# “ENCUESTA DE CIBERSEGURIDAD APLICADA A INSTALACIONES NUCLEARES Y RADIACTIVAS” VERSIÓN 6

**OBJETIVO:**
Esta encuesta evaluará la madurez del estado de la ciberseguridad en las instalaciones reguladas por CCHEN, para obtener una visión general de la postura de ciberseguridad en el sector.

**PÚBLICO OBJETIVO:**
El Representante Legal deberá designar un coordinador que sea el encargado de coordinar las respuestas de la encuesta con el apoyo de: operadores de instalaciones, oficiales de protección radiológica, profesionales de TI, personal de seguridad, jefe de operaciones.

**ACRÓNIMOS Y DEFINICIONES:**

- **Área segura:** Área donde se almacena información crítica, confidencial o sensible.
- **Información crítica, confidencial o sensible:** Información sensible para la seguridad nacional, tales como: inventario nuclear o radiactivo, planos y ubicación de sitios con material nuclear y radiactivo, procedimientos o planes de seguridad de instalaciones.
- **NDA:** Non-Disclosure Agreement que significa Acuerdo de No Divulgación o Confidencialidad.
- **SGSI:** Sistema de Gestión de Seguridad de la Información. **ISMS** en inglés.
- **TI:** Tecnologías de la Información. **IT** en inglés.
- **TIC:** Tecnologías de la Información y las Comunicaciones. **ICT** en inglés.
- **TO:** Tecnología de operaciones. **OT** en inglés.
- **ICS:** Sistemas de control industrial especializados.
- **CSP:** Plan de Seguridad Informática.

**REFERENCIAS:**

- 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.

**TABLA DE NIVELES DE CIBERSEGURIDAD**

| Nivel | Aspecto | % de cumplimiento | | Descripción |
|---|---|---|---|---|
| X | No aplica | X | | El elemento no aplica en la organización. |
| 0 | Sin respuesta | 0% | | No tiene el elemento o no sabe si existe. ¿Por qué? No se obtiene información al respecto. |
| 1 | Inicial | 0% | 20% | Existe este elemento clave pero no está aprobado formalmente o no se ejecuta como parte del Sistema de Ciberseguridad. Poco implementado. |
| 2 | Repetible o Planificado | 20% | 40% | (1) + Se planifica y se aprueba formalmente. Se programa la realización de actividades. Parcialmente implementado. |
| 3 | Definido o Ejecutado | 40% | 60% | (2) + Se ejecuta e implementa de acuerdo con lo aprobado y planificado. Medianamente implementado. |
| 4 | Gestionado o Verificado | 60% | 80% | (3) + Se realiza seguimiento y medición de las acciones asociadas a la ejecución. Altamente implementado. |
| 5 | Optimizado o Retroalimentado | 80% | 100% | (4) + Se retroalimenta y se toman medidas para mejorar el desempeño. Completamente implementado. |

**1. SGSI: ¿La entidad cuenta con un Sistema de Gestión de Seguridad de la Información en funcionamiento?**

La organización establece, implementa, mantiene y mejora continuamente su sistema de gestión de seguridad de la información (SGSI).

La seguridad de la información se logra mediante la implementación de un conjunto adecuado de controles, incluidas políticas, procesos, procedimientos, estructuras organizativas y funciones de software y hardware.

- X No aplica.
- 0 Sin respuesta.
- 1 Nivel inicial.
- 2 Nivel repetible o planificado.
- 3 Nivel definido o ejecutado.
- 4 Nivel gestionado o verificado.
- 5 Nivel optimizado o retroalimentado.

Observaciones o justificaciones:_____

**2. SGSI: ¿La entidad cuenta con un SGSI funcionando con el apoyo de la máxima dirección?**

El sistema de gestión de seguridad de la información (SGSI) está auspiciado por la máxima autoridad o titular de la entidad, y el máximo responsable asume el riesgo residual resultante de haber aplicado todos los controles establecidos por el SGSI.

- X No aplica.
- 0 Sin respuesta.
- 1 Nivel inicial.
- 2 Nivel repetible o planificado.
- 3 Nivel definido o ejecutado.
- 4 Nivel gestionado o verificado.
- 5 Nivel optimizado o retroalimentado.

