"CYBERSECURITY SURVEY APPLIED TO NUCLEAR AND RADIOACTIVE FACILITIES" VERSION 6

OBJECTIVE:
This survey will assess the maturity of the state of cybersecurity at CCHEN regulated facilities, to gain an overview of the cybersecurity posture in the sector.

TARGET AUDIENCE:
The Legal Representative must designate a coordinator who is in charge of coordinating the survey responses with the support of: facility operators, radiation protection officers, IT professionals, security personnel, operations manager.

ACRONYMS AND DEFINITIONS:

- **Secure area:** Area where critical, confidential or sensitive information is stored.
- **Critical, confidential or sensitive information:** Sensitive information for national security, such as: nuclear or radioactive inventory, plans and location of sites with nuclear and radioactive material, procedures or security plans for facilities.
- **NDA:** Non-Disclosure Agreement.
- **ISMS:** Information Security Management System. SGSI in Spanish.
- **IT:** Information Technologies. TI in Spanish.
- **ICT:** Information and Communication Technologies. TIC in Spanish.
- **OT:** Operations technology. TO in Spanish.
- **ICS:** Specialized industrial control systems.
- **CSP:** Information Security Plan.

REFERENCES:

- ISO/IEC 27001 de seguridad de la información.
- Norma CCHEN “Norma de Informática y Política de Seguridad de la Información” V6.0 nov2018.
- IAEA Nuclear Security Series No. 23-G Seguridad en la información nuclear.
- IAEA Nuclear Security Series No. 17 Seguridad informática en las instalaciones nucleares.

TABLE OF CYBERSECURITY LEVELS

Level	Aspect	% compliance		Description
X	Does not apply	X		The element does not apply in the organization.
0	Unanswered	0%		You don't have the item or don't know if it exists. Because? There is no information about it.
1	Initial	0%	20%	This key element exists but is not formally approved or implemented as part of the Cybersecurity System. Little implemented.
2	Repeatable or Planned	20%	40%	(1) + It is formally planned and approved. Activities are scheduled. Partially implemented.
3	Defined or Executed	40%	60%	(2) + It is executed and implemented as approved and planned. Moderately implemented.
4	Managed or Verified	60%	80%	(3) + The actions associated with the execution are monitored and measured. Highly implemented.
5	Optimized or Feedback	80%	100%	(4) + Feedback is given and action is taken to improve performance. Fully implemented.

1. **ISMS: Does the entity have an Information Security Management System in operation?**
   The organization establishes, implements, maintains and continuously improves its information security management system (ISMS).
   Information security is achieved by implementing an appropriate set of controls, including policies, processes, procedures, organizational structures, and software and hardware functions.

   - X Not applicable.
   - 0 No answer.
   - 1 Initial level.
   - 2 Repeatable or planned level.
   - 3 Level defined or executed.
   - 4 Level managed or verified.
   - 5 Optimized or feedback level.

   Observations or justifications:_____

2. **ISMS: Does the entity have an ISMS operating with the support of top management?**
   The information security management system (ISMS) is sponsored by the highest authority or owner of the entity, and the highest manager assumes the residual risk resulting from having applied all the controls established by the ISMS.

   - X Not applicable.
   - 0 No answer.
   - 1 Initial level.
   - 2 Repeatable or planned level.
   - 3 Level defined or executed.
   - 4 Level managed or verified.
   - 5 Optimized or feedback level.

   Observations or justifications:_____

3. **Organizational controls: Is there a matrix of roles and responsibilities related to information security?**
   The matrix of roles and responsibilities corresponds to the functions performed by the different people in terms of information security. They can be people dedicated to security or people who have different positions, but who have some role or responsibility in the event of a cybersecurity incident.

   - X Not applicable.
   - 0 No answer.
   - 1 Initial level.
   - 2 Repeatable or planned level.
   - 3 Level defined or executed.
   - 4 Level managed or verified.
   - 5 Optimized or feedback level.

   Observations or justifications:_____

4. **Organizational controls: Is there a classification of your information assets in terms of their criticality, sensitivity or confidentiality?**
   The objective is to ensure that the information receives the appropriate level of protection according to its importance to the organization, and thus be able to design internal controls to prevent internal personnel who do not have the necessary privileges from accessing sensitive information.
   Information should be classified in terms of legal requirements, value, criticality, and sensitivity to unauthorized disclosure or modification. Information protection classifications and controls should consider the entity's needs to share or restrict information, as well as legal requirements. The owners of information assets should be responsible for their classification.
   In the case of nuclear and radioactive facilities, we have: inventory of nuclear and/or radioactive material, geographical location of the facilities, information associated with the transport of nuclear and/or radioactive material, authorizations, physical protection plans, among others.

