NORMATIVA

GESTIÓN DE ACCESO DE USUARIO

Excmo. Ayuntamiento de Baeza

Octubre 2019

CONTROL DE DOCUMENTACIÓN:

CÓDIGO:	NR.28	DOCUMENTO:	NORMATIVA DE GESTIÓN DE ACCESO DE USUARIO

REVISIÓN NÚMERO:	1.0	FECHA DE ENTRADA EN VIGOR:	31 – Octubre - 2019

ES ORIGINAL:	☒	ES COPIA CONTROLADA:	☐	ES COPIA NO CONTROLADA:	☐

ELABORADOR POR:	REVISADO POR:	APROBADO POR:
[ÁREA]	[ÁREA]	Comité de Seguridad de la Información
[NOMBRE – INICIALES]	[NOMBRE – INICIALES]	[NOMBRE – INICIALES]
FECHA:	FECHA:	FECHA:
FIRMA:	FIRMA:	FIRMA:

CONTROL DE CAMBIOS:

REVISIÓN Nº:	FECHA:	APARTADO MODIFICADO:	CAUSA DEL CAMBIO:	ENTRADA EN VIGOR:

DOCUMENTACIÓN OBSOLETA:	☐	FECHA:	

CLASIFICACIÓN DE LA INFORMACIÓN:

SEGURIDAD

PÚBLICA:	☐	PUBLICABLE	☐	USO INTERNO	☒	CONFIDENCIAL:	☐	SECRETA:	☐

PRIVACIDAD

NO IP	☐	IP A	☒	IP B	☐	IP C	☐

Confidencialidad Acerca de este documento

Excmo. Ayuntamiento de Baeza

Pje. Cardenal Benavides, 10
23440 Baeza, Jaén
ESPAÑA
http://www.baeza.es/baeza/extranet/

1) OBJETO

El presente documento tiene la finalidad de definir el acceso de los usuarios autorizados y evitar el acceso no autorizado a los sistemas de información del Excmo. Ayuntamiento de Baeza (en adelante Ayuntamiento).

2) ALCANCE

La presente normativa se dicta en cumplimiento de las disposiciones legales vigentes con el objetivo de gestionar adecuadamente la seguridad de la información, los sistemas informáticos y el ambiente tecnológico de la organización.

Debe ser conocida y cumplida por todos los empleados de la organización que dan soporte a los servicios de la entidad, ya sea personal técnicos como no técnicos y sea cual fuere su nivel jerárquico.

Esta normativa ha sido aprobada por el Comité de Seguridad, atendiendo a las recomendaciones del Responsable de la Información, Responsable de la Entidad, Responsable de Seguridad, Responsable del Sistema y de todos los actores intervinientes en la misma.

Cualquier modificación posterior entrará en vigor al día siguiente de su aprobación y publicación por parte del Comité de Seguridad. En este caso, la versión anterior quedará anulada por la última versión de esta normativa.

3) RESPONSABILIDADES

Cada usuario de información, equipos o servicios ofrecidos por el Ayuntamiento deberá velar por el cumplimiento de las normas descritas en el presente documento.

El control y seguimiento de las medidas aquí descritas corresponden al Responsable del Sistema, a través del departamento de sistemas, o podrá ser delegado en la persona que este designe.

El Responsable del Sistema, actuará de manera coordinada con el departamento de Recursos Humanos.

4) REGISTRO Y BAJA DE USUARIO Y PROVISIÓN DE ACCESO DE USUARIOS

En el contexto de se pueden dar tres tipos de cuentas:

- De Administrador o Desarrolladores: aquellos que tienen la facultad de modificar programas, accesos, claves y privilegios de acceso de los usuarios.
- De Usuario de Directorio Activo (LDAP): todas las personas, empleados, usuarios autorizados o colaboradores que tengan acceso a la información contenida en las aplicaciones y sistemas de información para el desarrollo de sus funciones, sin capacidad de modificar sus privilegios de acceso. Cada persona tiene un perfil de usuario, estando el acceso regulado por medio del usuario y la contraseña que lo hacen unívoco y personal. Se incluye aquí el acceso de terceros, ajenos al Ayuntamiento, pero autorizados por ésta.
- De Sistemas o aplicaciones corporativas: cuentas específicas para el manejo de aplicaciones que no están integradas en el directorio activo del Ayuntamiento.

El procedimiento de alta de usuario es el siguiente:

- Recursos Humanos comunica mediante correo electrónico al Responsable del Sistema la incorporación de un nuevo empleado.
- El Responsable del área/departamento donde realizará su actividad el nuevo empleado, notificará al Responsable del Sistema la necesidad de acceso a la red enviándole cumplimentado los datos del formulario de Alta en el Sistema de Información (consultar *Anexo A - Datos para la Solicitud de Alta de Trabajador*).
- En caso de externalización de servicios o de usuarios ajenos a los servicios objeto de alcance del SGSI, será el Responsable del área/departamento que afecta el acceso por parte de personal externo quien comunique al Responsable del Sistema la necesidad de habilitar acceso a la red a dicho tercero, enviándole cumplimentado los datos del formulario de Alta en el Sistema de Información (consultar *Anexo A - Datos para la Solicitud de Alta de Cuenta*).

