x

NORMAS DE SEGURIDAD INFORMÁTICA

CENTRO INFORMÁTICO CIENTÍFICO DE ANDALUCÍA

NS04 – ACCESO REMOTO SEGURO

Fecha: 24 agosto 2020

Índice de contenido

1. OBJETIVO 3
2. ALCANCE 3
3. RESPONSABILIDADES 3
4. DEFINICIONES 3
5. ACCESO REMOTO SEGURO 4
5.1. REQUISITOS ESPECÍFICOS DE LA VPN 4
5.2. REQUISITOS GENERALES DEL SISTEMA VPN 4
5.2.1. MEDIDAS ORGANIZATIVAS 4
5.2.2. MEDIDAS OPERACIONALES DE PROTECCIÓN 5
5.2.3. MEDIDAS DE CONCIENCIACIÓN Y FORMACIÓN DEL PERSONAL 6
5.3. EQUIPOS DE SALTO 6
5.4. REVISIÓN PERIÓDICA DEL ACCESO REMOTO 7
5.5. MODELO DE ACEPTACIÓN Y COMPROMISO DE CUMPLIMIENTO 7

1.

2. OBJETIVO

1. El presente documento constituye la norma de seguridad del CICA en cuanto a la gestión y medidas de control seguro para el acceso remoto a la infraestructura, y forma parte del conjunto de normas de seguridad del CICA, “NS00 CICA – GENERAL”.
2. El objetivo es garantizar la seguridad de la información cuando se accede remotamente a los sistemas de información del CICA, tanto por usuarios internos como externos, y definir las condiciones y restricciones del acceso remoto o teletrabajo.

3. ALCANCE

3. Todo el personal, personal usuario y proveedores que requiera acceder remotamente a los sistemas de información del CICA, así como los dispositivos utilizados para tal fin.

4. RESPONSABILIDADES

4. El Responsable de Seguridad TIC debe velar por el cumplimiento de la presente norma.
5. Los Responsables de la Información, el Servicio y los Sistemas serán los encargados de proveer y mantener las condiciones necesarias para el cumplimiento de esta norma, así como establecer las reglas de uso del acceso remoto o del teletrabajo para el personal que lo requiera. Además, deberán proveer los medios técnicos para el cumplimiento de la presente norma.
6. El personal y personal usuario del CICA autorizados a trabajar remotamente o hacer uso remoto de la infraestructura son responsables por cumplir con lo establecido en la presente norma.
7. Es responsabilidad de la Dirección del CICA, planificar acciones de sensibilización a su personal respecto a la importancia de esta norma, destacando que el no cumplimiento aumenta la exposición de la información y el riesgo de tener un incidente de seguridad de la información. Por tanto, es responsabilidad última del personal el cumplimiento de la misma.

5. DEFINICIONES

8. **VPN**: Acrónimo de “*Virtual Private Network*”. Es una tecnología de red que permite una extensión segura de la red de área local (LAN) sobre una red pública o no controlada como Internet. Permite que el dispositivo en la red envíe y reciba datos sobre redes compartidas o públicas como si fuera una red privada, con toda la funcionalidad, seguridad y políticas de gestión de una red privada. Esto se realiza estableciendo una conexión virtual punto a punto mediante el uso de conexiones dedicadas, cifrado o la combinación de ambos métodos.

9. **Split-Tunneling**: Es una característica de las redes privadas virtuales (VPN) que permite configurar el tipo de tráfico en concreto que se desea que fluya por el túnel.
10. **EDR**: Acrónimo de "*Endpoint Detection and Response*". Es una herramienta que proporciona monitorización y análisis continuo del dispositivo final y la red. La finalidad es identificar, detectar y prevenir amenazas avanzadas (APT) con mayor facilidad.
11. **BYOD**: Acrónimo de "*Bring Your Own Device*". Consiste en utilizar los dispositivos personales de los empleados en el ámbito corporativo para el desarrollo de sus actividades profesionales.
12. **ENS**: Esquema nacional de seguridad. Es una norma de obligado cumplimiento que crea las condiciones necesarias de confianza en el uso de los medios electrónicos, a través de medidas para garantizar la seguridad de los sistemas, los datos, las comunicaciones y los servicios electrónicos, que permita a los ciudadanos y a las Administraciones públicas, el ejercicio de derechos y el cumplimiento de deberes a través de estos medios.
13. **CCN**: Centro Criptológico Nacional, es el Organismo responsable de coordinar la acción de los diferentes organismos de la Administración que utilicen medios o procedimientos de cifra, garantizar la seguridad de las Tecnologías de la Información en ese ámbito, informar sobre la adquisición coordinada del material criptológico y formar al personal de la Administración especialista en este campo.

