



Noray
GDPR - Recomendaciones de seguridad
08/10/2021

Índice

Aviso	2
Introducción	2
Objetivos del documento	3
Copias de seguridad	3
Contraseñas de acceso	3
Auditoría	4
Registros de accesos	4
Ejercicio de derechos.	4
Calidad de los datos	5
Deber de información	5
Activación Log de accesos.	6
Noray Control de Acceso.	6
Noray Htl.	7
Bloqueos de usuarios.	8
Noray Control de Acceso.	8
Noray Htl.	9
Gestión de ejercicio de derechos	10
Portabilidad de datos	10
Supresión de datos	10
Modificación de datos	10
Cancelación de datos.	11
Solicitudes de derechos.	11
Detectar y responder a fallos del sistema de seguridad.	11

Aviso

Este documento es una guía sobre el cumplimiento del Reglamento General de protección de datos (GDPR) en la fecha de publicación.

En este documento se recogen los aspectos más significativos del cumplimiento del GDPR. Por lo tanto, se proporciona para propósitos informativos, y por ello se le informa al cliente con el fin de que pueda aplicar en su organización las diferentes actuaciones y/o adaptaciones a la normativa en materia de Protección de Datos.

Noray en aras de informar a sus clientes y cumplir con la normativa vigente, les detalla una serie de recomendaciones que se han puesto a disposición en las aplicaciones de Noray con el fin de ayudar al cliente en dicho cumplimiento.

Noray no garantiza la información legal de forma continua de este documento, incluyendo los sitios web de Internet y referencias URL, debidas a que están sujetas a posibles cambios o modificaciones en cualquier momento sin previo aviso.

Noray proporciona estas pautas al cliente para que proceda conjuntamente con sus asesores o departamento de Privacidad y Protección de Datos de su organización/empresa a utilizar las aplicaciones de Noray de forma coherente con el GDPR. Por lo que Noray no es responsable de dicho cumplimiento y se exime de cualquier forma la no implementación de las pautas exhibidas e informadas de forma oportuna en este documento.

Introducción

El 25 de mayo de 2018 entra en vigor el Reglamento General de protección de datos (GDPR, Reglamento UE 2016/679). Este reglamento europeo de privacidad y seguridad establece un nuevo estándar global para los derechos de privacidad, seguridad y cumplimiento de normas y trata, fundamentalmente, sobre la protección y la habilitación de los derechos de privacidad de los individuos.

El GDPR establece estrictos requisitos de privacidad que rigen cómo las organizaciones administran y protegen los datos personales respetando la elección individual, sin importar dónde se envían, procesan o almacenan los datos. Para acceder al texto completo de la norma puede usar el siguiente enlace:

<https://www.boe.es/doue/2016/119/L00001-00088.pdf>



#orgullososdenuestrosclient

noray.com
902 440 053

Gran Canaria

Ruiz de Alda, 12, 3º
35007 Las Palmas de GC

Tenerife

Miraflores, 8, 3º
38003 SC de Tenerife

Madrid

Santiago Grisolia 2, of.38
28760 Tres Cantos, Madrid

Objetivos del documento

El objetivo de este documento es, por tanto, dar algunas recomendaciones acerca de los principales hitos a cubrir por parte de su organización, así como delimitar las responsabilidades de Noray en cada uno de ellos.

En cualquier caso, le animamos a que trabaje con profesionales cualificados para implementar el GDPR, y verificar cómo se aplicará específicamente a su organización/empresa, y para determinar la mejor manera de asegurar el cumplimiento de la norma en cuestión.

Copias de seguridad

Su organización es responsable de realizar las copias de seguridad periódicas, y realizará por su cuenta sus propias copias de seguridad para en el supuesto caso de que se produzca una pérdida de información o de datos, pueda realizarse el proceso de recuperación de la información de forma correcta.

Noray le recomienda realizar dichas copias periódicamente y comprobar el contenido de las mismas garantizando la salubridad de las mismas.

Noray no será responsable en ningún caso de la pérdida de información sufrida por el cliente cuando se deba a fallos informáticos o a falta de copias de seguridad correctas por parte del cliente.

