GOBIERNO DE ESPAÑA
MINISTERIO DE HACIENDA Y FUNCIÓN PÚBLICA

CCN Centro Criptológico Nacional

Guía de Seguridad de las TIC
CCN-STIC 821

APÉNDICE I: NORMATIVA GENERAL DE UTILIZACIÓN DE LOS RECURSOS Y SISTEMAS DE INFORMACIÓN DE LA ENTIDAD NG00

CCN Centro Criptológico Nacional

CENTRO CRIPTOLOGICO NACIONAL
2.5.4.13=Qualified Certificate: AAPP-SEP-M-SW-KPSC,
ou=sello electrónico, serialNumber=S2800155J,
o=CENTRO CRIPTOLOGICO NACIONAL, cn=CENTRO
CRIPTOLOGICO NACIONAL, c=ES
2018.02.22 16:59:13 +01'00'

FEBRERO 2018

ÍNDICE

1. OBJETIVO

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 (ENS, en adelante), este documento contiene la **Normativa General de Utilización de los Recursos y Sistemas de Información de la <<ENTIDAD>>**[1], gestionados o bajo la responsabilidad de la <<ENTIDAD>>, señalando asimismo los compromisos que adquieren sus usuarios respecto a su seguridad y buen uso.

   La presente Normativa General de Utilización de los Recursos y Sistemas de Información de la <<ENTIDAD>> deberá ser complementada, en su caso y en la medida oportuna, con la aplicación de las medidas de seguridad previstas en el Anexo II del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad (ENS).

2. Los **Sistemas de Información**[2] constituyen elementos básicos para el desarrollo de las misiones encomendadas a la <<ENTIDAD>>, por lo que los usuarios deben utilizar estos recursos de manera que se preserven en todo momento las dimensiones de la seguridad sobre las informaciones manejadas y los servicios prestados: disponibilidad, integridad, confidencialidad, autenticidad y trazabilidad.
3. La utilización de recursos tecnológicos para el tratamiento de la información tiene una doble finalidad para la <<ENTIDAD>>:
   - 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.
4. 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 <<ENTIDAD>> determinar las normas, condiciones y responsabilidades bajo las cuales se deben utilizar tales recursos tecnológicos.
5. Por tanto, la presente Normativa General de Utilización de los Recursos y Sistemas de Información de la <<ENTIDAD>> tiene como objetivo establecer normas encaminadas a alcanzar la mayor eficacia y seguridad en su uso.

6. Este documento se considera de uso interno de la <<ENTIDAD>> y, por consiguiente, no podrá ser divulgado salvo autorización de <<U/OC>>[3].

[1] Cualquier organismo de las Administraciones públicas del ámbito de aplicación del ENS. Puede ser también aplicado a unidades administrativas inferiores, si disponen de la autonomía correspondiente para decidir sobre su propia normativa.

[2] Siguiendo la definición dada por el ENS, en el ámbito de esta Normativa General se entiende por Sistema de Información todo conjunto organizado de recursos para que la información se pueda recoger, almacenar, procesar o tratar, mantener, usar, compartir, distribuir, poner a disposición, presentar o transmitir. (RD 3/2010, ENS – Anexo IV – Glosario.)

[3] **Unidad / Organismo Colegiado** competente para desarrollar la acción que se menciona. En ocasiones, un mismo párrafo puede contener varias de estas expresiones, que podrán referirse a la misma unidad o a unidades distintas, según corresponda.

2. ÁMBITO DE APLICACIÓN

7. Esta Normativa General es de aplicación a todo el ámbito de actuación de la <<ENTIDAD>>, y sus contenidos traen causa de las directrices de carácter más general definidas en la Política de Seguridad de la Información de la <<ENTIDAD>>.

8. 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 <<ENTIDAD>>, incluyendo el personal de proveedores externos, cuando sean usuarios de los Sistemas de Información de la <<ENTIDAD>>.

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

3. VIGENCIA

10. La presente Normativa General de Utilización de los Recursos y Sistemas de Información del <<ORGANSMO>> ha sido aprobada por la <<U/OC>> de la <<ENTIDAD>>, estableciendo de esta forma las directrices generales para el uso adecuado de los recursos de tratamiento de información que la <<ENTIDAD>> 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.

11. Cualquier modificación posterior entrará en vigor inmediatamente después de su publicación por parte de la <<ENTIDAD>>.

12. Las versiones anteriores que hayan podido distribuirse constituyen borradores que se han desarrollado temporalmente, por lo que su vigencia queda anulada por la última versión de esta Normativa General.

4. REVISIÓN Y EVALUACIÓN

13. La gestión de esta Normativa General corresponde a la <<U/OC>>, que es competente para:

    - Interpretar las dudas que puedan surgir en su aplicación.
    - Proceder a su revisión, cuando sea necesario para actualizar su contenido o se cumplan los plazos máximos establecidos para ello.
    - Verificar su efectividad.

14. Anualmente (o con menor periodicidad, si existen circunstancias que así lo aconsejen), la <<U/OC>> revisará la presente Normativa General, que se someterá, de haber modificaciones, a la aprobación de la <<U/OC>> de la <<ENTIDAD>>.

15. 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.

16. Será el Responsable de Seguridad la persona encargada de la custodia y divulgación

de la versión aprobada de este documento.

5. REFERENCIAS

17. *<<En este epígrafe se deben incluir aquellas referencias documentales que vengan a apoyar o completar esta Norma o que hubieren sido consideradas en su redacción.*

***Internas**:*

- ----
- ----
-

***Externas**:*

(Por ejemplo:

- *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.*
- *UNE - ISO/IEC 27002:2005 Código de buenas prácticas para la Gestión de la Seguridad de la información.*
- *UNE - ISO/IEC 27001:2007 Especificaciones para los Sistemas de Gestión de la Seguridad de la Información.*
- *ISO/IEC 9001:2000 Sistemas de gestión de la calidad.*
- *Documentos y Guías CCN-STIC.*
- *Etc.>>*

6. UTILIZACIÓN DEL EQUIPO INFORMÁTICO Y DE COMUNICACIONES

18. La <<ENTIDAD>> facilita a los usuarios que así lo precisen los equipos informáticos y dispositivos de comunicaciones, tanto fijos como móviles, necesarios para el desarrollo de su actividad profesional. Así pues, los datos, dispositivos, programas y servicios informáticos que la <<ENTIDAD>> pone a disposición de los usuarios deben utilizarse para el desarrollo de las funciones encomendadas, es decir, para fines profesionales. Cualquier uso de los recursos con fines distintos a los autorizados está estrictamente prohibido.

19. En general, el ordenador personal (PC) será el recurso informático que permitirá el acceso de los usuarios a los Sistemas de Información y servicios informáticos de la <<ENTIDAD>>, 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.

20. Este epígrafe concierne específicamente a todos los ordenadores personales facilitados y configurados por la <<ENTIDAD>> 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.

6.1. NORMAS GENERALES

- Los equipos informáticos serán asignados por la <<U/OC>>.
- Existirá un inventario actualizado de los equipos informáticos. La <<U/OC>> será la unidad encargada de gestionar dicho inventario.

- A cada nuevo usuario que se incorpore a la organización y así lo precise, la <<U/OC>> le facilitará un ordenador personal debidamente configurado y con acceso a los servicios y aplicaciones necesarias para el desempeño de sus competencias profesionales.

  Para el alta de nuevos usuarios, se requerirá:

  - Nombre, apellidos y NIF.
  - Despacho/ubicación, teléfono y dirección de correo electrónico.
  - Área a la que se incorpora.
  - Servicios a los que requiere acceso.
  - Aplicaciones y perfiles.
  - *<<señalar otros, si fuere preciso>>*.