6. ACCESO REMOTO SEGURO

14. La conexión a la infraestructura del CICA desde el exterior se realizará a través de una VPN.
15. Se deben realizar los esfuerzos necesarios para que la infraestructura y la información del CICA no se vean comprometidan. Para ello, es necesario el cumplimiento de los siguientes puntos:

6.1. REQUISITOS ESPECÍFICOS DE LA VPN

16. Se emplearán algoritmos criptográficos acreditados por el Centro Criptológico Nacional (CCN), definidos en su guía "CCN-CERT STIC-807–Criptografía de empleo en el ENS".
17. Deberá utilizarse un producto VPN cuyas funcionalidades de seguridad y cuyo nivel, hayan sido evaluados conforme a normas europeas o internacionales, y cuyos certificados estén reconocidos por el Esquema Nacional de Evaluación y Certificación de la Seguridad de las Tecnologías de la Información del Centro Criptológico Nacional.
18. Debe usarse, al menos, doble factor de autenticación.
19. Se hará uso de la versión más actual para la tecnología VPN usada.
20. Las credenciales se suspenderán tras un periodo definido de "no utilización".
21. Se establecerán elementos de seguridad que dictaminen el estado de salud del equipo usuario (estado del antivirus, conectividades, monitorización de usos y accesos, actualizaciones de aplicaciones etc.).

6.2. REQUISITOS GENERALES DEL SISTEMA VPN

6.2.1. MEDIDAS ORGANIZATIVAS

22. Deberá existir un procedimiento de alta, baja y modificación de elementos en la VPN (usuario, equipos, servicios o aplicaciones, etc.). Incluyendo auditorías periódicas de la lista de personal usuario autorizado, y la baja de aquellos que ya no sean necesarios.
23. Deberá existir un plan de operación y mantenimiento de la infraestructura VPN, acorde con los planes generales de operación y mantenimiento de la infraestructura hardware del CICA.
24. Deberá existir un plan de recuperación y backup de la infraestructura VPN, acorde con los planes generales de recuperación y backup de la infraestructura del CICA.

25. Deberá existir un procedimiento de gestión de eventos y registros de log VPN, acorde con el procedimiento general de gestión de eventos del CICA. Deberán incluirse aspectos como la información a registrar, cuánto tiempo debe conservarse, cada cuanto tiempo debe revisarse, envío de copias de los eventos a servidores centralizados de gestión, etc.
26. Deberá existir un protocolo de gestión y respuesta a incidentes de la VPN, acorde con el protocolo general de gestión de incidentes del CICA.
27. Deberá existir un procedimiento de auditorías periódicas de la infraestructura VPN, acorde con el procedimiento general de auditorías del CICA. Deberá incluirse aspectos como la periodicidad y el tipo de auditorías a realizar sobre cada componente.

6.2.2. MEDIDAS OPERACIONALES DE PROTECCIÓN

28. Se deberá definir una lista de servicios, redes y sistemas de información que pueden ser accedidos remotamente por el personal que realiza acceso remoto.
29. Se debe contar con un inventario de accesos remotos otorgados identificando a la persona que cuenta con el acceso y el motivo por el cual se le otorgó y el plazo por el cual está autorizado.
30. Se debe contar con una lista de equipos y/o tipos de equipos desde los cuales se puede acceder remotamente.
31. Se deben restringir las conexiones y accesos en función de las listas e inventario de los puntos anteriores. Se crearán perfiles en los equipos de seguridad perimetral para aplicar dichas restricciones.
32. Los equipos utilizados para el acceso remoto deben contar con protección ante software malicioso.
33. Los equipos utilizados para el acceso remoto deben estar encriptados.
34. Los equipos utilizados para el acceso remoto deberán contar con la instalación de las últimas actualizaciones del sistema operativo y los parches de seguridad correspondientes.
35. Se deberán de registrar accesos y conexiones. El acceso remoto a redes seguras debe quedar registrado con al menos: detalle de personal usuario, dispositivo, fecha y hora.
36. Se deberán registrar eventos de auditorías.
37. Se deberán de activar los servicios de monitorización con alertas definidas:
    - Accesos fuera de horario.
    - Accesos desde terceros países (si no existe causa justificada).
    - Múltiples errores de autenticación de usuario desde varias direcciones IP en un intervalo de tiempo T.
    - Múltiples errores de autenticación de varios usuarios desde una dirección IP en un intervalo de tiempo T.
    - Accesos simultáneos del mismo usuario desde dos direcciones IP en un intervalo de tiempo T.
    - Accesos correctos de diferentes usuarios desde la misma dirección IP en un intervalo de tiempo T.
    - Accesos remotos, o intentos, desde direcciones en lista negra (rangos, países, etc.).
    - Geolocalizaciones cambiantes.
    - Descarga de datos por encima de umbral.
    - Intentos de acceso desde redes privadas virtuales (VPN) a recursos no autorizados.
    - Intentos de ejecución remota desde clientes VPN).
38. Deberán evitarse las opciones de “Split-Tunneling”.
39. Se deberán revisar o tener controladas las unidades para intercambiar información.
40. Se asegurará si los antivirus escanean los dispositivos USB conectados a los equipos remotos o si se bloquea el acceso de USB en dichos equipos.
41. Se desplegará una solución EDR para los dispositivos corporativos, mientras que los usuarios con dispositivos personales (BYOD) deberán tener desplegada una solución EDR que cumpla con los niveles

