Centro Informático Científico de Andalucía
CONSEJERÍA DE ECONOMÍA, CONOCIMIENTO, EMPRESAS Y UNIVERSIDAD

JUNTA DE ANDALUCIA

NORMAS DE SEGURIDAD INFORMÁTICA

CENTRO INFORMÁTICO CIENTÍFICO DE ANDALUCÍA

NS00 – DOCUMENTO GENERAL

Fecha: 22 agosto 2019

Índice de contenido

1. OBJETIVO

1. Conforme a lo dispuesto en el Real Decreto 3/2010, de 8 de enero, por el que se regulal Esquema Nacional de Seguridad (ENS, en adelante), este documento contiene la Normativa General de Utilización de los Recursos y Sistemas de Información del CICA, gestionados o bajo la responsabilidad del CICA, señalando asimismo los compromisos que adquieren sus usuarios respecto a su seguridad y buen uso.
2. Los Sistemas de Información constituyen elementos básicos para el desarrollo de las misiones encomendadas al CICA, 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 el CICA:
   - 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 al CICA 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 del CICA tiene como objetivo establecer normas encaminadas a alcanzar la mayor eficacia y seguridad en su uso.
6. Este documento se considera de uso interno del CICA y, por consiguiente, no podrá ser divulgado salvo autorización del CICA.

2. ÁMBITO DE APLICACIÓN

7. Esta Normativa General es de aplicación a todo el ámbito de actuación del CICA, y sus contenidos traen causa de las directrices de carácter más general definidas en la Política de Seguridad de la Información del CICA.
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 el CICA, incluyendo el personal de proveedores externos, cuando sean usuarios de los Sistemas de Información del CICA.
9. En el ámbito de la presente normativa, se entiende por usuario cualquier empleado público perteneciente o ajeno al CICA, así como personal de organizaciones privadas externas, entidades colaboradoras o cualquier otro con algún tipo de vinculación con el CICA y que utilice o posea acceso a los Sistemas de Información del CICA.

3. VIGENCIA

10. La presente Normativa General de Utilización de los Recursos y Sistemas de Información del CICA ha sido aprobada por la Dirección General a la que pertenece el CICA, estableciendo de esta forma las directrices generales para el uso adecuado de los recursos de tratamiento de información que el CICA 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 del CICA.
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 CSTIC del CICA, 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), el CSTIC revisará la presente Normativa General, que se someterá, de haber modificaciones, a la aprobación de la Dirección General a la que pertenece el CICA.
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

5.1. INTERNAS

17. Política de Seguridad de la Junta de Andalucía.
18. Política de Seguridad del CICA.

5.2. EXTERNAS

19. Ver marco normativo de la Política de Seguridad del CICA.

6. UTILIZACIÓN DEL EQUIPO INFORMÁTICO Y DE COMUNICACIONES

El CICA 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 el CICA pone a disposición de los usuarios deben utilizarse para el desarrollo de las funciones encomendadas, es decir, para fines profesionales.

20. Cualquier uso de los recursos con fines distintos a los autorizados está estrictamente prohibido.
21. 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 del CICA, 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.
22. Este epígrafe concierne específicamente a todos los ordenadores personales facilitados y configurados por el CICA 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 el área responsable de Microinformática.

23. Existirá un inventario actualizado de los equipos informáticos. El área responsable de Microinformática será la unidad encargada de gestionar dicho inventario.
24. A cada nuevo usuario que se incorpore a la organización y así lo precise, el Área Responsable de Microinformática 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.
25. Los ordenadores personales deberán utilizarse únicamente para fines institucionales y como herramienta de apoyo a las competencias profesionales de los usuarios autorizados.
26. Se aplicará una política centralizada de Escritorios limpios que minimicen el riesgo de pérdida y confidencialidad de archivos, teniendo en cuenta que lo contenido en el escritorio es susceptible de perdidas en caso de fallas del sistema operativo.
27. Se aplicará un política para equipos desatendidos, que garantice la confidencialidad de la información cuando el usuario no esté en su puesto de trabajo, de manera que se bloquee automáticamente el acceso al equipo tras un periodo determinado de inactividad y haga preciso volver a identificarse para acceder a él.
28. Únicamente el personal autorizado por el Área de Seguridad 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 del CICA. Cuando se precise instalar dispositivos no provistos por el CICA deberá solicitarse autorización previa al Área de Seguridad.

29. 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 del Área de Seguridad. En todo caso, estas operaciones sólo podrán realizarse por el personal de soporte técnico autorizado.
30. Salvo autorización expresa del Área de Seguridad, los usuarios no tendrán privilegio de administración sobre los equipos.
31. 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.
32. 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 del Área de Seguridad, que tomará las oportunas medidas correctoras y dará traslado de la incidencia al RSEG.
33. 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.
34. Los usuarios deberán notificar al Área de Seguridad, 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.
35. 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.
36. El usuario deberá participar en el cuidado y mantenimiento del equipo que tiene asignado, detectando la ausencia de cables y accesorios, y dando cuenta al Área de Seguridad de tales circunstancias.
37. 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.
38. 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.
39. El cese de actividad de cualquier usuario debe ser comunicada de forma inmediata al Área de Seguridad, 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 el CICA 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.

40. Los centros de cableado, centros de datos, centros de monitoreo/vigilancia y centros eléctricos, están catalogados como zonas restringidas, con control de acceso y restricción a personal no autorizado.

6.2. USOS ESPECÍFICAMENTE PROHIBIDOS

41. 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 el CICA sin la previa autorización del Área de Seguridad.
    - Utilización de conexiones y medios inalámbricos con tecnologías WiFi, Bluetooth o infrarrojos que no estén debidamente autorizados por el Área de Seguridad.
    - Utilización de dispositivos USB, teléfonos móviles u otros elementos, como acceso alternativo a Internet, salvo autorización expresa del Área de Seguridad .
    - 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

42. 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.
43. El CICA 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.
44. No está permitido almacenar información privada, de cualquier naturaleza, en los recursos de almacenamiento compartidos o locales, salvo autorización previa del Área de Seguridad .

6.4. NORMAS ESPECÍFICAS PARA EQUIPOS PORTÁTILES Y MÓVILES

45. Los equipos portátiles y móviles serán asignados por el área responsable de Microinformática.
46. Existirá un inventario actualizado de los equipos portátiles y móviles. El área responsable de

Microinformática será la unidad encargada de gestionar dicho inventario.