- El Responsable del área/departamento en el que entre a trabajar el nuevo empleado comunicará al Responsable del Sistema los permisos de acceso que requiera, enviándole por correo electrónico los datos del *Anexo B - Datos para la Solicitud de Alta o Modificación en los Sistemas de Información.*
- El usuario o tercero solicitante de la cuenta firma por duplicado las Cláusulas del *Anexo D – Cláusulas de Confidencialidad* entregándose una copia al Responsable de Seguridad.
- El Responsable del Sistema procederá a dar de alta al usuario.
- El usuario y contraseña se comunica al usuario o tercero, que debe cambiar su contraseña en el primer acceso. Esta contraseña determina los privilegios de acceso tanto a la red como a las aplicaciones.

Se puede solicitar el alta en grupos de usuario con un mismo responsable a través de una sola petición para varios usuarios.

En la medida de lo posible se añadirá una fecha de Baja de cuenta a cumplimentar por el Responsable del área/departamento en caso de que se trate de un servicio que requiera de acceso externalizado.

4.1) ADMINISTRADORES Y DESARROLLADORES

Para los usuarios con perfil de administrador y/o desarrollador, cada usuario tendrá una cuenta diferenciada, a fin de que se puedan identificar los accesos al realizar auditorías de los sistemas.

Las cuentas correspondientes a los desarrolladores sólo existirán o tendrán privilegios de acceso en los sistemas de desarrollo y/o pruebas, nunca a producción.

4.2) PROCEDIMIENTO DE MODIFICACIÓN DE CUENTAS DE USUARIO

El Responsable del área/departamento que afecta el acceso por parte de personal externo, cumplimentará la solicitud de Alta o Modificación en los Sistemas de Información (Anexo B), y la enviará al Responsable del Sistema para que proceda a modificar la cuenta.

4.3) PROCEDIMIENTO DE BAJA O BLOQUEO DE CUENTA DE USUARIO

4.3.1) SOLICITUD DE LA BAJA O BLOQUEO DE CUENTA

El Responsable del área/departamento que afecta al acceso del personal externo, debe solicitar la baja de una cuenta siempre que el uso de la misma no sea necesario por más tiempo, ocurra un uso fraudulento de ella o haya sospecha de que ha sido comprometida.

- El Responsable del área/departamento externalizado solicita la baja o bloqueo de la cuenta de usuario por correo al Responsable del Sistema y con copia al departamento de RRHH si se trata de un empleado del Ayuntamiento, cumplimentando los datos del Anexo C.
- El Responsable del Sistema, procederá a la baja o bloqueo de la cuenta. En caso de bloqueo, se realizará por el tiempo indicado por el Responsable del área/departamento externalizado.

4.3.2) BAJA AUTOMÁTICA

Todos los usuarios se dan de alta con una fecha prevista de baja (que puede ser un valor que indique fecha indefinida). Al cumplir con esta fecha de baja, la cuenta se bloqueará automáticamente y posteriormente se borrará, según el siguiente procedimiento:

- Si el Responsable del área/departamento donde opera el empleado quiere ampliar la fecha de baja, enviará un correo electrónico interno de Modificación de datos de cuenta, ampliando la fecha de baja. En caso contrario no realizará ninguna acción.
- Al cumplir la fecha de baja, la cuenta se bloqueará automáticamente.
- A los 6 meses de estar bloqueada una cuenta, ésta se borrará definitivamente.

4.4) PROCEDIMIENTO DE AUTORIZACIÓN DE ACCESO A LOS SISTEMAS DE INFORMACIÓN

Siempre que se necesite acceder a los recursos o información de los sistemas, aplicaciones o servicios, se deberá obtener autorización previa del Responsable del Sistema (ver Anexo E – Relación de Administradores de Sistemas).

Cuando se solicita el alta de un usuario se puede indicar en el mismo formulario los accesos iniciales para dicho usuario.

Cualquier usuario podrá solicitar alta, modificación o baja de acceso, ya sea trabajador interno o externo del Ayuntamiento.

La baja de permisos de accesos debe solicitarse siempre que no sean necesarios por más tiempo. Es el Responsable del área/departamento el que tiene la obligación de solicitar esta baja. No será necesaria la autorización del responsable para bajas.

- El Responsable del área/departamento solicita, mediante correo electrónico interno al Responsable del Sistema el alta, modificación o baja de permisos de acceso a la cuenta del usuario, incluyendo los datos del Anexo B.
- Si la operación es de baja, ir al paso EJECUCIÓN.
- Si la operación es de alta o modificación, llegará una petición de autorización al Responsable del Sistema, o persona en quien delegue. El Responsable o persona en quien delegue, aceptará o denegará la solicitud.
    - En caso de aceptación, ir al paso EJECUCIÓN
    - En caso de denegación o error, al Responsable del Sistema lo comunicará, junto con el motivo, al Responsable del área/departamento.
- EJECUCIÓN: El Responsable del Sistema procederá a realizar la operación solicitada:
    - asignará o modificará los derechos de acceso; o bien,
    - eliminará los derechos de acceso solicitados y lo comunica por correo electrónico interno al Responsable del área/departamento.

