ANEXO I.

PROCEDIMIENTO DE GESTIÓN DE USUARIOS: ALTAS, BAJAS, IDENTIFICACIÓN, AUTENTICACIÓN Y CONTROL DE ACCESO LÓGICO
PR10

INDICE

1. OBJETO

1. El objeto del presente documento es la definición del **Procedimiento aplicable a la Gestión de Usuarios: Altas, Bajas, Identificación, Autenticación y Control de Acceso Lógico de los usuarios de los Sistemas de Información del <<ORGANISMO>>**, dentro del alcance señalado en el ENS.

Se implantará el presente Procedimiento atendiendo al **nivel de seguridad de la información y los servicios prestados, y la categoría de los sistemas del <<ORGANISMO>>,** que resulten de la aplicación de las previsiones contempladas en los Anexos I y II del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la administración electrónica (ENS).

2. ÁMBITO DE APLICACIÓN

2. Este Procedimiento es de aplicación a todo el ámbito de actuación del <<ORGANISMO>>, y sus contenidos traen causa de las directrices de carácter más general definidas en la Política de Seguridad de la Información y en las Normas de Seguridad del <<ORGANISMO>>.
3. El presente Procedimiento es de aplicación y de obligado cumplimiento para todo el personal que, de manera permanente o eventual, preste sus servicios en el <<ORGANISMO>>, incluyendo el personal de proveedores externos, cuando sean usuarios de los Sistemas de Información del <<ORGANISMO>>.
4. En el ámbito de la presente normativa, se entiende por usuario cualquier empleado público perteneciente o ajeno al <<ORGANISMO>>, así como personal de organizaciones privadas externas, entidades colaboradoras o cualquier otro con algún tipo de vinculación con el <<ORGANISMO>> y que utilice o posea acceso a los Sistemas de Información del <<ORGANISMO>>.

3. VIGENCIA

5. El presente Procedimiento ha sido aprobado por la <<U/OC>> del <<ORGANISMO>>, estableciendo de esta forma las directrices generales para el uso adecuado de los recursos de tratamiento de información que el <<ORGANISMO>> 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.
6. Cualquier modificación posterior entrará en vigor inmediatamente después de su publicación por parte del <<ORGANISMO>>.
7. 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 este Procedimiento.

4. REVISIÓN Y EVALUACIÓN

8. La gestión de este Procedimiento 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.
9. Anualmente (o con menor periodicidad, si existen circunstancias que así lo aconsejen), la <<U/OC>> revisará el presente Procedimiento, que se someterá, de haber modificaciones, a la aprobación de la <<U/OC>> del <<ORGANISMO>>.
10. 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.
11. Será el Responsable de Seguridad la persona encargada de la custodia y divulgación de la versión aprobada de este documento.

5. REFERENCIAS

12. La implantación de un Procedimiento como el descrito requiere el examen previo de la siguiente documentación:
    - Normativa de Seguridad [org.2]: Normativa General de Utilización de los Recursos y Sistemas de Información del <<ORGANISMO>>[1].
    - Normativa de Seguridad [org.2]: Normas Especiales o Particulares del <<ORGANISMO>>[2].

6. ROLES Y RESPONSABILIDADES

13. Las responsabilidades definidas por las tareas contempladas en el procedimiento son las siguientes:

Roles	Responsabilidades[3]
Usuarios	Aplicar el presente Procedimiento.
Responsable de Seguridad (RSEG)	• Mantener la seguridad de la información manejada y de los servicios prestados por los sistemas de información en su ámbito de responsabilidad, de acuerdo a lo

[1] Véase "Guía CCN-STIC 821. Normas de Seguridad en el ENS". En concreto, puede consultarse la Norma NG00-Normativa General de Utilización de los Recursos y Sistemas de Información del <<ORGANISMO>>, de Anexo I.
[2] Véase "Guía CCN-STIC 821. Normativa de Seguridad en el ENS". En concreto, pueden consultarse las Normas Particulares del Anexo II.
[3] Véase Guía CCN-STIC 801. Responsabilidades en el ENS.

	establecido en la Política de Seguridad del <<ORGANISMO>>. • Promover la formación y concienciación en materia de seguridad de la información dentro de su ámbito de responsabilidad. • Determinación de la categoría del sistema. • Análisis de riesgos. • Declaración de aplicabilidad. • Medidas de seguridad adicionales. • Elaborar configuración de seguridad. • Documentación de seguridad del sistema. • Elaborar Normativa de seguridad. • Aprobar Procedimientos de seguridad. • Elaborar planes de mejora de la seguridad. • Elaborar planes de concienciación y formación. • Validar Planes de Continuidad. • Aprobar el ciclo de vida de seguridad: especificación, arquitectura, desarrollo, operación y cambios. • Analizar y proponer salvaguardas que prevengan incidentes similares en el futuro.
Responsable del sistema (RSIS)	• Desarrollar, operar y mantener el Sistema de Información. • Definir la topología y sistema de gestión del Sistema de Información. • Cerciorarse de que las medidas específicas de seguridad se integren adecuadamente. • Elaborar os Procedimientos de seguridad. • Elaborar el Plan de mejora de la seguridad. • Elaborar el Plan de Continuidad. • Propone la suspensión temporal del servicio. • Elabora el ciclo de vida de seguridad: especificación, arquitectura, desarrollo, operación y cambios. • Planifica la implantación de las salvaguardas en el sistema. • Ejecuta el Plan de Seguridad

	aprobado.
Administrador de Seguridad del Sistema (ASS)	• Implantación, gestión y mantenimiento de las medidas de seguridad. • Gestión, configuración y actualización, en su caso, del hardware y software de seguridad, así como su supervisión. • Gestión de las autorizaciones y privilegios concedidos a los usuarios del sistema. • Aplicación de los Procedimientos de seguridad y verificación de su cumplimiento. • Aprobar los cambios en la configuración de seguridad. • Asegurar que los controles de seguridad se cumplen. • Monitorizar el estado de seguridad del sistema. • Informar al RSEG y RSIS de cualquier anomalía. • Colaborar en la investigación y resolución de incidentes de seguridad. • Llevar a cabo el registro, contabilidad y gestión de los incidentes de seguridad. • Aislar el incidente para evitar la propagación. • Tomar decisiones a corto plazo si la información se ha visto comprometida de tal forma que pudiera tener consecuencias graves. • Asegurar la integridad de los elementos críticos del Sistema si se ha visto afectada la disponibilidad de los mismos. • Mantener y recuperar la información almacenada por el Sistema y sus servicios asociados. • Investigar el incidente: Determinar el modo, los medios, los motivos y el origen del incidente.
Responsable de personal	Comunicar el alta y baja de usuarios, a través del procedimiento descrito en el presente documento.

7. GESTIÓN DE USUARIOS

7.1 ALTA/BAJA DE PERSONAL

14. A continuación se identifican las Áreas/Personal del <<ORGANISMO>> involucrado en la ejecución de alguna de las tareas que se van a describir en este epígrafe y que tendrán que ser debidamente informados para la correcta ejecución del procedimiento.

    - Responsable de Asignación de Recursos IT[4].
    - Secretaría.
    - Jefes de Área / Jefes de Servicio.
    - CAU.
    - Área de Sistemas.
    - Área de Comunicaciones.
    - Área de Desarrollo.
    - Área de Administración Electrónica.
    - Grupo de Telefonía Fija.
    - Grupo de Dispositivos Móviles.
    - RRHH
    - Habilitación General.
    - Área de Seguridad[5].

7.1.1 PROCESO DE ALTA DE EMPLEADOS PÚBLICOS EN EL <<ORGANISMO>>

15. El empleado público que se incorpore al <<ORGANISMO>> proporcionará, entre otros, los siguientes datos:

    - Nombre.
    - Apellidos.
    - DNI.
    - Otros datos de distinta naturaleza (bancarios, etc.)

16. Seguidamente, se describe el proceso requerido para la incorporación de un empleado público al <<ORGANISMO>>. En el momento en el que el empleado público se incorpore a su puesto en el área correspondiente del <<ORGANISMO>>, su responsable definirá sus necesidades tecnológicas, pudendo incluir: alta en ciertos sistemas, asignación de ordenador, teléfono, etc.

[4] Suele tratarse de una función asignada al Departamento de Sistemas de los organismos.
[5] En ciertos organismos, estas funciones están centralizadas en la Oficialía Mayor.

<table>
<tr><th colspan="3">Proceso de ALTA DE EMPLEADOS PÚBLICOS en el <<ORGANISMO>></th></tr>
<tr><td colspan="3">

- El responsable del empleado público enviará una solicitud vía correo electrónico al Responsable de Asignación de Recursos IT del <<ORGANISMO>> <<*señalar dirección de email*>>, indicándole las necesidades del nuevo usuario e incluyendo, entre otros, los siguientes datos:
  - Nombre y Apellidos.
  - NIF.
  - Perfil (permisos de acceso a recursos del sistema).
  - Puesto de trabajo (denominación del puesto y unidades administrativas a las que pertenece).
  - Ubicación (edificio, planta, despacho).
  - Teléfono, si ya se conoce.

</td></tr>
<tr><td colspan="3">

- El Responsable de Asignación de Recursos IT del <<ORGANISMO>> enviará un correo electrónico al Área de Seguridad del <<ORGANISMO>> <<*señalar dirección de email*>> solicitando la credencial[6] de acceso al <<ORGANISMO>>. El correo electrónico incluirá los datos del empleado público que se va a incorporar: nombre, apellidos, NIF, un teléfono de contacto, etc.

