C. NTRA. SEÑORA DEL CARMEN	RAT-POLITICA DE CONTRASEÑAS Y CONTROL DE ACCESO	POL-CONT 01
		Revisión 1/ noviembre de 2018

POLÍTICA DE CONTRASEÑAS Y CONTROL DE ACCESO

1.INTRODUCCIÓN.

El procedimiento seguido por **la entidad**, para la identificación y autenticación de los usuarios (*toda persona dependiente directa o indirectamente dentro de la entidad con acceso a datos de carácter personal*) cuando intentan acceder al sistema, la red o las aplicaciones está basado en la combinación de un código de identificación de usuario (ID) y una contraseña. A cada usuario se le ha sido asignado un identificador único tanto para el acceso al sistema, como para el acceso a las aplicaciones (en aquellos casos en los que sea posible). La utilización de ID compartidos será excepcional y deberá estar justificada claramente por necesidades de negocio o limitación de aplicaciones necesarias para el desarrollo de las operaciones de negocio por el responsable del mismo o la Dirección.

El sistema implementado dispone de un mecanismo que limita la posibilidad de intentar reiteradamente el acceso no autorizado al sistema de información.

2. PROCEDIMIENTO DE GERNERACIÓN, ALMACENAMIENTO Y MANTENIMIENTO DE CONTRASEÑAS.

2.1 Generación:

- La asignación y el uso de privilegios estarán restringidos y controlados por el departamento de sistemas/TIC.
- Se asignarán privilegios específicos y no generales. Los privilegios estarán definidos por aplicación y por nivel de documentación. Esto es, cada aplicación específica será tomada en consideración por separado para evitar accesos a información no autorizados.
- Los privilegios se asignarán a cada persona en base a las necesidades reales de uso y conforme a las indicaciones del superior responsable del usuario, será este quien indicará al departamento de sistemas los privilegios que deberá de conceder.
- Las contraseñas provisionales deben ser únicas y no adivinables. No se puede generar siempre la misma clave provisional y estas no deben contener parámetros que se puedan llegar a desentrañar, como por ejemplo, un DNI o fechas fácilmente adivinables.

2.2 Privacidad:

- Los identificadores de usuario y contraseñas de acceso asociadas serán de uso personal e intransferible y por tanto no pueden ser compartidos.
- Las contraseñas deben ser conocidas exclusivamente por el usuario propietario de la misma y tratadas como información personal e intransferible. Es responsabilidad del usuario asegurar la confidencialidad y custodia de la contraseña.
- La entidad ha establecido ciertas consideraciones a la hora de elegir una contraseña que deberán ser aplicadas por todos los usuarios del sistema:

  - ✓ Se generarán contraseñas seguras, en longitud y caracteres (mínimo 6 y alfanuméricos) y evitar cualquier referencia de índole personal, nombres de hijos o hijas, fechas de nacimiento etc.
  - ✓ Las contraseñas deben ser fáciles de recordar.
  - ✓ Evitar que una contraseña sea vulnerable a ataques de diccionario (aplicaciones que automáticamente prueban palabras de diccionario hasta dar con la contraseña).
  - ✓ No utilizar caracteres consecutivos numéricos o alfabéticos., como por ejemplo “aaaaa” “555555”.
  - ✓ Cambiar las contraseñas a intervalos regulares. Cuanto mayor nivel de acceso menor deberá ser la periodicidad del cambio de las contraseñas.
  - ✓ Se debería cambiar la contraseña en la primera entrada.

- ✓ No usar la misma contraseña para las aplicaciones individuales o personales que las del entorno laboral y evitar poner siempre la misma contraseña en los distintos sistemas.
- ✓ Se evitará la comunicación escrita que revele la contraseña de cualquier usuario.