47. Este tipo de dispositivos estará bajo la custodia del usuario que los utilice o del responsable del área responsable de Microinformática. Ambos deberán adoptar las medidas necesarias para evitar daños o sustracción, así como el acceso allos por parte de personas no autorizadas.
48. La sustracción de estos equipos se ha de poner inmediatamente en conocimiento del Área de Seguridad para la adopción de las medidas que correspondan y a efectos de baja en el inventario.
49. Los equipos portátiles y móviles deberán utilizarse únicamente para fines institucionales y autorizados, especialmente cuando se usen fuera de las instalaciones del CICA.
50. Los usuarios de estos equipos se responsabilizarán de que no serán usados por terceras personas ajenas al CICA o no autorizadas para ello.
51. 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). El CICA puede proporcionar accesos remotos autorizados y configurados por el Área de Comunicaciones a través de tarjetas móviles. Cuando este seal 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 el Área de Seguridad 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.
52. Los usuarios de equipos portátiles deberán realizar conexiones periódicas, con periodicidad mínima de al menos una vez al mes, a la red corporativa, según las instrucciones proporcionadas por el Área responsable de Microinformática, para permitir la actualización de aplicaciones, sistema operativo, firmas de antivirus y demás medidas de seguridad. En su defecto, cada mes, los equipos portátiles serán entregados al Área responsable de Microinformática para la actualización de tal software.
53. 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.).
54. 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 al Área de Seguridad, se podrán habilitar algunas o todas las funciones de salida de información.
55. Los usuarios no tendrán privilegio de administración sobre los equipos portátiles, teniendo prohibido realizar cualquier modificación hardware/software sobre los mismos. Corresponderá al Área responsable de Microinformática llevar a cabo estas modificaciones.
56. 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 al Área responsable de Microinformática, 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)

57. Con carácter general, el uso de memorias USB en el CICA no está autorizado. En su caso, la

autorización deberá proporcionar al Área de Seguridad.

58. 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 del área al que pertenece el usuario y del Área de Seguridad.
59. 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 el CICA, que serán conformes a las normas de seguridad de la organización. Estas memorias USB serán de uso exclusivo en los puestos de usuario del CICA, no debiendo ser usados fuera de éstos.
60. Se recuerda que las memorias USB están destinadas a un uso exclusivamente profesional, como herramienta de transporte de ficheros, no como herramienta de almacenamiento. El Área responsable de Microinformática podrá poner a disposición de los usuarios de aplicaciones, servicios y sistemas del CICA unidades de almacenamiento en red, que podrán usarse para tal propósito.
61. La pérdida o sustracción de una memoria USB, con indicación de su contenido, deberá ponerse en conocimiento del Área de Seguridad, de forma inmediata.

6.6. COPIAS DE SEGURIDAD

62. Mantener copias de seguridad es una cautela esencial de protección de la información.
63. La gestión de las copias de seguridad, será responsabilidad del Área de Sistemas, que debe implementar los procesos y procedimientos necesarios, que garanticen el adecuado tratamiento de los medios físicos internos y externos, y los medios digitales locales.
64. 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.
65. De forma periódica, se realizarán copias de seguridad, tanto completas como incrementales, de las unidades de red compartidas del CICA 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.
66. 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 al Centro de Soporte a los Usuarios (CSU), a la dirección de correo soporte@cica.es.

6.7.BORRADO Y ELIMINACIÓN DE SOPORTES INFORMÁTICOS

67. 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 el CICA y aprobados por el RSEG.
68. Cualquier petición de eliminación de soporte informático deberá ser autorizada expresamente por el Área de Seguridad, previa petición del responsable de la unidad a la que pertenece el usuario. Esta

petición deberá dirigirse a través de la apertura de una incidencia al CSU (soporte@cica.es), que seguirá procedimiento de destrucción o almacenamiento de los medios informáticos obsoletos.

6.8. IMPRESORAS EN RED, FOTOCOPIADORAS Y FAXES

69. Con carácter general, deberán utilizarse las impresoras en red y las fotocopiadoras corporativas. Excepcionalmente, podrán instalarse impresoras locales, conectadas a un puesto de trabajo de usuario. En este caso, la instalación irá precedida de la autorización pertinente por parte del jefe de la unidad a la que pertenece el peticionario. En ningún caso el usuario podrá hacer uso de impresoras, fotocopiadoras o equipos de fax que no hayan sido proporcionados por el CICA y, en su consecuencia, estén debidamente inventariados.
70. 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.
71. 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 del Área de Seguridad, que gestionará el incidente conforme a los procedimientos establecidos.
72. 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.

6.9. DIGITALIZACIÓN DE DOCUMENTOS

73. 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.
74. 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 del Área de Seguridad, que gestionará el incidente conforme a los procedimientos establecidos.

6.10. CUIDADO Y PROTECCIÓN DE LA DOCUMENTACIÓN IMPRESA

75. La documentación impresa que contenga datos sensibles, confidenciales o protegidos, debe ser especialmente resguardada, de forma que sólo tenga acceso allal personal autorizado, debiendo ser recogida rápidamente de las impresoras y fotocopiadoras y ser custodiada en armarios bajo llave.
76. Cuando concluya la vida útil de los documentos impresos con información sensible, confidencial o protegida, deberán ser eliminados en las máquinas destructoras del CICA, de forma que no sea recuperable la información que pudieran contener.
77. 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.

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

6.11. PIZARRAS Y FLIPCHARTS

79. Antes de abandonar las salas o permitir que alguien ajeno entre, se limpiarán 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.

6.12. PROTECCIÓN DE LA PROPIEDAD INTELECTUAL

80. Está estrictamente prohibida la ejecución de programas informáticos en los Sistemas de Información del CICA sin la correspondiente licencia de uso.
81. Los programas informáticos propiedad del CICA o licenciados al CICA están protegidos por la legislación vigente 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 del Área responsable de Microinformática.
82. 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 Gerencia del CICA.

6.13. PROTECCIÓN DE LA DIGNIDAD DE LAS PERSONAS

83. 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

84. Dentro de las medidas de austeridad y reducción del gasto del CICA, 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

85. Debe existir un inventario de las licencias de software del CICA, con el fin de facilitar la administración y control de software no licenciado y la planificación de la renovación del software licenciado que se

considere necesario.

86. Únicamente el personal de soporte técnico autorizado por el Área responsable de Microinformática podrá instalar software en los equipos informáticos o de comunicaciones de los usuarios.
87. Excepción a esta norma serán aquellas herramientas de uso común incluidas en el Catálogo de Aplicaciones Autorizadas del CICA, descargables desde los servidores internos al CICA.
88. Todo usuario podrá solicitar la inclusión de una aplicación en dicho Catálogo de Aplicaciones Autorizadas para su estudio por parte del Área responsable de Microinformática.
89. 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.
90. Todo software no comercial, es decir Freeware, Shareware, Trial, CPL, EPL, GNU, Open Source, debe tener el respectivo soporte de licencia, en el que se garantice el alcance de la licencia, y debe ser autorizado y gestionado por el Área de Seguridad.
91. Se prohíbe terminantemente la reproducción, modificación, transformación, cesión, comunicación o uso fuera del ámbito del CICA de los programas y aplicaciones informáticas instaladas en los equipos que pertenecen a la organización. La extracción, préstamo, copia, venta y/o renta de software corporativo para fines externos y/o personales, no está autorizado bajo ninguna circunstancia.
92. En ningún caso se podrán eliminar o deshabilitar las aplicaciones informáticas instaladas por el Área responsable de Microinformática, especialmente aquellas relacionadas con la seguridad.
93. La instalación de software no autorizado es responsabilidad del usuario, y cualquier daño en la configuración del equipo que se produzca por el incumplimiento de esta política debe ser asumido por el responsable del activo.