Observaciones o justificaciones:_____

**3. Controles organizacionales: ¿Existe una matriz de roles y responsabilidades relacionadas con la seguridad de la información?**

La matriz de roles y responsabilidades corresponde a las funciones que realizan las diferentes personas en materia de seguridad de la información. Pueden ser personas dedicadas a la seguridad o personas que tienen diferentes cargos, pero que tienen algún rol o responsabilidad en caso de un incidente de ciberseguridad.

- X No aplica.
- 0 Sin respuesta.
- 1 Nivel inicial.
- 2 Nivel repetible o planificado.
- 3 Nivel definido o ejecutado.
- 4 Nivel gestionado o verificado.
- 5 Nivel optimizado o retroalimentado.

Observaciones o justificaciones:_____

4. **Controles organizacionales: ¿Existe una clasificación de sus activos de información en términos de su criticidad, sensibilidad o confidencialidad?**

El objetivo es asegurar que la información reciba el nivel de protección adecuado según su importancia para la organización, y así poder diseñar controles internos para evitar que personal interno que no cuente con los privilegios necesarios acceda a información sensible.

La información debe clasificarse en términos de requisitos legales, valor, criticidad y sensibilidad a la divulgación o modificación no autorizada. Las clasificaciones y controles de protección asociados a la información deben considerar las necesidades de la entidad para compartir o restringir información, así como los requisitos legales. Los propietarios de los activos de información deben ser responsables de su clasificación.

En el caso de instalaciones nucleares y radiactivas contamos con: inventario de material nuclear y/o radiactivo, ubicación geográfica de las instalaciones, información asociada al transporte de material nuclear y/o radiactivo, autorizaciones, planes de protección física, entre otros.

- X No aplica.
- 0 Sin respuesta.
- 1 Nivel inicial.
- 2 Nivel repetible o planificado.
- 3 Nivel definido o ejecutado.
- 4 Nivel gestionado o verificado.
- 5 Nivel optimizado o retroalimentado.

Observaciones o justificaciones:_____

5. **Controles organizacionales: ¿Su infraestructura está preparada para la continuidad operativa en caso de una emergencia declarada?**

La entidad incorpora el hecho de que la preparación TIC debe planificarse, implementarse, mantenerse y probarse con base en la continuidad de las operaciones, manteniendo como objetivos y requisitos de continuidad TIC para asegurar la disponibilidad de la información de la organización y otros activos asociados en caso de una interrupción del servicio. Las estrategias de continuidad del negocio pueden comprender una o más soluciones. A partir de las estrategias, se deben desarrollar, implementar y probar planes para cumplir con el nivel requerido de disponibilidad de los servicios TIC y en los tiempos requeridos luego de la interrupción o falla de los procesos críticos del negocio.

- X No aplica.
- 0 Sin respuesta.
- 1 Nivel inicial.
- 2 Nivel repetible o planificado.
- 3 Nivel definido o ejecutado.
- 4 Nivel gestionado o verificado.
- 5 Nivel optimizado o retroalimentado.

Observaciones o justificaciones:_____

6. **Controles organizacionales: ¿La entidad realiza revisiones independientes de seguridad de la información?**

El objetivo es garantizar que la seguridad de la información se implemente y opere de acuerdo con las políticas y los procedimientos de la organización. El enfoque de la organización para gestionar la seguridad de la información y su implementación (es decir, objetivos de control, controles, políticas, procesos y procedimientos para la seguridad de la información) debe revisarse de forma independiente a intervalos planificados o cuando ocurran cambios significativos.

- X No aplica.
- 0 Sin respuesta.
- 1 Nivel inicial.
- 2 Nivel repetible o planificado.
- 3 Nivel definido o ejecutado.
- 4 Nivel gestionado o verificado.
- 5 Nivel optimizado o retroalimentado.