2.3 Almacenamiento:

- Las contraseñas se almacenan de forma ininteligible para terceros.
- Se deberá mantener la confidencialidad de las contraseñas y no proporcionárselas a nadie ante ninguna situación, independientemente de la persona que se las pregunte.
- Los perfiles superiores tendrán acceso a la información que necesiten y, en caso contrario, deberán solicitar autorización, pero nunca solicitar las claves a un compañero/a o tercero.
- Está prohibido guardar un registro de claves (en papel, en un documento en el equipo, o en dispositivos manual como agendas, libretas, etc.).
- Se deberá cambiar las contraseñas siempre que detecte que la seguridad de las mismas ha podido quedar comprometida.
- No incluir las claves en los procesos automáticos. Está prohibido almacenar las contraseñas en las aplicaciones que solicitan recordar contraseña.
- Las contraseñas son responsabilidad del usuario o la usuaria.

2.4 Mantenimiento:

- Todas las contraseñas deben ser modificadas por el usuario al menos con la frecuencia establecida en al apartado de periodicidad. En los entornos en los que sea posible se automatizará este requerimiento de caducidad. Cuando no sea posible, el usuario será responsable del cambio sistemático.
- En caso de olvido o cualquier dificultad relacionada con contraseñas, los usuarios contarán con la asistencia del administrador del sistema/departamento TIC.

3.CONTROL DE ACCESO.

El acceso a la información, los recursos de tratamiento de información y los procesos de negocio serán controlados según las necesidades de la entidad.

Las personas que poseen activos de información y que, por tanto, son responsables ante la dirección de la protección de "sus" activos, cuando la dirección así lo haya establecido tendrán/deberán definir y/o aprobar las reglas de control de acceso y otros controles de seguridad.

Los usuarios recibirán sus derechos de acceso siguiendo la política de mínimo privilegio. Es decir, únicamente a aquellos datos y recursos informáticos que precisen para el desempeño de sus funciones.

El responsable del departamento de cada usuario, en función de las tareas que prevea que va a desempeñar, determinará qué aplicaciones serán accesibles por el usuario.

El ANEXO 1 de este procedimiento incluye modelo de *RELACIÓN DE USUARIOS CON ACCESO AUTORIZADO* para cada usuario, que deberá ser completado por el responsable de cada departamento.

Por su parte el Responsable de Seguridad/Responsable TIC elaborará y mantendrá actualizado el modelo de *DERECHOS DE ACCESOS POR PERFIL LABORAL* correspondiente ANEXO 2 incluido en este procedimiento.

El Responsable de Seguridad/Responsable TIC es el encargado del mantenimiento de los usuarios del sistema y aplicaciones, teniendo en cuenta los siguientes criterios:

3.1 Alta de usuarios:

Únicamente el Responsable de Seguridad/Responsable TIC tiene competencias para dar de alta los identificadores de usuarios y asociarlos a los perfiles definidos para los distintos niveles de acceso a las aplicaciones y tratamientos.

Los responsables directos de los usuarios que tengan que dar de alta a uno nuevo en el sistema o a las aplicaciones, deberán notificárselo al Responsable de Seguridad/ Responsable TIC.

La Dirección de la entidad es quien tiene la última decisión sobre los derechos de acceso de los usuarios.

Una vez dada el alta, el Responsable de Seguridad/Responsable TIC comunicará al nuevo usuario y al responsable que autorizó la solicitud, indicando los datos del mismo y el identificador de usuario asignado.

Para el primer acceso del usuario al sistema, el Responsable de Seguridad/Responsable TIC comunicará de forma confidencial su identificador y su contraseña de acceso inicial, según lo dispuesto en el apartado 2 de la presente política.

Se tendrán en cuenta las siguientes normas en la asignación de identificadores:

- No se reutilizará un identificador.
- Deben utilizarse al menos cinco caracteres en la composición del identificador del usuario.
- Se pueden mantener únicamente aquellos nombres de usuario propios de los sistemas operativos y de las aplicaciones de software que no puedan ser modificados.