Se puede solicitar accesos en grupos de usuario con un mismo Responsable (una sola petición para varios usuarios).

Para la solicitud de acceso remoto se usará el mismo procedimiento y formulario.

4.5) REGISTRO Y REVISIONES

El Responsable del Sistema deberá guardar registro de todas las solicitudes cursadas.

El Responsable del Sistema, o aquella persona en quien delegue esta tarea, revisará semestralmente el listado de cuentas de usuario y privilegios en los sistemas, aplicaciones o servicios de su responsabilidad, con objeto de identificar posibles usuarios cuyos privilegios no estuvieran actualizados.

5) GESTIÓN DE PRIVILEGIOS DE ACCESO

La asignación de privilegios se basará en el principio de que todo acceso estará prohibido a menos que haya sido expresamente autorizado. El acceso a los sistemas, documentos, redes, aplicaciones y servicios se realizará siempre que sea posible, mediante asignación de roles, perfiles o grupos de usuarios.

En el Ayuntamiento existen distintos tipos de accesos que deben ser solicitados por el procedimiento específico de petición de accesos. Se pueden distinguir entre los siguientes:

- Directorios de red: son directorios o carpetas compartidos en servidores, los cuales contienen información de la organización. El acceso a ellos está restringido por una estructura de permisos. La petición de acceso debe ser aprobada por el responsable de dicho recurso.
- Listas de distribución y buzones compartidos: las listas de correo son utilizadas para agrupar a personas con un perfil común. La recepción de correo desde estas listas debe ser aprobada por el responsable de la lista de distribución. Los buzones compartidos son buzones de uso común entre personas de un perfil común para poder recibir y enviar comunicaciones genéricas relativas al desempeño de su trabajo. El acceso a estos buzones debe ser aprobado por el responsable del mismo.
- Otros accesos: Estos tipos de acceso incluyen peticiones de accesos al CPD y peticiones de acceso no englobadas en lo anteriormente descrito como acceso a internet e intranet. Son igualmente aprobados por el responsable del área/departamento determinado.
- Roles: es un grupo de permisos a directorios de red y listas de distribución correspondientes a un único departamento o área que son definidos para un determinado perfil de empleado. Estos deben ser aprobados de igual manera que los anteriores por el responsable del departamento o área.

Existe un control de privilegios. Consideramos privilegios aquellos permisos especiales de actuación sobre un sistema. Estos privilegios están asignados explícitamente a unos usuarios especiales del sistema. La finalidad de estos usuarios es la de la administración y gestión sobre un ámbito o dominio. Existen mecanismos de control para asegurar la correcta gestión de estos usuarios.

- Ningún ID de usuario principal de un empleado tendrá privilegios de administración.
- Estos son los diferentes tipos de usuarios privilegiados:
    - Administrador del dominio del Ayuntamiento: los privilegios del usuario administrador del dominio engloban al ámbito del dominio de Windows y son utilizados solo para tareas de administración relativas al dominio de Windows en los controladores de dominio (DCs) por el Responsable del Sistema. Este usuario no es utilizado para tareas diferentes a las indicadas. Se deberán tener en cuenta los siguientes puntos:
        - El usuario administrador del dominio nunca será usado para iniciar sesión ni para ejecutar ningún tipo de tarea o programa en máquinas distintas a los DCs.
        - Nunca añadirán privilegios a sus usuarios personales y solamente usarán el administrador para las tareas que así lo requieran.
        - A ningún ID de usuario principal de un empleado se le concederán privilegios de administración sobre el dominio. Para tales fines se usará el super usuario (definido más adelante) del administrador del dominio para así tener registrados los cambios efectuados por tal usuario y evitar errores.

5.1) DESCRIPCIÓN DE ÁMBITOS DE ADMINISTRACIÓN Y PRIVILEGIOS

Para facilitar la administración de usuarios privilegiados y poder mantener un nivel alto en la utilización de las credenciales de los mismos se han definido distintos ámbitos donde el Responsable del Sistema (o aplicaciones que se ejecuten en dichos sistemas y que requieran privilegios adicionales) puede identificarse con un usuario especial para realizar tareas. Al definir estos ámbitos y los usuarios necesarios para acceder a cada nivel se garantiza además una mayor trazabilidad de las acciones realizadas sobre los equipos para su posterior análisis en caso de que este sea necesario.

Para poder gestionar estos ámbitos se definen usuarios con las siguientes características:

- El usuario debe tener los mínimos permisos posibles para gestionar ese ámbito.
- La contraseña de todos los tipos de super usuarios (definidos más adelante en el apartado Descripción de privilegios) debe modificarse de forma periódica siguiendo la misma política de dominio ya establecida para usuarios regulares y definida en “ENS.CON.Política de contraseñas”, donde además se definen las normas de complejidad de contraseñas y todo lo relacionado alrededor de las mismas.