- Los ordenadores personales deberán utilizarse únicamente para fines institucionales y como herramienta de apoyo a las competencias profesionales de los usuarios autorizados.
- Únicamente el personal autorizado por la <<U/OC>> podrá distribuir, instalar o desinstalar software y hardware, o modificar la configuración de cualquiera de los equipos, especialmente en aquellos aspectos que puedan repercutir en la seguridad de los Sistemas de Información de la <<ENTIDAD>>. Cuando se precise instalar dispositivos no provistos por la <<ENTIDAD>> deberá solicitarse autorización previa a la <<U/OC>>.
- Está prohibido alterar, sin la debida autorización, cualquiera de los componentes físicos o lógicos de los equipos informáticos y dispositivos de comunicación, salvo autorización expresa de la <<U/OC>>. En todo caso, estas operaciones sólo podrán realizarse por el personal de soporte técnico autorizado.
- Salvo autorización expresa de la <<U/OC>>, los usuarios no tendrán privilegio de administración sobre los equipos.
- Los usuarios deberán facilitar al personal de soporte técnico el acceso a sus equipos para labores de reparación, instalación o mantenimiento. Este acceso se limitará únicamente a las acciones necesarias para el mantenimiento o la resolución de problemas que pudieran encontrarse en el uso de los recursos informáticos y de comunicaciones, y finalizará completado el mantenimiento o una vez resueltos aquellos.
- Si el personal de soporte técnico detectase cualquier anomalía que indicará una utilización de los recursos contraria a la presente norma, lo pondrá en conocimiento de la <<U/OC>>, que tomará las oportunas medidas correctoras y dará traslado de la incidencia a la <<U/OC>>.
- Los ordenadores personales de la organización deberán mantener actualizados los parches de seguridad de todos los programas que tengan instalados. Se deberá prestar especial atención a la correcta actualización, configuración y funcionamiento de los programas antivirus y cortafuegos.
- Los usuarios deberán notificar a la <<U/OC>>, a la mayor brevedad posible, cualquier comportamiento anómalo de su ordenador personal, especialmente cuando existan sospechas de que se haya producido algún incidente de seguridad

en el mismo.

- Salvo aquellos ordenadores instalados en las zonas comunes de acceso a Internet, cada equipo deberá estar asignado a un usuario o grupo de usuarios concreto. Tales usuarios son responsables de su correcto uso.
- El usuario deberá participar en el cuidado y mantenimiento del equipo que tiene asignado, detectando la ausencia de cables y accesorios, y dando cuenta a la <<U/OC>> de tales circunstancias.
- El usuario debe ser consciente de las amenazas provocadas por malware. Muchos virus y troyanos requieren la participación de los usuarios para propagarse, ya sea a través de disquetes, CDs/DVDs, memorias USB, mensajes de correo electrónico o instalación de programas descargados desde Internet. Es imprescindible, por tanto, vigilar el uso responsable los equipos para reducir este riesgo.
- El usuario será responsable de toda la información extraída fuera de la organización a través de dispositivos tales como memorias USB, CDs, DVDs, etc., que le hayan sido asignados. Es imprescindible un uso responsable de los mismos, especialmente cuando se trate información sensible, confidencial o protegida.
- El cese de actividad de cualquier usuario debe ser comunicada de forma inmediata a la <<U/OC>>, al objeto de que le sean retirados los recursos informáticos que le hubieren sido asignados. Correlativamente, cuando los medios informáticos o de comunicaciones proporcionados por la <<ENTIDAD>> estén asociados al desempeño de un determinado puesto o función, la persona que los tenga asignados tendrá que devolverlos inmediatamente a la unidad responsable cuando finalice su vinculación con dicho puesto o función.

6.2. USOS ESPECÍFICAMENTE PROHIBIDOS

21. Están terminantemente prohibidos los siguientes comportamientos:

- Ejecución remota -salvo autorización- de archivos de tipo audiovisual (música, vídeo, animaciones, etc.)
- 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 <<ENTIDAD>>, sin la previa autorización de la <<U/OC>>.
- Utilización de conexiones y medios inalámbricos con tecnologías WiFi, Bluetooth o infrarrojos que no estén debidamente autorizados por la <<U/OC>>.
- Utilización de dispositivos USB, teléfonos móviles u otros elementos, como acceso alternativo a Internet, salvo autorización expresa de la <<U/OC>>.
- Instalación y/o utilización de programas o contenidos que vulneren la legislación vigente en materia de Propiedad Intelectual. Este comportamiento estará sometido a las previsiones disciplinarias, administrativas, civiles o penales descritas en las leyes.

6.3. NORMAS ESPECÍFICAS PARA EL ALMACENAMIENTO DE INFORMACIÓN

- Con carácter general, la información almacenada de forma local en los ordenadores personales de los usuarios (disco duro local, por ejemplo) no será objeto de salvaguarda mediante ningún procedimiento corporativo de copia de seguridad. Por tanto, cuando tal almacenamiento esté autorizado en las normas internas correspondientes, se recomienda a los usuarios la realización periódica de copias de seguridad, especialmente de la información importante para el desarrollo de su actividad profesional.
- La <<ENTIDAD>> puede poner a disposición de ciertos usuarios unidades de red compartidas para contener las salvaguardadas periódicas de sus unidades locales. Debe tenerse en cuenta que tales unidades corporativas son un recurso limitado y compartido por todos los usuarios, por lo que sólo deberá salvaguardarse la información que se considere estrictamente necesaria.
- No está permitido almacenar información privada, de cualquier naturaleza, en los recursos de almacenamiento compartidos o locales, salvo autorización previa de la <<U/OC>>.

6.4. NORMAS ESPECÍFICAS PARA EQUIPOS PORTÁTILES Y MÓVILES

- Los equipos portátiles y móviles serán asignados por la <<U/OC>>.
- Existirá un inventario actualizado de los equipos portátiles y móviles. La <<U/OC>> será la unidad encargada de gestionar dicho inventario.
- Este tipo de dispositivos estará bajo la custodia del usuario que los utilice o del responsable de la <<U/OC>>. Ambos deberán 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 ha de poner inmediatamente en conocimiento de la <<U/OC>> para la adopción de las medidas que correspondan y a efectos de baja en el inventario.
- Los equipos portátiles y móviles deberán utilizarse únicamente para fines institucionales y autorizados, especialmente cuando se usen fuera de las instalaciones de la <<ENTIDAD>>.
- Los usuarios de estos equipos se responsabilizarán de que no serán usados por terceras personas ajenas a la <<ENTIDAD>> o no autorizadas para ello.
- En general, los equipos portátiles no deberán conectarse directamente a redes externas (incluyendo la red o el acceso a Internet del usuario en su domicilio). La <<ENTIDAD>> puede proporcionar accesos remotos autorizados y configurados por la <<U/OC>> a través de tarjetas móviles. Cuando este sea el caso, deberán realizar de forma obligatoria dicha conexión cuando requieran el acceso a Internet desde dichos equipos. En casos debidamente justificados y previamente autorizados por la <<U/OC>> se podrá hacer uso de conexiones alternativas, observando estrictas medidas de seguridad en cuanto a la navegación en Internet y el resto de los preceptos de la presente Normativa General que resulten de aplicación.

- Los usuarios de equipos portátiles deberán realizar conexiones periódicas <<señalar periodicidad>> a la red corporativa, según las instrucciones proporcionadas por la <<U/OC>>, para permitir la actualización de aplicaciones, sistema operativo, firmas de antivirus y demás medidas de seguridad. En su defecto, cada <<señalar periodicidad>>, los equipos portátiles serán entregados a la <<U/OC>> para la actualización de tal software.
- Cuando la tipología de la información tratada así lo requiera, los ordenadores portátiles afectados deberán tener cifrado el disco duro, disponer de software que garantice un arranque seguro, así como mecanismos de auditoría capaces de crear un registro por cada fichero extraído del sistema por cualquier medio (red, dispositivos extraíbles, impresoras, etc.).
- Como norma general, los equipos portátiles se configurarán por defecto con todos los canales, puertos y sistemas de comunicaciones de salida de información bloqueados (WiFi, Bluetooh, USB's, CD, DVD, tarjetas de red, etc.). Por petición justificada dirigida a la <<U/OC>>, se podrán habilitar algunas o todas las funciones de salida de información.
- Los usuarios no tendrán privilegio de administración sobre los equipos portátiles, teniendo prohibido realizar cualquier modificación hardware/software sobre los mismos. Corresponderá a la <<U/OC>> llevar a cabo estas modificaciones.
- 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 <<U/OC>>, 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.