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

94. Serán los Responsables de los Sistemas de Información (RSIS) los encargados de conceder, alterar o anular la autorización de acceso a los datos gestionados por el CICA.
95. De forma general, existirán protocolos de instalación, configuración, parametrización, gestión y soporte, de usuarios, roles y perfiles, para todos los sistemas de Información gestionados por el CICA, tanto de equipos de usuarios como de equipos servidores.
96. El alta de los usuarios será comunicada al CSU (soporte@cica.es), que pondrá en marcha los procedimientos establecidos para el alta efectiva. Para acceder a los recursos informáticos es necesario tener asignada previamente una cuenta de usuario y estar dado de alta en los servidores de directorio. 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.
97. Es responsabilidad del usuario hacer buen uso de su cuenta de usuario. La cuenta se podrá desactivar por el Área de Seguridad en caso de mala utilización.
98. 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. Por lo tanto, no tendrán acceso a opciones del Sistema de Información que no utilicen con motivo de su desempeño laboral.

99. 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 10 minutos.
100. La baja de los usuarios será comunicada al CSU (soporte@cica.es), para proceder a eliminación efectiva de los derechos de acceso y los recursos informáticos asignados al mismo, así como el acceso a los servidores internos al CICA. Ningún usuario debe ser eliminado de ningún sistema, servicio o aplicación, debiendo aplicarse la inactivación del usuario.
101. Las cuentas de usuario de la red serán suspendidas cada vez que un usuario se ausente por largo tiempo (mayor de 3 meses) por motivo de incapacidad, licencia, etc... La cuenta sólo será habilitada durante este período de tiempo bajo solicitud escrita debidamente justificada del responsable de Área al que pertenece el usuario dirigida al CSU.

10. IDENTIFICACIÓN Y AUTENTICACIÓN

102. Los usuarios dispondrán de un identificador de usuario (user-id) y una contraseña (password) o bien una tarjeta criptográfica con certificado digital, personales e intransferibles, para el acceso a los Sistemas de Información del CICA, y son responsables de la custodia de los mismos y de toda actividad relacionada con el uso de su acceso autorizado.
103. Para corregir, o exigir responsabilidades en su caso, cada usuario que acceda a la información del sistema debe estar identificado de forma única en la organización, de modo que se sepa, en todo momento, quién recibe derechos de acceso, de qué tipo son éstos, y quién ha realizado determinada actividad. Por lo tanto, cada persona tendrá asignado el mismo user-id para todos los sistemas y aplicaciones del CICA y dicho user-id será intransferible e independiente del equipo desde el que se realiza el acceso.
104. Queda prohibida la creación y el uso de cuentas de usuario genéricas, entendiendo como genérica aquellas que son utilizadas por varios usuarios de la organización.
105. Para garantizar la seguridad tanto de la información como de los equipos, el CSU asignará a cada usuario las claves de acceso estrictamente necesarias para la realización de las labores encomendadas: acceso al computador, acceso a la red interna, acceso al correo electrónico, acceso a las aplicaciones correspondientes, según los procedimientos y condiciones establecidas por los Responsables de los Sistemas de Información.
106. Los user-id seguirán una nomenclatura establecida, definida en sus procedimientos técnicos correspondientes.
107. La autorización para la creación, eliminación o modificación de perfiles de acceso es responsabilidad directa del RSIS de cada aplicación.
108. Los usuarios no deben revelar o entregar, bajo ningún concepto, sus credenciales de acceso o tarjeta

criptográfica a otra persona, ni mantener dichas credenciales por escrito a la vista o al alcance de terceros

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

110. Si un usuario tiene sospechas de que sus credenciales están siendo utilizadas por otra persona, debe proceder inmediatamente a comunicar al CSU la correspondiente incidencia de seguridad, que seguirá los procedimientos establecidos frente a tales incidentes.

111. El procedimiento para la creación y utilización de contraseñas robustas está descrito en el apartado normativo correspondiente a la creación y uso de contraseñas.

112. 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 al CSU por las vías establecidas, de forma inmediata.

113. Los Administradores de los Sistemas utilizarán cuentas nominativas e intransferibles, no pudiendo ser cuentas genéricas, para realizar sus cometidos, y se guiarán por el principio de lo mínimos permisos necesarios. No se utilizarán las cuentas preestablecidas de administrador o superusuario (root, Admin, Administrador, etc.) salvo casos de fuerza mayor, por lo que el conocimiento de dichas credenciales estará reservado exclusivamente al menor número de personas posible.

11. CREACIÓN Y USO DE CONTRASEÑAS

114. Las contraseñas (junto con el identificador de usuario o user-id) son el medio de acceso principal a los sistemas y servicios existentes en el CICA y que precisan de contraseñas como mecanismo de autenticación, tales como el ordenador del puesto de trabajo, el acceso a la red corporativa y a los distintos sistemas y aplicaciones corporativos, acceso a la cuenta de correo electrónico, etc. Es por esto que se redactan las normas de creación y uso de contraseñas que se encuentran en un documento específico, “NS03 CICA – CONTRASEÑAS” incluido en la misma ubicación que el presente documento.

12. ACCESO Y PERMANENCIA DE TERCEROS EN LOS EDIFICIOS, INSTALACIONES Y DEPENDENCIAS DEL CICA

12.1. NORMAS

115. Los terceros ajenos al CICA que, eventualmente, permanecieran en sus edificios, instalaciones o dependencias, deberán observar las siguientes normas:

- El personal ajeno al CICA que temporalmente deba acceder a los Sistemas de Información del CICA, deberá hacerlo siempre bajo la supervisión de algún miembro acreditado del CICA (enlace) y previa autorización del Área de Seguridad.
- Cualquier incidencia que surja antes o en el transcurso del acceso al CICA 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 del CICA, siempre que sea posible, se les crearán usuarios temporales que serán eliminados una vez concluido su trabajo en el CICA. 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 del CICA, especialmente en lo referente a los apartados de salida y confidencialidad de la información.
- Para acceder a los edificios, instalaciones o dependencias del CICA 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 del CICA, 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 del CICA, 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 distintas áreas del CICA.
- 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.

12.2. MODELO DE PROTOCOLO DE FIRMA

He leído y comprendido las presentes Normas de Acceso y Permanencia en _____ 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 del CICA: _____

DNI número: _____

12.3. 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:				

Planta 0	**Zona 1**			
	Zona 2			
	Zona 3			
Acceso a control de versiones:				
Acceso a gestor documental:				
Acceso a carpetas de red:				
Otras:				

13. CONFIDENCIALIDAD DE LA INFORMACIÓN

116. Como medida de protección de la información propia, confiada o tratada por el CICA, 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 el Área de Seguridad.