Observaciones o justificaciones:_____

7. **Controles de Personal: ¿La entidad establece términos y condiciones de empleo, relacionados con la seguridad de la información?**

Los acuerdos contractuales con empleados y contratistas deben indicar sus responsabilidades y las de la organización en materia de seguridad de la información. Las obligaciones contractuales de los empleados o contratistas deben reflejar las políticas de seguridad de la información de la organización, entre otros aspectos relacionados con la confidencialidad, responsabilidades legales, responsabilidades en cuanto a la clasificación de la información, responsabilidades por el manejo de la información recibida de otras empresas o terceros y acciones a tomar en caso de el empleado o proveedor no cumple con las políticas de seguridad de la información.

- X No aplica.
- 0 Sin respuesta.
- 1 Nivel inicial.
- 2 Nivel repetible o planificado.
- 3 Nivel definido o ejecutado.
- 4 Nivel gestionado o verificado.
- 5 Nivel optimizado o retroalimentado.

Observaciones o justificaciones:_____

8. **Controles de personal: ¿La entidad lleva a cabo un programa de concientización, educación y capacitación en ciberseguridad?**

Los empleados de la organización y, cuando corresponda, los contratistas deben recibir educación y capacitación de concientización adecuadas y actualizaciones periódicas sobre las políticas y procedimientos de la organización, según corresponda a su función laboral.

- X No aplica.
- 0 Sin respuesta.
- 1 Nivel inicial.
- 2 Nivel repetible o planificado.
- 3 Nivel definido o ejecutado.
- 4 Nivel gestionado o verificado.
- 5 Nivel optimizado o retroalimentado.

Observaciones o justificaciones:_____

9. **Controles de Personal: ¿La entidad establece la obligación para sus empleados y proveedores de firmar un acuerdo de confidencialidad o no divulgación (NDA)?**

Los requisitos para acuerdos de confidencialidad y no divulgación que reflejen las necesidades de la organización para la protección de la información deben identificarse, revisarse y documentarse periódicamente. La confidencialidad de los acuerdos de no divulgación debe abordar el requisito de proteger la información confidencial mediante términos legalmente exigibles. Los acuerdos de confidencialidad o no divulgación se aplican a partes externas o empleados de la organización. Se deben seleccionar o agregar elementos considerando el tipo de la otra parte y el acceso que se permite o el manejo de información confidencial.

- X No aplica.
- 0 Sin respuesta.
- 1 Nivel inicial.
- 2 Nivel repetible o planificado.
- 3 Nivel definido o ejecutado.
- 4 Nivel gestionado o verificado.
- 5 Nivel optimizado o retroalimentado.

Observaciones o justificaciones:_____

10. **Controles de Personal: ¿La entidad establece un protocolo seguro de trabajo remoto?**

Ha implementado una política y medidas que respaldan la seguridad para proteger la información a la que se accede, procesa o almacena en los sitios de teletrabajo. Las organizaciones que permitan actividades de teletrabajo deben emitir una política que defina las condiciones y restricciones del uso del teletrabajo. [Ley N° 21.220 - http://bcn.cl/2lz8x]

- X No aplica.
- 0 Sin respuesta.
- 1 Nivel inicial.
- 2 Nivel repetible o planificado.
- 3 Nivel definido o ejecutado.
- 4 Nivel gestionado o verificado.
- 5 Nivel optimizado o retroalimentado.

Observaciones o justificaciones:_____

11. **Controles de Personal: ¿La entidad establece un protocolo para que las personas reporten eventos de seguridad de la información a sus equipos de seguridad?**

Los empleados y contratistas son conscientes de su responsabilidad de reportar los eventos de seguridad de la información a la mayor brevedad. También deben conocer el procedimiento para informar eventos de seguridad de la información y el punto de contacto al que se deben informar los eventos. Las fallas u otros comportamientos anormales del sistema pueden ser un indicador de un ataque a la seguridad o una brecha de seguridad real y, por lo tanto, siempre deben informarse como un evento de seguridad de la información.

- X No aplica.
- 0 Sin respuesta.
- 1 Nivel inicial.
- 2 Nivel repetible o planificado.
- 3 Nivel definido o ejecutado.
- 4 Nivel gestionado o verificado.
- 5 Nivel optimizado o retroalimentado.