Se definen los siguientes ámbitos:

- Administración de servidores de dominio. Engloba a los servidores del dominio bajo responsabilidad del Responsable del Sistema. En estos equipos es necesario un nivel adicional de privilegios y solo pueden Bloguear aquellos usuarios que pertenecen al grupo de superusuarios, los cuales poseen permisos de administración en el dominio. En servidores de Bases de Datos y servidores con aplicaciones pueden loguearse además los súper usuarios creados para los administradores de estos departamentos.
- Administración de controladores de dominio (DCs). En los DCs solo está permitido el acceso a los super usuarios, debiendo utilizarse la cuenta de administrador del dominio solo para casos excepcionales donde no puedan utilizarse otras credenciales. No está permitido el acceso con usuarios regulares.
- Administración de servidores fuera de dominio. En estos equipos la administración se realizará con el usuario local de administración del equipo.
- Monitorización de equipos de red. Se realizará mediante un usuario de solo lectura de los parámetros a monitorizar de los equipos.

6) GESTIÓN DE LA INFORMACIÓN SECRETA DE AUTENTICACIÓN DE LOS USUARIOS

6.1) PROCEDIMIENTO DE ENTREGA DE PRIMERA CLAVE PARA USUARIOS

Una vez creado un alta de usuario siguiendo el procedimiento correspondiente, en el momento en el que el usuario se persone en el Responsable del Sistema para recoger su nuevo equipo, empezará este procedimiento:

1. El usuario mostrará su DNI para que el Responsable del Sistema valide su identidad.

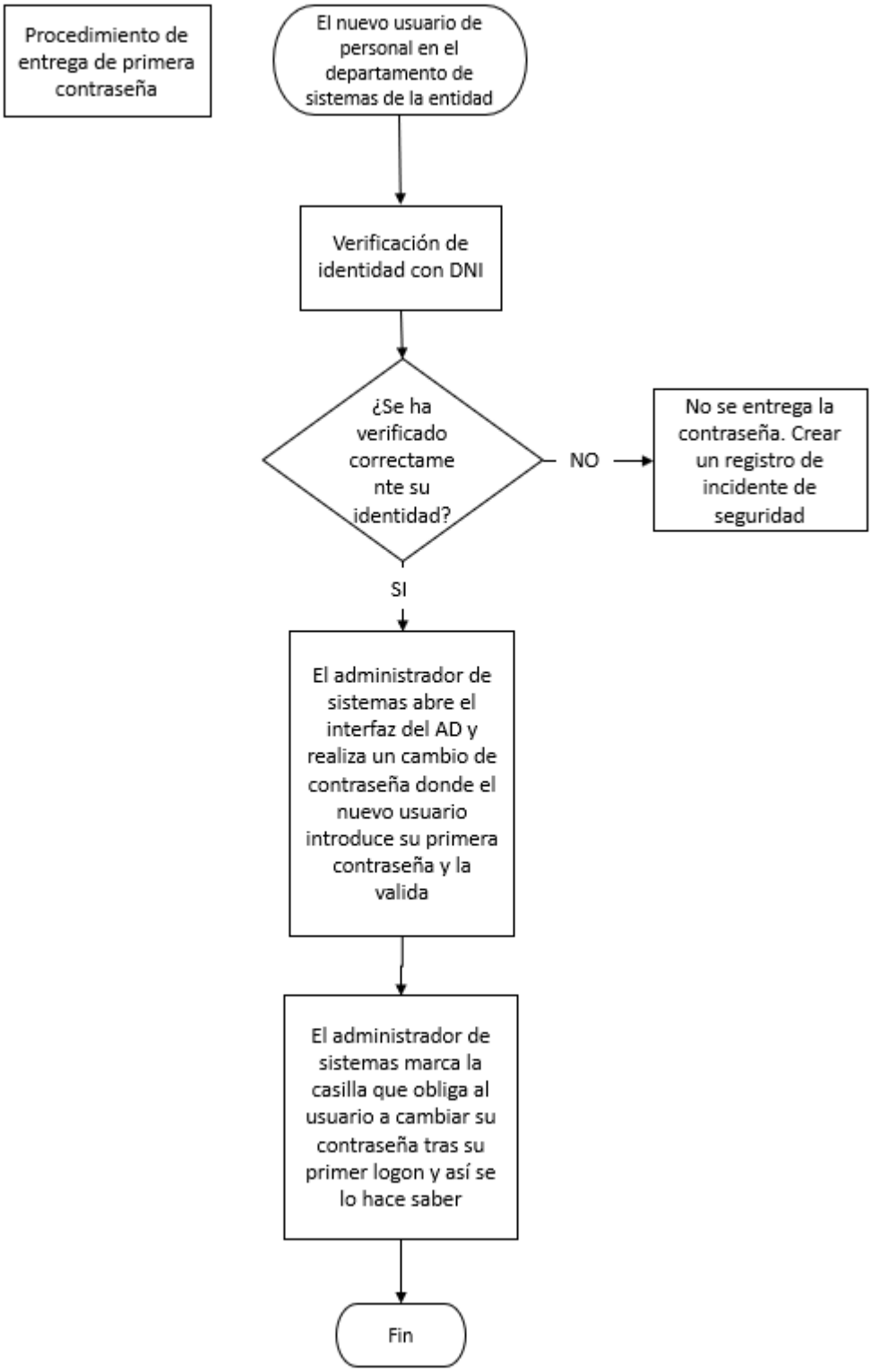
   1A- Si esta verificación de identidad no es válida, se abrirá un registro de incidente de seguridad y no se entregará la contraseña al usuario y se finalizará el proceso. Se recomendará al usuario que se ponga en contacto con Recursos Humanos para que verifiquen correctamente su identidad mediante otras medidas.