117. 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 el CICA (tal como datos personales, documentos, metodologías, claves, análisis, programas, etc.) deberán mantener sobre ella, por tiempo indefinido, una absoluta reserva.

118. 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.

119. 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.

120. 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.

121. La información contenida en los Sistemas de Información del CICA es propiedad del CICA, 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 del Área de Seguridad.

122. 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 al CSU, que seguirá el procedimiento de eliminación segura de soportes.

123. 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.

124. Los datos del CICA que tienen el carácter de datos protegidos, son los enumerados en los registros de actividades de tratamiento que se realizan en cumplimiento con el RGPD (Reglamento UE 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016). Para los datos especialmente protegidos se tomarán, además de las presentes medidas de seguridad, resultantes de la aplicación del Anexo II del ENS a cada uno de los Sistemas responsabilidad del CICA o de los cuales es el encargado del tratamiento.

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

125. La información contenida en las bases de datos del CICA 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 el CICA han de adoptar las medidas de seguridad que se correspondan con las exigencias previstas o derivadas de la antedicha normativa.

126. Todo usuario (del CICA 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 el CICA.

15. TRATAMIENTO DE LA INFORMACIÓN

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

128. Cualquier tratamiento en los Sistemas de Información del CICA deberá ser conforme con la normativa vigente, especialmente con lo dispuesto en la normativa vigente, europea y nacional, en materia de Protección de Datos.

129. Queda prohibido, asimismo, transmitir o alojar información sensible, confidencial o protegida propia del CICA en servidores externos al CICA salvo autorización expresa del Área de Seguridad, que comprobará la inexistencia de trabas legales para ello y verificará la suscripción de un contrato expreso entre el CICA 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.

16. SALIDAS DE INFORMACIÓN

130. La salida de información del CICA (en cualquier soporte o por cualquier medio de comunicación) deberá ser realizada exclusivamente por personal autorizado por el Área de Seguridad, autorización que contemplará igualmente a la propia información que sale.

131. 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.

132. Los usuarios se abstendrán de sacar al exterior cualquier información del CICA en cualquier dispositivo (CDs, DVDs, memorias USB, ordenadores o dispositivos portátiles, etc.), salvo en los supuestos indicados en los puntos anteriores.

17. COPIAS DE SEGURIDAD

133. 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.

134. Por parte del Área de Sistemas se realizarán diariamente copias de seguridad de los ficheros del sistema de almacenamiento en red (carpetas del servidor) y del resto de sistemas corporativos.

135. Si algún usuario desea recuperar algún fichero borrado del sistema de almacenamiento en red, lo participará al CSU, que tramitará la solicitud conforme a los procedimientos establecidos.

136. Se prestará especial atención a salvaguardar la información de configuración de los sistemas críticos, y se diseñarán planes de contingencia para restaurar los servicios según su importancia y criticidad, estableciendo los RTO (Recovery Point Objective) y RPO (Recovery Time Objective).

137. Toda la información histórica almacenada y respaldada debe contar con los medios, procesos, programas y sistemas de información que permitan su consulta en el tiempo, teniendo en cuenta la evolución de los componentes tecnológicos y las aplicaciones a través del tiempo.

18. CONEXIÓN DE DISPOSITIVOS A LAS REDES DE COMUNICACIONES

138. No se podrá conectar en la red de comunicaciones corporativa ningún dispositivo distinto de los admitidos, habilitados y configurados por el CICA, salvo autorización previa del Área de Seguridad.

19. GESTIÓN DE LA SEGURIDAD

19.1. HERRAMIENTAS DE SEGURIDAD

139. Existirá un Software Antivirus corporativo, que garantice la protección ante amenazas por virus informáticos, que a su vez debe contemplar como mínimo los siguientes componentes:

- Componente de consola de servidor: encargado de distribuir y actualizar las actualizaciones de antivirus en los equipos de cómputo de la red.
- Componente de correo externo: encargado filtrar el contenido y tráfico de correos entrantes y salientes.

140. Existirá software que de gestión de salida hacia internet y desde internet, filtrado de contenidos, filtrado de páginas y monitorización de navegación.

141. A nivel perimetral se debe contar con software de seguridad que permita controlar el acceso de virus, troyanos, malware, spyware, phishing y spam.
142. Deben existir protocolos de parametrización y directrices de seguridad informática para redes y herramientas de seguridad de red como Sistemas de Detección de Intrusos (IDS), Sistemas de Prevención de Intrusos (IPS), gestión de vulnerabilidades, y otras herramientas que sean convenientes.
143. El software de detección de virus y demás Software de Seguridad seleccionados por el CICA, deben ser instalado en todos los servidores y equipos de computo, incluyendo computadores portátiles del CICA.
144. Se realizará un escaneo de seguridad siempre, previamente a la la utilización de medios electrónicos externos, de uso corporativo y/o personal, correos electrónicos y descarga de archivos.
145. Los usuarios deben conocer los procedimientos de detección y eliminación de virus informáticos, para lo cual el Área de Seguridad debe garantizar la difusión necesaria para el uso de las herramientas de seguridad existentes.
146. Es responsabilidad del Área de Seguridad que todos los equipos asignados estén libres de virus, y responsabilidad de los usuarios que la información gestionada en los activos asignados, y medios de almacenamiento sean filtrados con el Software Antivirus y demás software de seguridad instalados en cada uno de los equipos del CICA.

19.2. GESTIÓN DE LA CONFIGURACIÓN DE SEGURIDAD

147. Debe existir un protocolo de gestión de aplicaciones de seguridad informática que contemple las actividades de instalación, configuración, parametrización, administración, mantenimiento y desinstalación.
148. Deben existir los protocolos de seguridad que describan los mecanismos de control y accesos a las diferentes redes y sistemas existentes en el CICA, que se mantendrán actualizados en todo momento.
149. Se documentará técnicamente la configuración de todos sistemas de información del CICA: configuraciones de equipamiento de comunicaciones, servidores, almacenamiento, de sistemas operativos, parametrización, middleware y software que soporte los distintos sistemas de información.
150. Debe realizarse la evaluación de la relevancia y criticidad o urgencia de los parches a implementar.
151. La instalación, configuración, parametrización, administración, mantenimiento y desinstalación del software antivirus existente, es responsabilidad los ATIs, previa autorización por parte del Área de Seguridad.
152. La actualización del antivirus debe ser gestionada de forma centralizada en el servidor de la aplicación y de forma automática en cada uno de los equipos de cómputo del CICA.
153. Las actualizaciones de nuevas versiones serán gestionadas únicamente por los ATIs previa autorización por el Área de Seguridad.
154. Existirá un protocolo de encriptación de Información en los distintos niveles de los Sistemas de Información: Redes de Comunicaciones, Sistemas Operativos, etc.
155. Todo tipo de información transmitida tanto por las redes internas de la organización, como desde y hacia entidades externas, se enviará por canales seguros y de forma cifrada, por lo que habilitarán

todas las funcionalidades de los Sistemas de Información, de tal forma que toda la información viaje por las redes (LAN o WAN) en forma encriptada, con el fin de preservar su confidencialidad.