6.5. NORMAS ESPECÍFICAS PARA MEMORIAS/LÁPICES USB (PENDRIVES)

22. Con carácter general, el uso de memorias USB en la <<ENTIDAD>> no está autorizado. En su caso, la autorización deberá proporcionarla la <<U/OC>>.
23. Por razones de seguridad, los interfaces USB de los puestos de usuario estarán deshabilitados. En caso de ser necesaria su habilitación, deberá justificarse por el usuario y requerirá la previa autorización del jefe de la unidad y la <<U/OC>>.
24. En el caso de que a un usuario se le autorice el uso del interfaz USB de su puesto de trabajo, las memorias USB utilizadas serán las proporcionadas por la <<ENTIDAD>>, que serán conformes a las normas de seguridad de la organización. Estas memorias USB serán de uso exclusivo en los puestos de usuario de la <<ENTIDAD>>, no debiendo ser usados fuera de éstos.
25. Se recuerda que las memorias USB están destinadas a un uso exclusivamente profesional, como herramienta de transporte de ficheros, no como herramienta de almacenamiento. La <<U/OC>> podrá poner a disposición de los usuarios de aplicaciones, servicios y sistemas de la <<ENTIDAD>> unidades de almacenamiento en red, que podrán usarse para tal propósito.
26. La pérdida o sustracción de una memoria USB, con indicación de su contenido, deberá ponerse en conocimiento de la <<U/OC>>, de forma inmediata.

6.6. GRABACIÓN DE CDs Y DVDs

27. Con carácter general, el uso de equipos grabadores de CDs y DVDs en la <<ENTIDAD>> no está autorizado. En su caso, la autorización deberá proporcionarla la <<U/OC>>.

28. Por razones de seguridad, los equipos grabadores de CDs y DVDs de los puestos de trabajo estarán deshabilitados. En el caso de ser necesaria su habilitación, deberá justificarse por el usuario y requerirá la previa autorización del jefe de la unidad y por la <<U/OC>>.

6.7. COPIAS DE SEGURIDAD

29. Mantener copias de seguridad es una cautela esencial de protección de la información.

30. Los datos generados por el usuario en el desempeño de sus competencias profesionales deberán mantenerse en un repositorio único, en una unidad de red compartida.

31. De forma periódica, se realizarán copias de seguridad, tanto completas como incrementales, de las unidades de red compartidas de la <<ENTIDAD>> donde se almacene la información del usuario. En ningún caso se realizará copia de seguridad de la información almacenada de forma local en el puesto del usuario.

32. 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 dirigirse a <<*herramienta de Atención a Usuarios*>>, gestionada por la <<U/OC>>.

6.8. BORRADO Y ELIMINACIÓN DE SOPORTES INFORMÁTICOS

33. Las copias de seguridad o los medios de almacenamiento que, por obsolescencia o degradación, pierdan su utilidad, y especialmente aquellos que contengan información sensible, confidencial o protegida, deberán ser eliminados de forma segura para evitar accesos ulteriores a dicha información. En este sentido, el usuario deberá:

    - Asegurarse del contenido de cualquier soporte antes de su eliminación.
    - Cuando contenga información sensible, confidencial o protegida, el soporte deberá destruirse según los procedimientos establecidos por la <<ENTIDAD>>.

34. Cualquier petición de eliminación de soporte informático deberá ser autorizada expresamente por la <<U/OC>>, previa petición del jefe de la unidad. Esta petición deberá dirigirse a través de la apertura de una incidencia a la <<*herramienta de Atención a Usuarios*>>, gestionada por <<U/OC>>, que será responsable de la destrucción o almacenamiento de los medios informáticos obsoletos.

6.9. IMPRESORAS EN RED, FOTOCOPIADORAS Y FAXES

35. Con carácter general, deberán utilizarse las impresoras en red y las fotocopiadoras corporativas. Excepcionalmente, podrán instalarse impresoras locales, gestionadas por un puesto de trabajo de usuario. En este caso, la instalación irá precedida de la autorización pertinente por parte del responsable del peticionario. En ningún caso

el usuario podrá hacer uso de impresoras, fotocopiadoras o equipos de fax que no hayan sido proporcionados por la <<ENTIDAD>> y, en su consecuencia, estén debidamente inventariados.

36. Cuando se imprima documentación, deberá permanecer el menor tiempo posible en las bandejas de salida de las impresoras, para evitar que terceras personas puedan acceder a la misma.

37. Conviene no olvidar tomar los originales de la fotocopiadora, una vez finalizado el proceso de copia. Si se encontrase documentación sensible, confidencial o protegida abandonada en una fotocopiadora o impresora, el usuario intentará localizar a su propietario para que éste la recoja inmediatamente. Caso de desconocer a su propietario o no localizarlo, lo pondrá inmediatamente en conocimiento de la <<U/OC>>[4].

38. Los documentos que se envíen por fax deberán retirarse inmediatamente del equipo, de modo que nadie tenga acceso a su contenido si no dispone de la autorización precisa.

6.10. DIGITALIZACIÓN DE DOCUMENTOS

39. Con carácter general, cuando se digitalicen documentos el usuario deberá ser especialmente cuidadoso con la selección del directorio compartido donde habrán de almacenarse las imágenes obtenidas, especialmente si contienen información sensible, confidencial o protegida.

40. Conviene no olvidar tomar los originales del escáner, una vez finalizado el proceso de digitalización. Si se encontrase documentación sensible, confidencial o protegida abandonada en un escáner, el usuario intentará localizar a su propietario para que éste la recoja inmediatamente. Caso de desconocer a su propietario o no localizarlo, lo pondrá inmediatamente en conocimiento de la <<U/OC>>[5].

6.11. CUIDADO Y PROTECCIÓN DE LA DOCUMENTACIÓN IMPRESA

41. La documentación impresa que contenga datos sensibles, confidenciales o protegidos, debe ser especialmente resguardada, de forma que sólo tenga acceso a ella el personal autorizado, debiendo ser recogida rápidamente de las impresoras y fotocopiadoras y ser custodiada en armarios bajo llave.

42. Cuando concluya la vida útil de los documentos impresos con información sensible, confidencial o protegida, deberán ser eliminados en las máquinas destructoras de la <<ENTIDAD>>, de forma que no sea recuperable la información que pudieran contener.

43. Si, una vez impresa, es necesario almacenar tal documentación, el usuario habrá de asegurarse de proteger adecuadamente y bajo llave aquellas copias que contengan información sensible, confidencial o protegida, o crítica para su trabajo.

44. Por razones ecológicas y de seguridad, antes de imprimir documentos, el usuario debe asegurarse de que es absolutamente necesario hacerlo.

[4] Dependiendo de la tipología de la información hallada, podrá abrirse el correspondiente incidente de seguridad.
[5] Ídem.

6.12. PIZARRAS Y FLIPCHARTS

45. Antes de abandonar las salas o permitir que alguien ajeno entre, se limpiaran adecuadamente las pizarras y *flipcharts* de las salas de reuniones o despachos, cuidando que no quede ningún tipo de información sensible o que pudiera ser reutilizada.

6.13. PROTECCIÓN DE LA PROPIEDAD INTELECTUAL

46. Está estrictamente prohibida la ejecución de programas informáticos en los Sistemas de Información de la <<ENTIDAD>> sin la correspondiente licencia de uso.

