



We were able to draw up an effective and intelligent roadmap to limit cybersecurity vulnerabilities.



PROJECT SHEET CYBERSECURITY AUDIT (PHASE 1)

■ CLIENT

CENTRE INTÉGRÉ
UNIVERSITAIRE EN
SANTÉ ET SERVICES
SOCIAUX DE L'ESTRIE |
CENTRE HOSPITALIER
UNIVERSITAIRE DE
SHERBROOKE (CIUSS
DE L'ESTRIE ET CHUS)

■ CHALLENGE

Assess cybersecurity capacity in light of the Ministère de la Santé et des Services Sociaux's new framework

Execution

In collaboration with ESI Technologies, our team took a two-pronged approach: an audit through workshops plus penetration tests. First, as soon as the client approved the intervention protocol, we conducted a series of interviews with the teams responsible for each department. These workshops allowed us to collect the necessary cybersecurity data by keeping a complete record of the information provided and classifying it. To complement this information phase, we conducted penetration tests to find vulnerabilities that could come under attack. One of the big challenges of this mandate was the importance of complete data privacy.

Results

The audit through workshops combined with the penetration tests allowed us to draw a portrait of the CIUSSS de l'Estrie's cybersecurity health in relation to the new security framework based on ISO 27002. Thanks to this portrait, we were able to present our recommendations to the Board of Directors to improve the existing structure.

Resource person Joël Paradis