

política de seguridad de sistema de control industrial

GNLM considera su política de seguridad del sistema de control industrial SCI en base a los siguientes principios fundamentales:

- ▶ en un campo en el que se experimentan cambios tecnológicos rápidos y una evolución dinámica de las amenazas, es importante mantener una seguridad efectiva y de largo plazo del SCI.
- ▶ el nivel de seguridad y resiliencia del SCI, debe ser capaz de cubrir los riesgos relevantes que pueden resultar en un impacto a la continuidad de las operaciones vitales del SCI.
- ▶ crear una cultura informando y formando sobre la seguridad a los usuarios del SCI de GNLM, ayuda a entender las necesidades en materia de ciberseguridad y poseer las habilidades necesarias para responder frente a un supuesto incidente de seguridad.
- ▶ incluir los requisitos de seguridad en los procesos de mantenimiento, cambios, adquisición, e inventarios de los componentes del SCI, permite realizar un trabajo con seguridad y cubrir los riesgos.

En este contexto GNLM define las siguientes directrices que deben ser aplicadas para todos y cada uno de los profesionales, internos o externos, que lleven a cabo acciones que puedan tener impacto en la seguridad del SCI:

- ▶ fomentar a los colaboradores y usuarios de los activos del SCI a dar cumplimiento a los controles de la política SCI.
- ▶ mantener y asegurar las competencias del personal administrador y usuarios del SCI, generando planes de sensibilización y entrenamientos dentro de los alcances declarados.
- ▶ asegurar las instalaciones, controlar los accesos, proteger información sensible y tomar las medidas indispensables para asegurar la continuidad de los sitios y sistemas del SCI.
- ▶ seguir las recomendaciones de cuerpos internacionales que han sido reconocidos en el campo de seguridad de SCI y los principios del estándar IEC 62443 relacionado con sistemas de administración de seguridad cibernética.
- ▶ se prohíbe la navegación por internet mediante las estaciones de operación, estaciones de ingeniería y cualquier otro dispositivo que componga el SCI.
- ▶ se prohíbe la tecnología wireless en el SCI del terminal.



Bernardo Echavarría
gerente recursos humanos



Jean-Michel Cabanes
gerente general