   1B- Si esta verificación de identidad fuera válida, se continuaría con el resto del proceso.

2. El Responsable del Sistema abrirá el interfaz del directorio activo, buscará el ID del usuario e instará al nuevo usuario a escribir una nueva contraseña y a verificarla en el interfaz, la contraseña será segura tal y como se describe en “ENS.CON.Política de contraseñas”.

El Responsable del Sistema marcará la casilla que obliga al usuario a cambiar la contraseña en el siguiente logado en el sistema y así se lo hará saber al usuario.

6.1.1) FLUJO



6.2) PROCEDIMIENTO DE ENTREGA DE PRIMERA CLAVE PARA UN USUARIO NO LOCALIZADO

Este es el procedimiento que debe seguir el Responsable del Sistema para entregar la primera contraseña de logon a un nuevo usuario que es alta en el Ayuntamiento.

Una vez creado un alta de usuario siguiendo el procedimiento correspondiente, en el momento en el que el usuario llame al Responsable del Sistema para recibir sus credenciales, empezará este procedimiento:

1. El usuario deberá llamar al responsable de su área/departamento para que valide su identidad y provea al Responsable del Sistema de un número de teléfono para localizar al usuario y de un medio alternativo de envío de credenciales, este medio puede ser un teléfono móvil o una dirección de correo empresarial en caso de ser un externo para poder enviar la contraseña.

   1A- Si esta verificación de identidad no es válida, se abrirá un registro de incidente de seguridad, no se entregará la contraseña al usuario y se finalizará el proceso.

   1B- Si esta verificación de identidad fuera válida, se continuaría con el resto del proceso.

2. El Responsable del Sistema abrirá la interfaz del directorio activo, buscará el ID del usuario y configurará una contraseña a la cuenta. La contraseña será segura tal y como se describe en “ENS.CON.Política de contraseñas”.
3. El Responsable del Sistema marcará la casilla que obliga al usuario a cambiar la contraseña en el siguiente logado en el sistema.
4. El Responsable del Sistema se pondrá en contacto con el usuario para comunicarle la cuenta y dirección de correo, así como la dirección de acceso al correo web.
5. Si el medio alternativo fuera un teléfono móvil, el responsable enviará un SMS de prueba al número proporcionado por el usuario previamente. Si el usuario no recibiera el SMS a ese teléfono, el administrador revisará con el usuario el número de teléfono usado y enviará mensajes de prueba hasta que el usuario reciba el mismo.
6. Una vez validado el número de teléfono, el Responsable del Sistema procederá a enviar por SMS la contraseña previamente generada.
7. El Responsable del Sistema esperará la aceptación del mensaje por parte del usuario y la confirmación de que ha sido posible su validación en el sistema.
8. El Responsable del Sistema borrará del teléfono móvil todos los SMS e instará al usuario a hacerlo una vez haya cambiado su contraseña.
9. Si el medio alternativo fuera una dirección de correo empresarial, el administrador enviará un mail con la contraseña enviada de manera segura siguiendo el procedimiento de envío seguro de contraseñas descrito en este mismo documento en el punto 6.4.
10. El responsable esperará confirmación del usuario de que ha sido posible su validación en el sistema.
11. El Responsable del Sistema marcará la casilla que obliga al usuario a cambiar la contraseña en el siguiente logado en el sistema y así se lo hará saber al usuario.

6.3) PROCEDIMIENTO DE PETICIÓN DE CAMBIO DE CONTRASEÑA DE UN USUARIO LOCALIZADO

Este procedimiento describe el flujo de tareas en una petición de cambio de contraseña para un usuario que esté localizado físicamente en las dependencias del Ayuntamiento.

El procedimiento de cambio de contraseña de un usuario se describe a continuación:

1. Si un usuario necesita cambiar su contraseña porque no recuerde cual es, deberá personarse en contacto con el Responsable del Sistema portando su DNI para que se realice una verificación de identidad. El usuario mostrará su DNI para que el Responsable del Sistema valide su identidad.

