RESOLUCIÓN DE 1 DE JULIO DE 2019, DE LA PRESIDENCIA DE LA COMISIÓN NACIONAL DE LOS MERCADOS Y LA COMPETENCIA, POR LA QUE SE APRUEBA LA NORMATIVA GENERAL DE UTILIZACIÓN DE LOS RECURSOS Y SISTEMAS DE INFORMACIÓN DE LA COMISIÓN NACIONAL DE LOS MERCADOS Y LA COMPETENCIA

El 18 de junio de 2018 se aprobó, por resolución de la presidencia y en cumplimiento del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica, la Política de Seguridad de la Información de la Comisión Nacional de los Mercados y la Competencia.

En el artículo 6.1 de la Política de Seguridad de la Información se crea, adscrita a la Secretaría General, la Comisión de Seguridad de la Información como órgano que gestionará y coordinará todas las actividades relacionadas con la seguridad de los sistemas de información. El nombramiento de sus miembros se produjo por resolución de presidencia el 23 de enero de 2019.

Entre las funciones de la Comisión de Seguridad de la Información, definidas en el artículo 6.3 de la Política de Seguridad de la Información, se encuentra la de aprobar las normas de desarrollo de segundo nivel que sean elaboradas por el Responsable de Seguridad, cuya figura y funciones se regulan en el artículo 7 de la Política de Seguridad de la Información.

En virtud de esa función que tiene atribuida, la Comisión de Seguridad de la Información de la CNMC, en la reunión mantenida el 13 de junio de 2019, aprobó la elevación para su aprobación por el Presidente de la *Normativa General de Utilización de los Recursos y Sistemas de Información de la CNMC*.

En virtud de lo anterior y previa comunicación a los representantes del personal de la CNMC, en uso de las facultades que legal y reglamentariamente tiene atribuidas esta presidencia, resuelve aprobar la *Normativa General de Utilización de los Recursos y Sistemas de Información de la CNMC* que acompaña a esta resolución.

Madrid, 1 de julio de 2019

EL PRESIDENTE

José María Marín Quemada

NORMATIVA GENERAL DE UTILIZACIÓN DE LOS RECURSOS Y SISTEMAS DE INFORMACIÓN DE LA COMISIÓN NACIONAL DE LOS MERCADOS Y LA COMPETENCIA (NG00)

1. OBJETIVO Y ÁMBITO DE APLICACIÓN 4

1.1. Introducción 4

1.2. Marco Normativo 4

1.3. Ámbito de aplicación 5

1.4. Vigencia 5

1.5. Revisión y evaluación 5

1.6. Distribución, comunicación y formación 6

1.7. Cumplimiento de la normativa 6

2. UTILIZACIÓN DEL EQUIPAMIENTO INFORMÁTICO Y DE COMUNICACIONES 7

2.1. Normas generales 7

2.2. Usos específicamente prohibidos 8

2.3. Normas específicas para equipos portátiles y móviles 9

2.4. Uso de memorias USB (*pendrives*) y unidades de CD y DVD 10

2.5. Copias de seguridad 10

2.6. Almacenamiento privado y correo particular en la nube 11

2.7. Borrado y eliminación de soportes informáticos 11

2.8. Impresoras en red, fotocopiadoras, faxes y escáneres 11

2.9. Protección de la propiedad intelectual 12

3. INSTALACIÓN DE SOFTWARE 13

4. ACCESO A LOS SISTEMAS DE INFORMACIÓN Y A LOS DATOS TRATADOS 14

4.1. Cuentas de usuario 14

4.2. Cuentas de usuario para personal externo 15

4.3. Identificación y autenticación 15

5. ACCESO A INTERNET 17

5.1. Normas generales de uso 17

5.2. Usos específicamente prohibidos 17

6. USO DEL CORREO ELECTRÓNICO CORPORATIVO 19

6.1. Normas generales de uso 19

6.2. Acceso web al correo electrónico 19

6.3. Usos especialmente prohibidos 19

6.4. Copias de seguridad de los buzones de correo corporativo 20

7. VIDEOCONFERENCIAS Y MENSAJERÍA INSTANTÁNEA 22

7.1. Aspectos generales 22

7.2. Normas generales 22

7.3. Usos especialmente prohibidos 22

8. WIFI 23

8.1. Aspectos generales 23

8.2. Normas generales 23

8.3. Usos especialmente prohibidos 23

9. ACCESOS REMOTOS 24

10. CONFIDENCIALIDAD DE LA INFORMACIÓN 25

11. PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL Y DEBER DE SECRETO 26

12. SALIDAS DE INFORMACIÓN 27

13. INCIDENTES DE SEGURIDAD 28

14. COMPROMISOS DE LOS USUARIOS 29

15. MONITORIZACIÓN Y AUDITORÍAS 30

1. OBJETIVO Y ÁMBITO DE APLICACIÓN

1.1. Introducción

1. Conforme a lo dispuesto en el Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica (ENS, en adelante), y atendiendo a la medida de seguridad relativa a la Normativa de Seguridad ([org.2]) de las medidas organizativas previstas en el Anexo II del citado Real Decreto, este documento contiene la Normativa General de Utilización de los Recursos y Sistemas de Información de la Comisión Nacional de los Mercados y la Competencia (en adelante CNMC), señalando los compromisos que adquieren sus usuarios respecto a su seguridad y buen uso.

2. La utilización de recursos tecnológicos para el tratamiento de la información tiene una doble finalidad para la CNMC:

   - Facilitar y agilizar la tramitación de procedimientos administrativos, mediante el uso de herramientas informáticas y aplicaciones de gestión, y
   - Proporcionar información completa, homogénea, actualizada y fiable.

3. La utilización de equipamiento informático y de comunicaciones es actualmente una necesidad en cualquier organización del sector público. Estos medios y recursos se ponen a disposición de los usuarios como instrumentos de trabajo para el desempeño de su actividad profesional, razón por la cual compete a la CNMC determinar las normas, condiciones y responsabilidades bajo las cuales se deben utilizar tales recursos tecnológicos.

4. La presente Normativa General de Utilización de los Recursos y Sistemas de Información tiene como objetivo establecer normas encaminadas a alcanzar la mayor eficacia y seguridad en su uso.