3.2 Baja de un usuario:

El área de Recursos Humanos o el responsable del departamento donde el usuario cause baja deberán comunicar dicha baja al Responsable de Seguridad/Responsable TIC quien se encargará de cancelar el usuario y sus derechos de acceso.

3.3 Modificación de permisos de un usuario:

La modificación de los derechos o permisos de acceso de un usuario requerirá de la misma autorización jerárquica, diferenciada para cada tipología de usuarios, ya descrita en el protocolo de alta. Por lo tanto, el procedimiento enunciado en el apartado de alta será extensible a este punto de modificación de permisos.

3.4 Reactivación de usuarios:

La reactivación de usuarios exige un procedimiento diferenciado respecto al resto de protocolos enunciados anteriormente, ya que parte de la premisa de la existencia de un alta previa y no requiere de un cambio de permisos del usuario en el sistema.

Para aquellos casos en que el acceso del usuario al sistema se haya revocado por causas accidentales, como el olvido de la contraseña, un periodo prolongado de inactividad o un excesivo número intentos fallidos, la reactivación del usuario exigirá su comunicación al Responsable de Seguridad/Responsable TIC para subsanar la situación.

4. REGISTRO DE ACCESOS.

Todos los usuarios deberán tener configurado su puesto de trabajo para que se exija la introducción de una contraseña al intentar volver al sistema, tras un periodo de 10 minutos de inactividad.

Exclusivamente el personal autorizado por Responsable de Seguridad/Responsable TIC podrá tener acceso a los lugares donde se hallen instalados los equipos físicos que den soporte a los sistemas de información (Centro de Procesado de Datos).

Registro de accesos:

Cuando el personal accede a datos especialmente protegidos (*origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, afiliación sindical, tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o las orientaciones sexuales de una persona*) la aplicación o el sistema gestor de la base de datos deberá registrar la siguiente información:

1. Identificación del usuario,
2. la fecha y hora en que se realizó el acceso,
3. el fichero accedido,
4. el tipo de acceso y,
5. si ha sido autorizado o denegado.
6. En el caso de que el acceso haya sido autorizado, se registrará el identificador del registro accedido.

El registro de accesos será revisado mensualmente y se elaborará un informe describiendo las incidencias detectadas.

La información del registro de accesos se conservará por un período mínimo de dos años.

Los mecanismos que habilitan el registro de los accesos no podrán, bajo ningún concepto, ser desactivados.

C. NTRA. SEÑORA DEL CARMEN	RAT-POLITICA DE CONTRASEÑAS Y CONTROL DE ACCESO	POL-CONT 01 Revisión 1/ noviembre de 2018

ANEXO 1 - RELACIÓN DE USUARIOS CON ACCESO AUTORIZADO.

NOMBRE Y APELLIDOS	PUESTO DE TRABAJO	FECHA ALTA, BAJA y BAJA EFECTIVA	RECURSOS / MODOS ACCESO
		Alta __/__/____ baja prevista __/__/____ baja efectiva __/__/____	Perfil ya definido en el documento Derechos de acceso
		Alta __/__/____ baja prevista __/__/____ baja efectiva __/__/____	Perfil ya definido en el documento Derechos de acceso
		Alta __/__/____ baja prevista __/__/____ baja efectiva __/__/____	Perfil ya definido en el documento Derechos de acceso
		Alta __/__/____ baja prevista __/__/____ baja efectiva __/__/____	Perfil ya definido en el documento Derechos de acceso