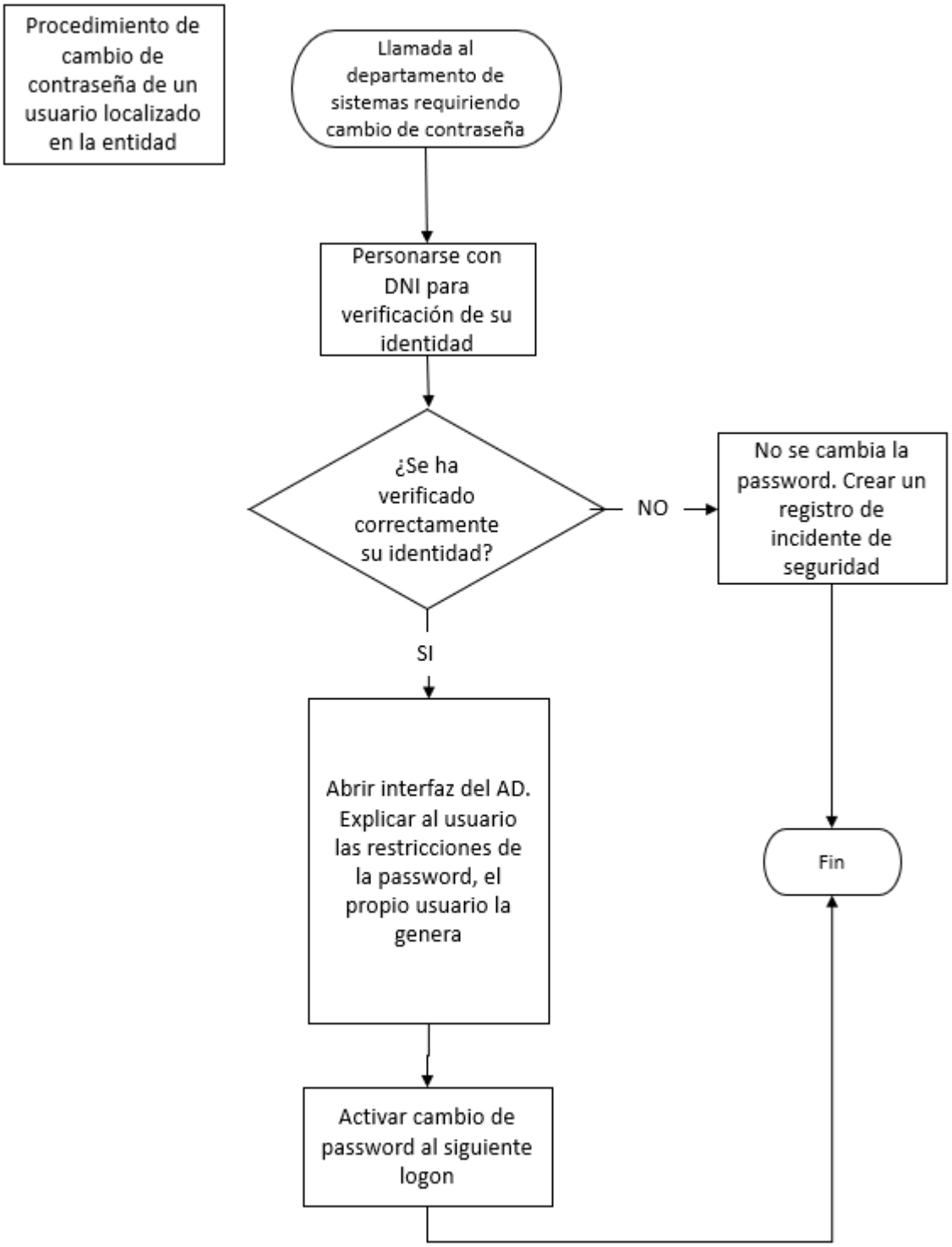
   1A- Si esta verificación de identidad no es válida, se abrirá un registro de incidente de seguridad y no se entregará la contraseña al usuario y se finalizará el proceso. Se recomendará al usuario que se ponga en contacto con Recursos Humanos para que verifiquen correctamente su identidad mediante otras medidas.

   1B- Si esta verificación de identidad fuera válida, se continuaría con el resto del proceso.

El Responsable del Sistema abrirá el interfaz del directorio activo, buscará el ID del usuario, e instará al usuario a escribir una nueva contraseña y a verificarla en el interfaz, la contraseña será segura tal y como se describe en “ENS.CON.Politica de contraseñas”.