5. Este documento se considera de uso interno de la CNMC y, por consiguiente, no podrá ser divulgado fuera del organismo salvo autorización de la Comisión de Seguridad de la Información.

1.2. Marco Normativo

6. Se han utilizado como referencias documentales que vengan a apoyar o completar esta Normativa General o que hubieren sido consideradas en su redacción las siguientes:

   - Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.
   - Resolución de 18 de junio de 2018, de la Presidencia de la Comisión Nacional de los Mercados y la Competencia, por la que se aprueba la Política de Seguridad de los Sistemas de Información de la Comisión, que establece en su artículo 15 de *Desarrollo de la Política de Seguridad*, la necesidad de desarrollarla en tres

niveles, formado el segundo de ellos por las disposiciones de seguridad entre las que se encuentra el presente documento.

- Documentos y Guías CCN-STIC (Centro Criptológico Nacional – Seguridad de las Tecnologías de la Información y las Comunicaciones). En especial, la Guía CCN-STIC 821 sobre Normas de Seguridad.

1.3. Ámbito de aplicación

7. La presente Normativa General de Utilización de los Recursos y Sistemas de Información es de aplicación y de obligado cumplimiento para todo el personal que, de manera permanente o eventual, preste sus servicios en la CNMC, incluyendo el personal de proveedores externos, cuando sean usuarios de los Sistemas de Información de la CNMC.

8. En el ámbito de la presente normativa, se entiende por usuario cualquier empleado público perteneciente o ajeno a la CNMC, así como personal de organizaciones privadas externas, entidades colaboradoras o cualquier otro con algún tipo de vinculación con la CNMC y que utilice o posea acceso a los Sistemas de Información de la misma.

1.4. Vigencia

9. La presente Normativa General de Utilización de los Recursos y Sistemas de Información de la CNMC ha sido aprobada por la Comisión de Seguridad de la Información de la CNMC, estableciendo de esta forma las directrices generales para el uso adecuado de los recursos de tratamiento de información que la CNMC pone a disposición de sus usuarios para el ejercicio de sus funciones y que, correlativamente, asumen las obligaciones descritas, comprometiéndose a cumplir con lo dispuesto en los siguientes epígrafes.

10. Se establece un periodo transitorio de dos meses desde su aprobación hasta su efectiva aplicación, a fin de posibilitar la formación necesaria y adecuar las expectativas de uso actuales de los empleados de la CNMC a la nueva normativa.

1.5. Revisión y evaluación

11. La gestión de esta Normativa General corresponde a la Comisión de Seguridad de la Información de la CNMC, que es competente para:

    - Interpretar las dudas que puedan surgir en su aplicación.
    - Aprobar las revisiones, cuando sea necesario.
    - Verificar su efectividad.

12. Anualmente (o con menor periodicidad, si existen circunstancias que así lo aconsejen), el Responsable de Seguridad revisará la presente Normativa General, que se someterá, de haber modificaciones, a la aprobación de la Comisión de Seguridad de la Información de la CNMC.

13. La revisión se orientará tanto a la identificación de oportunidades de mejora en la gestión de la seguridad de la información, como a la adaptación a los cambios habidos en el marco legal, infraestructura tecnológica, organización general, etc.

14. Será el Responsable de Seguridad el encargado de la custodia y divulgación de la versión aprobada de este documento.

1.6. Distribución, comunicación y formación

15. La presente Normativa General deberá ser conocida por todos los empleados públicos, y por el personal de servicios y asistencia técnica, a los que aplica, atendiendo a lo expuesto en el punto 1.3 de esta Normativa. A tal efecto, la Normativa se publicará en la Intranet de la CNMC, sin perjuicio de su publicación en otros portales internos si así se considerase.

16. La CNMC impulsará el desarrollo de acciones formativas en materia de seguridad de la información entre sus empleados, con especial atención a la divulgación y conocimiento de la presente Normativa.

1.7. Cumplimiento de la normativa

17. Todos los usuarios de los sistemas de información de la CNMC, están obligados a cumplir lo prescrito en la presente Normativa General de Utilización de los Recursos y Sistemas de Información, además del cumplimiento de las normativas específicas que se desarrollen a partir de ésta.

18. En el supuesto de que un usuario no observe la presente Normativa General, el Responsable de Seguridad podrá acordar la suspensión temporal del uso de los recursos informáticos asignados a tal usuario con la exclusiva finalidad de evitar el inminente riesgo al que el usuario estuviera exponiendo los sistemas o información de la organización.

19. Las acciones realizadas desde una cuenta de usuario o desde una cuenta de correo electrónico de usuario se considerarán responsabilidad de su titular, salvo que se comprobase la existencia de una suplantación de personalidad no causada por negligencia del usuario.

20. La SSTIC implantará los sistemas de protección de acceso a los sistemas que considere necesario, para evitar que se produzcan incidentes relacionados con el abuso de estos servicios.

2. UTILIZACIÓN DEL EQUIPAMIENTO INFORMÁTICO Y DE COMUNICACIONES

21. La CNMC facilita a los usuarios que así lo precisen los equipos informáticos y dispositivos de comunicaciones, tanto fijos como móviles, cuando ello resulte necesario para el desarrollo de su actividad profesional. Así pues, los datos, dispositivos, programas y servicios informáticos que la CNMC pone a disposición de los usuarios deben utilizarse para el desarrollo de las funciones encomendadas, es decir, para fines profesionales.

22. En general, el ordenador personal (PC), tanto de sobremesa como portátil, será el recurso informático que permitirá el acceso de los usuarios a los Sistemas de Información y servicios informáticos de la CNMC, constituyendo un elemento muy importante en la cadena de seguridad de los sistemas de información, razón por la que es necesario adoptar una serie de precauciones y establecer normas para su adecuada utilización.

23. Este epígrafe concierne específicamente a todos los ordenadores personales facilitados y configurados por la CNMC para su utilización por parte de los usuarios, incluyendo equipos de sobremesa, portátiles y dispositivos móviles con capacidades de acceso a los Sistemas de Información de la organización.

2.1. Normas generales

24. Las Normas Generales en todos los equipos informáticos de la CNMC serán:

- Existirá un inventario actualizado de los equipos informáticos.