</td></tr>
<tr><th>ALTA EN SISTEMAS Y ASIGNACIÓN DE EQUIPAMIENTO</th><th>ALTA EN TELEFONÍA FIJA</th><th>ALTA EN TELEFONÍA MÓVIL O DATOS EN MOVILIDAD</th></tr>
<tr><td>

- En caso de que la solicitud requiera el **ALTA EN LOS SISTEMAS DE INFORMACIÓN Y/O EQUIPAMIENTO INFORMÁTICO**, el Responsable de Asignación de Recursos IT del <<ORGANISMO>> remitirá un correo electrónico al CAU <<*señalar*

</td><td>

- En caso de que la solicitud requiera **TELÉFONO FIJO,** el Responsable de Asignación de Recursos IT del <<ORGANISMO>> remitirá un correo electrónico al Grupo de Telefonía Fija <<*señalar dirección de email*>> con la *Solicitud de Alta/Baja de Telefonía Fija*[9], incluyendo la

</td><td>

- En caso de que la solicitud requiera **TELÉFONO MÓVIL O CONEXIÓN DE DATOS DE MOVILIDAD PARA PORTÁTIL**, el Responsable de Asignación de Recursos IT del <<ORGANISMO>> remitirá un correo electrónico al Grupo de Móviles <<*señalar dirección de*

</td></tr>
</table>

[6] Suele ser frecuente el uso de tarjetas personalizadas, que pueden incluir ciertos datos personales tales como: nombre, apellidos, cargo, fotografía e, incluso, un chip criptográfico para contener certificados digitales.

dirección de email>> con la *Solicitud de Alta/Baja de Recursos IT*[7], incluyendo la información recibida del responsable del nuevo empleado público. ○ El CAU dará de alta al usuario e informará de ello al Responsable de Asignación de Recursos IT del <<ORGANISMO>> <<*señalar dirección de email*>>. Para ello, utilizará la *Solicitud de Alta/Baja de Recursos IT*[8], completando la información requerida en la plantilla. ○ El Responsable de Asignación de Recursos IT del <<ORGANISMO>> enviará la información del alta al responsable del funcionario que la ha solicitado.	información recibida del responsable del nuevo empleado público. ○ El Grupo de Telefonía Fija ejecutará las acciones pertinentes para asignar un teléfono y una línea al usuario e informará vía correo electrónico del número de teléfono fijo y su extensión al Responsable de Asignación de Recursos IT del <<ORGANISMO>>, utilizando la *Solicitud de Alta/Baja de Telefonía Fija*. ○ El Responsable de Asignación de Recursos IT del <<ORGANISMO>> enviará al responsable del nuevo empleado público funcionario que ha solicitado la línea de teléfono la información recibida del Grupo de Telefonía Fija y pondrá en copia del correo electrónico al nuevo empleado público.	*email*>> con la *Solicitud de Alta/Baja de Telefonía Móvil o Datos en Movilidad*[10]. ○ El Grupo de Móviles ejecutará las acciones pertinentes para asignar y entregar el teléfono móvil y/o configurar la conexión de datos de movilidad al nuevo empleado público, e informará vía correo electrónico la finalización de las tareas solicitadas, al Responsable de Asignación de Recursos IT del <<ORGANISMO>>, utilizando el formulario *Solicitud de Alta/Baja de Telefonía Móvil o Datos en Movilidad.* ○ El Responsable de Asignación de Recursos IT del <<ORGANISMO>> enviará al responsable del nuevo empleado público que ha solicitado el teléfono móvil o la conexión de

[9] Un modelo de esta solicitud puede encontrase en el Anexo II.
[7] Un modelo de esta solicitud puede encontrase en el Anexo I.
[8] Un modelo de esta solicitud puede encontrase en el Anexo I.
[10] Un modelo de esta solicitud puede encontrase en el Anexo III. Esta solicitud podrá requerir la inclusión de la autorización de la Jefatura de Comunicaciones.

		datos de movilidad, la información recibida del grupo de móviles y pondrá en copia del correo electrónico al nuevo empleado público.

- El Responsable de Asignación de Recursos IT del <<ORGANISMO>> deberá dar de alta al nuevo empleado público en la <<*Aplicación de Gestión de Accesos del Organismo*>>, para ello deberá recabar del empleado público los siguientes datos:

  - Nombre.
  - Apellidos.
  - NIF.
  - Fecha de alta.
  - Teléfono.
  - Puesto de trabajo.

  El Responsable de Asignación de Recursos IT del <<ORGANISMO>> será responsable del registro y seguimiento de las solicitudes realizadas a las distintas áreas. En el caso de que existiera algún problema, el Responsable de Asignación de Recursos IT del <<ORGANISMO>> deberá informar de la situación al solicitante, señalando la causa de la demora en la ejecución de las solicitudes.

7.1.2 PROCESO DE BAJA DE EMPLEADOS PÚBLICOS EN EL <<ORGANISMO>>

17. Procedimiento a seguir al producirse la baja de un empleado público destinado en el <<ORGANISMO>>, al objeto de proceder a la retirada del equipamiento tecnológico asignado, baja en los sistemas, etc.

<table>
<tr><th colspan="3">Proceso de BAJA DE EMPLEADOS PÚBLICOS en el <<ORGANISMO>></th></tr>
<tr><td colspan="3">

- El Responsable del empleado público que se da de baja informará mediante correo electrónico al Responsable de Asignación de Recursos IT del <<ORGANISMO>> <<*señalar dirección de email*>> de la baja del empleado público. En dicho correo electrónico se deberán identificar entre otros datos: nombre, apellidos, NIF, Área del <<ORGANISMO>> en la que trabaja, puesto de trabajo y la fecha de baja del personal.

</td></tr>
<tr><th>BAJA DE SISTEMAS Y RETIRADA DE EQUIPO</th><th>BAJA DE TELEFONÍA FIJA</th><th>BAJA EN TELEFONÍA MÓVIL O DATOS EN MOVILIDAD</th></tr>
<tr>
<td>

- El Responsable de Asignación de Recursos IT del <<ORGANISMO>> remitirá al CAU <<*señalar dirección de email*>> la *Solicitud de Alta/Baja de Recursos IT*, informando de la baja del empleado público y solicitando la baja del empleado público en los **sistemas,** la retirada del **equipo** que en su caso tenga asignado, y señalando la fecha de baja.
  - El CAU ejecutará las acciones pertinentes para dar de baja al usuario de los sistemas en la fecha de baja señalada.
  - El CAU se pondrá en contacto con el empleado público que va a causar baja y le reclamará la devolución del equipo facilitado

</td>
<td>

- El Responsable de Asignación de Recursos IT del <<ORGANISMO>> remitirá al Grupo de Telefonía Fija <<*señalar dirección de email*>> la *Solicitud de Alta/Baja de Telefonía Fija*, informando de la baja del empleado público y solicitando la retirada del equipamiento que tuviere asignado, y señalando la fecha de baja.
  - En el caso de que no tuviera ningún equipo de telefonía fija asignado, el Grupo de Telefonía Fija informará de ello al Responsable de Asignación de Recursos IT del <<ORGANISMO>> y se dará por cerrada la solicitud.
  - En el caso de tener asignado un

</td>
<td>

- El Responsable de Asignación de Recursos IT del <<ORGANISMO>>, remitirá al Grupo de Dispositivos Móviles <<señalar dirección de email>> la *Solicitud de Alta/Baja de Telefonía Móvil o Datos en Movilidad*, informando de la baja del empleado público y solicitando la retirada del equipo de telefonía móvil o tarjeta de conexión de datos de movilidad que tuviere asignado, y señalando la fecha de baja.
  - En el caso de que no tuviera ningún equipo de telefonía móvil o tarjeta de conexión de datos en movilidad asignada, el Grupo de Dispositivos Móviles informará de ello al Responsable de Asignación de Recursos IT del

</td>
</tr>
</table>

por el <<ORGANISMO>>. ○ Una vez completada la solicitud, el CAU informará mediante correo electrónico al Responsable de Asignación de Recursos IT de la SGTIC la finalización del trabajo solicitado. Para ello cumplimentará los campos asignados en el formulario de *Solicitud de Alta/Baja de Recursos IT*.	equipo de telefonía fija asignado, el Grupo de Telefonía Fija retirará el equipo del puesto de trabajo indicado en la solicitud. ○ Una vez realizadas las acciones solicitadas, el Grupo de Telefonía Fija informará mediante correo electrónico al Responsable de Asignación de Recursos IT del <<ORGANISMO>> la finalización del trabajo. Para ello utilizará los campos asignados en la *Solicitud de Alta/Baja de Telefonía Fija*.	<<ORGANISMO>> y se dará por cerrada la solicitud. ○ En el caso de tener asignado un equipo de telefonía móvil o tarjeta de conexión de datos en movilidad, el Grupo de Dispositivos Móviles, mediante su procedimiento interno, se pondrá en contacto con el empleado público que causa baja y retirará el material que el empleado público tuviera asignado. ○ Una vez completada la solicitud, el Grupo de Dispositivos Móviles informará mediante correo electrónico al Responsable de Asignación de Recursos IT del <<ORGANISMO>> la finalización del trabajo solicitado. Para ello utilizará los campos asignados en la *Solicitud de Alta/Baja de Telefonía Móvil o Datos en Movilidad.*
• El Responsable de Asignación de Recursos IT del <<ORGANISMO>> informará al Área de Seguridad del <<ORGANISMO>> <<*señalar dirección de email*>> la fecha de baja del empleado público, al objeto de que, a partir de dicha fecha, se revoque el permiso de acceso físico a las instalaciones. • En el día en el que el empleado público cause baja en el <<ORGANISMO>>, el Responsable de Asignación de Recursos IT del		

<<ORGANISMO>> se pondrá en contacto con el empleado público para retirarle la tarjeta de acceso. • El Responsable de Asignación de Recursos IT del <<ORGANISMO>> enviará a la unidad competente[11], por valija interna, las tarjetas de acceso de los empleados públicos dados de baja en el <<ORGANISMO>>. • El Responsable de Asignación de Recursos IT del <<ORGANISMO>> dará de baja al usuario en la <<*Aplicación de Gestión de Accesos del Organismo*>> y, en su caso, en la <<*Aplicación de Control Horario del Organismo*>>.
• Una vez confirmado que se ha dado de baja al usuario en los sistemas, que se le ha retirado el equipo, el teléfono y la tarjeta de acceso, el Responsable de Asignación de Recursos IT del <<ORGANISMO>> enviará la confirmación de la baja completa al responsable del empleado público que solicitó la baja.