Cuando utilice un servicio contratado en la nube suministrada por Noray, Noray exigirá al prestador del servicio de alojamiento/hosting la garantía de realización de las mismas correctamente. Estas garantías estarán publicadas en www.noray.com.

Contraseñas de acceso

Su organización será responsable de crear perfiles de acceso y facilitar un usuario y una contraseña para su personal, los que posteriormente deberán ser cambiados por cada uno. La aplicación de Noray facilita el control de usuarios pudiendo implementar el nivel de complejidad y extensión de las mismas, así como la periodicidad del cambio de las mismas, lo que deberá ser establecido por el cliente.

Noray le recomienda facilitar a cada usuario una clave e informarle de que deberá cambiarla debiendo respetar los parámetros de seguridad definidos por el cliente. Se recomienda el uso de contraseñas complejas y con una extensión mínima de 8 caracteres alfanuméricos.

Noray no será responsable en ningún caso de la pérdida de información, ni del acceso a información por parte del personal no autorizada, ni a sanciones en que pudiera incurrir el cliente por no adoptar dicha medida de seguridad.

Noray facilitará una herramienta en sus aplicaciones para que en caso de que un usuario de las mismas introduzca erróneamente su contraseña, se produzca el bloqueo del mismo cuando se haya superado un límite de intentos establecido por su organización (Se recomienda el bloqueo a los 3 intentos erróneos). Puede consultar el apartado '[Bloqueos de usuarios](#)' de este documento donde se describe cómo activarlo en cada caso. No obstante, si necesita asistencia en este sentido podrá requerir los servicios de Noray no considerándose éstos dentro de los servicios incluidos en el contrato de mantenimiento suscrito y por tanto se facturará en función del tiempo empleado en el mismo y siguiendo las normas de desplazamientos del catálogo de servicios publicado en www.noray.com.

Auditoría

Su organización podrá solicitar a Noray un informe sobre la realización/resultado de auditorías de seguridad relativas al cumplimiento del GDPR **en las aplicaciones Noray instaladas en su organización**. Este informe no se considerará dentro de los servicios incluidos en el contrato de mantenimiento suscrito y por tanto se facturará en función del tiempo empleado en el mismo y siguiendo las normas de desplazamientos del catálogo de servicios publicado en www.noray.com.

Cuando utilice un servicio contratado en la nube suministrada por Noray, Noray garantiza a través de su proveedor de servicio de alojamiento/hosting que dicho sistema cumple con los requisitos y medidas de seguridad adecuadas. Estas garantías estarán publicadas en www.noray.com.

Registros de accesos

Las aplicaciones de Noray permiten la activación de un registro de accesos log, permitiendo a Ud., establecer el periodo que desea conservar dicho registro por lo que Noray le recomienda activar dichos registros de accesos en cada una de las aplicaciones para cubrir en este requerimiento de la norma.

Noray no será responsable en ningún caso de la pérdida de información, ni del acceso a información por parte del personal no autorizada, así como de la inexistencia de los registros de accesos a la aplicación o a sanciones en que pudiera incurrir el cliente por no adoptar esta medida de seguridad.

Puede consultar el apartado '[Activación Log de Acceso](#)' de este documento donde se describe cómo activarlo en cada caso. No obstante, si necesita asistencia en este sentido podrá requerir los servicios de Noray no considerándose éstos dentro de los servicios incluidos en el contrato de mantenimiento suscrito y por tanto se facturará en función del tiempo empleado en el mismo y siguiendo las normas de desplazamientos del catálogo de servicios publicado en www.noray.com.

Ejercicio de derechos.

El GDPR permite a los sujetos de datos ejercitar diversos derechos de los sujetos de datos (DSR) relativos a sus datos personales. Si bien las aplicaciones Noray tienen herramientas actuales y agregará otras capacidades en las actualizaciones para ayudarle a responder a las solicitudes DSR, la decisión de cumplir con la solicitud DSR y su aplicación es responsabilidad del cliente.

Su organización será el responsable de tramitar dicha solicitud conforme a los protocolos establecidos de protección de datos en su entidad.

Noray no será responsable en ningún caso de la inexistencia de los registros de derechos de protección de datos ejercidos por los clientes finales y/o de las sanciones en que pudiera incurrir el cliente por no adoptar esta medida de seguridad.