- A cada nuevo usuario que se incorpore a la organización y así lo precise, la SSTIC le facilitará un ordenador personal debidamente configurado y con acceso a los servicios y aplicaciones necesarias para el desempeño de sus competencias profesionales. En función de las necesidades del puesto de trabajo, también podrán serle asignados otros dispositivos tales como portátiles, móviles o *tablets*.

- Para el alta de nuevos usuarios, se requerirá indicar a la SSTIC:
  - Nombre, apellidos y NIF
  - Relación laboral (Funcionario, Laboral, Externo, Becario)
  - Unidad
  - Puesto de trabajo
  - Nivel
  - Despacho/ubicación
  - Fecha de incorporación
  - Servicios adicionales a los estandarizados para los miembros de su unidad, a los que requiere acceso. En su caso, deberá ir acompañado de las correspondientes autorizaciones por parte de los Responsables de la Información y del Servicio.

- Salvo autorización de la SSTIC, los usuarios no tendrán privilegio de administración sobre sus equipos.

- Los usuarios deberán facilitar al personal de soporte técnico el acceso a sus equipos para labores de reparación, instalación o mantenimiento.

- Los medios informáticos de la organización deberán mantener actualizados los parches de seguridad de todos los programas que tengan instalados. La SSTIC será la responsable de prestar especial atención a la correcta actualización, configuración y funcionamiento del programa antivirus.

- Salvo aquellos ordenadores instalados en las zonas comunes de acceso a Internet (salas de reuniones, espacios compartidos, etc), cada equipo deberá estar asignado a un usuario o grupo de usuarios concreto que será responsable del cuidado y correcto uso del mismo.

- El usuario hará un uso responsable de la información y de los documentos acorde con el nivel de clasificación de los mismos.

- El cese de actividad de cualquier usuario debe ser comunicado de forma inmediata a la SSTIC, por el responsable de la unidad a la que perteneciera, al objeto de que le sean retirados los permisos correspondientes en la organización, y los recursos informáticos que le hubieren sido asignados. Correlativamente, cuando los medios informáticos o de comunicaciones proporcionados por la CNMC estén asociados al desempeño de un determinado puesto o función, la persona que los tenga asignados tendrá que devolverlos a la unidad responsable cuando finalice su vinculación con dicho puesto o función.

- Los usuarios harán un uso eficiente de los sistemas informáticos, apagando el PC (y la impresora local, en su caso), al finalizar la jornada laboral.

2.2. Usos específicamente prohibidos

25. Están terminantemente prohibidos los siguientes comportamientos:

- Utilización de hardware o software para impedir la ejecución de las políticas de seguridad y/o la auditoría de los requisitos de funcionamiento y seguridad establecidos.

- Utilización de cualquier tipo de software dañino.

- Utilización de programas que, por su naturaleza, hagan un uso abusivo de la red.

- Conexión a la red informática corporativa de cualquier equipo o dispositivo no facilitado por la SSTIC, sin la previa autorización de la misma.

- Utilización de dispositivos USB, teléfonos móviles u otros elementos, cuyo objetivo sea configurar un acceso alternativo a Internet desde los ordenadores de sobremesa, salvo autorización expresa de la SSTIC.

- Instalación y/o utilización de programas o contenidos que vulneren la legislación vigente en materia de Propiedad Intelectual.

- Acceso a servicios y/o contenidos de la CNMC con el propósito de violar su integridad o seguridad.

- Almacenar archivos personales en los servidores o en los recursos de almacenamiento compartido de la CNMC.

- El uso de los servicios de la CNMC para propósitos que puedan influir negativamente en la imagen de la CNMC, de sus representantes o de los organismos públicos o privados con los que se mantiene relación.

- La transmisión, distribución o almacenamiento de cualquier material obsceno, difamatorio, amenazador o que constituya un atentado contra la dignidad de las personas.

2.3. Normas específicas para equipos portátiles y móviles

26. Las normas descritas a continuación son de aplicación específica a los equipos informáticos y dispositivos de comunicaciones que no están necesariamente conectados a un punto físico de acceso e incluye los ordenadores portátiles, *tablets*, *smartphones* y similares.

- Este tipo de dispositivos estará bajo la custodia del usuario que los utilice, quien deberá adoptar las medidas necesarias para evitar daños o sustracción, así como el acceso a ellos por parte de personas no autorizadas.

- La sustracción de estos equipos se considera un incidente de seguridad y está sujeto a lo expuesto en el apartado 13 de esta Normativa.

- Los usuarios de estos equipos se responsabilizarán de que no serán usados por terceras personas ajenas o no autorizadas para ello.

- Los equipos portátiles no deberán conectarse directamente a redes WiFi no confiables o inseguras, tales como redes abiertas cuya propiedad se desconoce.

- Los usuarios de equipos portátiles y móviles deberán extremar la precaución en las conexiones a redes expuestas en lugares públicos incluso si resultan de confianza. Especialmente en la transmisión de contenidos de forma no cifrada (por ejemplo, sin https o sin VPN).

- La SSTIC puede proporcionar accesos remotos autorizados y configurados a través de tarjetas móviles. Cuando este sea el caso, la utilización de estos accesos deberá utilizarse con preferencia sobre las redes WiFi públicas.

- Los usuarios de equipos portátiles deberán realizar conexiones periódicas al menos cada mes a la red corporativa (por red local o VPN), según las instrucciones proporcionadas por la SSTIC, para permitir la actualización de aplicaciones, sistema operativo, firmas de antivirus y demás medidas de seguridad. En su defecto, cada cuatro meses, los equipos portátiles serán entregados a la SSTIC para la actualización del software.

- Como norma general, los dispositivos portátiles se entregarán con todos los canales, puertos y sistemas de comunicaciones de salida de información (WiFi, Bluetooth, IrDA, memorias USB, unidades CD, unidades DVD, tarjetas de red, y similares) habilitados y correctamente configurados. El usuario será responsable de toda la información extraída fuera de la organización a través de dichos canales, puertos y sistemas, así como del uso que se haga de la misma.

- Cuando se modifiquen las circunstancias profesionales (término de una tarea, cese en el cargo, etc.) que originaron la entrega de un recurso informático móvil, el usuario lo devolverá a la SSTIC, al objeto de proceder al borrado seguro de la información almacenada y restaurar el equipo a su estado original para que pueda ser asignado a un nuevo usuario.