Observaciones o justificaciones:_____

**12. Controles de Seguridad Física: ¿La entidad establece controles de acceso físico a los lugares donde se almacena la información?**

Las áreas seguras están protegidas con controles de entrada adecuados para garantizar que solo se permita el acceso al personal autorizado. Además, los puntos de acceso como las áreas de entrega y carga y otros puntos donde personas no autorizadas podrían ingresar a las instalaciones deben controlarse y, si es posible, aislarse de las instalaciones de procesamiento de información para evitar el acceso no autorizado.

- X No aplica.
- 0 Sin respuesta.
- 1 Nivel inicial.
- 2 Nivel repetible o planificado.
- 3 Nivel definido o ejecutado.
- 4 Nivel gestionado o verificado.
- 5 Nivel optimizado o retroalimentado.

Observaciones o justificaciones:_____

**13. Controles de Seguridad Física: ¿La entidad establece monitoreos de seguridad física de los lugares donde se almacena la información?**

Las instalaciones físicas son monitoreadas por sistemas de vigilancia, que pueden incluir guardias, alarmas de detección de intrusos, sistemas de monitoreo de video como CCTV e información de seguridad física y software de gestión administrado internamente o por un proveedor de servicios de monitoreo. El acceso a los edificios que albergan sistemas críticos debe monitorearse continuamente para detectar accesos no autorizados o comportamientos sospechosos. El diseño de los sistemas de monitoreo debe mantenerse de forma confidencial, ya que la divulgación podría facilitar brechas de seguridad no detectadas. Cualquier mecanismo de monitoreo y registro debe ser utilizado de conformidad con las leyes y reglamentos vigentes; esto incluye la protección de datos, especialmente en lo que respecta a los trabajadores relacionados con el sistema de monitoreo.

- X No aplica.
- 0 Sin respuesta.
- 1 Nivel inicial.
- 2 Nivel repetible o planificado.
- 3 Nivel definido o ejecutado.
- 4 Nivel gestionado o verificado.
- 5 Nivel optimizado o retroalimentado.

Observaciones o justificaciones:_____

**14. Controles de seguridad física: ¿La entidad establece una política de pantalla limpia?**

Se debe adoptar una política de pantalla limpia durante el procesamiento de información instalaciones. El objetivo de este control es reducir los riesgos de acceso no autorizado, pérdida y daño de la información considerando otros lugares accesibles durante y fuera del horario normal de trabajo.

- X No aplica.
- 0 Sin respuesta.
- 1 Nivel inicial.
- 2 Nivel repetible o planificado.
- 3 Nivel definido o ejecutado.
- 4 Nivel gestionado o verificado.
- 5 Nivel optimizado o retroalimentado.

Observaciones o justificaciones:_____

15. **Controles de Seguridad Física: ¿La entidad establece seguridad en la instalación de su cableado para los dispositivos que manejan información?**

Los cables de electricidad y telecomunicaciones que transportan datos o soportan servicios de información deben estar protegidos contra intercepciones, interferencias o daños (cableado subterráneo o sujeto a protección alternativa adecuada).

- X No aplica.
- 0 Sin respuesta.
- 1 Nivel inicial.
- 2 Nivel repetible o planificado.
- 3 Nivel definido o ejecutado.
- 4 Nivel gestionado o verificado.
- 5 Nivel optimizado o retroalimentado.

Observaciones o justificaciones:_____

16. **Controles de seguridad física: ¿La entidad establece y aplica un protocolo para desechar o reutilizar de manera segura los dispositivos?**

Todos los dispositivos que contienen medios de almacenamiento deben ser verificados para garantizar que los datos confidenciales y el software con licencia se hayan eliminado o sobrescrito de forma segura antes de su eliminación o reutilización.

- X No aplica.
- 0 Sin respuesta.
- 1 Nivel inicial.
- 2 Nivel repetible o planificado.
- 3 Nivel definido o ejecutado.
- 4 Nivel gestionado o verificado.
- 5 Nivel optimizado o retroalimentado.

Observaciones o justificaciones:_____

17. **Controles de seguridad física: ¿Se define y utiliza un perímetro de seguridad para proteger áreas que contienen información crítica y otros activos asociados?**

Las instalaciones deben tener una definición de perímetros de seguridad. La ubicación y fortaleza de cada uno de los perímetros debe depender de los requisitos de seguridad de los activos dentro del perímetro y los resultados de una evaluación de riesgos.