ANEXO 2 – DERECHOS DE ACCESOS POR PERFIL LABORAL

ACCESO A SISTEMAS DE INFORMACIÓN POR PERFIL LABORAL / PUESTO DE TRABAJO													
La siguiente plantilla describe el acceso y la utilización a los diferentes sistemas de información de la organización, por parte de los distintos perfiles de usuarios laborales: propios, externos y personal en prácticas.		PUESTO DE TRABAJO											
			RRHH	DEPARTAMENTO "A"		DEPARTAMENTO DE "B"		DEPARTAMENTO "C"		INFORMÁTICA		DEPARTAMENTO CALIDAD	
		DIRECTOR GENERAL	RECURSOS HUMANOS	PUESTO DE TRABAJO "X"	PUESTO DE TRABAJO "X"	PUESTO DE TRABAJO "X"	PUESTO DE TRABAJO "X"	PUESTO DE TRABAJO "X"	PUESTO DE TRABAJO "X"	RESPONSABLE INFORMÁTICA	INFORMÁTICO	EJEMPLO DIRECTOR DE CALIDAD	EJEMPLO ADJUNTO CALIDAD
ACCESO A SISTEMAS DE INFORMACIÓN	*Aplicación/BBDD "X"*	TOTAL	TOTAL	TOTAL	TOTAL	TOTAL	TOTAL	TOTAL	TOTAL	TOTAL	TOTAL	TOTAL	TOTAL
	Aplicación/BBDD "X"	TOTAL	TOTAL	TOTAL	TOTAL	TOTAL	TOTAL	TOTAL	TOTAL	TOTAL	PARCIAL	TOTAL	TOTAL
	Aplicación/BBDD "X"	TOTAL	TOTAL	TOTAL	PARCIAL	PARCIAL	PARCIAL	PARCIAL	PARCIAL	PARCIAL	PARCIAL	PARCIAL	PARCIAL
	Aplicación/BBDD "X"	TOTAL	TOTAL	TOTAL	PARCIAL GENERAL	PARCIAL	PARCIAL	PARCIAL	PARCIAL	PARCIAL	TOTAL	TOTAL	TOTAL

COPIA DE RESPALDO	Custodia de los soportes	SI	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO
	Realización de la copia	NO	NO	NO	NO	NO	NO	NO	NO	SI	SI	NO	NO
	Restauración de los datos copiados	NO	NO	NO	NO	NO	NO	NO	NO	SI	SI	NO	NO
	Traslado de los soportes	SI	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO
ACCESO A ARCHIVOS Y DOCUMENTOS	Archivo Recursos Humanos	SI	SI	SI	NO	NO	NO	NO	NO	NO	NO	NO	NO
	Archivo Administración y finanzas	SI	PARCIAL	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
	Archivo "X"	SI	NO	NO	NO	SI	SI	SI	SI	NO	NO	SI	SI
	Realización de COPIAS de DOCUMENTOS	SI	NO	NO	NO	SI	NO	SI	SI	NO	NO	NO	NO
ACCESOS REMOTOS	*Servidor*	SI	NO	SI	NO	SI	NO	SI	SI	SI	SI	SI	NO
	TeamViewer	SI	NO	SI	NO	SI	NO	NO	NO	SI	SI	NO	NO
ESO A LOC ALES	*Aplicación/BBDD*	SI	NO	NO	NO	NO	NO	NO	NO	SI	SI	NO	NO

	"X"												
	Aplicación/BBDD "X"	SI	NO	NO	NO	NO	NO	NO	NO	SI	SI	NO	NO
	Aplicación/BBDD "X"	SI	NO	NO	NO	NO	NO	NO	NO	SI	SI	NO	NO
	Aplicación/BBDD "X"	SI	NO	NO	NO	NO	NO	NO	NO	SI	SI	NO	NO
AUTORIZACIONES	Salida de documentación en papel	SI	SI	SI	NO	NO	NO	SI	SI	NO	NO	NO	NO
	Salida de documentación anexa al correo electrónico	SI	SI	SI	SI	SI	NO	SI	SI	NO	NO	NO	NO
	Salida de soportes	SI	NO	SI	NO	SI	NO	SI	SI	SI	SI	SI	NO
	Salida de soportes con datos de carácter personal	SI	NO	SI	NO	NO	NO	NO	NO	NO	NO	NO	NO