Puede consultar el apartado '[Gestión de ejercicio de derechos](#)' de este documento donde se describe cómo activarlo en cada caso. No obstante, si necesita asistencia en este sentido podrá requerir los servicios de Noray no considerándose éstos dentro de los servicios incluidos en el contrato de mantenimiento suscrito y por tanto se facturará en función del tiempo empleado en el mismo y siguiendo las normas de desplazamientos del catálogo de servicios publicado en www.noray.com.

Calidad de los datos

Las aplicaciones Noray permiten conocer las acciones realizadas por un cliente final, por lo que basándose en dichas estadísticas, Ud. podrá mantener los datos actualizados y en su caso cancelar o suprimir aquellos que hayan dejado de ser necesarios para el cumplimiento de la finalidad para la que fueron recabados.

Deber de información

Las aplicaciones Noray permiten incluir textos relativos al cumplimiento del deber de información en relación con el tratamiento de los datos personales de los clientes finales.

Para ello es recomendable incluir en los documentos a entregar a clientes tales como facturas, partes de entrada de viajeros, tarjetas de bienvenida, etc.... las políticas y cláusulas previstas para el tratamiento de datos personales vigentes para su inclusión así como, en cumplimiento del Reglamento Europeo de Protección de Datos, recabar el consentimiento expreso para cada uno de los tratamientos de datos previstos.