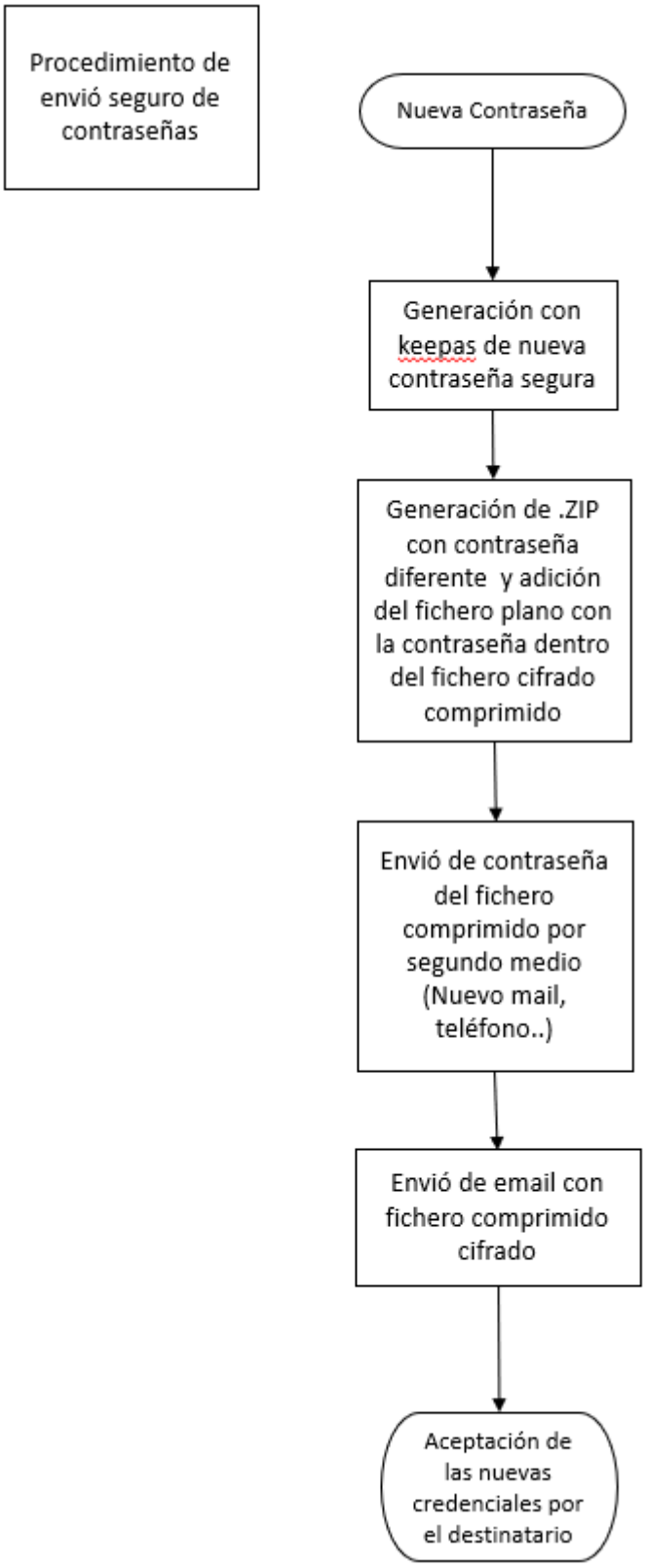
El Responsable del Sistema marcará la casilla que obliga al usuario a cambiar la contraseña en el siguiente logado en el sistema y así se lo hará saber al usuario.

6.3.1) FLUJO



6.4) PROCEDIMIENTO DE ENVÍO SEGURO DE CLAVES

6.4.1) FLUJO



6.4.2) DESCRIPCIÓN DEL PROCEDIMIENTO

El propósito de este procedimiento es definir el proceso estándar de envío de credenciales de manera segura para todos los envíos de credenciales, sean del servicio que sean, siempre que no haya un procedimiento explícito de envío de credenciales de un servicio concreto.

1. Se generará la contraseña usando el generador XXXX y siendo segura tal y como se describe en "ENS.CON.Politica de contraseñas".
2. Se almacenará la contraseña dentro de un fichero comprimido cifrado con otra contraseña diferente.
3. Se enviará un correo electrónico con el fichero comprimido cifrado con contraseña al usuario al que haya que comunicarle el cambio de contraseña sin la contraseña del fichero comprimido cifrado.
4. Se enviará la contraseña del comprimido cifrado en otro correo electrónico diferente.
5. Se esperará a la validación de recepción de cambio de credenciales por parte del usuario.

7) REVISIÓN DE LOS DERECHOS DE ACCESO DE USUARIO

Todos los grupos de permisos, listas de distribución y permisos especiales, incluyendo permisos de administración y cuentas privilegiadas en el Ayuntamiento son auditados por un proceso anual que consiste en:

1. La tarea comprobará todos los grupos, listas de distribución y buzones compartidos del directorio activo del Ayuntamiento, para mandar un mail a su responsable o delegado, mostrándole todos los usuarios que pertenecen al grupo en un informe anual.
2. Los responsables de cada activo deberán comprobar los permisos para asegurarse de que nadie disponga de derechos incorrectos. En caso de haber algún acceso o privilegio que no debiera seguir existiendo, el responsable de ese activo, pedirá al Responsable del Sistema por los medios oficiales (Formularios de peticiones de acceso o bien mediante un mail), la cancelación de dicho acceso.
3. El Responsable del Sistema procesará los cambios de permisos necesarios aprobados por el responsable de cada activo después de la petición de cancelación de acceso debido a la revisión del responsable del activo.

Todos los grupos de administradores, tanto locales como del dominio son auditados por un proceso anual que consiste en:

1. La primera tarea comprueba los grupos de acceso a cada máquina y envía un mail a su responsable o delegado mostrándole todos los usuarios que pertenecen al grupo en un informe anual. Adicionalmente, la pertenencia a los grupos de administradores de dominio es enviados al Responsable del Sistema para su revisión.
2. La segunda tarea comprueba los grupos de administradores locales y de usuarios de cada máquina y envía un mail al Responsable del Sistema mostrándole todos los usuarios administradores y usuarios locales de cada máquina en un informe.
3. Los responsables de cada activo deberán comprobar los permisos para asegurarse de que nadie disponga de derechos incorrectos. En caso de haber algún acceso o privilegio que no debiera seguir existiendo, el responsable de ese activo, pedirá al Responsable del Sistema por los medios oficiales (Formularios de peticiones de acceso o bien mediante un mail), la cancelación de dicho acceso.
4. El Responsable del Sistema procesará los cambios de permisos necesarios aprobados por el responsable del activo después de la petición de cancelación de acceso debido a la revisión del responsable del activo.

