Coordinador Eléctrico da paso en estrategia de ciberseguridad: **unidad supervisará avances**


JULIO CASTRO

El 6 de enero se aprobó la creación de esta área, que reportará directamente al Consejo Directivo, buscando darle independencia a su función.

POR KAREN PEÑA C.

El desarrollo de las nuevas tecnologías ha puesto en el sistema eléctrico -así como en otras áreas de la economía- a la ciberseguridad como un elemento estratégico. Y dentro de los pasos que se han venido dando para mejorar los estándares, el Coordinador Eléctrico Nacional tomó una decisión relevante para supervisar los avances.

El consejo directivo del Coordinador tomó la decisión de crear una nueva dependencia dentro de la estructura organizacional: la Unidad de Ciberseguridad e Infraestructura crítica. Esto, luego de que en octubre se lanzara el estándar de ciberseguridad para el sector, en que se establecen requisitos y medidas de control -tanto para el organismo como para las empresas que participan en el sistema-, para proteger las instalaciones eléctricas y activos informáticos contra amenazas que puedan poner en riesgo la seguridad y continuidad del sistema eléctrico nacional.

Según consigna el acta de la sesión extraordinaria del consejo directivo del Coordinador Eléctrico, que se realizó el pasado 6 de enero, el director ejecutivo de la entidad, Rodrigo Bloomfield, planteó la necesidad de crear esta nueva unidad dependiente del consejo directivo, la que ya había sido comunicada a la organización el 18 de diciembre, abriendo un canal para recoger la opinión de los colaboradores.

De acuerdo al documento, los consejeros dejaron constancia que la creación de la unidad "consagra la importancia e independencia necesaria a la gobernanza de la ciberseguridad dentro del Coordinador, en línea con los más altos estándares de la materia".

Esto, porque la nueva posición -que aún no tiene un encargado definitivo, a la espera de que se haga el proceso de selección- supervisará los avances de la implementación de los nuevos estándares que se definieron para el sistema, tanto en el Coordinador como en las empresas que son miembros. Por eso era relevante que reportara directamente al consejo de la organización.

"La misión principal de quien sea designado como jefe de dicha unidad, será la implementación del estándar NERC-CIP, tanto internamente como en las tareas que le competen al Coordinador en cuanto al monitoreo del cumplimiento de dicho estándar por parte de las empresas coordinadas", se sostiene en el acta.

El consejo del organismo independiente que supervisa el funcionamiento del sistema eléctrico dio por unanimidad luz verde a la posición.

> El mecanismo elegido "consagra la importancia e independencia necesaria a la gobernanza de la ciberseguridad dentro del Coordinador".

> Las más de 500 empresas coordinadas del sistema eléctrico deberán cumplir una serie de requisitos en cuanto a ciberseguridad.

El estándar del Coordinador

Los riesgos cibernéticos del sistema es un tema que se maneja en completo hermetismo, por los efectos que podrían traer. De todos modos, ha habido casos puntuales conocidos.

Por ejemplo, en 2020, trascendió que el grupo italiano Enel registró dos episodios de este tipo en menos de un año, lo que llamó la atención de la industria y las autoridades, incluso a nivel local.

Por esto, aunque hasta el momento los incidentes no han provocado impactos en el sistema eléctrico -como sí se ha visto en otras industrias-, la preocupación por el tema se materializó en el estándar de ciberseguridad del sector.

En la elaboración se detalló que se analizaron las diferentes normativas internacionales existentes en materia de ciberseguridad para el sector eléctrico, y junto al apoyo especializado de CAISO (California Independent System Operator), el Coordinador ha definido adoptar el estándar CIP (Critical Infrastructure Protection) de NERC (North American Electric Reliability Corporation), un organismo independiente de Estados Unidos que ha creado un estándar que cubre tanto la seguridad física e informática del sistema. Esto -dicen conocedores del tema- da una mirada más completa para estos eventuales riesgos.

Según se detalló en su lanzamiento en octubre, las más de 500 empresas coordinadas del sistema eléctrico deberán cumplir una serie de requisitos en cuanto a ciberseguridad, como la autoevaluación de las medidas que toman en esta materia, además de entregar un reporte anual al Coordinador, quien podrá notificar los incumplimientos a la Superintendencia de Electricidad y Combustibles (SEC).

Entre los principales aspectos del documento, está el reporte de incidentes de este tipo a la SEC y al Coordinador, los cuales tendrán un carácter reservado para proteger la información relacionada con la ciberseguridad de las instalaciones del sistema.

Las claves del nuevo estándar

- En octubre del año pasado se presentó formalmente el estándar de ciberseguridad, que busca estandarizar un tema que organismos y empresas del sistema ya venían trabajando de algún modo.
- Cuando se comunicó esto, se estableció que se realizarán monitoreos y auditorías de la situación interna, con una autoevaluación y la entrega de reportes anuales de cumplimiento al Coordinador. Este organismo notifica a la SEC de cualquier incumplimiento. Además, se establece que cualquier incidente debe ser notificado a la Superintendencia y al Coordinador dentro de una hora de ocurrido. Todos los reportes son de carácter reservado a fin de proteger la información relacionada.