#orgullososdenuestrosclient

noray.com
902 440 053

Gran Canaria

Ruiz de Alda, 12, 3º
35007 Las Palmas de GC

Tenerife

Miraflores, 8, 3º
38003 SC de Tenerife

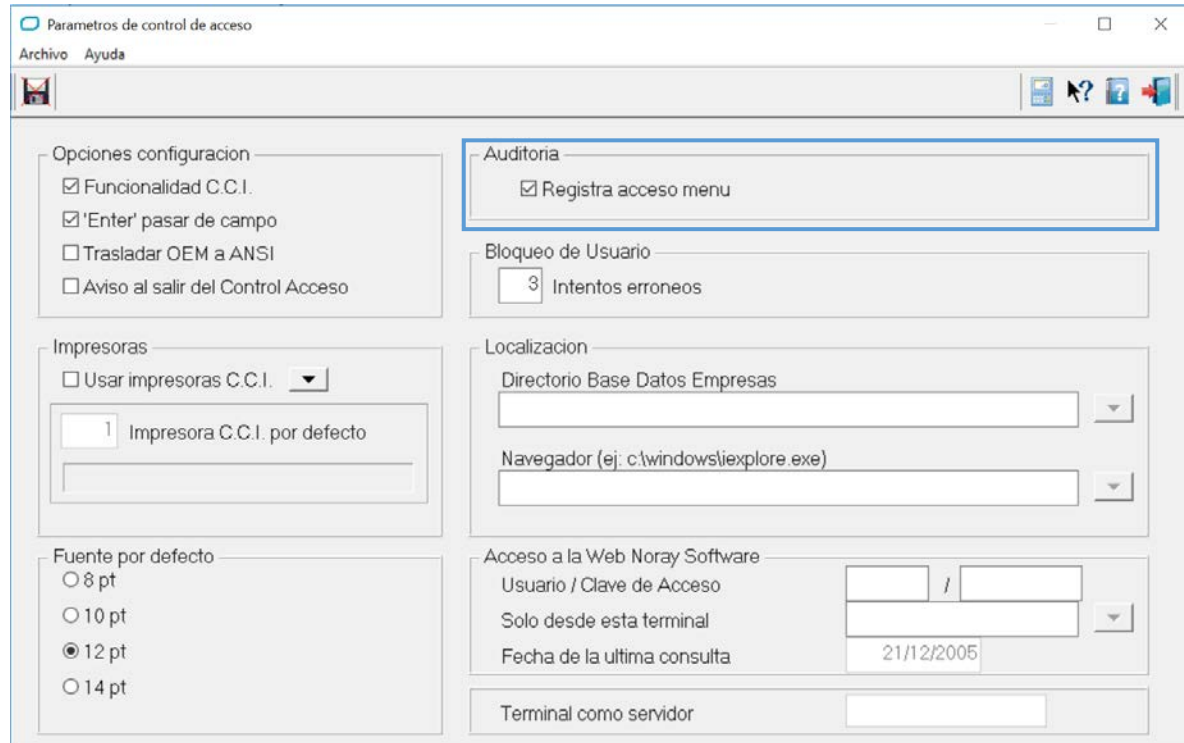
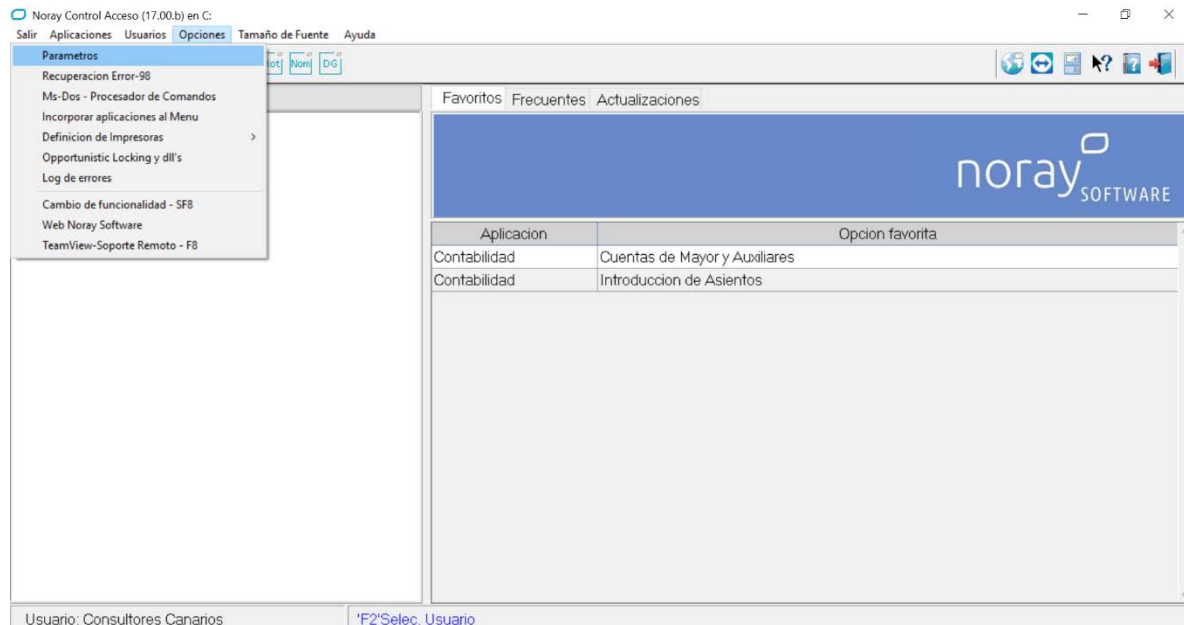
Madrid

Santiago Grisolia 2, of.38
28760 Tres Cantos, Madrid

Activación Log de accesos.

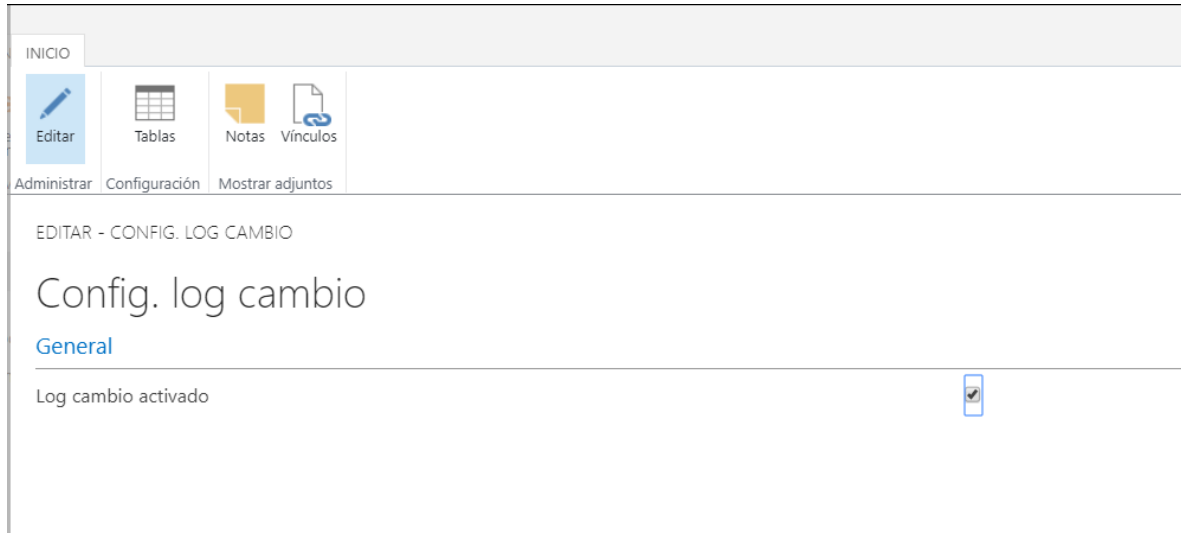
Noray Control de Acceso.