156. Debe realizarse una evaluación periódica, con periodicidad mínima de 2 años, de la gestión y desempeño de las herramientas de seguridad informática existentes, para asegurarse de su idoneidad, planificando la sustitución por aquellas que generen mejores características y niveles de seguridad. En especial se tendrá en cuenta lo indicado en el apartado 23.1 del presente documento en lo relativo al Catálogo de Productos de Seguridad TIC, CPSTIC, recomendados por el Centro Criptológico Nacional.

19.3. INCIDENCIAS DE SEGURIDAD

157. Cuando un usuario detecte cualquier anomalía o incidencia de seguridad que pueda comprometer el buen uso y funcionamiento de los Sistemas de Información del CICA o su imagen, deberá informar inmediatamente al CSU a través de los canales habilitados al efecto, que lo registrará debidamente y elevará, en su caso.

158. Debe existir un procedimiento de gestión de incidentes que registre todo el seguimiento de los incidentes presentados hasta su solución.

159. Todos los registros de detección de virus y otras vulnerabilidades, serán revisados y analizados por el personal técnico del CICA, y notificados al Área de Seguridad.

19.4. AUDITORÍAS

160. Se realizarán con una periodicidad mínima de un año, análisis de riesgos, teniendo en cuenta la criticidad de la información gestionada por los Sistemas Operativos, Bases de Datos, Sistemas de Información, que identifique y defina los datos y los sistemas a los que deben aplicar las pistas de auditoría.

161. Debe existir un protocolo de configuración, implementación, gestión, respaldo y recuperación de pistas de auditoría, Log's y/o registros auditables.

162. Todos los Sistemas Operativos, Bases de Datos, Sistemas de Información, debe tener activa y habilitada las funciones de Log's.

163. Las pistas de auditoría deben ser contempladas como un archivo adicional a los de datos, que evidencie todas las actividades realizadas por los usuarios, conteniendo como mínimo: fecha, hora, usuario, tipo de operación realizada (modificación, inclusión y borrado de información), archivo o tabla en la que se realizó la operación, numero del registro o id, para el caso de modificación de información, debe incluir los campos de valor anterior y nuevo valor del dato.

164. El acceso a las pistas de Auditoría estará limitado exclusivamente a las personas que deban acceder con motivo de su función. Solamente aquellos autorizados expresamente por CSTIC a través del RSEG podrán consultar su contenido.

165. Se garantizará la integridad de los datos de auditoría, por lo que solamente serán modificados por los propios sistemas que los generan, deberá evitarse su modificación por parte de los administradores de los sistemas, y se habilitará auditoría adicional sobre dichos datos de auditoría. Esto se realizará para todos los Sistemas de Información, Sistemas Operativos, Bases de Datos, etc.

166. Todas las pistas de Auditoria deben contar con una Copia de Seguridad periódica, programado y automática.

167. Debe garantizarse la disponibilidad, integridad y preservación de las Copias de Seguridad durante el periodo de retención establecido al efecto, que será de al menos dos (2) años.

19.5. TRATAMIENTO DE VULNERABILIDADES

168. Se debe contemplar una política de cuarentena, que garantice que las vulnerabilidades encontradas no se difundan por las redes a otros equipos, hasta que se realice un análisis y tratamiento por parte del Área de Seguridad.

169. Cuando los virus no puedan ser eliminados a pesar de haber agotado los mecanismos existentes para tal fin, se notificará el incidente al CSTIC, encargado de evaluar los aspectos de Seguridad de la Información.

170. Debe existir un protocolo de Hacking Ético (ataques de seguridad éticos), que garantice la generación de ataques de intrusión controlados (interna y externa) a las redes del CICA, con el fin de determinar las debilidades y adoptar nuevos controles a implementar. Estas pruebas deben ser generadas por entes externos que garanticen la independencia y objetividad en los resultados.

171. Debe existir un protocolo de seguridad en todas las redes que permita periódicamente la realización de monitoreo a los ataques en tiempo real, y garantice la seguridad de las redes ante terceros no autorizados e intrusos.

172. Se debe realizar una monitorización permanente tanto de la infraestructura de comunicaciones como de los servidores, de manera que se detecten los problemas que pueden llegar a causar fallas en la disponibilidad de los servicios de las redes del CICA.

173. Deben existir protocolos de verificación física a las redes del CICA que garanticen la calidad de las instalaciones de cableado de datos.

20. COMPROMISOS DE LOS USUARIOS

174. Es responsabilidad directa del usuario:

- Custodiar las credenciales que se le proporcionen y seguir todas las recomendaciones de seguridad que elabore el Área de Seguridad, 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.
- 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 del CICA establezca al respecto.
- Garantizar la disponibilidad de toda la información importante para el CICA alojada en el equipo del usuario -si no residiera en los servidores corporativos-, mediante la realización de copias de seguridad periódicas.
- Cada usuario es responsable del cuidado y uso adecuado de los recursos informáticos que se le asignen para el desarrollo normal de sus funciones.

- Los recursos informáticos asignados a cada usuario, son para uso limitado para el desarrollo de sus funciones, por lo tanto no está permitido el uso de cualquiera de los recursos con propósitos de ocio o lucro.
- Los usuarios de los activos de información no podrán usar los elementos de cómputo asignados para realizar actividades personales distintas a las contratadas.
- Los usuarios de activos de información son responsables de la información y los recursos asignados, por lo cual deben ser responsables de notificar, la definición de controles de acceso y otros controles de seguridad, con el fin de garantizar su responsabilidad por incumplimientos, no conformidades y otros incidentes que se presenten en la organización.
- El uso de activos de información o recursos corporativos para actividades personales será considerado como un incumplimiento a esta política.

175. Además de lo anterior, no se podrá acceder a los recursos informáticos y telemáticos del CICA para desarrollar actividades que persigan o tengan como consecuencia:
    - El uso intensivo de recursos de proceso, memoria, almacenamiento o comunicaciones, para usos no profesionales.
    - La degradación de los servicios.
    - La destrucción o modificación no autorizada de la información, de manera premeditada.
    - La violación de la intimidad, del secreto de las comunicaciones y del derecho a la protección de los datos personales.
    - El deterioro intencionado del trabajo de otras personas.
    - El uso de los sistemas de información para fines ajenos a los del CICA, salvo aquellas excepciones que contempla la presente Normativa.
    - Dañar intencionadamente los recursos informáticos del CICA o de otras instituciones.
    - Incurrir en cualquier otra actividad ilícita, del tipo que sea.