   - X Not applicable.
   - 0 No answer.
   - 1 Initial level.
   - 2 Repeatable or planned level.
   - 3 Level defined or executed.
   - 4 Level managed or verified.
   - 5 Optimized or feedback level.

   Observations or justifications:_____

5. **Organizational controls: Is your infrastructure prepared for operational continuity in the event of a declared emergency?**
   The entity incorporates the fact that ICT readiness must be planned, implemented, maintained and tested based on the continuity of operations, maintaining ICT continuity objectives and requirements to ensure the availability of the organization's information and other associated assets in event of a service interruption.
   Business continuity strategies can comprise one or more solutions. Based on the strategies, plans must be developed, implemented and tested to meet the required level of availability of ICT services and in the required times after the interruption or failure of critical business processes.

   - X Not applicable.
   - 0 No answer.
   - 1 Initial level.
   - 2 Repeatable or planned level.
   - 3 Level defined or executed.
   - 4 Level managed or verified.
   - 5 Optimized or feedback level.

   Observations or justifications:_____

6. **Organizational controls: Does the entity perform independent information security reviews?**
   The goal is to ensure that information security is implemented and operated in accordance with the organization's policies and procedures. The organization's approach to managing information security and its implementation (i.e., control objectives, controls, policies, processes, and procedures for information security) should be independently reviewed at planned intervals or when significant changes occur.

   - X Not applicable.
   - 0 No answer.
   - 1 Initial level.
   - 2 Repeatable or planned level.
   - 3 Level defined or executed.
   - 4 Level managed or verified.
   - 5 Optimized or feedback level.

   Observations or justifications:_____

7. **Personnel Controls: Does the entity establish terms and conditions of employment related to information security?**
   Contractual agreements with employees and contractors should indicate their and the organization's responsibilities for information security. The contractual obligations of employees or contractors must reflect the organization's information security policies, among other aspects related to confidentiality, legal responsibilities, responsibilities regarding the classification of information, responsibilities for handling the information received from other companies or third parties and actions to be taken in case the employee or supplier does not comply with the information security policies.

   - X Not applicable.
   - 0 No answer.
   - 1 Initial level.
   - 2 Repeatable or planned level.
   - 3 Level defined or executed.
   - 4 Level managed or verified.
   - 5 Optimized or feedback level.

   Observations or justifications:_____

8. **Personnel controls: Does the entity carry out a cybersecurity awareness, education and training program?**
   Employees of the organization and, where applicable, contractors must receive appropriate education and awareness training and regular updates on the organization's policies and procedures, as appropriate to their job role.

   - X Not applicable.
   - 0 No answer.
   - 1 Initial level.
   - 2 Repeatable or planned level.
   - 3 Level defined or executed.
   - 4 Level managed or verified.
   - 5 Optimized or feedback level.

   Observations or justifications:_____

9. **Personnel Controls: Does the entity establish the obligation for its employees and suppliers to sign a confidentiality or non-disclosure agreement (NDA)?**
   Requirements for confidentiality and nondisclosure agreements that reflect the organization's needs for information protection should be identified, reviewed, and documented on a regular basis. Confidentiality non-disclosure agreements should address the requirement to protect confidential information using legally enforceable terms. Confidentiality or non-disclosure agreements apply to external parties or employees of the organization. Elements must be selected or added considering the type of the other party and the access that is allowed or the handling of confidential information.

   - X Not applicable.
   - 0 No answer.
   - 1 Initial level.
   - 2 Repeatable or planned level.
   - 3 Level defined or executed.
   - 4 Level managed or verified.
   - 5 Optimized or feedback level.

   Observations or justifications:_____

10. **Personnel Controls: Does the entity establish a secure remote work protocol?**
    It has implemented a policy and measures that support security to protect the information that is accessed, processed or stored on the telecommuting sites. Organizations that allow telework activities must issue a policy that defines the conditions and restrictions on the use of telework. [Law No. 21,220 - http://bcn.cl/2lz8x]

    - X Not applicable.
    - 0 No answer.
    - 1 Initial level.
    - 2 Repeatable or planned level.
    - 3 Level defined or executed.
    - 4 Level managed or verified.
    - 5 Optimized or feedback level.