8) RETIRADA O REASIGNACIÓN DE LOS DERECHOS DE ACCESO

Con una periodicidad diaria y a última hora de la jornada laboral el departamento de RR.HH. y Sistemas comprueba las bajas que se han producido ese día. Posteriormente el Responsable del Sistema procede a eliminar todos los permisos lógicos y físicos de los usuarios. El acceso a su equipo informático o a cualquier otro de la organización es denegado al cancelar las credenciales.

Semestralmente, para revisar los accesos y permisos de los empleados, se generan unos informes que se envían a los responsables de estos recursos para que estos evalúen quien debe seguir manteniendo dichos accesos.

En caso de que el empleado o externo de Ayuntamiento saliente o en proceso de cambio tenga conocimientos de contraseñas de IDs genéricos de la organización, éstas deben ser cambiadas por el Responsable del Sistema.

9) RESPONSABLE DE LA NORMATIVA

Será responsabilidad del Responsable de Seguridad velar por el cumplimiento de la presente normativa.

10) REFERENCIAS

- 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.
- Real Decreto 951/2015, de 23 de octubre, de modificación 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.
- Guía de Seguridad CCN-STIC 821: Normas de Seguridad.
- Guía de Seguridad de las TIC CCN-STIC 883: Guía de Implantación del ENS para Entidades Locales.
- Guía de Seguridad CCN-STIC 804: Guía de Implantación.
- Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.
- Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.
- RGPD (UE) 2016/679, del parlamento europeo y del consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.
- Ley Orgánica 3/2018, de 5 de diciembre de Protección de Datos Personales y garantía de derechos digitales.
- Política de Contraseñas.

11) REGISTROS/ANEXOS

11.1) ANEXO A - DATOS PARA LA SOLICITUD DE ALTA DE CUENTA DE USUARIO

- Fecha de Solicitud.
- Fecha de Alta efectiva.
- Fecha de Fin de contrato.
- Servicio al que se destina.
- Datos de usuario a dar de Alta.
    - Nombre, Apellidos, DNI y Tipo (Interno, Externo).
    - Pertenece a: (Servicio/Unidad, Empresa Externa, etc.).
- Método de acceso remoto (si procede).

11.2) ANEXO B - DATOS PARA LA SOLICITUD DE ALTA O MODIFICACIÓN DE ACCESO EN LOS SISTEMAS DE INFORMACIÓN

- Fecha de Solicitud.
- Fecha de asignación de permisos efectiva.
- Fecha de fin de asignación de permisos.
- Sistema, Aplicación o Servicio.
- Datos de usuario:
    - Nombre y apellidos.
    - Derechos de acceso.
        - Acceso Remoto (sí/no).
        - Método de Acceso Remoto.
    - Módulo / Carpeta / Aplicación / --- Derechos (Lectura, Escritura y/o Borrado).

11.3) ANEXO C - DATOS PARA LA SOLICITUD DE BAJA/BLOQUEO DE CUENTA DE USUARIO

- Fecha de Solicitud.
- Fecha de Baja/Bloqueo efectiva.
- Datos de usuario:
    - Nombre y Apellidos.
    - Cuenta de usuario.

- Baja o bloqueo --- Duración
    - Motivo.

11.4) ANEXO D - CLÁUSULAS DE CONFIDENCIALIDAD

Acuerdo de confidencialidad

- _____ se compromete a guardar estricta confidencialidad de la información que con motivo de su autorización de acceso al equipamiento informático del Ayuntamiento para el desarrollo de sus funciones.
- _____ guardará secreto profesional sobre la información, documentos y asuntos a los que tenga acceso, estando obligado a no hacerlo público o transmitir cuantos datos conozca como consecuencia o con ocasión de su ejecución, incluso después de finalizar el plazo o la duración del acceso.
- Finalizadas las tareas, y previo a la desconexión de los equipos informáticos, se borrará toda información utilizada o que se derive de la ejecución del acceso.
- _____ reconoce que cualquier difusión, divulgación pública o cualquier otro tipo de transferencia de información confidencial por quien tiene obligación contractual de guardar secreto sobre la misma constituye un delito previsto en el derecho internacional y las leyes españolas y que tales actos serían procesados de acuerdo a la ley aplicable.
- La información necesaria para el acceso (identificador de usuario, contraseñas, parámetros de configuración, direcciones IP internas, etc.) no podrá ser divulgada bajo ningún concepto a terceras personas, ajenas o no al departamento.

Firmado: _____ (Solicitante de acceso)

Firmado: _____ (departamento de Sistemas / RRHH)