[11] Por ejemplo, la Oficialía Mayor.

7.1.3 PROCESO DE ALTA DE PERSONAL EXTERNO EN EL <<ORGANISMO>>

18. El trabajador externo que se incorpore al <<ORGANISMO>> proporcionará, entre otros, los siguientes datos:
    - Nombre.
    - Apellidos.
    - NIF.
    - Empresa.
    - Categoría Profesional.
    - Proyecto.
    - Jefe de Proyecto en el <<ORGANISMO>>.
    - Tiempo estimado de estancia.
19. Seguidamente se describe el proceso de Alta.

Proceso de ALTA DE PERSONAL EXTERNO en el <<ORGANISMO>>

- Con anterioridad a la incorporación de nuevo personal externo en el área correspondiente del <<ORGANISMO>>, se identificarán las necesidades de tal personal externo por parte del responsable del personal externo, pudendo incluir: alta en los sistemas, asignación de ordenador, teléfono, etc.

- Para satisfacer las anteriores necesidades, el responsable del personal externo enviará una solicitud vía correo electrónico al Responsable de Asignación de Recursos IT del <<ORGANISMO>> <<*señalar dirección de email*>>, indicándole las necesidades del nuevo usuario e incluyendo la siguiente información:

  - Nombre.
  - Apellidos.
  - NIF.
  - Perfil.
  - Puesto de trabajo.
  - Empresa.
  - Fecha de incorporación.
  - Fecha prevista de finalización.

  Adicionalmente, en esa misma comunicación, el responsable del personal externo deberá informar si el nuevo personal externo va a utilizar el equipo de su propia organización o si, por el contrario, va a ser necesario que se le asigne un equipo perteneciente al <<ORGANISMO>>.

- El Responsable de Asignación de Recursos IT del <<ORGANISMO>> enviará un correo electrónico solicitando al Área de Seguridad del <<ORGANISMO>>[12] <<*señalar dirección de email*>> las credenciales de acceso al <<ORGANISMO>>[13] para el nuevo personal externo. El correo electrónico incluirá los datos de la persona externa que se va a incorporar: nombre, apellidos, NIF, organización a la

[12] En muchas ocasiones, se trata de la Oficialía Mayor.
[13] Usualmente, una tarjeta personalizada, que podrá incluir un chip criptográfico para alojar certificados digitales.

que pertenece y un teléfono de contacto.

ALTA EN SISTEMAS Y/O ASIGNACIÓN DE EQUIPAMIENTO	ALTA EN TELEFONÍA FIJA	ALTA EN TELEFONÍA MÓVIL O DATOS EN MOVILIDAD
• En caso de solicitud de **alta en los sistemas y/o equipamiento informático** del <<ORGANISMO>>, el Responsable de Asignación de Recursos IT del <<ORGANISMO>> remitirá un correo electrónico al CAU <<*señalar dirección de email*>> con la *Solicitud de Alta/Baja de Recursos IT*, incluyendo la información recibida del responsable del personal externo. o El CAU ejecutará las acciones pertinentes para de alta al usuario y/o para asignarle equipo y tras su finalización, informará vía correo electrónico al Responsable de Asignación de Recursos IT del <<ORGANISMO>>. Para ello, utilizará la *Solicitud de Alta/Baja de Recursos IT*, completando la información requerida en la plantilla. o El Responsable de Asignación de	• En caso de requerir **teléfono fijo,** el Responsable de Asignación de Recursos IT del <<ORGANISMO>> remitirá un correo electrónico al Grupo de Telefonía Fija <<*señalar dirección de email*>> con la *Solicitud de Alta/Baja de Telefonía Fija*, incluyendo la información recibida del responsable del personal externo. o El Grupo de Telefonía Fija ejecutará las acciones pertinentes para asignar un teléfono y una línea al usuario, e informará al Responsable de Asignación de Recursos IT del <<ORGANISMO>> del teléfono fijo y la extensión vía correo electrónico utilizando el formulario de *Solicitud de Alta/Baja de Telefonía Fija.* o El Responsable de Asignación de Recursos IT del	• En caso de requerir **teléfono móvil o conexión de datos en movilidad**, el Responsable de Asignación de Recursos IT del <<ORGANISMO>> remitirá un correo electrónico al Grupo de Dispositivos Móviles <<señalar dirección de email>> con la *Solicitud de Alta/Baja de Telefonía Móvil o Datos en Movilidad*[14]. o El Grupo de Dispositivos Móviles realizará las acciones pertinentes para asignar y entregar el teléfono móvil y/o configurar la conexión de datos de movilidad al personal externo, e informará al Responsable de Asignación de Recursos IT del <<ORGANISMO>>, la finalización de las tareas solicitadas. Para ello utilizará la *Solicitud de Alta/Baja de Telefonía Móvil o Datos en Movilidad.*

[14] Que podrá incluir la autorización del Jefe de Área de Comunicaciones (o unidad equivalente).

Recursos IT del <<ORGANISMO enviará la información del alta o baja al responsable del personal externo que la ha solicitado.	<<ORGANISMO>> remitirá al responsable del personal externo que ha solicitado la línea de teléfono fijo la información recibida del Grupo de Telefonía Fija y pondrá en copia del correo electrónico al usuario final.	○ El Responsable de Asignación de Recursos IT del <<ORGANISMO>> remitirá al responsable del personal externo que ha solicitado el teléfono móvil y/o la conexión de datos en movilidad, la información recibida del Grupo de Dispositivos Móviles y pondrá en copia del correo electrónico al personal externo.
• Como norma general, el personal externo no podrá conectar sus propios **equipos** al dominio del <<ORGANISMO>>, utilizando los que le sean proporcionados por el <<ORGANISMO>>. En casos excepcionales en los que se autorice aquel uso, se adoptarán las siguientes cautelas: ○ El responsable del personal externo que va a utilizar su propio equipamiento (ordenador portátil, por ejemplo) debe de realizar las tareas definidas en el procedimiento de <<*Normativa de seguridad para ordenadores de usuarios externos*>>. ○ El Responsable de Asignación de Recursos IT del <<ORGANISMO>> remitirá vía correo electrónico al CAU <<*señalar dirección de email*>> la *Solicitud de Alta/Baja de Recursos IT*, que incluirá la autorización del responsable del personal externo. ○ El Responsable de Asignación de Recursos IT del <<ORGANISMO>> acompañará al CAU al personal externo incorporado. ○ El CAU realizará el procedimiento interno definido e informará al Responsable de Asignación de Recursos IT, vía correo electrónico, la finalización del trabajo solicitado. Para ello usará la *Solicitud de Alta/baja de Recursos IT*. ○ El Responsable de Asignación de Recursos IT del <<ORGANISMO>> enviará la información del alta al responsable del personal externo que la ha solicitado y pondrá en copia del correo electrónico al usuario final.		
• El Responsable de Asignación de Recursos IT del <<ORGANISMO>> deberá de dar de alta al usuario externo en la <<*Aplicación de Gestión de Accesos del Organismo*>>. Para ello, deberá recabar los datos necesarios, tales como: ○ Nombre.		

- Apellidos.
- NIF.
- Perfil.
- Puesto de trabajo.
- Empresa.
- Fecha de incorporación.
- Fecha de finalización.

El Responsable de Asignación de Recursos IT del <<ORGANISMO>> será responsable del registro y seguimiento de las solicitudes realizadas a las distintas áreas. En el caso de que existiera algún problema, el Responsable de Asignación de Recursos IT del <<ORGANISMO>> deberá informar de la situación al solicitante, señalando la causa de la demora en la ejecución de las solicitudes.

7.1.4 PROCESO DE BAJA DE PERSONAL EXTERNO EN EL <<ORGANISMO>>

20. Seguidamente se describe el proceso de baja de personal externo, al objeto de revocar los permisos de acceso a los sistemas, retirada de equipamiento, etc.

<table>
<tr><th colspan="3">Proceso de BAJA DE PERSONAL EXTERNO en el <<ORGANISMO>></th></tr>
<tr><td colspan="3">

- El Responsable de Asignación de Recursos IT del <<ORGANISMO>>, realiza un **seguimiento continuo** de las fechas de expiración de las credenciales de identificación del personal externo al <<ORGANISMO>>. Para ello, en el momento en el que a un personal externo se le entregue una credencial de acceso, el Responsable de Asignación de Recursos IT del <<ORGANISMO>> deberá registrar la fecha en la que le caduca la misma en la <<*Aplicación de Gestión de Accesos del Organismo*>>.