21. GESTIÓN DE BIENES TIC

21.1. ADQUISICIÓN

176. Toda adquisición de tecnología informática se efectuará a través del CSTIC, que será quien apruebe en última instancia las adquisiciones. Los ATI, al planear las operaciones relativas a la adquisición de bienes informáticos, establecerán prioridades y en su selección deberá tomar en cuenta los siguientes parámetros:
    - **Calidad:** Es uno de los parámetros más importantes a tener en cuenta a la hora de adquirir recursos informáticos. Se tendrán especialmente en cuenta los certificados de calidad de los organismos mundialmente reconocidos.
    - **Experiencia:** Deben ser productos de éxito probado en el mercado, con estructura de servicio postventa que asegure su mantenimiento durante su ciclo de vida.
    - **Desarrollo Tecnológico:** Se deberá analizar su grado de obsolescencia, su nivel tecnológico con

respecto a la oferta existente en el mercado y su permanencia en el mercado.

- **Estándares:** Toda adquisición debe de cumplir los estándares, tanto nacionales como internacionales. En especial, se tendrá en cuenta la pertenencia al Catálogo de Productos de Seguridad TIC, CPSTIC, recomendados por el Centro Criptológico Nacional, como Productos Aprobados para el manejo de información clasificada y los Productos Cualificados para el manejo de información sensible.
- **Capacidades:** De cara al dimensionamiento de las capacidades del equipamiento, se tendrá en cuenta tanto la necesidad actual como el crecimiento de demanda esperado a medio-largo plazo.
- El equipo que se desee adquirir estará dentro de las listas de ventas vigentes de los fabricantes y/o distribuidores del mismo y dentro de los estándares.
- Los equipos complementarios deberán tener una garantía mínima de un año y deberán contar con el servicio técnico correspondiente.
- El fabricante de los equipos o componentes deberá contar con presencia y permanencia demostrada en el mercado nacional, así como con asistencia técnica y de repuestos local.
- Los dispositivos de almacenamiento, así como las interfaces de entrada y salida, deberán estar acordes con la tecnología de punta vigente, tanto en velocidad de transferencia de datos, como en procesamiento.
- Las impresoras deberán cumplir con los estándares de Hardware y Software vigentes en el mercado, corroborando que los suministros (cintas, papel, etc.) se consigan fácilmente en el mercado y no estén sujetas a un solo proveedor.
- Los equipos adquiridos deben contar con asistencia técnica durante la instalación de los mismos.
- En lo que se refiere a los servidores, equipos de comunicaciones, concentradores, switches y otros equipos que se justifiquen por ser de operación crítica y/o de alto costo, deben de contar con un programa de mantenimiento preventivo y correctivo que incluya el suministro de repuestos al vencer su período de garantía.
- En lo que se refiere a los computadores personales, al vencer su garantía por adquisición, deberán de contar por lo menos con un programa de servicio de mantenimiento correctivo que incluya el suministro de repuestos.
- Todo proyecto de adquisición de bienes de tecnología, debe sujetarse al análisis, aprobación y autorización del CSTIC.

21.2. GESTIÓN DE LOS ACTIVOS

177. Se debe garantizar la elaboración y actualización de un inventario de activos al mayor detalle posible, que garantice un fácil nivel de acceso, recuperación, trazabilidad, auditabilidad y responsabilidad de sus activos.

178. Se deben destinar las herramientas necesarias que permitan la oportuna gestión de inventarios de los activos, empleando como mínimo identificación plaquetas o etiquetas de identificación externa, contemplando tecnologías que faciliten la gestión de inventarios y el control de entradas y salidas de activos de las instalaciones de la organización.

179. Todo cambio a la configuración de los computadores puede efectuarse únicamente por personal de soporte, con la supervisión del Área de Sistemas, y previa aprobación de los RSIS y RSER implicados.
180. Todo el equipamiento TIC debe estar protegido por reguladores de voltajes y sus instalaciones eléctricas deben haber sido realizadas técnicamente controlando las fases correspondientes.
181. Todos los equipos de cómputo y comunicaciones deben estar protegidos y soportados por equipos ininterrumpidos de electricidad UPS y sus instalaciones eléctricas deben haber sido realizadas técnicamente controlando las fases correspondientes. Cuando se concentren varios equipos en un área se debe hacer un estudio del consumo por equipo para determinar que el circuito no presente sobrecarga.
182. El sistema eléctrico que proporciona energía al Centro de Proceso de Datos será independiente del resto del sistema eléctrico del edificio.
183. Todo el sistema eléctrico de cableado estructurado debe ser conectado de manera independiente al sistema de energía de iluminación, y su gestión debe estar centralizada, acogiendo las normas eléctricas correspondientes para tal fin.

21.3. CONFIGURACIÓN

184. El Área de Sistemas debe implementar los protocolos y/o guías de configuración de todos los servidores de la organización, deben ser establecidas y actualizadas por cada tipo de activo TIC,.
185. Se debe tener toda la información de configuración por cada activo TIC, que garantice como mínimo: función principal, configuración de Hardware, configuración de Software, inventario de aplicaciones, servicios y servidores, ubicación de las copias de respaldo.
186. Debe existir un diagrama de configuración de plataformas, servidores, equipos personales, equipos de comunicaciones y demás activos TIC.
187. La configuración de los activos TIC se debe hacer de acuerdo a los procedimientos y guías técnicas establecidas por las Áreas responsables según su tipo de activo. La configuración será estandarizada según el tipo de activo.

21.4. CONTROL DE ACCESOS

188. Para la parametrización de los accesos privilegiados a los activos TIC, la clave maestra de superusuario o “administrador” será gestionada únicamente por el responsable del Área, y debe existir una copia de respaldo compartida de la misma en poder de un máximo de dos usuarios designados por la dirección.
189. Los Administradores de los Sistemas utilizarán cuentas nominativas e intransferibles, no pudiendo ser cuentas genéricas, para realizar sus cometidos, y se guiarán por el principio de lo mínimos permisos necesarios. No se utilizarán las cuentas preestablecidas de administrador o superusuario (root, Admin, Administrador, etc.) salvo casos de fuerza mayor.
190. Las claves para la administración de red y sistemas de información deben ser cambiadas en forma forzosa por lo menos una vez cada seis meses.
191. La gestión de servidores se debe realizar únicamente bajo la utilización de canales seguros.

192. El acceso físico a servidores debe ser gestionado, programado y autorizado por el Área de Sistemas.

21.5. GESTIÓN

193. La gestión, operación, instalación, desinstalación y mantenimiento del equipamiento TIC es responsabilidad de las Áreas correspondientes según el tipo de activo TIC.
194. El personal técnico perteneciente a las Área responsables de los activos TIC debe ser personal altamente calificado en la gestión de servidores y notificar todas las novedades inherentes a la gestión del mismo.
195. La operación de activos TIC desde áreas de trabajo diferentes a las designadas para soporte técnico, debe ser autorizada por el Área de Seguridad.
196. Los cambios en la configuración de los servidores deben hacerse siguiendo los procedimientos establecidos para dicha operación.