de seguridad establecidos en el conjunto de normas.

6.2.3. MEDIDAS DE CONCIENCIACIÓN Y FORMACIÓN DEL PERSONAL

42. Se deberá concienciar regularmente al personal acerca de su papel y responsabilidades en el uso de la VPN. En particular hay que refrescar regularmente al menos, la normativa relativa al uso aceptable de la VPN y el reporte de incidencias.

43. Se deberá formar regularmente al personal acerca de las técnicas que requieran para el desempeño de sus funciones. Se impartirá la formación necesaria, por ejemplo, para poder llevar a cabo la instalación, configuración, administración, operación y mantenimiento de la VPN y para la gestión de incidentes en la misma.

44. Se asegurará el compromiso de los empleados de no realizar actividades ilícitas, vulnerar las políticas del CICA o utilizar el acceso remoto suministrado para obtener lucro comercial.

6.3. EQUIPOS DE SALTO

45. Si para tener acceso remoto se debe dejar el equipo del usuario instalado en el edificio, se asegurarán las siguientes medidas:

    46. Tener actualizado el puesto de trabajo con los últimos parches de seguridad (Sistema operativo, herramientas de seguridad, aplicaciones, etc.).

    47. Cerrar todas las conexiones que no sean estrictamente necesarias.

    48. Cerrar todas las aplicaciones cuando no se estén utilizando.

    49. Realizar análisis programado de los antivirus (exhaustivos) a los puestos de trabajo, aunque los ordenadores no se reinicien.

    50. Aplicar las actualizaciones programadas en el CICA.

    51. Prever mecanismos que permitan el reinicio de estas máquinas de forma remota y acceder por canales establecidos a las mismas desde fuera del CICA una vez se reinicie el equipo.

6.4. REVISIÓN PERIÓDICA DEL ACCESO REMOTO

52. Se debe definir un procedimiento de revisión periódica de las condiciones de uso del acceso remoto y de los usuarios que hacen uso de éste, que contemple la revisión de todos los puntos incluidos en la presente norma.

6.5. MODELO DE ACEPTACIÓN Y COMPROMISO DE CUMPLIMIENTO

53. Todo el personal usaurio de los recursos informáticos y/o Sistemas de Información del CICA deberán tener acceso permanente, durante el tiempo de desempeño de sus funciones, a la presente Norma, debiendo suscribirla.

54. Todo el personal del CICA que figure como destinatario de esta norma, ya sea interno o externo, tiene la obligación de conocer y cumplir la misma, así como el resto del cuerpo normativo y procedimientos.

55. En el supuesto que una persona no observe alguno de los preceptos señalados en la presente normativa, sin perjuicio de las acciones disciplinarias y administrativas que procedan y, en su caso, las responsabilidades legales correspondientes, se podrá acordar la suspensión temporal o definitiva del acceso a los Sistemas de Información usados.

56. En el caso de personal externo, se estará también a lo recogido para estos casos en los contratos de servicio suscritos con las empresas contratistas correspondientes.

Mediante la cumplimentación de la siguiente declaración, el abajo firmante, [personal del CICA/empleado de la Empresa _____/personal usuario de los servicios del CICA_____], como personal usuario de recursos informáticos y sistemas de información del CICA, declara haber leído y comprendido las Normas Acceso Remoto Seguro del CICA y se compromete, bajo su responsabilidad, a su cumplimiento.

<<En _____, a ____ de _____ de 20__>>

Empresa/Personal usuario:	
Trabajador (Nombre y Apellidos):	
DNI número:	
Número de Registro de Personal:	
Firmado:	

Revisor por parte del CICA: _____

DNI número: _____

Número de Registro de Personal: _____