- El Responsable de Asignación de Recursos IT del <<ORGANISMO>> controlará periódicamente las tarjetas próximas a caducar y remitirá un correo electrónico a los distintos responsables para interesarse por su eventual renovación o la confirmación de su definitiva baja.

</td></tr>
<tr><td colspan="3">

- El responsable de cada personal externo consultado confirmará al Responsable de Asignación de Recursos IT del <<ORGANISMO>> si es necesaria o no la renovación de las credenciales de acceso del personal externo. En el caso de que lo sea, el Responsable de Asignación de Recursos IT del <<ORGANISMO>> acompañará al personal externo a renovar la credencial, de manera análoga a la que se ha descrito anteriormente en el procedimiento.

- En el caso de que el responsable del personal externo informe al Responsable de Asignación de Recursos IT del <<ORGANISMO>> que el usuario externo va a causar baja definitiva en el <<ORGANISMO>>, entonces se deberán realizar las acciones pertinentes para que le sea retirado el equipamiento tecnológico del <<ORGANISMO>> que se le hubiere entregado o que tuviere asignado, así como darle de baja de los sistemas.

</td></tr>
<tr><th>BAJA DE SISTEMAS Y RETIRADA DE EQUIPO</th><th>BAJA DE TELEFONÍA FIJA</th><th>BAJA EN TELEFONÍA MÓVIL O DATOS EN MOVILIDAD</th></tr>
<tr><td>

- El Responsable de Asignación de Recursos IT del <<ORGANISMO>> remitirá por correo electrónico al CAU <<*señalar dirección de email*>> la *Solicitud de Alta/Baja de Recursos IT*, solicitando la baja del usuario del

</td><td>

- El Responsable de Asignación de Recursos IT del <<ORGANISMO>> remitirá por correo electrónico al Grupo de Telefonía Fija del <<ORGANISMO>> <<*señalar dirección de email*>> la *Solicitud de*

</td><td>

- El Responsable de Asignación de Recursos IT del <<ORGANISMO>> remitirá por correo electrónico al Grupo de Dispositivos Móviles del <<ORGANISMO>> <<*señalar dirección de email*>> la *Solicitud de*

</td></tr>
</table>

sistema y, en su caso, la retirada del **equipo** propiedad del <<ORGANISMO>> que tuviere asignado**,** y señalando la fecha de baja del externo. ○ El CAU ejecutará las acciones pertinentes para dar de baja al usuario externo de los sistemas, en la fecha señalada. ○ En caso de que tuviera asignado un equipo del <<ORGANISMO>>, el CAU, mediante su procedimiento interno, retirará tal equipo en el puesto de trabajo indicado en la solicitud. ○ En caso de que no tuviera asignado ningún equipo del <<ORGANISMO>> por haber estado utilizando el personal externo su propio equipamiento, es necesario que el Jefe de Proyecto del <<ORGANISMO>> realice las tareas definidas en el procedimiento de <<*Normativa de seguridad para ordenadores de usuarios externos*>>.	*Alta/Baja de Telefonía Fija,* informando de la baja del personal externo, y solicitando la retirada del equipo de **telefonía fija** que tuviere asignado, señalando la fecha de baja del personal externo. ○ En caso de que no tuviera ningún equipo de telefonía fija asignado, el Grupo de Telefonía Fija informará de ello al Responsable de Asignación de Recursos IT del <<ORGANISMO>> y se dará por cerrada la solicitud. ○ En caso de tener asignado un equipo de telefonía fija, el Grupo de Telefonía Fija del <<ORGANISMO>> retirará tal el equipo en el puesto de trabajo indicado en la solicitud. ○ Una vez realizadas las acciones pertinentes, el Grupo de Telefonía Fija del <<ORGANISMO>> informará mediante correo electrónico al Responsable de Asignación de Recursos IT del <<ORGANISMO>> la finalización del trabajo solicitado. Para ello	*Alta/Baja de Telefonía Móvil o Datos en Movilidad,* informando sobre la baja del personal externo y solicitando, en su caso, la retirada del equipo de **telefonía móvil o la tarjeta de conexión de datos de movilidad** que tuviere asignados, y la fecha de baja del personal externo. ○ En caso de que no tuviera ningún equipo de telefonía móvil o tarjeta de conexión de datos en movilidad asignados, el Grupo de Dispositivos Móviles informará de ello al Responsable de Asignación de Recursos IT del <<ORGANISMO>> y se dará por cerrada la solicitud. ○ En caso de tener asignado un equipo de telefonía móvil o una tarjeta de conexión de datos en movilidad, el Grupo de Dispositivos Móviles del <<ORGANISMO>>, mediante su procedimiento interno, retirará tales equipos. ○ Una vez realizadas las acciones pertinentes, el Grupo de

<table>
<tr>
<td>Adicionalmente, se informará al personal externo que debe de acudir al CAU para retirar su equipo del dominio.

o El CAU reclamará al personal externo la devolución del material informático facilitado por el<<ORGANISMO>>.

• Una vez realizadas las acciones pertinentes, el CAU remitirá un correo electrónico al Responsable de Asignación de Recursos IT del <<ORGANISMO>>, informándole sobre la finalización del trabajo solicitado.</td>
<td>cumplimentará los campos correspondientes en la Solicitud de Alta/Baja de Telefonía Fija.</td>
<td>Dispositivos Móviles informará mediante correo electrónico al Responsable de Asignación de Recursos IT del <<ORGANISMO>> la finalización del trabajo solicitado. Para ello cumplimentará los campos correspondientes en la Solicitud de Alta/Baja de Telefonía Móvil o Datos en Movilidad.</td>
</tr>
<tr>
<td colspan="3">• El Responsable de Asignación de Recursos IT del <<ORGANISMO>>, informará al Área de Seguridad del <<ORGANISMO>> <<señalar dirección de email>> la fecha de baja del personal externo, al objeto de, a partir de tal fecha, se le revoque el permiso de acceso físico a las instalaciones.

• En el día en el que el personal externo cause baja en el <<ORGANISMO>>, el Responsable de Asignación de Recursos IT del <<ORGANISMO>> se pondrá en contacto con el externo para retirarle la tarjeta de acceso.</td>
</tr>
<tr>
<td colspan="3">• El Responsable de Asignación de Recursos IT del <<ORGANISMO>> remitirá a la unidad competente[15], por valija interna, las tarjetas de acceso del personal externo dado de baja en el <<ORGANISMO>>.</td>
</tr>
</table>

[15] En ocasiones será la Oficialía Mayor.

• El Responsable de Asignación de Recursos IT del <<ORGANISMO>> dará de baja al externo en la <<*Aplicación de Gestión de Accesos del Organismo*>>.
• Una vez confirmada la baja del personal externo en los sistemas del <<ORGANISMO>>, y verificado que se le ha retirado el equipo, el teléfono y la tarjeta de acceso, el Responsable de Asignación de Recursos IT del <<ORGANISMO>> enviará la **confirmación de la baja** completa al jefe de Área del <<ORGANISMO>> a la que el externo pertenecía.

7.1.5 INCORPORACIÓN DE NUEVO EMPLEADO PÚBLICO

21. Seguidamente se describe un ejemplo del proceso de alta de un nuevo empleado público en el <<ORGANISMO>>[16].

[16] Este proceso suele ofrecer múltiples variantes, dependiendo de la tipología del Organismo de que se trate. El Organismo en cuestión deberá adaptarlo a sus especiales circunstancias administrativas.

Incorporación de NUEVO EMPLEADO PÚBLICO

- El nuevo empleado público solicitará acceso temporal al <<ORGANISMO>>, facilitando su DNI en el Control de Acceso.

- El nuevo empleado público accederá al <<ORGANISMO>> y se dirigirá a la Secretaría del <<ORGANISMO>> <<*señalar ubicación física, telefónica y electrónica*>>, donde comunicará su incorporación como empleado público del <<ORGANISMO>>.

- Desde la Secretaría del <<ORGANISMO>>, se informará de la incorporación de un nuevo empleado público al Responsable de Asignación de Recursos IT del <<ORGANISMO>>, quién deberá dirigirse a la Secretaría del <<ORGANISMO>> para acompañar físicamente al nuevo empleado público.

- El nuevo empleado público esperará al Responsable de Asignación de Recursos IT del <<ORGANISMO>> al que acompañará al Departamento de RRHH. Del <<ORGANISMO>> <<*señalar ubicación física, telefónica y electrónica*>>. Una vez en RRHH, se iniciarán los trámites de gestión del alta del nuevo empleado público.

- En RRHH el nuevo empleado público cumplimentará, en general, los siguientes documentos:

    - Toma de Posesión.
    - Cumplimiento de funciones.
    - Documento de incompatibilidades.
    - Justificante de la toma de posesión.

  Todos los documentos entregados serán cumplimentados por el nuevo empleado público, que los entregará a RRHH. Excepcionalmente, el empleado público guardará el justificante de la toma de posesión que posteriormente deberá ser firmado y sellado por el cargo personal competente del <<ORGANISMO>> en el momento de su presentación al área correspondiente y entregado a RRHH para que se realice una copia del mismo.

- Por lo general, a continuación el Responsable de Asignación de Recursos IT del <<ORGANISMO>> acompañará al nuevo empleado público al departamento de Habilitación General del <<ORGANISMO>> <<señalar ubicación física, telefónica y electrónica>>, donde

cumplimentará los formularios de gestión de las nóminas.