21.6. MONITORIZACIÓN

197. Para todos los eventos críticos de seguridad y los sistemas sensibles es necesario mantener registros o log's y se deben gestionar de acuerdo a los protocolos establecidos.
198. Todos los servidores deben tener activos los servicios de auditoría de eventos que garanticen la auditabilidad de las transacciones realizadas en ellos.
199. Todos los eventos relacionados con la seguridad, rendimiento, fallas y vulnerabilidades se deben reportar al Área de Seguridad, estos eventos se contemplan en los protocolos establecidos.
200. Debe existir un protocolo de acceso remoto, que garantice el adecuado uso de las herramientas existentes para tal fin.

21.7. ACCESOS REMOTOS

201. Toda herramienta de acceso remoto a servidores y equipos de cómputo, debe ser autorizada por el Área de Seguridad e instalada por el ingeniero de Soporte designado.
202. El acceso remoto a los equipos de cómputo será autorizado por el Área de Seguridad, previa solicitud por parte del RSIS, garantizando la confidencialidad de la información de cada usuario.
203. Las conexiones de soporte remotas se realizaran únicamente en caso de no tener acceso directo al equipo que requiera el soporte, por eventos de localización física externa o distante del CICA.
204. Los accesos desde Internet/Intranet para utilizar sistemas de información de la Organización en forma remota y en tiempo real deben ser autorizados por el Área de Sistemas y el Área de Seguridad.
205. Todo acceso remoto debe ser establecido sobre Redes Privadas Virtuales - VPN con encriptación, previa configuración y aprobación por parte del Área de Seguridad.
206. Los accesos remotos para soportes en redes de computadores por terceros y proveedores de Servicios, deben ser asignados, aprobados y documentados por el Área de Comunicaciones.
207. La asignación de claves a terceros y proveedores de servicio, para la comunicación remota con la red central, debe estar supervisada permanentemente y será de asignación temporal.

21.8. MANTENIMIENTO

208. Se debe hacer el mantenimiento periódico del equipamiento TIC, utilizando los procedimientos y/o guías técnicas diseñado por el Área responsable de su soporte, y será documentado acorde a los procedimientos establecidos.
209. Los procedimientos de instalación y mantenimiento de equipamiento TIC deben ser actualizados con cada cambio de versión.
210. Se deben verificar, aprobar e instalar los parches más recientes de seguridad en todo el equipamiento TIC, así como en el software de base y el resto de aplicaciones de uso en el CICA, a menos que esta actividad interfiera con la producción.
211. Los servicios, servidores y aplicaciones que no se utilicen, deben ser deshabilitadas y/o desinstaladas.
212. Debe mantenerse un inventario actualizado de software y hardware de todo el equipamiento TIC del CICA.
213. Se deben redactar los procedimientos y protocolos necesarios que garanticen la adecuada generación, custodia y disposición de las copias de seguridad para los servidores del CICA, acordes con la política de copias de respaldo.

21.9. RESTRICCIONES

214. Todos los usuarios de equipos de cómputo y dispositivos de almacenamiento portátiles, deben registrar la entrada y salida de los mismos en los mecanismos destinados para tal fin.
215. Todos los equipos de uso personal del usuario deben ser registrados en la entrada y salida de las instalaciones en los mecanismos destinados para tal fin.
216. Por el alto riesgo en la manipulación externa de los equipos de cómputo y dispositivos de almacenamiento portátiles, se deben contemplar las siguientes recomendaciones de seguridad.
    - No transportar los equipos de cómputo y dispositivos de almacenamiento portátiles, en vehículos a la vista, o en maletines que sugieran el contenido, mitigando el riesgo de robo / hurto.
    - No prestar o reasignar equipos de cómputo y dispositivos de almacenamiento portátiles a personal externo no autorizado por el CICA.
    - En caso de pérdida o robo / hurto, se debe notificar el incidente de forma inmediata al CSU.
217. Todos los usuarios de los equipos de cómputo y dispositivos de almacenamiento portátiles deben tener en cuenta los siguientes aspectos:
    - No ingerir bebidas y/o alimentos cerca de los equipos de cómputo y dispositivos de almacenamiento portátiles.
    - No fumar cerca a los equipos de cómputo y dispositivos de almacenamiento portátiles.
    - No insertar objetos extraños en las ranuras de los equipos de cómputo y periféricos.
    - No realizar actividades de mantenimiento de hardware.
    - No Instalar Software no autorizado en los equipos de cómputo y dispositivos de almacenamiento

portátiles, si se instala software no licenciado, el usuario debe asumirá las consecuencias legales y económicas.

- Apagar los equipos cuando no estén en uso.
- Bloquear la sesión cuando esté ausente.

218. Es responsabilidad del Área de Sistemas:
    - Mantener una adecuada protección contra fluctuaciones de voltaje, dentro de las instalaciones.
    - Garantizar que únicamente el personal de Soporte pueda instalar software en los equipos de cómputo y periféricos.
    - Establecer programas de mantenimiento de equipos de cómputo y dispositivos de almacenamiento portátiles.

22. CONTROL DE ACTUACIONES SOBRE LAS BASES DE DATOS DEL CICA

219. El CICA 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.

220. 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.

221. Se prohíbe realizar cualquier tipo de actualización en Bases de Datos corporativas, masiva o puntual, sin utilizar las herramientas que los propios sistemas provean, sin la autorización previa de los Responsables de los Sistemas a los que pertenecen las Bases de Datos.

23. USO DEL CORREO ELECTRÓNICO CORPORATIVO

222. El correo electrónico corporativo es una herramienta de mensajería electrónica centralizada, puesta a disposición de los usuarios del CICA, para el envío y recepción de correos electrónicos mediante el uso de cuentas de correo corporativas.

223. Junto con los mensajes también pueden ser enviados ficheros adjuntos. Las características peculiares de este medio de comunicación (universalidad, bajo coste, anonimato, etc.) han propiciado la aparición de amenazas que utilizan el correo electrónico para propagarse o que aprovechan sus vulnerabilidades.

224. 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.

225. Por ello, sus normas de uso forman parte de un documento específico, "*NS01 CICA – CORREO ELECTRONICO*" incluido en la misma ubicación que el presente documento.

24. ACCESO A INTERNET Y OTRAS HERRAMIENTAS DE COLABORACIÓN

226. El acceso corporativo a Internet es un recurso centralizado que el CICA 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.

227. El CICA 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.

228. Por ello, sus normas de uso forman parte de un documento específico, "*NS02 CICA – INTERNET*" incluido en la misma ubicación que el presente documento.

25. USO ABUSIVO DE LOS SISTEMAS DE INFORMACIÓN.

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

230. Con carácter general, se enumeran seguidamente un conjunto de acciones que se consideran uso abusivo de los sistemas de información del CICA:

25.1. 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 del CICA archivos personales, salvo autorización previa expresa del Área de Seguridad.
  - 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.
  - Publicación o envío de información sensible, confidencial, protegida o propiedad del CICA, 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 del CICA, de sus representantes o de los organismos públicos o privados con los que se mantiene relación.