- X No aplica.
- 0 Sin respuesta.
- 1 Nivel inicial.
- 2 Nivel repetible o planificado.
- 3 Nivel definido o ejecutado.
- 4 Nivel gestionado o verificado.
- 5 Nivel optimizado o retroalimentado.

Observaciones o justificaciones:_____

18. **Controles de seguridad física: ¿Ha diseñado e implementado procedimientos de seguridad para trabajar en áreas seguras?**

Se debe considerar las siguientes pautas en el procedimiento: la identidad de los empleados y visitantes debe ser autenticada por un medio adecuado, la fecha y hora de entrada y salida de los empleados y visitantes debe registrarse, el acceso de los empleados y visitantes solo debe ser otorgados para propósitos específicos y autorizados y deben ser emitidos con instrucciones sobre los requisitos de seguridad del área y sobre los procedimientos de emergencia, los empleados y visitantes deben ser supervisados a menos que se otorgue una excepción explícita.

- X No aplica.
- 0 Sin respuesta.
- 1 Nivel inicial.
- 2 Nivel repetible o planificado.
- 3 Nivel definido o ejecutado.
- 4 Nivel gestionado o verificado.
- 5 Nivel optimizado o retroalimentado.

Observaciones o justificaciones:_____

19. **Controles de seguridad física: ¿Tiene protección contra cortes de energía y otras interrupciones causadas por fallas en los servicios públicos?**

Se debe evitar la pérdida, daño o compromiso de la información y otros activos asociados debido a la falla e interrupción de los servicios públicos de apoyo o la interrupción de las operaciones de la organización.

- X No aplica.
- 0 Sin respuesta.
- 1 Nivel inicial.
- 2 Nivel repetible o planificado.
- 3 Nivel definido o ejecutado.
- 4 Nivel gestionado o verificado.
- 5 Nivel optimizado o retroalimentado.

Observaciones o justificaciones:_____

20. **Controles de Seguridad Física: ¿Existe un programa de mantenimiento de los equipos que componen el sistema de seguridad?**

La organización debe tener implementado un programa de mantenimiento con recursos para mantener la operación normal. Deben existir revisiones periódicas del hardware y sus componentes.

- X No aplica.
- 0 Sin respuesta.
- 1 Nivel inicial.
- 2 Nivel repetible o planificado.
- 3 Nivel definido o ejecutado.
- 4 Nivel gestionado o verificado.
- 5 Nivel optimizado o retroalimentado.

Observaciones o justificaciones:_____

**21. Controles tecnológicos: ¿La entidad establece y aplica protocolos para restringir el acceso a la información?**

El acceso a las funciones del sistema de información y aplicación debe estar restringido de acuerdo con la política de control de acceso. Las restricciones de acceso deben basarse en los requisitos de las aplicaciones comerciales individuales y de acuerdo con la política de control de acceso definida.

- X No aplica.
- 0 Sin respuesta.
- 1 Nivel inicial.
- 2 Nivel repetible o planificado.
- 3 Nivel definido o ejecutado.
- 4 Nivel gestionado o verificado.
- 5 Nivel optimizado o retroalimentado.

Observaciones o justificaciones:_____

**22. Controles tecnológicos: ¿La entidad establece y aplica protocolos y tecnologías para la autenticación segura?**

Cuando lo requiera la política de control de acceso, el acceso a los sistemas y aplicaciones debe controlarse mediante un procedimiento de inicio de sesión seguro. Se debe seleccionar un método de autenticación adecuado para verificar la identidad que un usuario dice tener: Política de contraseñas fuertes, doble factor de autenticación, cifrado de datos.

- X No aplica.
- 0 Sin respuesta.
- 1 Nivel inicial.
- 2 Nivel repetible o planificado.
- 3 Nivel definido o ejecutado.
- 4 Nivel gestionado o verificado.
- 5 Nivel optimizado o retroalimentado.

Observaciones o justificaciones:_____

**23. Controles Tecnológicos: ¿La entidad establece y aplica protocolos y tecnologías de protección contra malware (ransomware, virus, phishing, entre otros)?**

Se implementan controles de detección, prevención y recuperación para protegerse contra el malware en combinación con la concientización adecuada del usuario. La protección contra malware debe basarse en controles de software de detección y reparación de malware, conciencia de seguridad de la información, acceso adecuado al sistema y gestión de cambios.