- En Habilitación General, por lo general, se le suministrarán varios formularios para cumplimentar, entre ellos:
  - El formulario de datos a cumplimentar en las altas en nómina.
  - El formulario de datos del pagador - Retenciones sobre rendimientos de trabajo. Modelo 145.

  El nuevo empleado público devolverá ambos formularios, una vez cumplimentados.

- El Responsable de Asignación de Recursos IT del <<ORGANISMO>> y el nuevo empleado público deberán dirigirse a la Secretaría del <<ORGANISMO>> <<*señalar ubicación física, telefónica y electrónica*>> y solicitar el formulario autenticado de solicitud de la credencial de acceso al <<ORGANISMO>> <<*Impreso Solicitud Acreditación Personal empleado público*>>.
- El Responsable de Asignación de Recursos IT del <<ORGANISMO>> acompañará al nuevo empleado público al Área de Seguridad del <<ORGANISMO>> <<*señalar ubicación física, telefónica y electrónica*>> donde solicitará al personal responsable la tarjeta de acceso.
- En el Área de Seguridad, el nuevo empleado público deberá de entregar el formulario <<*Impreso Solicitud Acreditación Personal empleado público*>> cumplimentado, firmado y autenticado. Se le realizará una fotografía para ser incluida en la tarjeta de acceso y se le entregarán dos impresos, uno con las <<*Normas de Uso de la Tarjeta*>> que deberá firmar y devolver, y una <<*Nota Informativa sobre las Capacidades de la Tarjeta*>>, para su conocimiento.
  - El Área de Seguridad proporcionará una tarjeta provisional, activada con una duración máxima de <<x>> meses.
  - Una vez que la tarjeta definitiva esté disponible, la unidad competente[17] comunicará al empleado público que pase a recoger su tarjeta definitiva.

- El Responsable de Asignación de Recursos IT del <<ORGANISMO>>, junto con el nuevo empleado público, se dirigirán al Área del <<ORGANISMO>> en la que el nuevo empleado público debe incorporarse y se le presentará al Jefe de Área o al Jefe de Servicio que corresponda.

[17] Puede tratarse de la Oficialía Mayor.

- El Responsable de Asignación de Recursos IT del <<ORGANISMO>> deberá obtener los datos del usuario así como el número de tarjeta del nuevo empleado público para ser dado de alta, en su caso, en la <<*Aplicación de Control Horario del Organismo*>>.

7.1.6 INCORPORACIÓN DE NUEVO PERSONAL EXTERNO COLABORADOR

22. Seguidamente se describe un ejemplo del proceso de alta de un nuevo personal externo colaborador del <<ORGANISMO>>[18].

[18] Este proceso suele ofrecer múltiples variantes, dependiendo de la tipología del Organismo de que se trate. El Organismo en cuestión deberá adaptarlo a sus especiales circunstancias administrativas.

Incorporación de NUEVO PERSONAL EXTERNO COLABORADOR

- En el momento en el que el Jefe de Área o Jefe de Servicio conoce la fecha y los datos del personal externo que se va a incorporar en el <<ORGANISMO>>, informará al Responsable de Asignación de Recursos IT del <<ORGANISMO>>.
- El nuevo personal externo solicitará acceso temporal al <<ORGANISMO>> facilitando el DNI en el Control de Acceso.
- El nuevo personal externo deberá dirigirse a la Secretaría del <<ORGANISMO>> <<señalar ubicación física, telefónica y electrónica>> y solicitar el formulario *Impreso Solicitud Acreditación Personal Colaborador*, para obtener la credencial de acceso al <<ORGANISMO>>. Dicho formulario estará debidamente autenticado.
- Desde la Secretaría del <<ORGANISMO>>, se informará al Responsable de Asignación de Recursos IT del <<ORGANISMO>> de la incorporación de nuevo personal externo.
- El Responsable de Asignación de Recursos IT del <<ORGANISMO>> deberá dirigirse a la Secretaría del <<ORGANISMO>> para acompañar al nuevo personal externo, para la tramitación de la credencial de acceso al <<ORGANISMO>>.
- El nuevo personal externo y el Responsable de Asignación de Recursos IT del <<ORGANISMO>> se dirigirán al Área de Seguridad del <<ORGANISMO>> <<señalar ubicación física, telefónica y electrónica>> donde deberá dirigirse al personal responsable junto con el Impreso *Solicitud Acreditación Personal Colaborador* cumplimentado.
- En el Área de Seguridad, el nuevo personal externo deberá de entregar el *<<Impreso Solicitud Acreditación Personal Colaborador>>*, completado, firmado y sellado. Se le realizará una fotografía para ser incluida en la tarjeta y se le entregará un impreso con las *<<Normas de Uso de la Tarjeta>>* que la tendrá que firmar y entregar y se le proporcionará otra copia del mismo para su conocimiento.
- El Área de Seguridad proporcionará al nuevo usuario una tarjeta activada con una duración máxima de seis meses.
- El Responsable de Asignación de Recursos IT del <<ORGANISMO>>, deberá registrar la fecha de caducidad de la tarjeta del nuevo colaborador externo para incluirlo dentro de la ficha del usuario en la *<<Aplicación de Gestión de Accesos del Organismo>>* para realizar un seguimiento de la caducidad de las tarjetas de acceso.

7.2. GESTIÓN DE PRIVILEGIOS

7.2.1 INTRODUCCIÓN

23. Los privilegios de acceso de los usuarios a los Sistemas de Información del <<ORGANISMO>> deben ser gestionados y controlados adecuadamente para evitar accesos o usos no autorizados de la información y de los sistemas que la soportan. Por ello, se realizarán revisiones periódicas de los privilegios asignados, que posibiliten la adopción de las medidas correctivas, en su caso.
24. A falta de realización de los procesos descritos en el epígrafe anterior, y con carácter general, el acceso a los Recursos y Sistemas de Información del <<ORGANISMO>> está totalmente prohibido.
25. Todos los accesos deben estar basados en la necesidad de saber. Sólo se permitirá el acceso a los recursos cuando exista una necesidad legítima para el desarrollo de las actividades profesionales del usuario. Por otro lado, los permisos otorgados a cada usuario deberán ser los mínimos para el desarrollo de sus funciones.

7.2.2 GESTIÓN DE PRIVILEGIOS

26. La asignación, modificación o revocación de privilegios en los Sistemas de Información del <<ORGANISMO>> será solicitada por los responsables del departamento o área a la que pertenezca el destinatario de dichos privilegios.
27. Se mantendrá una Inventario para Control de Accesos, en la que se identifiquen los usuarios y los privilegios autorizados y denegados.
28. Existirán privilegios asociados a:
    - Cada usuario.
    - Cada perfil, tales como:
        - Administrador
        - Operador
        - Usuario Externo
        - Usuario Interno
        - Usuario Temporal
        - Etc.
    - Cada recurso, tales como:
        - Bases de datos.
        - Aplicaciones.
        - Etc.
    - Cada permiso, tales como:
        - Lectura.
        - Escritura.
        - Control total.
        - Etc.

29. El Departamento de Sistemas del <<ORGANISMO>> será responsable de registrar, mantener y custodiar los permisos otorgados a los usuarios[19].
30. Los sistemas deben estar diseñados o configurados de tal forma que sólo se acceda a las funciones permitidas.
31. Los soportes y documentos que contengan datos de carácter personal serán accesibles únicamente por el personal autorizado en el correspondiente Documento de Seguridad, conforme a lo dispuesto en el Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de Desarrollo de la LOPD.
32. Por tanto, será necesario crear y mantener un Inventario de Privilegios de Acceso, que contendrá información relativa a cada usuario y sus privilegios de acceso concedidos, para cada uno de os Sistemas de Información en los que hubiere sido segregada la Seguridad IT.
33. La información se creará al dar de alta a un usuario por primera vez en alguno de los sistemas afectados, y deberá mantenerse actualizada, registrándose todas aquellas modificaciones que se produzcan en los privilegios de acceso hasta el momento en que el usuario haya causado baja en todos los sistemas incluidos en el alcance.
34. En el epígrafe 11 del presente Procedimiento se incluye un modelo para el inventariado de privilegios de acceso.

7.2.3 REVISIÓN DE PRIVILEGIOS

35. Al menos, cada <<señalar periodicidad>>, se realizará una revisión de los privilegios de acceso de todos los usuarios.
36. Cuando se trate de privilegios especiales (administrador, root, etc.), tal revisión de privilegios se deberá realizar, al menos, cada <<señalar periodicidad>>, y, en cualquier caso, siempre que existan:
    - Alta de nuevos usuarios
    - Baja de usuarios
37. Además, los privilegios de acceso de usuarios, tanto internos como externos, deben ser revisados siempre que existan cambios en las funciones o responsabilidades.
38. Para ambos tipos de usuarios se tendrán en cuenta, al menos, las siguientes cuestiones:
    - Necesidad de nuevos permisos.
    - Cancelación de antiguos permisos.
    - Segregación de funciones.
    - Devolución de activos y modificación o cancelación de permisos de accesos físicos.
    - Modificación de contraseñas de acceso.
    - Notificación al personal implicado de su baja o cambio.
    - Necesidad de retención de registros.

[19] Funciones encomendadas a las figuras del Responsable del Sistema / Administrador de Seguridad del Sistema, según los casos. Ver Guía CCN-STIC 801. Responsabilidades en el ENS.

7.2.4 CANCELACIÓN DE PRIVILEGIOS

39. Todos los privilegios de accesos de usuarios tanto internos como externos deben ser cancelados en el momento de la finalización de su contrato o prestación de sus servicios en el <<ORGANISMO>>.

