Cybersecurity Awareness and Training

Global Policy

OBJECTIVE

To establish an awareness and training program that allow us to foster a Cybersecurity culture amongst all of Sigma employees.

DEFINITIONS

Cybersecurity:
Procedures and tools implemented to protect information generated and processed through computers, servers, mobile devices, networks, and electric systems.

Social Engineering:
Techniques used by cybercriminals to trick unaware users to retrieve confidential data, damage their computer with malign programs or through infected websites.

Phishing, Vishing y Smishing:
Refers to e-mails (Phishing), phone calls (Vishing), or text messages (Smishing) sent by alleged trust sources – such as banks, companies, among others – who's intention is to manipulate the receptor to steal confidential information / credentials.

POLICY

The Information Security responsible of each Business Unit (hereinafter BU) shall define, plan, create, and implement a Cybersecurity awareness and training program.

Team leaders shall guarantee their participation in all Cybersecurity awareness and training sessions when required.

All employees shall complete their Cybersecurity training, assist to the scheduled meetings, and comply with the applicable policies, laws, and regulations.

Requirements:

The objective of the Cybersecurity program is to ensure all employees meet and maintain at least a basic comprehensive level of Cybersecurity matters, including general obligations in accordance with policies, procedures, guidelines, laws, regulations, contractual conditions, ethical norms, and acceptable behaviors.

The Information Security responsible of each BU shall identify critical areas and personnel who usually are or may be subject to cybernetic attacks, applying specific and advanced trainings to strengthen them. Employees who perform Cybersecurity functions shall be part of advanced programs in accordance with their role.

These programs will be part of the formation plans of each department and be financed as such. Formative requirements will reflect previous experience, education, and professional qualifications.

The Cybersecurity awareness and training activities shall be implemented from the onboarding process. All employees shall participate in an induction to Cybersecurity course (live or virtually) defined by the Information Security responsible of each BU.

Whenever necessary and feasible, the awareness and training materials and activities shall be adapted to each region where we operate in matters of language, culture, style, formats, complexity, technical content, among others.

The Information Security responsible of each BU shall provide employees the location of the Cybersecurity awareness and training material, local security policies, and guidelines. Additionally, the Information Security responsible of each BU shall provide guidance and orientation in Cybersecurity matters when needed.

Cybersecurity Awareness:

The Information Security responsible of each BU shall foster and strengthen Cybersecurity awareness at Sigma, through communication channels / material such as:

- E-mails with relevant Cybersecurity news, notices, guides, and recommendations.
- Live or virtual seminars to attend specific Cybersecurity matters.

- Audiovisual content.

Cybersecurity Trainings:

All Sigma employees, when hired and every year since then, shall successfully complete the assigned Cybersecurity trainings. Critical areas and personnel may be required to complete additional modules in accordance with their role.

Employees will have 15 workdays to complete each training, not counting vacations and holydays.

The Information Security responsible of each BU shall notify employees as soon as a training is assigned, sending additional reminders before the final day is due. If an employee fails to successfully complete a training within the defined timeframe, the corresponding Information Security responsible and Human Capital responsible shall apply an adequate sanction to prevent its recurrence.

Social Engineering Simulations:

The Information Security responsible of each BU shall perform periodic simulated attacks (Phising, Vishing, Smishing, USB tests, physical evaluations, among others). These tests will be executed in accordance with an annual schedule defined and known only by the Information Security responsible of each BU. Simulations may be specifically directed to critical departments or personnel, considering the risk of being targeted by a real attack.

If an employee fails to prevent a simulated attack, he / she will be immediately notified by the Information Security responsible of the corresponding BU, who shall specify the actions required to strengthen his / her position. The purpose of these actions is to reinforce the level of awareness and required training by the employee, to protect Sigma's data and information assets.

If the employee fails to comply, despite the additional trainings, corrective actions will be applied alongside the Human Capital responsible of the BU (i.e. warnings from immediate supervisor, temporal account blockage, among others).

The Information Security responsible of each BU shall foster a recognition program for employees who exceed expectations on the Cybersecurity program.