47. Los programas informáticos propiedad de la <<ENTIDAD>> o licenciados a la <<ENTIDAD>> 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 <<U/OC>>.

48. Análogamente, está estrictamente prohibido el uso, reproducción, cesión, transformación o comunicación pública de cualquier otro tipo de obra protegida por derechos de Propiedad Intelectual, sin la debida autorización de la <<U/OC>>.

6.14. PROTECCIÓN DE LA DIGNIDAD DE LAS PERSONAS

49. Está terminantemente prohibida toda transmisión, distribución o almacenamiento de cualquier material obsceno, difamatorio, amenazador o que constituya un atentado contra la dignidad de las personas.

7. USO EFICIENTE DE EQUIPOS Y RECURSOS INFORMÁTICOS

50. Dentro de las medidas de austeridad y reducción del gasto de la <<ENTIDAD>>, se promueven las siguientes acciones para un uso más eficiente de los medios tecnológicos puestos a disposición de los usuarios.

    - Apagar el PC (y la impresora local, en su caso), al finalizar la jornada laboral. Esta medida obedece tanto a razones de seguridad como de eficiencia energética.
    - 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.
    - Se optará por usar las impresoras en red antes que las locales.
    - Puesto que los recursos de almacenamiento en red son limitados y compartidos entre todos los usuarios, es preciso hacer un uso responsable de los mismos y almacenar únicamente aquella información que sea estrictamente necesaria.

8. INSTALACIÓN DE SOFTWARE

51. Únicamente el personal de soporte técnico autorizado por la <<U/OC>> podrá instalar software en los equipos informáticos o de comunicaciones de los usuarios.

52. Excepción a esta norma serán aquellas herramientas de uso común incluidas en el <<*Catálogo de Aplicaciones Autorizadas*>> de la <<ENTIDAD>>, descargables desde

los servidores internos a la <<ENTIDAD>>.

53. Todo usuario podrá solicitar la inclusión de una aplicación en dicho <<*Catálogo de Aplicaciones Autorizadas*>> para su estudio por parte de <<U/OC>>.

54. No se podrá instalar o utilizar software que no disponga de la licencia correspondiente o cuya utilización no sea conforme con la legislación vigente en materia de Propiedad Intelectual.

55. Se prohíbe terminantemente la reproducción, modificación, transformación, cesión, comunicación o uso fuera del ámbito de la <<ENTIDAD>> de los programas y aplicaciones informáticas instaladas en los equipos que pertenecen a la organización.

56. En ningún caso se podrán eliminar o deshabilitar las aplicaciones informáticas instaladas por la <<U/OC>>, especialmente aquellas relacionadas con la seguridad.

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

57. Los datos gestionados por la <<ENTIDAD>> y tratados por cualquier Sistema de Información de la <<ENTIDAD>> deben tener asignado un responsable, que será el encargado de conceder, alterar o anular la autorización de acceso a dichos datos por parte de los usuarios.

58. El alta de los usuarios será comunicada a la <<U/OC>>. Para acceder a los recursos informáticos es necesario tener asignada previamente una cuenta de usuario y estar dado de alta en los servidores de dominio. La autorización del acceso establecerá el perfil necesario con el que se configuren las funcionalidades y privilegios disponibles en las aplicaciones según las competencias de cada usuario, adoptando una política de asignación de privilegios mínimos necesarios para la realización de las funciones encomendadas.

59. Es responsabilidad del usuario hacer buen uso de su cuenta de usuario. La cuenta se podrá desactivar por la <<U/OC>> en caso de mala utilización.

60. Los usuarios tendrán autorizado el acceso únicamente a aquella información y recursos que precisen para el desarrollo de sus funciones. El acceso a la información será personal y las credenciales de acceso, intransferibles.

61. Cuando un usuario deje de atender un PC durante un cierto tiempo, es necesario bloquear la sesión de usuario o activar el salvapantallas, para evitar que ninguna persona pueda hacer un mal uso de sus credenciales, pudiendo llegar a suplantarlo. Deberá salvaguardar cualquier información, documento, soporte informático, dispositivo de almacenamiento extraíble, etc., que pueda contener información confidencial o protegida frente a posibles revelaciones o robos de terceros no autorizados. Por razones de seguridad, el PC de un usuario se bloqueará automáticamente tras un periodo de inactividad de <<x>> minutos.

62. La baja de los usuarios será comunicada a la <<U/OC>>, para proceder a la eliminación efectiva de los derechos de acceso y los recursos informáticos asignados al mismo.

10. IDENTIFICACIÓN Y AUTENTICACIÓN

63. Los usuarios dispondrán de un código de usuario (*user-id*) y una contraseña (*password*) o bien una tarjeta criptográfica con certificado digital, para el acceso a los Sistemas de Información de la <<ENTIDAD>>, y son responsables de la custodia de los mismos y de toda actividad relacionada con el uso de su acceso autorizado. El código de usuario es único para cada persona en la organización, intransferible e independiente del PC o terminal desde el que se realiza el acceso.

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

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

66. Si un usuario tiene sospechas de que sus credenciales están siendo utilizadas por otra persona, debe proceder inmediatamente a comunicar a <<U/OC>> la correspondiente incidencia de seguridad.

67. El procedimiento para la creación y utilización de contraseñas robustas está descrito en el Apéndice V de la presente Guía.

68. Si, en un momento dado, un usuario recibiera una llamada telefónica solicitándole su nombre de usuario y contraseña, nunca facilitará dichos datos y procederá a comunicar este hecho a la <<U/OC>>, de forma inmediata.

11. ACCESO Y PERMANENCIA DE TERCEROS EN LOS EDIFICIOS, INSTALACIONES Y DEPENDENCIAS DE LA <<ENTIDAD>>

11.1. NORMAS

69. Los terceros ajenos a la <<ENTIDAD>> que, eventualmente, permanecieran en sus edificios, instalaciones o dependencias, deberán observar las siguientes normas:

- El personal ajeno a la <<ENTIDAD>> que temporalmente deba acceder a los Sistemas de Información de la <<ENTIDAD>>, deberá hacerlo siempre bajo la supervisión de algún miembro acreditado de la <<ENTIDAD>> (*enlace*) y previa autorización de la <<U/OC>>.
- Cualquier incidencia que surja antes o en el transcurso del acceso a la <<ENTIDAD>> deberá ponerlo en conocimiento de su *enlace*. La función del *enlace* será dar asesoramiento, atender consultas o necesidades, transmitir instrucciones, ponerle al corriente de sus cometidos, objetivos, etc.
- Para los accesos de terceros a los sistemas de información de la <<ENTIDAD>>, siempre que sea posible, se les crearán usuarios temporales que serán eliminados una vez concluido su trabajo en la <<ENTIDAD>>. Si, de manera excepcional, tuvieran que utilizar identificadores de usuarios ya existentes, una vez finalizados dichos trabajos, se procederá al cambio inmediato de las contraseñas de los usuarios utilizados.
- Tales personas, en lo que les sea de aplicación, deberán cumplir puntualmente la presente Normativa General, así como el resto de normativa de seguridad de la <<ENTIDAD>>, especialmente en lo referente a los apartados de salida y

confidencialidad de la información.

- Para acceder a los edificios, instalaciones o dependencias de la <<ENTIDAD>> deberá estar en posesión de la correspondiente documentación de identificación personal admitida en Derecho (DNI., pasaporte, etc.), debiendo estar incluido en la relación nominal proporcionada previamente por la empresa a la que perteneciere. La primera vez que acceda físicamente deberá identificarse al personal de Control de Acceso y solicitar la presencia de la persona responsable de la <<ENTIDAD>>, que constituirá su enlace durante su estancia en él.
- La acreditación personal que se le proporcione en el Control de Acceso deberá portarse en lugar visible en todo momento, debiendo ser entregada a la salida.
- Una vez en el interior de los edificios, dependencias o instalaciones de la <<ENTIDAD>>, los terceros sólo tendrán autorización para permanecer en el puesto de trabajo que les haya sido asignado y en las zonas de uso común (aseos, comedor, zona de máquinas de cafetería, etc.).
- Asimismo, deberán tener autorización del enlace cuando tengan necesidad de realizar desplazamientos entre distintos departamentos de la <<ENTIDAD>>.
- Los terceros atendrán siempre los requerimientos que le hiciere el personal de control y seguridad de los edificios, instalaciones o dependencias a los que tuvieren acceso.

