ANEXO 4

Requisitos de Ciberseguridad pata la Infraestructura de TIC

* 1. **Introducción**
     1. El presente anexo establece los requisitos en materia de Ciberseguridad que el CENACE, Transportista, Distribuidor, Central Eléctrica o Centro de Carga deben adoptar para asegurar la confidencialidad, integridad y disponibilidad de la información transmitida, necesarias para la operación del SEN y el Mercado Eléctrico Mayorista.
     2. Para efectos de este anexo, resultan aplicables las definiciones señaladas en el numeral 1.4 del Manual.
     3. Sin perjuicio de lo señalado en este anexo, el CENACE, el Transportista, el Distribuidor, la Central Eléctrica y el Centro de Carga deben cumplir con las disposiciones de Ciberseguridad que emita la CRE.
     4. Para efectos de este anexo, cuando se hable de las partes, debe entenderse el CENACE, Transportista, Distribuidor, Central Eléctrica y Centro de Carga, cada uno en su ámbito de acción.
  2. **Requisitos generales de Ciberseguridad**

La conectividad de acceso hacia el CENACE está diseñada, desarrollada y supervisada de tal manera que sólo los usuarios autorizados tienen acceso a la información, comunicación y herramientas necesarias, por tal motivo, las partes deben cumplir con los requisitos que se indican a continuación.

* + 1. Sólo al personal facultado por las partes se le debe permitir el acceso y uso de equipos de cómputo, comunicaciones o seguridad ubicados en los Puntos de Conectividad, según sea el caso: entre el CENACE y el Transportista, Distribuidor, Central Eléctrica o Centro de Carga; entre el Transportista y Distribuidor; o entre el Transportista o Distribuidor y la Central Eléctrica o Centro de Carga. Las partes involucradas en un Punto de Conectividad deben compartir entre ellas sus respectivas listas de personal facultado.
    2. Cuando así lo consideren necesario y en coordinación con su contraparte en el Punto de Conectividad, el personal autorizado del CENACE, en el Punto de Conectividad entre el CENACE y el Transportista, Distribuidor, Central Eléctrica o Centro de Carga, y el personal autorizado del Transportista o Distribuidor, en el Punto de Conectividad que tengan entre sí o con la Central Eléctrica o Centro de Carga, según sea el caso, podrán llevar a cabo el diagnóstico de problemas y la validación de las políticas de seguridad convenidas. Para tal efecto, utilizarán herramientas de software no invasivas. El CENACE, el Transportista y el Distribuidor podrán obtener información de su contraparte en el Punto de Conectividad para corroborar que todas las conexiones en la infraestructura de red han sido autorizadas y que se han implementado de manera correcta el equipo firewall, las conexiones y los sistemas antivirus. Estos trabajos de monitoreo y supervisión se llevarán a cabo desde sus respectivas instalaciones.
    3. El CENACE, el Transportista y el Distribuidor deben mantener estricta confidencialidad sobre cualquier información que obtengan de las actividades de monitoreo y supervisión, y no deben compartirla con terceros, por lo cual están obligados a firmar entre ellos los acuerdos de confidencialidad conducentes.
    4. La Infraestructura de TIC del CENACE, del Transportista, del Distribuidor, de la Central Eléctrica o del Centro de Carga en los Puntos de Conectividad debe estar configurada solamente para aquellos protocolos, puertos y direccionamientos autorizados y originados en los equipos y sistemas de TIC para la conectividad.
    5. Las partes deben compartir, con su contraparte involucrada en cada Punto de Conectividad de los referidos en el numeral 2.2 de este anexo, el diagrama correspondiente a cada Punto de Conectividad. Dichos diagramas deben incluir el direccionamiento, los puertos y la topología.
    6. Previo a la implementación de cualquier modificación o mantenimiento a la Infraestructura de TIC que afecte la comunicación, topología o seguridad de los equipos localizados en los Puntos de Conectividad mencionados en el numeral 2.2 de este anexo, las partes involucradas en dicho punto deben coordinarse conforme a lo que establezcan las guías operativas o procedimientos relativos al mantenimiento de los sistemas de TIC.
    7. Cada parte será responsable de la protección de sus redes internas para tráfico no autorizado.
    8. La Infraestructura de TIC de cada parte, que tenga conectividad con Infraestructura de TIC de otra parte debe estar lógicamente aislada a través de equipos firewall. El CENACE, el Transportista, el Distribuidor, la Central Eléctrica y el Centro de Carga deben integrar dichos equipos firewall a sus respectivas Redes Operativas. Para el caso de los Puntos de Conectividad entre el Transportista o el Distribuidor y la Central Eléctrica o el Centro de Carga, según corresponda, la Central Eléctrica y el Centro de Carga deberán seguir lo indicado en el esquema de conectividad que corresponda, según lo indicado en el anexo 7 “Alternativas de Conectividad”.
    9. Cuando las partes detecten alguna evidencia de una posible actividad maliciosa, la parte que realice el descubrimiento lo notificará a su contraparte inmediatamente, y proveerá dicha evidencia conforme a los plazos y procedimientos que la CRE prevea para tal efecto. La parte responsable del equipo en el que se detectó la actividad maliciosa debe realizar la investigación y tomar las medidas de contención y erradicación de manera inmediata, en coordinación con su contraparte en el Punto de Conectividad. En caso de que existan o puedan existir daños a la información, se realizará conjuntamente un recurso de remediación.
    10. En el momento en que ocurra algún incidente de seguridad entre los equipos localizados en el Punto de Conectividad, las partes involucradas en dicho punto deberán coordinarse e intercambiar la información necesaria, conforme a lo que establezcan las guías operativas o procedimientos relativos al mantenimiento de los sistemas de TIC, a efecto de resolver dicho incidente.
    11. Red Privada Virtual (VPN)
    12. Para que una parte pueda acceder por VPN a los sistemas del CENACE, o en su caso, del Transportista o Distribuidor, deberá contar con autorización del CENACE, del Transportista o del Distribuidor. Además, debe contar con métodos de autenticación y cifrado de datos.
    13. El acceso por VPN a los sistemas del CENACE, del Transportista o del Distribuidor queda restringido exclusivamente a los equipos autorizados para ello.
    14. Cuando se pretenda conectar al sistema RID a través de una VPN, la Central Eléctrica o el Centro de Carga deben cumplir con los requisitos solicitados en el numeral 3.1.4 de este anexo.
    15. El Transportista, Distribuidor, Central Eléctrica o Centro de Carga que cuente con acceso por VPN será el responsable del uso que se dé a dicho servicio.
    16. Bitácoras
    17. El CENACE, Transportista, Distribuidor, Central Eléctrica y Centro de Carga deben llevar bitácoras sobre los equipos críticos definidos con base en los criterios de confiabilidad que emita la CRE. Estas bitácoras deben almacenarse durante al menos un año.
    18. Las bitácoras deben contener el tipo de consulta o los cambios realizados en la configuración de las aplicaciones, acompañados del nombre del usuario, el nombre de equipo, la dirección IP, y las horas de entrada y salida del sistema.
    19. Las bitácoras deberán ser utilizadas por la parte responsable como documentación para la solución y reporte de incidentes, con el fin de validar cambios de configuración del equipo.
    20. Endurecimiento