2.4. Uso de memorias USB (*pendrives*) y unidades de CD y DVD

27. Las memorias USB se deben utilizar como herramienta de transporte de ficheros, no como herramienta de almacenamiento. Para cubrir las necesidades de almacenamiento, la SSTIC pone a disposición de los usuarios unidades de almacenamiento en red.

28. Además, como alternativa a las USB, la SSTIC pondrá a disposición de todo el personal herramientas adecuadas para la transferencia de ficheros dentro de la CNMC.

29. Por razones de seguridad, la SSTIC podrá deshabilitar los interfaces periféricos de los puestos de usuario (USB, CD, DVD).

30. La pérdida o sustracción de una memoria USB, CD o DVD, se considera un incidente de seguridad y está sujeto a lo expuesto en el apartado 13 de esta Normativa.

2.5. Copias de seguridad

31. De forma periódica, se realizarán copias de seguridad, tanto completas como incrementales, de las unidades de red compartidas de la CNMC donde se almacene la información del usuario, tanto de las unidades asignadas de forma personal como de las asociadas a grupos de usuarios.

32. En ningún caso se realizará copia de seguridad de la información almacenada de forma local en el puesto del usuario.

33. La información almacenada en las copias de seguridad podrá ser recuperada en caso de que se produzca algún incidente. Para recuperar esta información el usuario habrá de solicitarlo a la SSTIC.

2.6. Almacenamiento privado y correo particular en la nube

34. Con carácter general, el almacenamiento privado en la nube, o en el espacio que asignan algunos proveedores de correo electrónico, debe evitarse para evitar la fuga de información corporativa.

35. La CNMC se reserva el derecho de bloquear el acceso a dichas nubes públicas de forma que cualquier acceso a éstas cuando, por motivos profesionales, deba ser desbloqueado por la SSTIC, será realizado bajo petición y requerirá la autorización del responsable de la unidad. El derecho de acceso se mantendrá sólo por el tiempo estrictamente necesario para obtener la información deseada.

2.7. Borrado y eliminación de soportes informáticos

36. Cuando el soporte contenga información que, de acuerdo a su nivel de clasificación, deba ser sometida a un borrado seguro, el usuario deberá entregarlo a la SSTIC y el responsable de la unidad deberá realizar una petición de borrado seguro a la SSTIC.

2.8. Impresoras en red, fotocopiadoras, faxes y escáneres

37. Con carácter general, deberán utilizarse exclusivamente las impresoras en red y las fotocopiadoras, equipos de fax y escáneres corporativos.

38. Excepcionalmente, podrán instalarse de forma local, y gestionados por un puesto de trabajo de usuario, alguno de los dispositivos mencionados en los puntos anteriores. Para ello, será requisito imprescindible que el responsable de la unidad del peticionario realice una solicitud a la SSTIC justificando la necesidad.

39. En el caso de los faxes, sólo se instalarán cuando exista una necesidad que no pueda ser cubierta con el uso de otros medios de comunicación que no supongan la utilización de papel, tales como el correo electrónico.

40. Cuando se haga uso de fotocopiadoras o impresoras, será necesario recoger los originales de la misma una vez finalizado el proceso de copia.

41. Cuando se envíe un fax, el usuario deberá comprobar cuidadosamente el número de destino y los documentos enviados deberán retirarse inmediatamente del equipo.

42. Cuando se digitalicen documentos, el usuario deberá prestar especial atención a la selección del destino de las imágenes obtenidas, y no olvidar retirar los originales.

43. Si un usuario encontrase documentación abandonada en alguna impresora, fotocopiadora, equipo de fax o escáner, intentará localizar a su propietario para que éste la recoja inmediatamente y, en caso de desconocer a su propietario o no localizarlo, lo pondrá inmediatamente en conocimiento de la SSTIC.

44. Los usuarios deberán imprimir únicamente aquellos documentos que sean estrictamente necesarios. La impresión se hará, preferiblemente, a doble cara y evitando, siempre que sea posible, la impresión en color.

2.9. Protección de la propiedad intelectual

45. Está estrictamente prohibida la ejecución de programas informáticos en los Sistemas de Información de la CNMC sin la correspondiente licencia de uso.

46. Los programas informáticos propiedad de la CNMC o licenciados por la CNMC están protegidos por la vigente legislación sobre Propiedad Intelectual y, por tanto, está estrictamente prohibida su reproducción, modificación, cesión, transformación o comunicación, salvo que los términos del licenciamiento lo permitan y con la autorización previa de la SSTIC.

3. INSTALACIÓN DE SOFTWARE

47. De forma general, únicamente el personal de soporte técnico autorizado por la SSTIC podrá instalar software en los equipos informáticos o de comunicaciones de los usuarios.

48. Todo usuario podrá solicitar la instalación de una aplicación, que será objeto de estudio por parte de la SSTIC.

49. Excepcionalmente, justificando la necesidad y con la aprobación de la SSTIC, un usuario podrá disponer de un usuario con permisos suficientes para la instalación de software en su propio equipo informático (usuario ADM).

50. Los identificadores de los usuarios ADM que se asignen deberán ser diferentes que los identificadores de los usuarios habituales del personal y claramente distinguibles.

51. Los usuarios ADM no deben utilizarse para iniciar sesión en los equipos informáticos, salvo para realizar funciones de administración, y sólo por el tiempo necesario para esa tarea. No deberán utilizarse en ningún caso para realizar un uso cotidiano, como por ejemplo navegar por internet, leer el correo o realizar trabajos habituales por razón de su cargo en la CNMC.

52. Los usuarios no deberán instalar ningún software desde una fuente no confiable y, en caso de duda, se solicitará la evaluación de la misma a la SSTIC.

4. ACCESO A LOS SISTEMAS DE INFORMACIÓN Y A LOS DATOS TRATADOS

53. Los datos y servicios gestionados por la CNMC y tratados por cualquier sistema de Información de la CNMC deben tener asignado un Responsable de la Información y un Responsable del Servicio, según el caso, que serán los encargados de conceder, alterar o anular la autorización de acceso a dichos datos y servicios.

4.1. Cuentas de usuario

54. Todas las altas de usuarios que deban acceder a los recursos informáticos de la CNMC deberán solicitarse a la SSTIC, para la asignación de una cuenta de usuario.