11.2. MODELO DE PROTOCOLO DE FIRMA

He leído y comprendido las presentes Normas de Acceso y Permanencia en <<*Organismo y Dependencia*>> y acepto íntegramente su contenido, en los términos expresados, comprometiéndome a su cumplimiento.

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

Empresa:	
Trabajador (Nombre y Apellidos):	
DNI número:	
Firmado:	

Enlace de la <<ENTIDAD>>: _____

DNI número: _____

11.3. MODELO DE AUTORIZACIONES Y HABILITACIONES PERSONALES

<<Cada entidad o, dentro de ella, cada dependencia con requisitos concretos de seguridad, podrá disponer de su propio Modelo de Autorizaciones y Habilitaciones personales>>

Autorizaciones y Habilitaciones				
Horario de trabajo:				
Ubicación del puesto de trabajo:				
Áreas con acceso físico autorizado				
		SÍ	NO	Observaciones
Planta 0	Zona 1			
	Zona 2			
	Zona 3			
Planta 1	Zona 1			
	Zona 2			
	Zona 3			
Uso de teléfono:				
Uso del puesto de trabajo:				
Uso ordenador portátil:				
Conexión a la red corporativa:				
Salida a Internet:				
Servidores con acceso autorizado	Tipo 1			
	Tipo 2			
	Tipo 3			
Acceso a control de versiones:				
Acceso a gestor documental:				
Acceso a carpetas de red:				
Otras:				

12. CONFIDENCIALIDAD DE LA INFORMACIÓN

70. Como medida de protección de la información propia, confiada o tratada por la <<ENTIDAD>>, está absolutamente prohibido el envío al exterior de información, electrónicamente, mediante soportes informáticos o por cualquier otro medio, que

no hubiere sido previamente autorizada por la <<U/OC>>.

71. 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 <<ENTIDAD>> (tal como datos personales, documentos, metodologías, claves, análisis, programas, etc.) deberán mantener sobre ella, por tiempo indefinido, una absoluta reserva.

72. 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. Asimismo, se deberán devolver los soportes de información utilizados inmediatamente después de la finalización de las tareas que hubieren originado su uso.

73. 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.

74. Los derechos de acceso a la información y a los Sistemas de Información que la tratan deberán siempre otorgarse en base a los principios de mínimo privilegio posible y necesidad de conocer.

75. La información contenida en los Sistemas de Información de la <<ENTIDAD>> es propiedad de la <<ENTIDAD>>, por lo que los usuarios deben abstenerse de comunicar, divulgar, distribuir o poner en conocimiento o al alcance de terceros (externos o internos no autorizados) dicha información, salvo autorización expresa de la <<U/OC>>.

76. 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 <<U/OC>>.

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

78. Los datos de la <<ENTIDAD>> que tienen el carácter de datos protegidos, son los siguientes: <<*enumerar*>> y, sobre ellos, además de las anteriores, se deberán observar las siguientes cautelas:

- *Precisar, en su caso.*
- ---
- ---

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

79. La información contenida en las bases de datos de la <<ENTIDAD>> que comprenda datos de carácter personal está protegida por la normativa vigente, europea y nacional, en materia de Protección de Datos. Los Ficheros o Tratamientos de datos

de carácter personal gestionados por la <<ENTIDAD>> han de adoptar las medidas de seguridad que se correspondan con las exigencias previstas o derivadas de la antedicha normativa.

80. Todo usuario (de la <<ENTIDAD>> 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, deber que se mantendrá de manera indefinida, incluso más allá de la relación laboral o profesional con la <<ENTIDAD>>.

14. TRATAMIENTO DE LA INFORMACIÓN

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

82. Cualquier tratamiento en los Sistemas de Información de la <<ENTIDAD>> deberá ser conforme con la normativa vigente, especialmente con lo dispuesto en la normativa vigente, europea y nacional, en materia de Protección de Datos.

83. Queda prohibido, asimismo, transmitir o alojar información sensible, confidencial o protegida propia de la <<ENTIDAD>> en servidores externos a la <<ENTIDAD>> salvo autorización expresa de la <<U/OC>>, que comprobará la inexistencia de trabas legales para ello y verificará la suscripción de un contrato expreso entre la <<ENTIDAD>> y la empresa responsable de la prestación del servicio, incluyendo los Acuerdos de Nivel de Servicio que procedan, el correspondiente Acuerdo de Confidencialidad, y siempre previo análisis de los riesgos asociados a tal externalización.

15. SALIDAS DE INFORMACIÓN

84. La salida de información de la <<ENTIDAD>> (en cualquier soporte o por cualquier medio de comunicación) deberá ser realizada exclusivamente por personal autorizado por la <<U/OC>>, autorización que contemplará igualmente a la propia información que sale.

85. La salida de datos sensibles, confidenciales o protegidos, requerirá su cifrado o la utilización de cualquier otro mecanismo que garantice que la información no será inteligible durante su remisión o transporte. Adicionalmente, si la información en cuestión contiene datos de carácter personal, se actuará conforme a lo dispuesto en la normativa vigente en materia de Protección de Datos.

86. Los usuarios se abstendrán de sacar al exterior cualquier información de la <<ENTIDAD>> en cualquier dispositivo (CDs, DVDs, memorias USB, ordenadores o dispositivos portátiles, etc.), salvo en los supuestos indicados en los puntos anteriores.

16. COPIAS DE SEGURIDAD

87. Si un usuario está autorizado para almacenar información en forma local (por ejemplo, en el disco duro del PC asignado), deberá tener en cuenta que es responsable de realizar las copias de seguridad de la misma. Por este motivo, se recomienda que los usuarios almacenen sus ficheros de trabajo en las carpetas de red habilitadas al efecto.

88. Por parte de la <<U/OC>> se realizarán <<*señalar periodicidad*>> copias de seguridad de los ficheros del sistema de almacenamiento en red (carpetas del servidor) y del resto de sistemas corporativos.

89. Si algún usuario desea recuperar algún fichero borrado del sistema de almacenamiento en red, lo participará a <<U/OC>>.

17. CONEXIÓN DE DISPOSITIVOS A LAS REDES DE COMUNICACIONES

90. No se podrá conectar en la red de comunicaciones corporativa ningún dispositivo distinto de los admitidos, habilitados y configurados por la <<ENTIDAD>>, salvo autorización previa de la <<U/OC>>.

18. USO DEL CORREO ELECTRÓNICO CORPORATIVO[6]

91. El correo electrónico corporativo es una herramienta de mensajería electrónica centralizada, puesta a disposición de los usuarios de la <<ENTIDAD>>, para el envío y recepción de correos electrónicos mediante el uso de cuentas de correo corporativas.

92. Se trata de un recurso compartido por todos los usuarios de la organización, por lo que un uso indebido del mismo repercute de manera directa en el servicio ofrecido a todos.

93. Por ello, se dictan las siguientes normas de uso.

18.1. NORMAS GENERALES

- 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.
- Únicamente podrán utilizarse las herramientas y programas de correo electrónico suministrados, instalados y configurados por la <<ENTIDAD>>.
- El correo corporativo deberá utilizarse, única y exclusivamente, para la realización de las funciones encomendadas al personal, quedando totalmente prohibido el uso privado del mismo.
- Se deberá notificar a la <<U/OC>> cualquier tipo de anomalía detectada, así como los correos no deseados (*spam*) que se reciban, a fin de configurar adecuadamente las medidas de seguridad oportunas.
- 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 <<U/OC>>.
- Está terminantemente prohibido suplantar la identidad de un usuario de internet, correo electrónico o cualquier otra herramienta colaborativa.