Siempre que no afecte la operación y mantenimiento del propio equipo, se debe aplicar endurecimiento a todos los equipos utilizados, a su sistema operativo, al manejador de base de datos y a los aplicativos, como lo son, con carácter enunciativo mas no limitativo, el deshabilitado de puertos físicos y lógicos no usados, la actualización a la última versión estable de software, la aplicación de parches de seguridad y el deshabilitado de servicios que no son utilizados o que son considerados como no seguros, como Telnet y ftp.

* + 1. Planes de contingencia
    2. El CENACE, Transportista, Distribuidor, Central Eléctrica y Centro de Carga deben contar con planes de contingencia de TIC para mantener o restaurar las operaciones ante eventos de emergencia, fallas del sistema o desastres naturales.
    3. En dichos planes se debe especificar los roles y responsabilidades, la asignación del personal y las actividades asociadas a la restauración.
    4. Para llevar a cabo la coordinación de actividades entre el CENACE, Transportista, Distribuidor, Central Eléctrica y Centro de Carga, cuando así corresponda, éstos deben compartir la lista de asignación de personal y su información de contacto.
    5. Autenticación

Toda conectividad indicada en el Manual debe realizarse bajo autenticación. La implementación de parámetros de contraseñas (password) quedará sujeta a las restricciones del sistema operativo o al software de seguridad, con el fin de maximizar la facilidad de uso sin sacrificar la seguridad en ninguna sección de la infraestructura o comunicaciones.

* + 1. Sistemas antivirus

Se requiere instalar sistemas antivirus con licencia vigente y firmas actualizadas en aquellos equipos donde sea técnicamente factible.

* + 1. Uso de certificados digitales
    2. Para las aplicaciones que requieran autenticación hacia el CENACE, Transportista, Distribuidor, Central Eléctrica o Centro de Carga, ésta deberá realizarse a través de certificados digitales.
    3. Los certificados digitales pueden ser utilizados por alguna persona, sistema, dispositivo o aplicación perteneciente al CENACE, Transportista, Distribuidor, Central Eléctrica o Centro de Carga, según sea el caso.
    4. El CENACE, Transportista, Distribuidor, Central Eléctrica y Centro de Carga deben proteger los certificados digitales, con base en lo señalado en los estándares aceptables de la industria.
    5. Cualquier transacción que ocurra con el uso del certificado digital es responsabilidad del suscriptor del certificado digital.
    6. El CENACE, Transportista, Distribuidor, Central Eléctrica y Centro de Carga no tienen permitido compartir entre ellos sus certificados digitales ni las contraseñas relacionadas.
    7. El CENACE, el Transportista, el Distribuidor, la Central Eléctrica o el Centro de Carga notificarán a su contraparte para revocar el certificado digital cuando:

1. la información utilizada en el certificado digital ha sufrido cambios;
2. sospecha que la llave privada está comprometida;
3. no requiere más el uso del certificado digital, o
4. el personal asignado al certificado digital ha sido cambiado o ya no labora en el CENACE, el Transportista, Distribuidor, Central Eléctrica o Centro de Carga.
   * 1. La revocación la realizarán:
5. el suscriptor mencionado en el certificado;
6. el CENACE en coordinación con el Transportista, Distribuidor, Central Eléctrica o Centro de Carga, que utilice el certificado;
7. cuando aplique, el Distribuidor o Transportista en coordinación con el CENACE, la Central Eléctrica o Centro de Carga que utilice el certificado, o
8. la Central Eléctrica o Centro de Carga en coordinación con la contraparte que utilice el certificado.
   * 1. Cifrado

En los equipos que utilicen el CENACE, Transportista, Distribuidor, Central Eléctrica y Centro de Carga para tener acceso a su contraparte en un Punto de Conectividad, y que soporten cifrado, éste debe habilitarse con mecanismos estándares de cifrado de datos con un grado no menor a 256 bits.

* + 1. Banners

Todos los dispositivos (p. ej. routers, equipos firewall, etc.) conectados entre el CENACE y el Transportista, Distribuidor, Central Eléctrica o Centro de Carga, incluidos los dispositivos del CENACE, deben tener configurado el siguiente banner o uno equivalente:

*\*\*\* SÓLO USUARIOS AUTORIZADOS \*\*\**

*Éste es un sistema de cómputo privado, sólo para uso autorizado. Todo el tráfico es monitoreado sin excepción (usuarios autorizados o no autorizados).*

*Todos los usos de este sistema o toda la información pueden ser interceptados, monitoreados, grabados, copiados, inspeccionados y divulgados únicamente por personas autorizadas. Al usar este sistema el usuario acepta todas las condiciones antes mencionadas.*

*CIERRE LA SESIÓN INMEDIATAMENTE si no está de acuerdo con las condiciones antes mencionadas.*

*\*\*\* SÓLO USUARIOS AUTORIZADOS \*\*\**

* + 1. Seguridad física
    2. El equipo de cómputo, comunicaciones y seguridad del CENACE, Transportista, Distribuidor, Central Eléctrica o Centro de Carga, que esté asociado con algún enlace para el intercambio de información, debe estar físicamente protegido contra accesos no autorizados.
    3. La Infraestructura de TIC debe contar con las condiciones ambientales indicadas por el fabricante.
    4. El equipo debe tener suministro de energía ininterrumpible.
  1. **Requisitos de Ciberseguridad específicos para el Control Operativo del SEN y la Operación del MEM, incluida la medición para liquidaciones**
     1. Para incrementar la confiabilidad y reducir el riesgo asociado al tráfico de voz y datos, el CENACE, el Transportista, el Distribuidor, la Central Eléctrica y el Centro de Carga deben instalar en los Puntos de Conectividad, cada parte en sus instalaciones, dispositivos de seguridad para el control de tráfico.
     2. Los dispositivos de seguridad para el control de tráfico referidos en el numeral anterior deben:
     3. soportar puerto de aplicación (TCP/UDP);
     4. soportar control por direcciones IP;
     5. tener la capacidad de realizar NAT (Network Address Translation) y cifrado de tráfico;
     6. soportar tráfico VoIP en el puerto de operación SIP (Session Initiation Protocol), y
     7. soportar tráfico de monitoreo en el puerto de operación SNMP (Single Network Management Protocol).
     8. Además de lo señalado en los numerales 1.3.1 y 1.3.2, el Transportista, el Distribuidor, la Central Eléctrica y el Centro de Carga deben asegurarse de que una vez implementado los dispositivos de seguridad para el control de tráfico no se afecte el intercambio de información.
     9. La Central Eléctrica y el Centro de Carga deben realizar las acciones necesarias para que el equipo donde se aloje la aplicación RID:
     10. Sea de uso exclusivo para dicho sistema
     11. Cuente con endurecimiento de acuerdo a lo señalado en el numeral 2.13 de este anexo.
     12. Cuente con autenticación de acuerdo a lo señalado en el numeral 2.15 de este anexo
     13. Cuente con sistema antivirus de acuerdo a lo señalado en el numeral 2.16 de este anexo.
     14. Esté aislado de internet.
     15. Las instalaciones cuyo sistema RID se deba conectar al CENACE mediante VPN, conforme a lo señalado en las tablas contenidas en los numerales 6.1.4 y 7.1.4 del Manual, deben cumplir con los parámetros de conectividad que señale el CENACE.