55. Cada unidad de la CNMC dispondrá de un perfil de acceso estandarizado a recursos informáticos, que tendrá la consideración de mínimo para todos los usuarios de dicha unidad. La SSTIC será la responsable de mantener actualizada esta relación entre perfiles de acceso y recursos informáticos.

56. Los Responsables de la Información y Responsables del Servicio aprobarán la lista de perfiles estandarizados que tienen acceso a los activos de su responsabilidad.

57. Adicionalmente, en la solicitud de alta de nuevo usuario y con la correspondiente autorización de los Responsables de la Información y Responsables del Servicio, se podrá solicitar acceso a recursos adicionales a los del perfil de acceso estandarizado para la unidad a la que pertenece el usuario.

58. La concesión, alteración o anulación de la autorización de acceso a un determinado servicio o información, o a sus recursos asociados, será competencia del Responsable de dicho Servicio o Información. De esta forma, cualquier solicitud de acceso a un servicio o información que no forme parte del perfil de acceso estandarizado para la unidad del usuario, deberá realizarse a la SSTIC acompañada de la correspondiente autorización del Responsable del Servicio o Información, y del responsable de la unidad a la que pertenezca el usuario.

59. Cuando un usuario deje de atender un PC durante un cierto tiempo, es necesario bloquear la sesión de usuario, para evitar que ninguna persona pueda hacer un mal uso de sus credenciales, pudiendo llegar a suplantarlo. Por razones de seguridad, el PC de un usuario se bloqueará automáticamente tras un periodo de inactividad de 15 minutos.

60. La baja de los usuarios será comunicada a la SSTIC que procederá a la eliminación de todos los servicios asociados a la misma a excepción del servicio de correo electrónico. Para el correo electrónico se permite un período de cortesía, fijado en la normativa específica, tras la baja efectiva del usuario. Transcurrido el periodo de cortesía, se procederá a la baja total de la cuenta, junto con la supresión de todo dato de carácter personal asociado al usuario.

4.2. Cuentas de usuario para personal externo

61. El personal ajeno a la CNMC que temporalmente deba acceder a los sistemas de información, deberá hacerlo siempre bajo la supervisión de algún miembro acreditado de la CNMC (enlace). Este enlace realizará ante la SSTIC la solicitud del acceso.

62. Cuando el enlace responsable realice una solicitud de acceso, deberá indicar siempre una fecha de expiración para el acceso, justificando la elección de la misma. Esta fecha podrá ampliarse mediante solicitud expresa del enlace responsable.

63. Como norma general, el acceso a la red de la CNMC se realizará desde dispositivos informáticos proporcionados por la SSTIC para tal fin.

64. Si, excepcionalmente, el acceso a la red de la CNMC se fuera a realizar desde dispositivos informáticos que no sean propiedad de la CNMC, éstos deberán de cumplir con los requisitos mínimos de seguridad (antivirus actualizado, sistema operativo correctamente parcheado, etc) que la CNMC tenga establecidos y de los que el enlace debe informar.

4.3. Identificación y autenticación

65. Los usuarios dispondrán de un identificador de usuario y una contraseña para el acceso a los Sistemas de Información de la CNMC, y son responsables de la custodia de los mismos y de toda actividad relacionada con el uso de su acceso autorizado. Estos datos tienen carácter personal y se tratarán conforme a lo establecido en el Registro de Tratamientos de la CNMC.

66. El identificador de usuario es único para cada persona en la organización, intransferible e independiente del PC o terminal desde el que se realiza el acceso.

67. La SSTIC adoptará las medidas técnicas y organizativas necesarias respecto de los sistemas de información de la CNMC que garanticen la confidencialidad de las credenciales de acceso de los usuarios e impidan que puedan ser conocidas por terceros.

68. Los usuarios no deben revelar o entregar, bajo ningún concepto, sus credenciales de acceso a otra persona, ni mantenerlas por escrito a la vista o al alcance de terceros.

69. Los usuarios no deben utilizar ningún acceso autorizado de otro usuario, aunque dispongan de la autorización de su titular.

70. Cada identificador de usuario tendrá establecida una contraseña individual y no se permitirá la existencia de ningún identificador de usuario sin la misma.

71. Los usuarios deben utilizar contraseñas que cumplan los requisitos de seguridad.

72. El acceso a los sistemas de información de la CNMC mediante el par identificador de usuario y contraseña podrá servir como prueba para delimitar responsabilidades frente a usos indebidos de los sistemas de información.

73. Si un usuario tiene sospechas de que sus credenciales están siendo utilizadas por otra persona, debe proceder inmediatamente a comunicar el incidente de seguridad según lo expuesto en el apartado 13 de esta Normativa.

74. Las características que deben cumplir las contraseñas de la CNMC estarán definidas en su normativa específica.

5. ACCESO A INTERNET

5.1. Normas generales de uso

75. Las normas generales de uso del acceso a internet de la CNMC serán:

- Las conexiones que se realicen a internet deben obedecer a fines profesionales, teniendo siempre en cuenta que se están utilizando recursos informáticos restringidos y escasos. El acceso a Internet para fines personales debe limitarse y sólo utilizarse durante un tiempo razonable que no interfiera en el rendimiento profesional ni en la eficiencia de los recursos informáticos corporativos.

- Sólo se podrá acceder a Internet mediante los navegadores suministrados y configurados por la CNMC en los puestos de usuario. No podrá alterarse la configuración del mismo ni utilizar un navegador alternativo, sin la debida autorización de la SSTIC.

- En el caso de dispositivos móviles, portátiles y *tablets*, se podrá también acceder a internet haciendo uso de la red WiFi de la CNMC.

- Deberá notificarse, según lo expuesto en el apartado 13 de esta Normativa, cualquier anomalía detectada en el uso del acceso a internet, así como la sospecha de posibles problemas o incidentes de seguridad relacionados con dicho acceso.

- El acceso a sitios de internet considerados maliciosos o inapropiados estará restringido atendiendo a categorías que se establecen de forma automática. En el caso de que un usuario precise acceder a un sitio y considere que éste está mal categorizado, deberá informar a la SSTIC para que se corrija la situación.

5.2. Usos específicamente prohibidos

76. Están terminantemente prohibidos los siguientes comportamientos:

- La descarga de programas informáticos desde sitios no confiables o de dudosa reputación o ficheros con contenido dañino que supongan una fuente de riesgos para la organización. En todo caso, en caso de duda, debe consultarse a la SSTIC.