    Observations or justifications:_____

11. **Personnel Controls: Does the entity establish a protocol for people to report information security events to its security teams?**
    Employees and contractors are aware of their responsibility to report information security events as soon as possible. They should also be aware of the procedure for reporting information security events and the point of contact to which events should be reported. System failures or other abnormal behavior can be an indicator of a security attack or actual security breach and should therefore always be reported as an information security event.

    - X Not applicable.
    - 0 No answer.
    - 1 Initial level.
    - 2 Repeatable or planned level.
    - 3 Level defined or executed.
    - 4 Level managed or verified.
    - 5 Optimized or feedback level.

    Observations or justifications:_____

12. **Physical Security Controls: Does the entity establish physical access controls to the places where the information is stored?**
    Secure areas are protected with appropriate entry controls to ensure that only authorized personnel are allowed access. In addition, access points such as delivery and loading areas and other points where unauthorized persons could enter the premises should be controlled and, if possible, isolated from the information processing facilities to prevent unauthorized access.

    - X Not applicable.
    - 0 No answer.
    - 1 Initial level.
    - 2 Repeatable or planned level.
    - 3 Level defined or executed.
    - 4 Level managed or verified.
    - 5 Optimized or feedback level.

    Observations or justifications:_____

13. **Physical Security Controls: Does the entity establish physical security monitoring of the places where the information is stored?**
    Physical facilities are monitored by surveillance systems, which may include guards, intrusion detection alarms, video monitoring systems such as CCTV, and physical security information and management software managed internally or by a monitoring service provider. Access to buildings that house critical systems must be continuously monitored for unauthorized access or suspicious behavior. The design of monitoring systems must be kept confidential, as disclosure could facilitate undetected security breaches. Any monitoring and recording mechanism must be used in accordance with current laws and regulations; this includes data protection, especially with regard to workers related to the monitoring system.

    - X Not applicable.
    - 0 No answer.
    - 1 Initial level.
    - 2 Repeatable or planned level.
    - 3 Level defined or executed.
    - 4 Level managed or verified.
    - 5 Optimized or feedback level.

    Observations or justifications:_____

14. **Physical security controls: Does the entity establish a clean screen policy?**
    A clean screen policy should be adopted during facility information processing. The objective of this control is to reduce the risks of unauthorized access, loss and damage to information by considering other accessible places during and outside normal working hours.

    - X Not applicable.
    - 0 No answer.
    - 1 Initial level.
    - 2 Repeatable or planned level.
    - 3 Level defined or executed.
    - 4 Level managed or verified.
    - 5 Optimized or feedback level.

    Observations or justifications:_____

15. **Physical Security Controls: Does the entity establish security in the installation of its cabling for the devices that handle information?**
    Electricity and telecommunications cables that carry data or support information services must be protected against interception, interference or damage (underground cabling or subject to adequate alternative protection).

    - X Not applicable.
    - 0 No answer.
    - 1 Initial level.
    - 2 Repeatable or planned level.
    - 3 Level defined or executed.
    - 4 Level managed or verified.
    - 5 Optimized or feedback level.

    Observations or justifications:_____

16. **Physical security controls: Does the entity establish and enforce a protocol for the safe disposal or reuse of devices?**
    All devices containing storage media must be verified to ensure that sensitive data and licensed software have been securely removed or overwritten prior to disposal or reuse.

    - X Not applicable.
    - 0 No answer.
    - 1 Initial level.
    - 2 Repeatable or planned level.
    - 3 Level defined or executed.
    - 4 Level managed or verified.
    - 5 Optimized or feedback level.

    Observations or justifications:_____

17. **Physical security controls: Is a security perimeter defined and used to protect areas containing critical information and other associated assets?**
    The facilities must have a definition of security perimeters. The location and strength of each of the perimeters should depend on the security requirements of the assets within the perimeter and the results of a risk assessment.

    - X Not applicable.
    - 0 No answer.
    - 1 Initial level.
    - 2 Repeatable or planned level.
    - 3 Level defined or executed.
    - 4 Level managed or verified.
    - 5 Optimized or feedback level.