25.2. 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 del CICA para enviar mensajes o cartas en cadena y/o correos basura o spam (correo electrónico no solicitado).
- Usar cualquier cuenta de correo del CICA 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 del CICA 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 del CICA, de sus representantes o de los organismos públicos o privados con los que se mantiene relación.

25.3. USO ABUSIVO DE OTROS SERVICIOS Y SISTEMAS DEL CICA

- Acceso a servicios y/o contenidos del CICA 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 del CICA.
  - El uso de mensajería instantánea (Messenger, Skype, etc.).
  - Transferencia de ficheros entre usuarios del CICA no relativa a las actividades profesionales.
  - Realizar cualquier actividad de promoción de intereses personales.
- Uso de cualquier servicio del CICA para:
  - La publicación o envío de información no solicitada.
  - La publicación o envío de información confidencial, propiedad del CICA, 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 del CICA para propósitos que puedan influir negativamente en la imagen del CICA, 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.

- La comunicación a terceros del contenido de cualquier dato reservado o confidencial propiedad del CICA o de terceros, salvo que tal actuación fuera realizada en cumplimiento de fines estrictamente profesionales con el previo consentimiento de los afectados.
- Las acciones realizadas desde una cuenta de usuario o desde una cuenta de correo electrónico de usuario son responsabilidad de su titular.
- El CICA 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.

26. MONITORIZACIÓN Y APLICACIÓN DE ESTA NORMATIVA

231. El CICA, por motivos legales, de seguridad y de calidad del servicio, y cumpliendo en todo momento los requisitos que al efecto establece la legislación vigente, tal y como establece el artículo 23 del Real Decreto 3/2010, de 8 de enero, por el que se regula el ENS:

> **Artículo 23. Registro de actividad**
>
> 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 monitorizar, analizar, investigar y documentar actividades indebidas o no autorizadas, permitiendo identificar en cada momento a la persona que actúa..

232. Por lo tanto, el CICA:

- Revisará periódicamente el estado de los equipos, el software instalado, los dispositivos y redes de comunicaciones de su responsabilidad.
- Monitorizará los accesos a la información contenida en sus sistemas.
- Auditará la seguridad de las credenciales y aplicaciones.
- Monitorizará los servicios de Internet, correo electrónico y otras herramientas de colaboración.

233. El CICA 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 (Guía CCN-STIC 831 Registro de la actividad de los usuarios).

234. 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. El Área de Seguridad, con la colaboración de las restantes unidades del CICA, velará por el cumplimiento de la presente Normativa General e informará a la Dirección del CICA sobre los incumplimientos o deficiencias de seguridad observados, al objeto de que se tomen las medidas oportunas.

235. 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.

236. El sistema que proporciona el servicio de navegación en Internet 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 al Área de Seguridad sobre usos prolongados e indebidos del servicio.

237. Las actividades realizadas por los Administradores de los Sistemas deben reflejarse en un registro, que debe ser monitorizado periódicamente por el Administrador de Seguridad de los Sistemas (ASS), y que será salvaguardado y custodiado de forma que se mantenga su disponibilidad e integridad para poder consultar los eventos sucedidos con una antigüedad de al menos dos (2) años.

27.INCUMPLIMIENTO DE LA NORMATIVA

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

238. En el supuesto de que un usuario no observe alguno 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 correspondientes, se podrá acordar la suspensión temporal o definitiva del uso de los recursos informáticos asignados a tal usuario.

28. MODELO DE ACEPTACIÓN Y COMPROMISO DE CUMPLIMIENTO

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

Mediante la cumplimentación de la siguiente declaración, el abajo firmante, [personal del CICA/ empleado de la <<EMPRESA>>], como usuario de recursos informáticos y sistemas de información del CICA, declara haber leído y comprendido la Normativa General de Utilización de los Recursos y Sistemas de Información del CICA (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 el CICA: _____

DNI número: _____

Número de Registro de Personal: _____

29. COMPENDIO DE NORMAS

NORMATIVA GENERAL DE UTILIZACIÓN DE LOS RECURSOS Y SISTEMAS DE INFORMACIÓN DEL CICA (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 del CICA serán devueltos por el usuario cuando este finalice su relación laboral con el CICA.	-	X	X	X
	El dispositivo asignado a un usuario de el CICA 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	-
	El usuario no conectará a la red corporativa ningún equipo o dispositivo sin autorización expresa.	X	X	X	X

NORMATIVA GENERAL DE UTILIZACIÓN DE LOS RECURSOS Y SISTEMAS DE INFORMACIÓN DEL CICA (Compendio de las normas más significativas)					
Área	**Norma**	**PC**	**Dispositivo móvil (teléfono, tablet, ...)**	**Ordenador Portátil**	**Pen drive**
	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 el CICA.	X	X	X	-
	Los usuarios no podrán borrar, desinstalar o modificar la configuración de las aplicaciones informáticas instaladas en el CICA	X	X	X	-
	Las aplicaciones informáticas instaladas en el CICA 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 del CICA 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 del CICA 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	-
	No se dejará información accesible con datos de carácter personal, datos técnicos de sistemas o información sensible, confidencial o protegida del CICA 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 del CICA, cuando se utilicen soportes o dispositivos extraíbles, se cifrarán talles datos.	-	X	X	X

NORMATIVA GENERAL DE UTILIZACIÓN DE LOS RECURSOS Y SISTEMAS DE INFORMACIÓN DEL CICA (Compendio de las normas más significativas)					
Área	**Norma**	**PC**	**Dispositivo móvil (teléfono, tablet, ...)**	**Ordenador Portátil**	**Pen drive**
Correo electrónico	El correo electrónico es un servicio proporcionado por el CICA 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 el CICA 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 el CICA.	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	-
Redes Inalámbricas	Por motivos de seguridad no se deben utilizar conexiones inalámbricas con tecnología Wifi distintas a las proporcionadas, en su caso, por el CICA.	X	X	X	-
	Por motivos de seguridad, se recomienda que se mantenga desactivado el reconocimiento de dispositivos Bluetooth, especialmente fuera de las instalaciones del CICA. 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	-	-

NORMATIVA GENERAL DE UTILIZACIÓN DE LOS RECURSOS Y SISTEMAS DE INFORMACIÓN DEL CICA (Compendio de las normas más significativas)					
Área	**Norma**	**PC**	**Dispositivo móvil (teléfono, tablet, ...)**	**Ordenador Portátil**	**Pen drive**
	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 al CSU.	X	X	X	X
	Cualquier incidente de seguridad como consecuencia de virus, spam o vulneración de la confidencialidad, será comunicado de forma urgente a Cualquier incidente de seguridad como consecuencia de virus, spam o vulneración de la confidencialidad, será comunicado de forma urgente al CSU.	X	X	X	X