- La utilización de aplicaciones o herramientas (especialmente, el uso de programas de intercambio de información, P2P) para la descarga masiva de archivos, programas u otro tipo de contenido (música, películas, etc.) que no esté expresamente autorizada por la SSTIC.

- La conexión al equipo del puesto de trabajo de módems, teléfonos móviles u otros elementos de comunicación, con el fin de ser utilizados como punto de acceso alternativo a Internet.

- Uso de cualquier software, servicio o mecanismo cuya finalidad sea modificar la seguridad perimetral o las limitaciones de navegación establecidas.

6. USO DEL CORREO ELECTRÓNICO CORPORATIVO

6.1. Normas generales de uso

77. Todos los usuarios que lo precisen para el desempeño de su actividad profesional, dispondrán de una cuenta de correo electrónico, para el envío y recepción de mensajes internos y externos a la organización.

78. El sistema tendrá establecidas limitaciones en el intercambio de correos en función de su tamaño.

79. El correo corporativo deberá utilizarse para la realización de las funciones encomendadas al personal, evitando el uso privado del mismo.

80. El usuario notificará cualquier anomalía detectada, así como los correos no deseados (spam) que se reciban, utilizando los canales establecidos al efecto por la SSTIC, a fin de configurar adecuadamente las medidas de seguridad oportunas.

81. Se deberá prestar especial atención a los ficheros adjuntos en los correos recibidos. No deben abrirse ni ejecutarse ficheros de fuentes no fiables, puesto que podrían contener virus o código malicioso. En caso de duda sobre la confiabilidad de los mismos, se deberá notificar esta circunstancia a la SSTIC.

82. No se debe utilizar el correo electrónico como espacio de almacenamiento. La capacidad de espacio en los servidores de correo de la CNMC es limitada. Cuando una cuenta se satura puede ser que se restrinjan por parte del servidor los privilegios de envío y/o recepción de mensajes. Por todo ello, se recomienda conservar únicamente los mensajes imprescindibles y revisar periódicamente aquellos que hubieran quedado obsoletos.

6.2. Acceso web al correo electrónico

83. El acceso al correo corporativo podrá hacerse de forma remota a través de una dirección de internet (correo electrónico vía web).

84. Los navegadores utilizados para acceder al correo vía web deben estar permanentemente actualizados a su última versión, al menos en cuanto a parches de seguridad, así como correctamente configurados.

85. Una vez finalizada la sesión web, es obligatoria la desconexión con el servidor cerrando la sesión.

86. Durante el acceso web al correo electrónico, se deberán desactivar las características de recordar contraseñas por el navegador.

6.3. Usos especialmente prohibidos

87. Las siguientes actuaciones están explícita y especialmente prohibidas:

- El envío de correos electrónicos con contenido inadecuado, ilegal, ofensivo, difamatorio, inapropiado o discriminatorio por razón de sexo, raza, edad, discapacidad, que contengan programas informáticos (software) sin licencia, que vulneren los derechos de propiedad intelectual de los mismos, de alerta de virus falsos o difusión de virus reales y código malicioso, o cualquier otro tipo de contenidos que puedan perjudicar a los usuarios, identidad e imagen corporativa y a los propios sistemas de información de la organización.

- El envío de mensajes que contengan amenazas, ofensas o imputación de hechos que puedan lesionar la dignidad personal y, en general, la utilización del correo electrónico de manera ilegal o infringiendo cualquier norma que pudiera resultar de aplicación.

- El acceso a un buzón de correo electrónico distinto del propio y el envío de correos electrónicos con usuarios distintos del propio. Está terminantemente prohibido suplantar la identidad de un usuario de internet, correo electrónico o cualquier otra herramienta colaborativa.

- La difusión de la cuenta de correo del usuario en listas de distribución, foros, servicios de noticias, etc, que no sean consecuencia de la actividad profesional del usuario.

- Responder mensajes de los que se tenga sospechas sobre su autenticidad, confiabilidad y contenido, o mensajes que contengan publicidad no deseada.

- La utilización del correo corporativo como medio de intercambio de ficheros especialmente voluminosos. En el caso de requerir intercambiar ficheros voluminosos con personal externo a la organización, se deberán de utilizar, en su lugar, las herramientas que la SSTIC ponga a disposición de los usuarios que lo soliciten para este fin.

- El envío de información protegida (sensible o confidencial) sin contar con la autorización de su Responsable.

- La utilización del correo corporativo para recoger correo de buzones que no pertenezcan a la CNMC o el reenvío automático del correo corporativo a buzones ajenos a la organización. Para ello se necesitará la autorización expresa de la SSTIC.

6.4. Copias de seguridad de los buzones de correo corporativo

88. El sistema de correo está configurado de forma que durante los primeros 14 días tras la eliminación de un correo, éste podrá ser recuperado por el propio usuario o bien solicitar a la SSTIC su recuperación.

89. Más allá de ésta retención de correo durante 14 días, no existe otra configuración de copiado de seguridad ni recuperación del correo electrónico de la CNMC ante una eliminación expresa del correo.

90. La SSTIC adoptará las medidas técnicas y organizativas necesarias que garanticen la seguridad e integridad de la información conservada, impidan la manipulación y uso de misma para fines distintos de los previstos en esta norma, su destrucción accidental o ilícita y su pérdida accidental, así como su almacenamiento, tratamiento, divulgación o acceso no autorizados.

7. VIDEOCONFERENCIAS Y MENSAJERÍA INSTANTÁNEA

7.1. Aspectos generales

91. La CNMC pone a disposición del personal de la organización un servicio de videoconferencia con personal interno y externo, desde el puesto de trabajo y en las salas de reuniones.

92. La CNMC pondrá a disposición del personal de la organización, igualmente, el servicio de mensajería instantánea corporativo, al que se puede solicitar acceso a través de petición a la SSTIC.

7.2. Normas generales

93. Cualquier videoconferencia en la CNMC tiene que realizarse desde los equipos y aplicaciones que la SSTIC pone a disposición de los usuarios.

94. Se deberá notificar a la SSTIC cualquier tipo de anomalía detectada, a fin de configurar adecuadamente las medidas de seguridad oportunas. Cuando el hecho notificado suponga un incidente de seguridad, la SSTIC informará al Responsable de Seguridad.