    Observations or justifications:_____

18. **Physical security controls: Have you designed and implemented security procedures for working in secure areas?**
    The following guidelines must be considered in the procedure: the identity of employees and visitors must be authenticated by an appropriate means, the date and time of entry and exit of employees and visitors must be recorded, the access of employees and visitors must only be be granted for specific and authorized purposes and must be issued with instructions on the security requirements of the area and on emergency procedures, employees and visitors must be supervised unless an explicit exception is granted.

    - X Not applicable.
    - 0 No answer.
    - 1 Initial level.
    - 2 Repeatable or planned level.
    - 3 Level defined or executed.
    - 4 Level managed or verified.
    - 5 Optimized or feedback level.

    Observations or justifications:_____

19. **Physical security controls: Do you have protection against power outages and other interruptions caused by utility failures?**
    The loss, damage or compromise of information and other associated assets due to the failure and interruption of public support services or the interruption of the operations of the organization must be avoided.

    - X Not applicable.
    - 0 No answer.
    - 1 Initial level.
    - 2 Repeatable or planned level.
    - 3 Level defined or executed.
    - 4 Level managed or verified.
    - 5 Optimized or feedback level.

    Observations or justifications:_____

20. **Physical Security Controls: Is there a maintenance program for the equipment that makes up the security system?**
    The organization must have a maintenance program in place with resources to maintain normal operation. There must be periodic reviews of the hardware and its components.

    - X Not applicable.
    - 0 No answer.
    - 1 Initial level.
    - 2 Repeatable or planned level.
    - 3 Level defined or executed.
    - 4 Level managed or verified.
    - 5 Optimized or feedback level.

    Observations or justifications:_____

21. **Technological controls: Does the entity establish and apply protocols to restrict access to information?**
Access to information and application system functions should be restricted in accordance with the access control policy. Access restrictions should be based on the requirements of individual business applications and in accordance with the defined access control policy.

- X Not applicable.
- 0 No answer.
- 1 Initial level.
- 2 Repeatable or planned level.
- 3 Level defined or executed.
- 4 Level managed or verified.
- 5 Optimized or feedback level.

Observations or justifications:_____

22. **Technological controls: Does the entity establish and apply protocols and technologies for secure authentication?**
When required by the access control policy, access to systems and applications should be controlled through a secure login procedure. An appropriate authentication method must be selected to verify the identity that a user claims to have: Strong password policy, two-factor authentication, data encryption.

- X Not applicable.
- 0 No answer.
- 1 Initial level.
- 2 Repeatable or planned level.
- 3 Level defined or executed.
- 4 Level managed or verified.
- 5 Optimized or feedback level.

Observations or justifications:_____

23. **Technological Controls: Does the entity establish and apply protocols and protection technologies against malware (ransomware, viruses, phishing, among others)?**
Detection, prevention, and recovery controls are implemented to protect against malware in combination with proper user awareness. Protection against malware should be based on malware detection and repair software controls, information security awareness, proper system access, and change management.

- X Not applicable.
- 0 No answer.
- 1 Initial level.
- 2 Repeatable or planned level.
- 3 Level defined or executed.
- 4 Level managed or verified.
- 5 Optimized or feedback level.

Observations or justifications:_____

24. **Cybersecurity: Does the entity use secure communication methods for the transfer of confidential data?**
The use of cryptography on web sites or systems has several objectives, among which are to safeguard the confidentiality of the information exchanged between the web site or system and the user, alert of any possible problem that is affecting the integrity of the information , or provide reliable information about the entity that owns the system. As an example, the most visible and common within the Internet environment is the use of HTTPS.

- X Not applicable.
- 0 No answer.
- 1 Initial level.
- 2 Repeatable or planned level.
- 3 Level defined or executed.
- 4 Level managed or verified.
- 5 Optimized or feedback level.

Observations or justifications:_____

25. **Cybersecurity: Does the entity monitor the security performance of the servers?**
These measures should include proper definition of server users versus administrators, enforcing access controls on program and system directories and files, and enabling audit logging, particularly of security and other events. of server failure. the system.

- X Not applicable.
- 0 No answer.
- 1 Initial level.
- 2 Repeatable or planned level.
- 3 Level defined or executed.
- 4 Level managed or verified.
- 5 Optimized or feedback level.