- X No aplica.
- 0 Sin respuesta.
- 1 Nivel inicial.
- 2 Nivel repetible o planificado.
- 3 Nivel definido o ejecutado.
- 4 Nivel gestionado o verificado.
- 5 Nivel optimizado o retroalimentado.

Observaciones o justificaciones:_____

**24. Ciberseguridad: ¿La entidad utiliza métodos de comunicación seguros para la transferencia de datos confidenciales?**

El uso de la criptografía en sitios o sistemas web tiene varios objetivos, entre los que se destacan, salvaguardar la confidencialidad de la información intercambiada entre el sitio o sistema web y el usuario, alertar de cualquier posible problema que esté afectando la integridad de la información, o proporcionar información confiable sobre la entidad propietaria del sistema. Como ejemplo, el más visible y común dentro del entorno de Internet es el uso de HTTPS.

- X No aplica.
- 0 Sin respuesta.
- 1 Nivel inicial.
- 2 Nivel repetible o planificado.
- 3 Nivel definido o ejecutado.
- 4 Nivel gestionado o verificado.
- 5 Nivel optimizado o retroalimentado.

Observaciones o justificaciones:_____

**25. Ciberseguridad: ¿La entidad monitorea el desempeño de seguridad de los servidores?**

Estas medidas deben incluir una definición adecuada de los usuarios del servidor frente a los administradores, hacer cumplir los controles de acceso en los directorios y archivos del programa y del sistema, y permitir el registro de auditoría, en particular, de la seguridad y otros eventos de falla del servidor. el sistema.

- X No aplica.
- 0 Sin respuesta.
- 1 Nivel inicial.
- 2 Nivel repetible o planificado.
- 3 Nivel definido o ejecutado.
- 4 Nivel gestionado o verificado.
- 5 Nivel optimizado o retroalimentado.

Observaciones o justificaciones:_____

**26. Ciberseguridad: ¿La entidad se asegura de que los usuarios finales utilicen aplicaciones de software y sistemas operativos debidamente actualizados con los parches de seguridad más recientes?**

Los usuarios deben utilizar sistemas operativos compatibles con los últimos parches de seguridad que se hayan instalado. Los usuarios tienen la responsabilidad de conocer y seguir la política de la organización con respecto a los sistemas operativos compatibles. En todos los casos, el sistema operativo debe estar actualizado con al menos parches de seguridad. Esto se aplica igualmente a las aplicaciones de software. Es decir, Windows y Office deben estar actualizados con sus parches al día, por ejemplo.

- X No aplica.
- 0 Sin respuesta.
- 1 Nivel inicial.
- 2 Nivel repetible o planificado.
- 3 Nivel definido o ejecutado.
- 4 Nivel gestionado o verificado.
- 5 Nivel optimizado o retroalimentado.

Observaciones o justificaciones:_____

27. **NST 17: ¿Tiene la entidad un programa completo del ciclo de vida del sistema de seguridad que incluye el diseño, la implementación, todas las modalidades operativas y la disposición del sistema?**

Estas fases del ciclo de vida y los múltiples modos de operación pueden requerir diferentes sistemas y entornos operativos. Por ejemplo, los períodos de mantenimiento pesado a menudo requieren reemplazo, modificación y prueba de equipos, o pueden requerir personal adicional y acceso de terceros/subcontratistas. Esta diversidad debe ser tenida en cuenta en el Plan de Seguridad Informática (CSP). En particular, la diversidad de etapas de la vida podría requerir revisiones extensas del CSP.

- X No aplica.
- 0 Sin respuesta.
- 1 Nivel inicial.
- 2 Nivel repetible o planificado.
- 3 Nivel definido o ejecutado.
- 4 Nivel gestionado o verificado.
- 5 Nivel optimizado o retroalimentado.