95. El solicitante del evento se hace responsable del buen uso de los equipos, mobiliario y servicios utilizados en la Sala de Videoconferencia.

96. El equipo instalado en la Sala de Videoconferencia debe ser operado por el personal de la SSTIC o, en su caso, por el usuario solicitante siguiendo las instrucciones proporcionadas por la SSTIC.

7.3. Usos especialmente prohibidos

97. Las siguientes actuaciones están explícita y especialmente prohibidas:

- Manipular los equipos de videoconferencia para alterar su configuración y funcionamiento.

- Trasladar los equipos de videoconferencia sin la autorización expresa de la SSTIC.

8. WIFI

8.1. Aspectos generales

98. La CNMC pone a disposición del personal de la organización un servicio de red inalámbrica (WiFi corporativa). Este servicio permite conectarse a internet desde equipos inalámbricos, pero no conectarse a la red interna de la CNMC.

99. Además, la CNMC pone a disposición del personal invitado a las instalaciones de la CNMC un servicio de red inalámbrica específico para invitados (WiFi invitados). Este servicio permite conectarse a internet desde equipos inalámbricos, pero no conectarse a la red interna de la CNMC.

100. La cobertura de estas redes no es completa en todos los edificios y se centra, principalmente, en las zonas de mayor concurrencia pública y en las salas de reuniones.

8.2. Normas generales

101. El acceso a la red wifi corporativa, se otorgará automáticamente a todos los empleados de la CNMC y se configurará por parte del personal técnico de la SSTIC en los equipos corporativos de movilidad (portátiles, móviles, *tablets*, etc).

102. La red WiFi es una red de menor velocidad y capacidades que la red cableada además de un recurso compartido y limitado por lo que deberá utilizarse con responsabilidad.

103. El personal de la CNMC que actúe como *enlace* del personal invitado a las instalaciones de la CNMC será el responsable de proporcionarle las credenciales de acceso a la wifi invitados y de informar de las normas para su correcto uso.

8.3. Usos especialmente prohibidos

104. Cualquier tipo de conexión dual que pueda proporcionar acceso a la red corporativa a terceros. En especial, permanecer conectado a la red wifi corporativa o de invitados desde un dispositivo que esté compartiendo su conexión o actuando como hot-spot por cualquier medio.

105. Manipular los puntos de acceso wifi para alterar su orientación o estado.

106. Instalar cualquier punto de acceso wifi no autorizado por la SSTIC.

9. ACCESOS REMOTOS

107. La CNMC ofrecerá accesos de conexión remota a los servicios corporativos y sistemas de información para aquellos usuarios que así lo precisen.

108. Los accesos remotos se realizarán mediante el establecimiento de conexiones cifradas y estarán basados en perfiles en función de la necesidad de acceso e interacción con los sistemas.

109. Los accesos remotos estarán, en todo caso, configurados de forma que la seguridad de la información esté garantizada mediante el control de accesos y el cifrado de las comunicaciones y se basarán en el principio de mínimo privilegio.

110. El usuario podrá hacer uso de los servicios e infraestructuras de la CNMC a través del acceso remoto mediante la utilización de equipos proporcionados por la SSTIC, los cuales vendrán configurados con todas las medidas de seguridad necesarias y les será de aplicación lo dispuesto en el apartado 2.1 de la presente Normativa.

111. El usuario que haga uso de los servicios e infraestructuras de la CNMC a través de acceso remoto mediante la utilización de un ordenador doméstico será responsable de tener perfectamente instalado y actualizado un antivirus en su equipo de acceso, así como las actualizaciones de seguridad del sistema operativo y de las aplicaciones. La SSTIC no prestará ningún tipo de soporte a estos dispositivos y conexiones.

112. En todo caso, el acceso remoto a los servicios e infraestructuras de la CNMC desde ordenadores públicos, entendiendo por estos aquellos que se alquilan por tiempo de conexión, salas de internet de disponibilidad pública, cibercafés y similares está estrictamente prohibido.

10. CONFIDENCIALIDAD DE LA INFORMACIÓN

113. Todo el personal de la organización o ajeno a la misma que, por razón de su actividad profesional, hubiera tenido acceso a información gestionada por la CNMC (tal como datos personales, documentos, metodologías, claves, análisis, programas, etc.) deberán mantener sobre ella, por tiempo indefinido, una absoluta reserva. El personal externo a la CNMC deberá firmar un documento de confidencialidad.

114. En el caso de entrar en conocimiento de información que no sea de libre difusión, en cualquier tipo de soporte, deberá entenderse que dicho conocimiento es estrictamente temporal mientras dure la función encomendada, con la obligación de secreto o reserva indefinidas y sin que ello le confiera derecho alguno de posesión, titularidad o copia del mismo.

115. Los usuarios sólo podrán acceder a aquella información para la que posean las debidas y explícitas autorizaciones, en función de las labores que desempeñen, no pudiendo en ningún caso acceder a información perteneciente a otros usuarios o grupos de usuarios para los que no se posea tal autorización.

116. Los soportes de información que vayan a ser reutilizados o causen baja deberán ser previamente tratados para eliminar permanentemente la información que pudieran contener, de manera que resulte imposible su recuperación. Estos soportes deberán entregarse a la SSTIC.

117. Se evitará almacenar información protegida (sensible o confidencial) en medios desatendidos (tales como CDs, DVDs, memorias USB, listados, etc.) o dejar visible tal información en la misma pantalla del ordenador.

118. Toda la información contenida en los Sistemas de Información de la CNMC o que circule por sus redes de comunicaciones debe ser utilizada únicamente para el cumplimiento de las funciones encomendadas a la CNMC y a su personal.

11. PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL Y DEBER DE SECRETO

119. La información contenida en las bases de datos de la CNMC que comprenda datos de carácter personal está protegida por el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos) y por su normativa derivada o de desarrollo. Igualmente será de aplicación lo dispuesto en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

120. Todo usuario (de la CNMC o de terceras organizaciones) que, en virtud de su actividad profesional, pudiera tener acceso a datos de carácter personal, está obligado a guardar secreto sobre los mismos.