Observations or justifications:_____

26. **Cybersecurity: Does the entity ensure that end users use software applications and operating systems duly updated with the most recent security patches?**
Users must use compatible operating systems with the latest security patches that have been installed. Users are responsible for knowing and following the organization's policy regarding supported operating systems. In all cases, the operating system must be up to date with at least security patches. This applies equally to software applications. That is, Windows and Office must be updated with their patches up to date, for example.

- X Not applicable.
- 0 No answer.
- 1 Initial level.
- 2 Repeatable or planned level.
- 3 Level defined or executed.
- 4 Level managed or verified.
- 5 Optimized or feedback level.

Observations or justifications:_____

27. **NST 17: Does the entity have a complete security system life cycle program that includes the design, implementation, all operational modalities and disposition of the system?**
    These lifecycle phases and multiple modes of operation may require different systems and operating environments. For example, periods of heavy maintenance often require equipment replacement, modification, and testing, or may require additional personnel and third-party/subcontractor access. This diversity must be taken into account in the Information Security Plan (CSP). In particular, the diversity of life stages could require extensive revisions to the CSP.

    - X Not applicable.
    - 0 No answer.
    - 1 Initial level.
    - 2 Repeatable or planned level.
    - 3 Level defined or executed.
    - 4 Level managed or verified.
    - 5 Optimized or feedback level.

    Observations or justifications:_____

28. **NST17: Does the entity establish the actions and separations between computer systems, surveillance systems and industrial control systems (SCADA/HMI/PLC)?**
    Computer systems and network architectures that support industrial operations and/or controls are not standardized computer systems in terms of architecture, configuration, or behavioral requirements. These systems can be classified as specialized industrial control systems (ICS). Although ICS has moved from strictly proprietary applications to more generalized computing architectures, there are still major differences between ICS and standard IT systems that must be considered in any CSP.

    - X Not applicable.
    - 0 No answer.
    - 1 Initial level.
    - 2 Repeatable or planned level.
    - 3 Level defined or executed.
    - 4 Level managed or verified.
    - 5 Optimized or feedback level.

    Observations or justifications:_____

29. **NST17: Does the entity have a risk assessment program associated with additional connectivity needs?**
    The need for remote scanning, maintenance, or updates can also lead to similar vulnerabilities. Before tackling any additional connectivity demands, you should perform a detailed risk analysis.

    - X Not applicable.
    - 0 No answer.
    - 1 Initial level.
    - 2 Repeatable or planned level.
    - 3 Level defined or executed.
    - 4 Level managed or verified.
    - 5 Optimized or feedback level.

    Observations or justifications:_____

30. **NST17: Does the entity establish and apply considerations related to software updates?**
IT security plans and best practices call for regular updates and fixes to software and digital components, as the latter become outdated more quickly. Therefore, it is important to take into account the problem posed by software corrections and updates in digital nuclear monitoring or control systems.

- X Not applicable.
- 0 No answer.
- 1 Initial level.
- 2 Repeatable or planned level.
- 3 Level defined or executed.
- 4 Level managed or verified.
- 5 Optimized or feedback level.

Observations or justifications:_____

31. **NST17: Does the entity establish and apply cyber security specifications within the purchases and acquisitions of digital technologies?**
The recent trend towards the connectivity of systems and processes, the integration of commercial computer systems and the excess of malicious computer activities (such as hacking) have prompted the need to consider computer security as one of the basic requirements in the acquisition of new equipment. . Consequently, security requirements must be formalized in the context of contract negotiation with vendors.

- X Not applicable.
- 0 No answer.
- 1 Initial level.
- 2 Repeatable or planned level.
- 3 Level defined or executed.
- 4 Level managed or verified.
- 5 Optimized or feedback level.

Observations or justifications:_____

32. **NST17: Does the entity establish and apply a duly documented and widely known procedure for cyber security controls that third parties/suppliers must follow to engage with the entity?**
It is important that the management personnel responsible for each facility/entity in the nuclear sector maintain a close working relationship with the subcontracting company in order to ensure that during the preparation and execution of the contract, and at the time of final delivery, issues are addressed critical security issues. If deemed necessary, checks and checks should be carried out to ensure that the subcontractor's management system adequately addresses security concerns and that the entity's practices and measures comply with that system.

- X Not applicable.
- 0 No answer.
- 1 Initial level.
- 2 Repeatable or planned level.
- 3 Level defined or executed.
- 4 Level managed or verified.
- 5 Optimized or feedback level.

Observations or justifications:_____