[6] Por la especial incidencia del correo electrónico en el mantenimiento de la seguridad IT de los Sistemas de Información, el organismo puede optar por redactar una Normativa Especial sobre esta materia. Por tanto, las normas que se citan en este epígrafe deben considerarse generales. La norma NP20 de esta misma Guía contiene un Modelo.

- Para verificación y monitorización, los datos de conexión y tráfico se guardarán en un registro durante el tiempo que establezca la normativa vigente en cada supuesto. En ningún caso esta retención de datos afectará al secreto de las comunicaciones[7].

18.2. USOS ESPECIALMENTE PROHIBIDOS

94. 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 acceso a un buzón de correo electrónico distinto del propio y el envío de correos electrónicos con usuarios distintos del propio.
- 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 sin autorización, y el envío de información sensible, confidencial o protegida. El sistema evitará el intercambio de correos de tamaños superiores a <<*señalar tamaño máximo*>>.
- La utilización del correo corporativo para recoger correo de buzones que no pertenezcan a la <<ENTIDAD>> o el reenvío automático del correo corporativo a buzones ajenos a la organización. Para ello se necesitará la autorización expresa de la <<U/OC>>.

18.3. RECOMENDACIONES ADICIONALES

- Asegurar que los reenvíos de mensajes previamente recibidos se transmitan únicamente a los destinatarios apropiados.
- Evitar, en la medida de lo posible, el uso ineficiente en los envíos de correo: agrupar los envíos a múltiples destinatarios en un solo mensaje, evitar la incorporación de firmas escaneadas, imágenes y fondos como formato habitual de los correos (ya que incrementan innecesariamente el tamaño y volumen de los mismos), envíos innecesarios, etc.
- Los buzones de correo se configuran con un tamaño para almacenamiento limitado (<<*señalar tamaño máximo*>>). El sistema indicará cuándo se encuentra al límite de su capacidad, tras el cual no se permitirá enviar y recibir correos.

[7] De conformidad con lo dispuesto en el art. 23. Registro de actividad, del ENS.

19. ACCESO A INTERNET Y OTRAS HERRAMIENTAS DE COLABORACIÓN[8]

95. El acceso corporativo a Internet es un recurso centralizado que la <<ENTIDAD>> pone a disposición de los usuarios, como herramienta necesaria para el acceso a contenidos y recursos de Internet y como apoyo al desempeño de su actividad profesional.

96. La <<ENTIDAD>> velará por el buen uso del acceso a Internet, tanto desde el punto de vista de la eficiencia y productividad del personal, como desde los riesgos de seguridad asociados a su uso.

19.1. NORMAS GENERALES

- El acceso a Internet deberá ser autorizado por la <<U/OC>>, siempre que se estime necesario para el desempeño de la actividad profesional del usuario o solicitante y exista disponibilidad para ello. En otro caso, se podrá acceder a Internet desde un puesto de acceso común habilitado para ese fin.
- 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 <<*está totalmente prohibido / debe limitarse y, de ser absolutamente necesario, sólo debe utilizarse un tiempo razonable, que no interfiera en el rendimiento profesional ni en la eficiencia de los recursos informáticos corporativos*.>>[9]
- Sólo se podrá acceder a Internet mediante el navegador suministrado y configurado por la <<ENTIDAD>> en los puestos de usuario. No podrá alterarse la configuración del mismo ni utilizar un navegador alternativo, sin la debida autorización de la <<U/OC>>.
- Deberá notificarse a la <<U/OC>> 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.

19.2. USOS ESPECÍFICAMENTE PROHIBIDOS

97. Quedan prohibidas las siguientes actuaciones:

- La descarga de archivos muy voluminosos, especialmente en horarios coincidentes con la atención al público, salvo autorización expresa.
- La descarga de programas informáticos sin la autorización previa de la <<U/OC>> o ficheros con contenido dañino que supongan una fuente de riesgos para la organización. En todo caso debe asegurarse que el sitio Web visitado es confiable.
- El acceso a recursos y páginas-web, o la descarga de programas o contenidos que vulneren la legislación en materia de Propiedad Intelectual.

[8] Por la especial incidencia del acceso a Internet en el mantenimiento de la seguridad IT de los Sistemas de Información, la entidad puede optar por redactar una Normativa Especial sobre esta materia. Por tanto, las normas que se citan en este epígrafe deben considerarse generales. Véase Norma NP10, Normas de Acceso a Internet, en esta misma Guía.

[9] La entidad deberá elegir una de las dos opciones. Como resulta obvio, el mantenimiento más riguroso de la seguridad aconseja prohibir totalmente tal acceso.

- 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 <<U/OC>>.

20. INCIDENCIAS DE SEGURIDAD

98. 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 <<ENTIDAD>> o su imagen, deberá informar inmediatamente a la <<U/OC>>, que lo registrará debidamente y elevará, en su caso.

21. COMPROMISOS DE LOS USUARIOS

99. Es responsabilidad directa del usuario:

    a) Custodiar las credenciales que se le proporcionen y seguir todas las recomendaciones de seguridad que elabore la <<U/OC>>, 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.

    b) En el caso de que su equipo contenga información sensible, confidencial o protegida, esta deberá cumplir todos los requisitos legales aplicables y las medidas de protección que la normativa de la <<ENTIDAD>> establezca al respecto.

    c) Garantizar la disponibilidad de toda la información importante para la <<ENTIDAD>> alojada en el equipo del usuario -si no residiera en los servidores corporativos-, mediante la realización de copias de seguridad periódicas.

100. Además de lo anterior, no se podrá acceder a los recursos informáticos y telemáticos de la <<ENTIDAD>> para desarrollar actividades que persigan o tengan como consecuencia:

    a) El uso intensivo de recursos de proceso, memoria, almacenamiento o comunicaciones, para usos no profesionales.

    b) La degradación de los servicios.

    c) La destrucción o modificación no autorizada de la información, de manera premeditada.

    d) La violación de la intimidad, del secreto de las comunicaciones y del derecho a la protección de los datos personales.

    e) El deterioro intencionado del trabajo de otras personas.

    f) El uso de los sistemas de información para fines ajenos a los de la <<ENTIDAD>>, salvo aquellas excepciones que contempla la presente Normativa.

    g) Dañar intencionadamente los recursos informáticos de la <<ENTIDAD>> o de otras instituciones.

h) Incurrir en cualquier otra actividad ilícita, del tipo que sea.

22. CONTROL DE ACTUACIONES SOBRE LAS BASES DE DATOS DE LA <<ENTIDAD>>

101. La <<ENTIDAD>> podrá habilitar Sistemas de Información cuyo acceso y/o modificación de la información contenida quedarán registrados en una Base de Datos, lo que permitirá su ulterior auditoría.

102. Las modificaciones de los datos deben realizarse sólo por parte de los usuarios autorizados y deberán estar siempre respaldadas por un expediente administrativo que justifique los cambios o la carga de ficheros de información suministrados y debidamente registrados en los registros de entrada/salida, de acuerdo con los procedimientos establecidos.

103. Se prohíbe realizar cualquier tipo de actualización en Bases de Datos corporativas, masiva o puntual, desde fuera de las aplicaciones de la <<ENTIDAD>> sin la autorización previa de la <<U/OC>>.

23. USO ABUSIVO DE LOS SISTEMAS DE INFORMACIÓN.

104. El uso de Internet, del correo electrónico y el acceso al resto de los servicios y sistemas de la <<ENTIDAD>> estará debidamente controlado para todos los usuarios. Si se hiciese un uso abusivo o inapropiado de estos servicios, la <<ENTIDAD>> podrá adoptar las medidas disciplinarias que considere oportunas, sin perjuicio de las acciones civiles o penales a las que hubiere lugar[10].