40. Existirán flujos de comunicación que aseguren que este Procedimiento se realiza correctamente, tal y como hemos visto en el epígrafe anterior de este Procedimiento.

8. CONTROL DE ACCESO

8.1 IDENTIFICADORES

41. Reglas generales:

- Todos los identificadores personales del <<ORGANISMO>> deben estar normalizados, para posibilitar la identificación biunívoca y fiel de los usuarios.
- La creación de un identificador de usuario debe estar autorizada por su superior jerárquico, de acuerdo con las normas internas y procedimentales del <<ORGANISMO>>[20], tal y como hemos señalado en el epígrafe anterior de este documento.
- No se permitirá el uso de identificadores de grupo, salvo cuando sea estrictamente necesario y por razones operacionales. Esta circunstancia deberá estar debidamente justificada y aprobada formalmente, aplicando los controles de seguridad precisos.
- Los identificadores de usuarios anónimos y los identificadores por defecto estarán siempre deshabilitados.
- Los identificadores no deben dar indicios de nivel de privilegio asociado.
- Siempre que sea posible:

  - Se deben establecer listas de control de acceso a los recursos de información.
  - Los identificadores deben tener asignada una fecha de validez, tras la cual se deshabilitarán.

8.2 SERVICIO DE IDENTIDAD DIGITAL

42. Dentro de la <<U/OC>> del <<ORGANISMO>> se configurará un Servicio de Identidad Digital (SID), encargado de la gestión de las credenciales digitales de los usuarios de los Sistemas de Información del <<ORGANISMO>>[21.]

43. Reglas generales:

- Se deben aplicar controles de acceso en todos los niveles de la arquitectura y topología de los Sistemas de Información del <<ORGANISMO>>. Esto incluye: redes, plataformas o sistemas operativos, bases de datos y aplicaciones. Los atributos

[20] Véase Guía CCN-STIC 821. Normativa de Seguridad y Procedimiento PR10 Procedimiento de Gestión de Usuarios y Contraseñas, en esta misma Guía.
[21] Este Servicio de Identidad Digital puede encuadrase dentro de la estructura del Departamento de Sistemas, Responsable del Sistema o del CAU.

de cada uno de ellos deben reflejar alguna forma de identificación y autenticación, autorización de acceso, verificación de recursos de información y registro y monitorización de las actividades.

- Los usuarios son responsables de todas las actividades realizadas con sus identificadores, contraseñas y dispositivos de acceso. Por lo tanto, no deben permitir que otras personas los utilicen y conozcan.

8.3 PRINCIPIOS DE CONTROL DE ACCESO

44. Los principios que determinan el control de acceso a los Sistemas de Información del <<ORGANISMO>> son las siguientes:

    - El acceso a los Sistemas de Información del <<ORGANISMO>> requerirá siempre de autenticación.
    - El control de acceso a los Sistemas de Información del <<ORGANISMO>> se gestionará a través de los Servicios de Identidad Digital descritos en el apartado anterior.
    - Los usuarios deberán siempre autenticarse como usuarios no privilegiados del sistema, excepcionalmente y sólo con fines de administración podrán autenticarse como administradores del mismo.
    - Los usuarios deberán en todo momento hacer un uso responsable de la información y los sistemas de información accedidos, garantizando el nivel de seguridad adecuado de acuerdo a las directrices marcadas en la Normativa General de Utilización de los Recursos y Sistemas de Información del <<ORGANISMO>>[22], de aplicación a todos los usuarios.
    - Todas las contraseñas asignadas a las cuentas de usuario deberán respetar la política de contraseñas detallada en el apartado anterior[23].

8.4 REVISIÓN DEL CONTROL DE ACCESO

45. Reglas generales:

    - Cada <<señalar periodicidad>> se realizará una revisión periódica de los derechos de acceso asignados a los usuarios.
    - Los derechos de acceso privilegiados deberán revisarse con una periodicidad menor. Esta periodicidad será de <<señalar periodicidad>.
    - Además de lo anterior, deberá realizarse una revisión de los permisos de acceso correspondientes a un usuario siempre que hubiere sufrido modificación significativa de sus responsabilidades, posición o rol en el <<ORGANISMO>>.

[22] Véase Guía CCN-STIC 821. Normativa de Seguridad. En concreto, Norma NG00: Normativa General de Utilización de los Recursos y Sistemas de Información del <<ORGANISMO>>.
[23] Véase Guía CCN-STIC 821. Normativa de Seguridad. En concreto, Norma Particular NP40 – Creación y Uso de Contraseñas.

9. AUTENTICACIÓN DE USUARIOS

9.1 AUTENTICACIÓN MEDIANTE CONTRASEÑAS

Alta y baja de contraseñas

46. Las gestiones asociadas a la creación o eliminación de contraseñas son responsabilidad de los administradores de los Servicios de Identidad Digital del <<ORGANISMO>> y deberá aplicarse lo contemplado en el epígrafe anterior de este Procedimiento.

Sustitución de contraseñas

47. El cambio de contraseñas podrá obedecer a:

    - Cumplimiento del periodo de rotación establecido para la contraseña.
    - Cambio de contraseña decidido por el usuario o el Departamento de Sistemas del <<ORGANISMO>>.
    - Cambio de contraseña por olvido, pérdida o sospecha de haber sido comprometida la seguridad de la anterior.
    - Cambio de una contraseña por defecto.

48. El responsable de iniciar un procedimiento de cambio de contraseña podrá ser el dueño de la cuenta cuya contraseña ha de cambiarse, o el Departamento de Sistemas (Responsable del Sistema) del <<ORGANISMO>>, y constará de los siguientes pasos:

<table>
<tr><td rowspan="2">Por decisión del usuario:</td><td rowspan="2">El usuario dispone de contraseña válida para acceder al servicio:</td><td>Si el Servicio de Identidad Digital (SID) dispone de autoservicio de credenciales de autenticación, se seguirá el procedimiento específico del SID para gestionar el cambio de contraseña.</td></tr>
<tr><td>Si el Servicio de Identidad Digital (SID) no dispone de autoservicio de credenciales de autenticación, contactará con el administrador del sistema de información para que haga uso de sus privilegios de administración y realice el cambio de contraseña por una contraseña provisional, de un solo uso, que el usuario deberá sustituir en el inicio de la siguiente sesión.</td></tr>
</table>

	Si el usuario no dispone de contraseña válida para acceder al servicio:	Contactará con el administrador del sistema de información para que haga uso de sus privilegios de administración y realice el cambio de contraseña por una contraseña provisional, de un solo uso, que el usuario deberá sustituir en el inicio de la siguiente sesión.
Por decisión del Departamento de Sistemas (Responsable del Sistema).	El administrador del sistema de información, haciendo uso de sus privilegios de administración, realizará el cambio de contraseña por una contraseña por una contraseña provisional, de un solo uso, que el usuario deberá sustituir en el inicio de la siguiente sesión.	

Directiva de contraseñas

49. Todos los usuarios, independientemente del sistema de información para el que se definan o sean válidas, son responsables de sus contraseñas de acceso a servicios y de los accesos que se produzcan haciendo uso de dichas contraseñas.

50. En este sentido, se recomienda a los usuarios observar las siguientes indicaciones en cuanto a la custodia de sus contraseñas[24:]

    - No compartir sus contraseñas con otros usuarios.
    - No anotar sus contraseñas ni introducirlas si alguien está observando.
    - No enviar contraseñas por medios electrónicos o almacenarlas en ficheros de ordenador sin cifrar.

51. El usuario deberá custodiar sus contraseñas de forma efectiva siguiendo las directrices indicadas en la Normativa General de Utilización de los Recursos y Sistemas de Información del <<ORGANISMO>>[25,] de aplicación a todos los usuarios.

[24] Véase Guía CCN-STIC 821. En concreto, Norma Particular NP40 – Creación y Uso de Contraseñas.
[25] Puede encontrarse un modelo en la Guía CCN-STIC 821. En concreto, Norma General NG00 Normativa General de Utilización de los Recursos y Sistemas de Información del <<ORGANISMO>>.

52. Los servicios de Identidad Digital del <<ORGANISMO>>, siempre que sea posible, deberán emplear herramientas de control que garanticen el cumplimiento de la Directiva de Contraseñas.

53. Todas las contraseñas asignadas a las cuentas activas en los sistemas de información del <<ORGANISMO>> deberán observar las restricciones que se detallan en la siguiente tabla.

Parámetro	Valor[26]
Periodo máximo de rotación	• <<x>> días para cuentas de usuario. • <<y>> días para cuentas de administración de sistemas.
Caducidad de contraseñas	Automática, al finalizar el periodo máximo de rotación, excepto para contraseñas de administración de sistemas.
Reutilización de contraseñas	Ninguna de las <<z>> últimas
Intervalo mínimo entre cambios	<<d>> días
Longitud mínima	8 caracteres.

Requisitos de complejidad	• No contener en parte o en su totalidad el nombre de usuario.
	• Estar compuesta por al menos 3 de entre los siguientes 4 conjuntos de caracteres:
	  ○ Caracteres alfanuméricos en mayúsculas.
	  ○ Caracteres alfanuméricos en minúsculas.
	  ○ Caracteres numéricos.
	  ○ Símbolos/caracteres especiales.