Observaciones o justificaciones:_____

28. **NST17: ¿La entidad establece las acciones y separaciones entre sistemas informáticos, sistemas de vigilancia y sistemas de control industrial (SCADA/HMI/PLC)?**

Los sistemas informáticos y las arquitecturas de red que soportan operaciones y/o controles industriales, no son sistemas informáticos estandarizados en términos de arquitectura, configuración o requisitos de comportamiento. Estos sistemas se pueden clasificar como sistemas de control industrial especializados (ICS). Aunque ICS ha pasado de aplicaciones estrictamente propietarias a arquitecturas informáticas más generalizadas, todavía existen grandes diferencias entre ICS y los sistemas de TI estándar que deben tenerse en cuenta en cualquier CSP.

- X No aplica.
- 0 Sin respuesta.
- 1 Nivel inicial.
- 2 Nivel repetible o planificado.
- 3 Nivel definido o ejecutado.
- 4 Nivel gestionado o verificado.
- 5 Nivel optimizado o retroalimentado.

Observaciones o justificaciones:_____

29. **NST17: ¿La entidad tiene un programa de evaluación de riesgos asociado con necesidades de conectividad adicionales?**

La necesidad de realizar análisis, mantenimiento o actualizaciones remotas también puede generar vulnerabilidades similares. Antes de abordar cualquier demanda de conectividad adicional, debe realizar un análisis de riesgo detallado.

- X No aplica.
- 0 Sin respuesta.
- 1 Nivel inicial.
- 2 Nivel repetible o planificado.
- 3 Nivel definido o ejecutado.
- 4 Nivel gestionado o verificado.
- 5 Nivel optimizado o retroalimentado.

Observaciones o justificaciones:_____

30. **NST17: ¿La entidad establece y aplica las consideraciones relacionadas con las actualizaciones de software?**

Las mejores prácticas y planes de seguridad de TI exigen actualizaciones y correcciones periódicas del software y los componentes digitales, ya que estos últimos se vuelven obsoletos más rápidamente. Por tanto, es importante tener en cuenta el problema que plantean las correcciones y actualizaciones de software en los sistemas digitales de control o seguimiento nuclear.

- X No aplica.
- 0 Sin respuesta.
- 1 Nivel inicial.
- 2 Nivel repetible o planificado.
- 3 Nivel definido o ejecutado.
- 4 Nivel gestionado o verificado.
- 5 Nivel optimizado o retroalimentado.

Observaciones o justificaciones:_____

31. **NST17: ¿La entidad establece y aplica especificaciones de seguridad cibernética dentro de las compras y adquisiciones de tecnologías digitales?**

La tendencia reciente hacia la conectividad de sistemas y procesos, la integración de sistemas informáticos comerciales y la excedencia de actividades informáticas maliciosas (como el hacking) han impulsado la necesidad de considerar la seguridad informática como uno de los requisitos básicos en la adquisición de nuevos equipos. En consecuencia, los requisitos de seguridad deben formalizarse en el contexto de la negociación del contrato con los proveedores.

- X No aplica.
- 0 Sin respuesta.
- 1 Nivel inicial.
- 2 Nivel repetible o planificado.
- 3 Nivel definido o ejecutado.
- 4 Nivel gestionado o verificado.
- 5 Nivel optimizado o retroalimentado.

Observaciones o justificaciones:_____

32. **NST17: ¿La entidad establece y aplica un procedimiento debidamente documentado y conocido por todos para los controles de seguridad cibernética que los terceros/proveedores deben seguir para relacionarse con la entidad?**

Es importante que el personal directivo responsable de cada instalación/entidad del sector nuclear mantenga una estrecha relación de trabajo con la empresa subcontratista con el fin de asegurar que durante la preparación y ejecución del contrato, y en el momento de la entrega final, se abordan los problemas críticos de seguridad. Si se considera necesario, se deben realizar controles y verificaciones para garantizar que el sistema de gestión del subcontratista aborde adecuadamente los problemas de seguridad y que las prácticas y medidas de la entidad cumplan con ese sistema.

- X No aplica.
- 0 Sin respuesta.
- 1 Nivel inicial.
- 2 Nivel repetible o planificado.
- 3 Nivel definido o ejecutado.
- 4 Nivel gestionado o verificado.
- 5 Nivel optimizado o retroalimentado.

Observaciones o justificaciones:_____