105. Con carácter general, se enumeran seguidamente un conjunto de acciones que se consideran uso abusivo de los sistemas de información de la <<ENTIDAD>>:

23.1. USO ABUSIVO DEL ACCESO A INTERNET

- Acceso a otras redes, con el propósito de violar su integridad o seguridad.
- Acceso a contenidos no relacionados con los cometidos profesionales del usuario, tales como:
  - Acceder, recuperar o visualizar textos o gráficos que excedan los límites de la ética.
  - Almacenar en la estación de trabajo del usuario o en los servidores de la <<ENTIDAD>> archivos personales[11].
  - Utilizar el acceso a Internet para el uso de mensajería instantánea (Messenger, Skype, etc.).
  - Transferencia de ficheros no relativa a las actividades profesionales del usuario (tales como juegos, ficheros de sonido, fotos, videos o películas, etc.).
  - Realizar cualquier actividad de promoción de intereses personales.
- Publicación o envío de información no solicitada.

[10] Véase: Guía CCN-STIC 831 Registro de actividad de los usuarios.
[11] Salvo autorización previa de la <<U/OC>>.

- Publicación o envío de información sensible, confidencial, protegida o propiedad de la <<ENTIDAD>>, a personas, empresas o sistemas de información externos no autorizados. En este sentido, los usuarios se comprometen a garantizar la privacidad de estos datos y contraseñas de acceso, así como a evitar la difusión de los mismos.
- Publicación o envío de mensajes a través de Internet que contengan amenazas, ofensas o imputación de hechos que puedan lesionar la dignidad personal y, en general, la utilización del servicio de Internet de manera ilegal o infringiendo cualquier norma interna que pudiera resultar de aplicación.
- Empleo de utilidades de intercambio de información en Internet (tales como redes P2P).
- Uso de Internet para propósitos que puedan influir negativamente en la imagen de la <<ENTIDAD>>, de sus representantes o de los organismos públicos o privados con los que se mantiene relación.

23.2. USO ABUSIVO DEL CORREO ELECTRÓNICO

- Utilizar el correo electrónico para fines distintos a los derivados de las actividades profesionales del usuario, especialmente:
  - Intercambiar contenidos (textos o gráficos) que excedan los límites de la ética.
  - Transferencia de ficheros ajena a las actividades profesionales del usuario (por ejemplo: software sin licencia, ficheros de sonido, fotos y videos, gráficos, virus, código malicioso, etc.).
  - Realizar cualquier actividad de promoción de intereses personales.
  - Usar cualquier la cuenta de correo de la <<ENTIDAD>> para enviar mensajes o cartas en cadena y/o correos basura o *spam* (correo electrónico no solicitado).
- Usar cualquier cuenta de correo de la <<ENTIDAD>> para enviar 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.
- Revelar a terceros el contenido de cualquier dato reservado o confidencial propiedad de la <<ENTIDAD>> o de terceros, salvo que tal actuación fuera realizada en cumplimiento de fines estrictamente profesionales con el previo consentimiento de los afectados.
- Utilizar para propósitos que puedan influir negativamente en la imagen de la <<ENTIDAD>>, de sus representantes o de los organismos públicos o privados con los que se mantiene relación.

23.3. USO ABUSIVO DE OTROS SERVICIOS Y SISTEMAS DE LA <<ENTIDAD>>

- Acceso a servicios y/o contenidos de la <<ENTIDAD>> con el propósito de violar su integridad o seguridad.
- De forma general, realizar actividades no relacionadas con las tareas profesionales del usuario, tales como:

- Acceder, recuperar, o visualizar textos o gráficos que excedan los límites de la ética.
- Almacenar archivos personales en la estación de trabajo o en los servidores de la <<ENTIDAD>>.
- El uso de mensajería instantánea (Messenger, Skype, etc.).
- Transferencia de ficheros entre usuarios de la <<ENTIDAD>> no relativa a las actividades profesionales.
- Realizar cualquier actividad de promoción de intereses personales.

- Uso de cualquier servicio de la <<ENTIDAD>> para:
  - La publicación o envío de información no solicitada.
  - La publicación o envío de información confidencial, propiedad de la <<ENTIDAD>>, a personas, empresas o sistemas de información externos no autorizados. Los usuarios se comprometen a garantizar la privacidad de estos datos y contraseñas de acceso, así como a evitar la difusión de los mismos.
  - El uso de los servicios de la <<ENTIDAD>> para propósitos que puedan influir negativamente en la imagen de la <<ENTIDAD>>, de sus representantes o de los organismos públicos o privados con los que se mantiene relación.
  - 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.
- Comunicación a terceros del contenido de cualquier dato reservado o confidencial propiedad de la <<ENTIDAD>> o de terceros, salvo que tal actuación fuera realizada en cumplimiento de fines estrictamente profesionales con el previo consentimiento de los afectados.

106. Las acciones realizadas desde una cuenta de usuario o desde una cuenta de correo electrónico de usuario son responsabilidad de su titular.

107. La <<ENTIDAD>> 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.

24. MONITORIZACIÓN Y APLICACIÓN DE ESTA NORMATIVA

103. La <<ENTIDAD>>, por motivos legales, de seguridad y de calidad del servicio, y cumpliendo en todo momento los requisitos que al efecto establece la legislación vigente[12]:

[12] En este sentido, el Artículo 23. Registro de actividad, del ENS, señala: *"Con la finalidad exclusiva de lograr el cumplimiento del objeto del presente real decreto, con plenas garantías del derecho al honor, a la intimidad personal y familiar y a la propia imagen de los afectados, y de acuerdo con la normativa sobre protección de datos personales, de función pública o laboral, y demás disposiciones que resulten de aplicación, se registrarán las actividades de los usuarios, reteniendo la información necesaria para*

a) Revisará periódicamente el estado de los equipos, el software instalado, los dispositivos y redes de comunicaciones de su responsabilidad.

b) Monitorizará los accesos a la información contenida en sus sistemas.

c) Auditará la seguridad de las credenciales y aplicaciones.

d) Monitorizará los servicios de internet, correo electrónico y otras herramientas de colaboración.

104. La <<ENTIDAD>> llevará a cabo esta actividad de monitorización de manera proporcional al riesgo, con las cautelas legales pertinentes y las señaladas en la jurisprudencia y con observancia de los derechos de los usuarios[13].

105. 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. El servicio se restablecerá cuando la causa de su inseguridad o degradación desaparezca. La <<U/OC>>, con la colaboración de las restantes unidades de la <<ENTIDAD>>, velará por el cumplimiento de la presente Normativa General e informará a la <<U/OC>> sobre los incumplimientos o deficiencias de seguridad observados, al objeto de que se tomen las medidas oportunas.

106. 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.

107. El sistema que proporciona el servicio de navegación podrá contar con filtros de acceso que bloqueen el acceso a páginas web con contenidos inadecuados, programas lúdicos de descarga masiva o páginas potencialmente inseguras o que contengan virus o código dañino. Igualmente, el sistema podrá registrar y dejar traza de las páginas a las que se ha accedido, así como del tiempo de acceso, volumen y tamaño de los archivos descargados. El sistema permitirá el establecimiento de controles que posibiliten detectar y notificar a la <<U/OC>> sobre usos prolongados e indebidos del servicio.

25. INCUMPLIMIENTO DE LA NORMATIVA

Todos los usuarios de la <<ENTIDAD>> están obligados a cumplir lo prescrito en la presente Normativa General de Utilización de los Recursos y Sistemas de Información.

108. En el supuesto de que un usuario no observe alguna de los preceptos señalados en la presente Normativa General, sin perjuicio de las acciones disciplinarias y administrativas que procedan y, en su caso, las responsabilidades legales

monitorizar, analizar, investigar y documentar actividades indebidas o no autorizadas, permitiendo identificar en cada momento a la persona que actúa."

