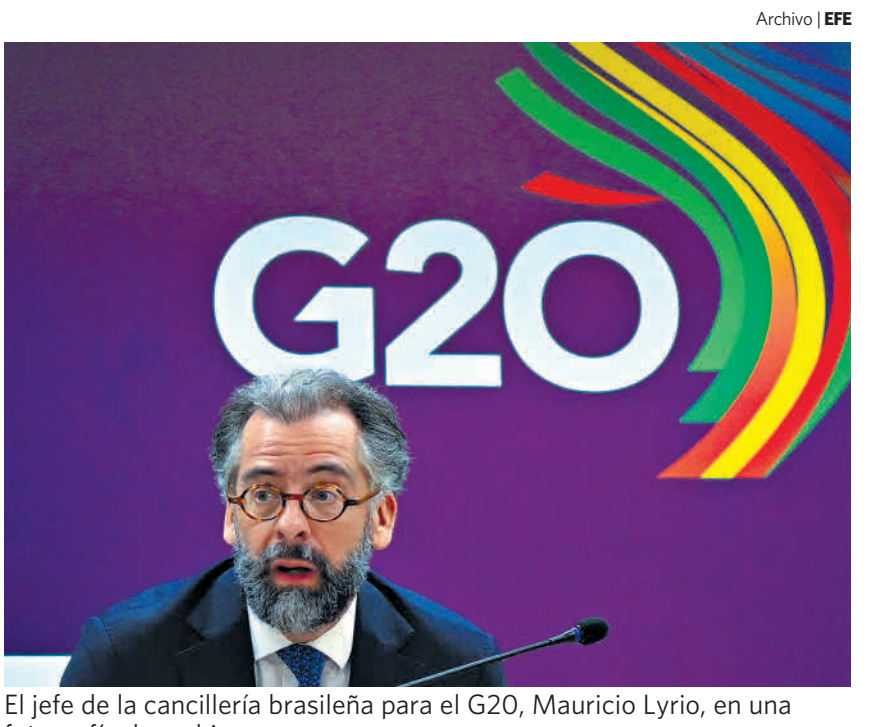
La delegación brasileña también ha puesto sobre la mesa lo que Rosito calificó de "imperiosa necesidad" de encontrar "soluciones estructurales para el problema de la deuda de los países más pobres", que atenaza sus posibilidades de desarrollo.

Asimismo, Brasil ha planteado avanzar en la discusión sobre los fondos globales volcados a mitigar los efectos del cambio climático y hacia la construcción de "una arquitectura financiera" que vuelque a organismos como el Fondo Monetario Internacional (FMI) o el Banco Mundial a acciones de apoyo al cuidado del planeta.

El grupo de Finanzas del G20 está integrado por viceministros de Economía y vicepresidentes de bancos centrales, que en los próximos meses mantendrán consultas permanentes sobre la agenda definitiva que se discutirá en la reunión ministerial de febrero.

El G20 está formado por Alemania, Arabia Saudí, Argentina, Australia, Brasil, Canadá, China, Corea del Sur, Estados Unidos, Francia, la India, Indonesia, Italia, Japón, México, el Reino Unido, Rusia, Sudáfrica y Turquía, además de la Unión Europea y la Unión Africana.

Archivo | EFE



El jefe de la cancillería brasileña para el G20, Mauricio Lyrio, en una fotografía de archivo.