Semántica de contraseñas	Se deberán evitar las contraseñas basadas en: • Repetición de caracteres. • Palabras del diccionario. • Secuencias simples de letras, números o secuencias de teclado. • Información fácilmente asociable al usuario como nombres de familiares o mascotas, números de teléfono, matrículas, fechas o en general información biográfica del usuario.
Cautelas generales	• Mantenerlas en secreto. Las contraseñas no deben compartirse con nadie. • Preferiblemente, las contraseñas iniciales deben

[26] Véase Guía CCN-STIC 821. Normativa de Seguridad. En concreto, Norma Particular NP40 – Creación y Uso de Contraseñas.

	ser entregadas en mano o a través de algún medio que no permita su acceso por personas no autorizadas. En el caso de enviarlas por medios telemáticos (correo electrónico, SMS, etc.) o en un soporte, se enviarán separadas del identificador. • Las contraseñas iniciales deben ser generadas automáticamente y se cambiarán en el primer acceso a los sistemas. • Los ficheros de contraseñas se deben almacenar con algún método de protección que garantice su confidencialidad e integridad (p. e. cifrado). • Los sistemas, no deben mostrar las contraseñas en claro por pantalla. • Todas las contraseñas por defecto de los sistemas o aplicaciones deben ser cambiadas o desactivadas cuando no sean necesarias. • La autenticación en los sistemas debe ser individual, no estando permitida la autenticación por grupo. Cuando sea necesario por razones operacionales, deberá estar justificado y aprobado formalmente, aplicando los controles de seguridad compensatorios necesarios. • El número de intentos de accesos sin éxito consecutivos debe estar limitado, tras el cual, se bloquearán los sistemas. • Los salvapantallas deben tener activada la protección por contraseña, bloqueándose tras un periodo de inactividad. • Cuando se considere necesario en servicios críticos, se contará con medidas adicionales a las establecidas en este Procedimiento. • No deben ser incluidas en correos electrónicos o en otros medios de comunicación electrónica ni comunicadas por teléfono. • No se deben escribir o almacenar contraseñas en texto claro o en formas fácilmente reversibles. • Se debe evitar la característica “Recordar Contraseña” existente en algunas aplicaciones y formularios. • Deben existir mecanismos de expiración y caducidad de contraseñas para obligar a los usuarios al cambio de la misma. • Todas las contraseñas con privilegios especiales (administrador, root, etc.) deben cambiarse, al menos, <<*señalar*

	periodicidad>>. • Todas las cuentas de usuario (acceso a sistema operativo, correo, servicios web, etc.) deben cambiarse, al menos, <<*señalar periodicidad*>>. • Adicionalmente, deberán modificarse siempre que se sospeche que está comprometida a través de los procedimientos establecidos.

9.2 AUTENTICACIÓN PERSONAL MEDIANTE CERTIFICADO DIGITAL

54. Normas generales27:

- Cada certificado digital debe identificar inequívocamente a un solo usuario, y sólo deberá ser utilizado por él.
- El certificado digital debe haber sido emitido por un Prestador de Servicios de Certificación válido y de confianza.
- Cada certificado debe tener asignado un periodo de de vida, tras el cual su uso se considerará ineficaz a todos los efectos, y deberá procederse a su renovación.
- En el supuesto de pérdida, robo o indicios de uso indebido por terceros, el certificado deberá ser revocado a la mayor brevedad posible.
- En autenticaciones basadas en certificado digital, su validez e identidad del usuario deberá ser verificada contra una infraestructura de PKI.

9.3 GESTIÓN DE INICIOS DE SESIÓN

55. Se describen seguidamente los aspectos que deben tenerse en cuenta de cara a minimizar el número de accesos no autorizados a los sistemas.

- Hasta que no se haya completado con éxito el proceso de autenticación, no se deberá mostrar ningún tipo de información relativa al sistema (tal como identificadores del sistema o versiones de software instalado), que puedan ayudar a identificarlo, así como cualquier otro tipo de información que pueda facilitar su acceso no autorizado.
- Una vez se haya accedido correctamente al sistema, se deberá mostrar un mensaje que advierta que el uso del sistema sólo está permitido a usuarios autorizados. Un ejemplo de tal mensaje podría ser el siguiente:

> ***AVISO A LOS USUARIOS DEL SISTEMA:***
>
> *El uso de este sistema sólo está permitido a los usuarios autorizados.*
> *El acceso no autorizado está terminantemente prohibido y podrá ser objeto de acciones disciplinarias, sin perjuicio de las restantes acciones de naturaleza*

[27] Sin perjuicio de contemplar lo regulado en la Resolución de 19 de julio de 2011, de la Secretaría de Estado para la Función Pública, por la que se aprueba la Norma Técnica de Interoperabilidad de Política de Firma Electrónica y de certificados de la Administración.

legal a las que hubiere lugar.
Toda la actividad de este sistema se registra y es revisada periódicamente por el personal designado por la dirección del <<ORGANISMO>>.
Cualquier usuario que acceda al sistema lo hace declarando conocer y aceptar íntegramente estas reglas y la Normativa General de Utilización de los Recursos y Sistemas de Información del <<ORGANISMO>>, accesibles en <<URL>> y <<localización física>>.

- Respecto del proceso de validación de entrada, los sistemas deberán tener en cuenta los siguientes extremos:
  - La validación de la información de entrada se realizará únicamente cuando se hayan completado todos los datos de entrada. Si ocurre alguna condición de error, el sistema no deberá indicar en ningún caso la parte del dato que es incorrecta. (Por ejemplo, nunca deberá indicar si lo que se ha introducido de forma incorrecta es el nombre de usuario, o la contraseña, etc.).
  - Se limitará a <<número de intentos>> el número de intentos de acceso.
  - Si se alcanza el número máximo de intentos de acceso fallidos, se deberá bloquear la cuenta de usuario, al menos durante <<tiempo de bloqueo>>[28]
  - Una vez completado con éxito el proceso de autenticación en el sistema, deberá mostrarse la información de la última entrada satisfactoria.
  - Siempre que sea posible, deberán utilizarse protocolos de comunicación que permitan el envío de las credenciales de usuario de forma cifrada para evitar que sean capturadas en algún punto intermedio de la comunicación.

9.4 CONTROL DE ACCESO A BASES DE DATOS Y APLICACIONES

- El acceso a las aplicaciones y bases de datos debe ser independiente del acceso al sistema operativo.
- Se debe tener en cuenta el aislamiento de sistemas sensibles.

9.5 CONTROL DE ACCESO A LA RED

- Se debe establecer un control de acceso a la red, tanto interna como externamente, implantando medidas de seguridad y procedimientos de autorización de acceso.
- Se debe establecer autenticación de usuarios en los accesos remotos a través de técnicas criptográficas, "tokens", protocolos de pregunta/respuesta, líneas dedicadas privadas, verificación de origen de conexión, etc.
- Se protegerán los servicios de red, puertos de configuración y diagnóstico remoto. Cuando no sean necesarios estarán deshabilitados.
- La red debe estar segmentada según su criticidad.

[28] Puede expresarse en minutos, horas, días o de forma permanente.

- Se debe contar con controles de conexión a la red (filtros, reglas, etc.), de enrutamiento y de identificación del equipamiento en la red.

9.6 MONITORIZACIÓN DE LOS ACCESOS

56. Se deben realizar labores periódicas de monitorización de los sistemas con el fin de detectar accesos no autorizados y desviaciones, registrando eventos que suministren evidencias en caso de producirse incidentes relativos a la seguridad.

57. A tal efecto, se tendrán en cuenta:

- Registro de eventos:
  - Intentos de acceso fallidos.
  - Bloqueos de cuenta.
  - Debilidad de contraseñas.
  - Normalización de identificadores.
  - Cuentas inactivas y deshabilitadas.
  - Últimos accesos a cuentas.
  - Etc.
- Registro de uso de los sistemas:
  - Accesos no autorizados.
  - Uso de Privilegios.
  - Alertas de sistema.
  - Etc.

58. Debe existir sincronización de relojes para exactitud de los registros de tiempo.

10. REGISTROS E INDICADORES

10.1. TABLA DE REGISTROS

(Ejemplos de uso)

Identificador	Nombre	Frecuencia	Archivo	Genera	Custodia
Procedimiento de que se trate	Altas personal interno	N/A	Gestor de incidencias	Dirección Departamento Sistemas	Departamento Sistemas
Procedimiento de que se trate	Bajas personal interno	N/A	Gestor de incidencias	Dirección Departamento Sistemas	Departamento Sistemas
Procedimiento de que se trate	Altas personal	N/A	Gestor de incidencias	Responsable de proyecto	Departamento Sistemas

	externo				
Procedimiento de que se trate	Bajas personal externo	N/A	Gestor de incidencias	Responsable de proyecto	Departamento Sistemas
Procedimiento de que se trate	Revisión Permisos de acceso usuarios	6 meses	Gestor documental	Departamento Sistemas	Departamento Sistemas
Procedimiento de que se trate	Revisión permisos de acceso usuarios admin	3 meses	Gestor documental	Departamento Sistemas	Departamento Sistemas

10.2. TABLA DE INDICADORES

Identificador	Rango	Freq	Métrica	Objetivo	Descripción
XXXX	%	1 / A	Porcentaje de operaciones sobre bajas de usuarios con una variación del tiempo superior a un día	0%	Se comprobará que una vez abierta la petición, se dio de baja al usuario en todos los servicios corporativos en menos de 24 horas

10.3 REGISTRO DE SUCESOS

59. Los sistemas de información qué procesen, transmitan o almacenen información deben generar un registro de los accesos lógicos producidos, siempre que técnicamente sea posible, y bajo las siguientes características:

    - Este registro recogerá los sucesos en orden cronológico, posibilitando la reconstrucción, revisión y examen de la secuencia de actividades relacionadas con un determinado evento.
    - El registro de sucesos será siempre obligatorio en todos los sistemas que contengan información confidencial, así como en aquellos que conforman el perímetro de

seguridad como los cortafuegos, con el objeto de aportar las pruebas necesarias para el seguimiento de los mismos, en el caso de accesos no autorizados.