[13] Véase Guía CCN-STIC 831 Registro de la actividad de los usuarios.

correspondientes, se podrá acordar la suspensión temporal o definitiva del uso de los recursos informáticos asignados a tal usuario.

26. MODELO DE ACEPTACIÓN Y COMPROMISO DE CUMPLIMIENTO

109. Todos los usuarios de los recursos informáticos y/o Sistemas de Información de la <<ENTIDAD>> deberán tener acceso permanente, durante el tiempo de desempeño de sus funciones, a la presente Normativa General de Utilización de los Recursos y Sistemas de Información, debiendo suscribirla.

Mediante la cumplimentación de la siguiente declaración, el abajo firmante, [*personal de la <<ENTIDAD>>/empleado de la <<EMPRESA>>*], como usuario de recursos informáticos y sistemas de información de la <<ENTIDAD>>, declara haber leído y comprendido la Normativa General de Utilización de los Recursos y Sistemas de Información de la <<ENTIDAD>> (*versión x*) y se compromete, bajo su responsabilidad, a su cumplimiento.

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

Organismo:	
Trabajador (Nombre y Apellidos):	
DNI número:	
Número de Registro de Personal:	
Firmado:	

Por la <<ENTIDAD>>: <<*Nombre y Apellidos*>>

DNI número: _____

Número de Registro de Personal: _____

27. COMPENDIO DE NORMAS

NORMATIVA GENERAL DE UTILIZACIÓN DE LOS RECURSOS Y SISTEMAS DE INFORMACIÓN DE LA <<ENTIDAD>> (Compendio de las normas más significativas)					
Área	**Norma**	**PC**	**Dispositivo móvil (teléfono, tablet, …)**	**Ordenador Portátil**	**Pen drive**
Acceso a Sistemas de Información	Se debe guardar reserva sobre el *código de usuario (user-id)* y la *contraseña (password)* para el acceso a los sistemas de información (dispositivos y aplicaciones). No deben compartirse con otras personas. Son de uso estrictamente personal e intransferible.	X	X	X	-
	Las contraseñas deben ser robustas. No se deberán elegir contraseñas que puedan deducirse fácilmente (fechas de nacimiento, DNI, nombres de personas, etc.). No deberán dejarse escritas en lugares visibles.	X	X	X	-
Acceso a Dispositivos Móviles	El usuario deberá utilizar siempre contraseñas o códigos (PIN) para el acceso a los dispositivos bajo su responsabilidad. Evitará que sean conocidos por otras personas.	-	X	X	-
	Si el usuario dispone de tarjeta DUAL (línea privada + oficial), tendrá especial cuidado de realizar su conexión con el código (PIN) de su línea oficial.	-	X	-	-
Equipos y Dispositivos	Los equipos propiedad de la <<ENTIDAD>> serán devueltos por el usuario cuando este finalice su relación laboral con la <<ENTIDAD>>.	-	X	X	X
	El dispositivo asignado a un usuario de la <<ENTIDAD>> queda bajo la custodia del mismo, por lo que deberá evitar el acceso al mismo por personas no autorizadas.	X	X	X	X
	Siempre que sea posible, el equipo portátil se anclará, mediante cable de seguridad, al puesto de trabajo, para evitar su sustracción.	-	-	X	-

Área	Norma	PC	Dispositivo móvil (teléfono, tablet, …)	Ordenador Portátil	Pen drive
	El usuario no conectará a la red corporativa ningún equipo o dispositivo sin autorización expresa.	X	X	X	X
	Se debe bloquear el equipo cuando no esté siendo utilizado (protector de pantalla con clave, bloquear teclado, llave, etc.).	X	X	X	-
	El usuario no conectará sus dispositivos a otras redes distintas a la corporativa.	X	X	X	X
Software	No está permitida la instalación de software no autorizado en los equipos o dispositivos proporcionados por la <<ENTIDAD>>.	X	X	X	-
	Los usuarios no podrán borrar, desinstalar o modificar la configuración de las aplicaciones informáticas instaladas en la <<ENTIDAD>>.	X	X	X	-
	Las aplicaciones informáticas instaladas en la <<ENTIDAD>> están protegidas por la legislación de Propiedad Intelectual. Queda prohibida su copia, reproducción, modificación, transformación, cesión o comunicación, sin la debida autorización.	X	X	X	-
Utilización de la Información	No se debe trasladar o enviar al exterior de la <<ENTIDAD>> información sensible, confidencial, protegida o de uso interno, así como datos de carácter personal, salvo los expresamente autorizados.	X	X	X	X
	Cuando se remita información de la <<ENTIDAD>> al exterior, por cualquier medio (telefonía, SMS, correo electrónico, formulario web, etc.), se deberá asegurar que los destinatarios de la información son los adecuados.	X	X	X	-

Área	Norma	PC	Dispositivo móvil (teléfono, tablet, …)	Ordenador Portátil	Pen drive
	No se dejará información accesible con datos de carácter personal, datos técnicos de sistemas o información sensible, confidencial o protegida de la <<ENTIDAD>> en la pantalla o en el puesto de trabajo (papel, CD, DVD, USB, etc.).	X	X	X	X
	En los desplazamientos de datos de carácter personal o de naturaleza sensible, confidencial o protegida fuera de las instalaciones de la <<ENTIDAD>>, cuando se utilicen soportes o dispositivos extraíbles, se cifrarán talles datos.	-	X	X	X
Correo electrónico	El correo electrónico es un servicio proporcionado por la <<ENTIDAD>> al usuario, como herramienta para facilitar su trabajo. Deberá ser utilizado conforme a las necesidades de uso en relación al número de correos y tamaño de ficheros adjuntos.	X	X	X	-
	Los ficheros recibidos por correo electrónico de los que se tenga dudas respecto a su emisor o a su contenido, no se abrirán ni se ejecutarán sus archivos adjuntos.	X	X	X	-
Internet	El acceso a Internet es un servicio proporcionado por la <<ENTIDAD>> al usuario como herramienta para facilitar su trabajo. Deberá hacer un uso responsable y limitado del mismo.	X	X	X	-
	Sólo estará permitido el acceso a Internet utilizando las conexiones proporcionadas por la <<ENTIDAD>>.	X	X	X	-
	Las transferencias de ficheros, acceso a servicios, descargas o conexiones a través de Internet, que no estén directamente relacionadas con las actividades profesionales, podrán estar prohibidas/limitadas por motivos de seguridad.	X	X	X	-

Área	Norma	PC	Dispositivo móvil (teléfono, tablet, …)	Ordenador Portátil	Pen drive
Redes inalámbricas	Por motivos de seguridad no se deben utilizar conexiones inalámbricas con tecnología Wifi distintas a las proporcionadas, en su caso, por la <<ENTIDAD>>.	X	X	X	-
	Por motivos de seguridad, se recomienda que se mantenga desactivado el reconocimiento de dispositivos Bluetooth, especialmente fuera de las instalaciones de la <<ENTIDAD>>. Dicha activación se realizará únicamente para iniciar la sincronización de dispositivos con el equipo portátil, protegida por contraseña, volviéndose a desactivar a su fin.	X	X	X	-
Telefonía / SMS	La utilización de estos servicios deberá restringirse al uso estrictamente necesario para el desempeño de sus funciones profesionales.	-	X	-	-
	En función de las necesidades profesionales del usuario, se podrá limitar el ámbito de las llamadas: corporativo, provincial, nacional o internacional.	-	X	-	-
Incidentes de Seguridad	Cualquier incidente en relación con los equipos o dispositivos (tales como pérdida, robo, deterioro, etc.), deberá ser comunicado a la mayor brevedad posible a la <<U/OC>>.	X	X	X	X
	Cualquier incidente de seguridad como consecuencia de virus, spam o vulneración de la confidencialidad, será comunicado de forma urgente a <<U/OC>>.	X	X	X	X