121. En cualquier caso, la información de la CNMC que comprenda datos de carácter personal, así como su tratamiento, estarán sujetos a las normas y directrices correspondientes, bajo el asesoramiento y supervisión del Delegado de Protección de Datos de la CNMC.

12. SALIDAS DE INFORMACIÓN

122. La salida de información se realizará de conformidad con las autorizaciones que en su caso se prevean, y de acuerdo con el Responsable de la Información.

123. La salida de datos protegidos (sensibles o confidenciales), requerirá su cifrado o la utilización de cualquier otro mecanismo que garantice que la información no será inteligible durante su remisión o transporte.

13. INCIDENTES DE SEGURIDAD

124. La SSTIC pondrá a disposición de los usuarios un medio para informar de los incidentes de seguridad que permita registrar debidamente el incidente e informar de forma simultánea al Responsable de Seguridad y a la SSTIC.

125. Cuando un usuario detecte cualquier anomalía o incidencia de seguridad que pueda comprometer el buen uso y funcionamiento de los Sistemas de Información de la CNMC o su imagen, deberá informar inmediatamente de esta situación mediante los canales que la SSTIC tenga establecidos.

126. Cuando se tenga conocimiento o sospechas fundadas de que una información se ha visto comprometida o se ha perdido, la SSTIC informará de este hecho al Responsable de la Información y al Responsable de Seguridad, y se tomarán todas las medidas oportunas legalmente establecidas.

127. Si la información comprometida contuviese datos de carácter personal, el Responsable de Seguridad o en su defecto la propia SSTIC alertarán al Delegado de Protección de Datos a la mayor brevedad, a fin de que se apliquen los procedimientos de protección de datos establecidos en la CNMC[1].

128. Si el personal de soporte técnico detectase cualquier anomalía que indicara una utilización de los recursos contraria a la presente Normativa, lo pondrá en conocimiento de la SSTIC, que tomará las oportunas medidas correctoras y dará traslado de la incidencia al Responsable de Seguridad.

129. En relación a aquellas categorías de incidencias informáticas diferentes de "incidentes de seguridad", el Responsable de Seguridad podrá requerir a la SSTIC el acceso temporal o permanente a las mismas.

[1] PRC-DPD-014, Procedimientos en materia de Protección de Datos Personales en el ámbito de la Comisión Nacional de los Mercados y la Competencia

14. COMPROMISOS DE LOS USUARIOS

130. Usar los sistemas de información con fines profesionales, salvo excepciones ocasionales.

131. Custodiar las credenciales que se le proporcionen y seguir todas las recomendaciones de seguridad que elaboren el Responsable de Seguridad y la SSTIC, para garantizar que aquellas no puedan ser utilizadas por terceros. Deberá cerrar su cuenta al terminar la sesión o bloquear el equipo cuando lo deje desatendido.

132. No destruir o modificar de forma no autorizada la información, de manera premeditada.

133. No incurrir en actuaciones que violen la intimidad de otras personas o el secreto de las comunicaciones.

134. No deteriorar intencionadamente los recursos informáticos de la CNMC ni el trabajo de otras personas.

135. No conectar a la red corporativa cableada de comunicaciones dispositivos distintos de los admitidos, habilitados y configurados por la CNMC, salvo autorización de la SSTIC.

136. Notificar, utilizando los medios expuestos en el apartado 13 de esta Normativa, cualquier sospecha de un incidente de seguridad.

15. MONITORIZACIÓN Y AUDITORÍAS

137. La SSTIC revisará periódicamente el estado de los equipos, el software instalado, los dispositivos y las redes de comunicaciones de su responsabilidad y comprobará la seguridad de las credenciales y de las aplicaciones de los sistemas de información.

138. La SSTIC será la encargada de establecer los sistemas de monitorización, auditoría y control de los sistemas de información de la CNMC, con la finalidad exclusiva de lograr el cumplimiento del objeto de esta Normativa. Ello sin perjuicio de la función de control auditor que pueda recabar y realizar el Departamento de Control Interno. A tal fin, la SSTIC y DCI se coordinarán en las funciones de auditoría y control para evitar duplicidades.

139. De acuerdo con lo previsto en el artículo 23 del Esquema Nacional de Seguridad, la SSTIC llevará a cabo esta actividad de monitorización de manera proporcional al riesgo, con las cautelas legales pertinentes y con respeto y observancia de los derechos de los usuarios.

140. Para el cumplimiento de lo dispuesto en el punto anterior, los datos de conexión y tráfico podrán ser almacenados en un registro a efectos de investigación de incidentes de seguridad o de violaciones de la presente Normativa.

141. El uso de Internet, del correo electrónico, y el acceso al resto de los servicios y sistemas de la CNMC podrá ser monitorizado para todos los usuarios, a los exclusivos fines de seguridad previstos en esta Normativa.

142. La SSTIC monitoriza el tráfico de navegación en Internet a fin de detectar volúmenes de tráfico masivo o conexiones sospechosas que puedan ser indicadores de alguna actividad de software malicioso o de alguna amenaza para la seguridad.

143. La SSTIC podrá limitar o cortar el servicio de Internet a aquellos usuarios que, haciendo uso de la reproducción de archivos multimedia o de la descarga de ficheros, generen un volumen de tráfico que vaya en detrimento de la prestación del servicio o que suponga un incumplimiento de la presente Normativa.

144. La SSTIC, mediante el sistema que proporciona el servicio de correo electrónico podrá, de forma automatizada, rechazar, bloquear o eliminar parte del contenido de los mensajes enviados o recibidos en los que se detecte algún problema de seguridad o de incumplimiento de la presente Normativa. Se podrá insertar contenido adicional en los mensajes enviados con objeto de advertir a los receptores de los mismos de los requisitos legales y de seguridad que deberán cumplir en relación con dichos correos.

145. La SSTIC adoptará las medidas técnicas y organizativas necesarias que garanticen la seguridad e integridad de la información conservada, impidan la manipulación y uso de misma para fines distintos de los previstos en esta norma, su destrucción accidental o ilícita y su pérdida accidental, así como su almacenamiento, tratamiento, divulgación o acceso no autorizados.

146. Los sistemas en los que se detecte un uso inadecuado, o en los que no se cumplan los requisitos mínimos de seguridad, podrán ser bloqueados o suspendidos

temporalmente, restableciéndose el servicio cuando la causa de su inseguridad o degradación desaparezca.