- El registro de accesos lógicos y su auditoria deben proporcionar trazabilidad sobre los accesos al sistema, actividades de administración y otros eventos críticos.
- Tipo de actividades a registrar:
  - I. Actividad sospechosa.
  - II. Intentos de acceso no autorizado.
  - III. Excepciones y otro tipo de actividad inusual.
  - IV. Conexiones establecidas con éxito.
  - V. Intentos de conexión denegados y rechazados.
  - VI. Inicios de sesión válidos y erróneos.
  - VII. Mensajes de error y alertas
  - VIII. Tiempos de conexión elevados.
  - IX. Uso concurrente de identificadores de usuario duplicados.
  - X. Acceso remoto de proveedores para tareas de mantenimiento y diagnostico.
  - XI. Actividad del cortafuegos.
  - XII. Actividad del administrador.
  - XIII. Inicio y apagado del sistema. Válido o fallido.
  - XIV. Acceso fallido a ficheros u objetos.
  - XV. Cambios en la política de seguridad. Logrados y fallidos.
  - XVI. Cambios en los ficheros del sistema o en el registro.
  - XVII. Copias de seguridad y restauración de las mismas.
  - XVIII. Actividad del antivirus.
  - XIX. En general, todas las actividades de administración de seguridad.
- Para facilitar la monitorización y la investigación de sucesos, los registros de conexiones y otros eventos relativos a la seguridad serán almacenados durante, al menos, <<señalar periodicidad>> (excepto los sujetos a la LOPD, que se custodiarán por el periodo señalado en dicha ley).
- Dichos registros contendrán, como mínimo, la siguiente información:
  - I. Identificador del Usuario.
  - II. Actividad del usuario.
  - III. Fecha / hora del inicio y fin de sesión.
  - IV. Identificación del inicio y fin de sesión remota.
  - V. Identificación de la identidad del terminal y/o su localización (si es posible).
  - VI. Causa del evento de conexión (ej. acceso prohibido)

- El responsable del área o departamento correspondiente, o la persona que designe a tal fin, revisaran el contenido de los registros de sucesos con una periodicidad mínima de <<señalar periodicidad>>.
- El acceso a los registros estará restringido al responsable del área o departamento correspondiente y a las personas designadas por este. Se evitara el acceso de personas no autorizadas que puedan ver, alterar o eliminar registros.
- Los registros deberán ser protegidos y custodiados adecuadamente puesto que podrán usarse en el seguimiento y obtención de pruebas de eventos o incidentes.
- Se usarán herramientas o utilidades que faciliten la revisión de los registros de sucesos. Todas las redes y sistemas operativos dependientes de cada área o departamento, deberán contar con medios para monitorizarlos y generar alarmas o alertas.
- Los responsables de cada área o departamento deberán ser informados cuando los registros de sucesos muestren evidencias de problemas en la seguridad de los sistemas monitorizados.
- Todos los equipos que cuenten con un reloj interno estarán sincronizados entre sí para garantizar la precisión de los sucesos registrados y permitir la correlación de los diferentes eventos.
- Los registros de sucesos serán almacenados siguiendo lo establecido en la planificación que establezca cada área o departamento sobre los sistemas monitorizados de su responsabilidad, y protegidos según el nivel de clasificación de la información tratada.
- En el caso de los servidores de ficheros los registros de sucesos serán almacenados durante, al menos, <<señalar periodicidad, por ejemplo: 1 mes>>. En aquellos equipos que contengan información sensible los registros de sucesos serán almacenados durante un periodo no inferior a <<señalar periodicidad, por ejemplo: 1 año>>. No obstante, el periodo mínimo de almacenamiento podrá aumentar cuando así lo exija la legislación vigente.
- La rotación de los registros de sucesos se realizará en base a los criterios propuestos por la propia aplicación/producto/herramienta y en el tamaño de los ficheros de registro de sucesos. Como norma, los registros de sucesos serán rotados con una periodicidad <<señalar periodicidad, por ejemplo: mensual>> siempre que los anteriores condicionantes lo permitan.
- Los ficheros de registro de sucesos estarán protegidos física y lógicamente para prevenir su acceso no autorizado.
- Los sistemas de registro de sucesos no deben ser configurados para sobrescribir registros antes de su rotación y archivado.
- Si la rotación automática de los ficheros de registro de sucesos no es posible, el sistema deberá avisar cuando los ficheros de registro de sucesos se encuentren en el límite de su almacenamiento y no sea posible registrar sucesos adicionales. Los ficheros de registro de sucesos deberán ser archivados antes del restablecimiento o borrado derivado de su rotación.

11. SOPORTE Y MODELOS

11.1. SOPORTE

60. El soporte necesario para la implantación de este procedimiento se realiza en base a los siguientes elementos:

- Gestor de incidencias.
- Servicio de directorio del dominio del <<ORGANISMO>>.
- Dispositivo de generación de túneles VPN-SSL.
- Inventario de privilegios de acceso.

11.2. MODELOS

61. A continuación se detalla el modelo para el inventariado de privilegios de acceso de los usuarios del <<ORGANISMO>>.

Nombre Usuario	Cód. Usuario	Sistema o Servidor	Fecha de Alta	Permisos de Acceso	Vigente	Fecha de Caducidad	Fecha de Baja

ANEXO I:

MODELO DE SOLICITUD DE ALTA/BAJA DE RECURSOS IT

<<ORGANISMO>>
Solicitud de Alta/Baja de Recursos IT

[Información que deberá cumplimentar el Responsable de Asignación de Recursos IT del <<ORGANISMO>>] para remitir al CAU <<señalar dirección de email>>

1. Datos del usuario	
Apellidos y Nombre (*)	DNI, NIE o Pasaporte (*)
Teléfono de contacto	Empresa (*) (Sólo personal externo)
Proyecto	Perfil (*)
Ubicación física	
Fecha de incorporación	¿Necesita correo electrónico? (*)

2. Tipo de usuario (*)
- ◯ Empleado público del <<ORGANISMO>>
- ◯ Personal externo

3. Solicitante (*)	
Apellidos y Nombre	Cargo
Fecha de solicitud	Teléfono + email

4. Motivo de la solicitud (*)	
◯ Alta en los Sistemas	◯ Asignar equipo
◯ Baja en los Sistemas	◯ Retirar equipo

5. Equipo procedente de	
◯ <<U/OC>> del <<ORGANISMO>>	◯ Equipo propio

6. Software que se solicita instalar en el equipo
- ◯ Software de Base
- ◯ Otros (especificar)

7. Permisos adicionales requeridos (especificar)

Datos procedentes del CAU del <<ORGANISMO>>

8. Información del usuario	
Usuario de dominio	Dirección de correo electrónico
Contraseña (de un solo uso, en su caso)	

9. Fecha de alta o baja en los sistemas	
Para equipos del <<ORGANISMO>>	Para equipos ajenos
10. Fecha en la que se ha proporcionado/retirado el equipo	11. Fecha en la que se ha incluido/excluido del dominio
12. Comentarios	

(*) Estos campo son obligatorios

ANEXO II:

MODELO DE SOLICITUD ALTA/BAJA DE TELEFONÍA FIJA

<<ORGANISMO>>
Solicitud de Alta/Baja de Telefonía Fija

[Información que deberá cumplimentar el Responsable de Asignación de Recursos IT del <<ORGANISMO>>] para remitir al Grupo de Telefonía Fija del <<ORGANISMO>> <<señalar dirección de email>>

1. Datos del usuario para el que se solicita teléfono fijo (*)	
Apellidos y Nombre	Ubicación física

2. Tipo de solicitud (*)
- ◯ Alta
- ◯ Baja

3. Solicitante (*)	
Apellidos y Nombre	Cargo
Fecha de solicitud	Teléfono + email

4. Comentarios

Datos procedentes del Grupo de Telefonía Fija del <<ORGANISMO>>

5. Teléfono Fijo (*)	
Número externo	Extensión

6. Comentarios

(*) Estos campo son obligatorios

ANEXO III:

MODELO DE SOLICITUD ALTA/BAJA DE TELEFONÍA MÓVIL Y/O DATOS EN MOVILIDAD

<<ORGANISMO>>
Solicitud de Alta/Baja de Telefonía Móvil o Datos en Movilidad

[Información que deberá cumplimentar el Responsable de Asignación de Recursos IT del <<ORGANISMO>>] para remitir al Grupo de Dispositivos Móviles del <<ORGANISMO>> <<señalar dirección de email>>

1. Datos del usuario para el que se solicita teléfono móvil y/o datos en movilidad (*)	
Apellidos y Nombre	Ubicación física

2. Tipo de solicitud (*)
- ◯ Teléfono móvil.
- ◯ Tarjeta de Datos en Movilidad.

3. Solicitante (*)	
Apellidos y Nombre	Cargo
Fecha de solicitud	Teléfono + email

4. Motivo de la solicitud (*)
- ◯ Alta
- ◯ Baja

5. Comentarios

Datos procedentes del Grupo de Dispositivos Móviles del <<ORGANISMO>>

6. Teléfono Móvil (*)	
Número externo	Extensión
Tarjeta de Datos en Movilidad	
Número externo	Extensión

7. Comentarios

(*) Estos campo son obligatorios