Para activar el control de acceso a las distintas aplicaciones de Noray simplemente debe acceder a los Parámetros a través del menú de Opciones y activar la casilla correspondiente señalada en la imagen.



Noray Htl.

Para activar el log de cambios en Noray Htl debe acceder a la opción de Configuración del Log de cambios y activarlo.



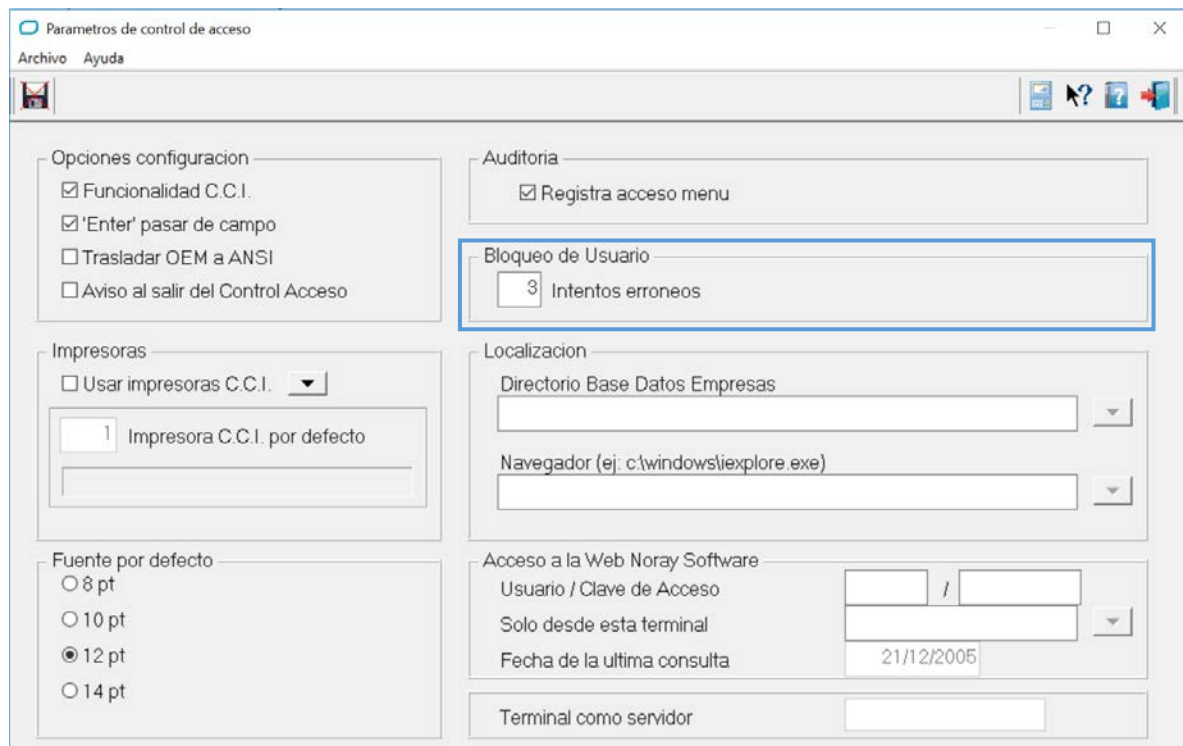
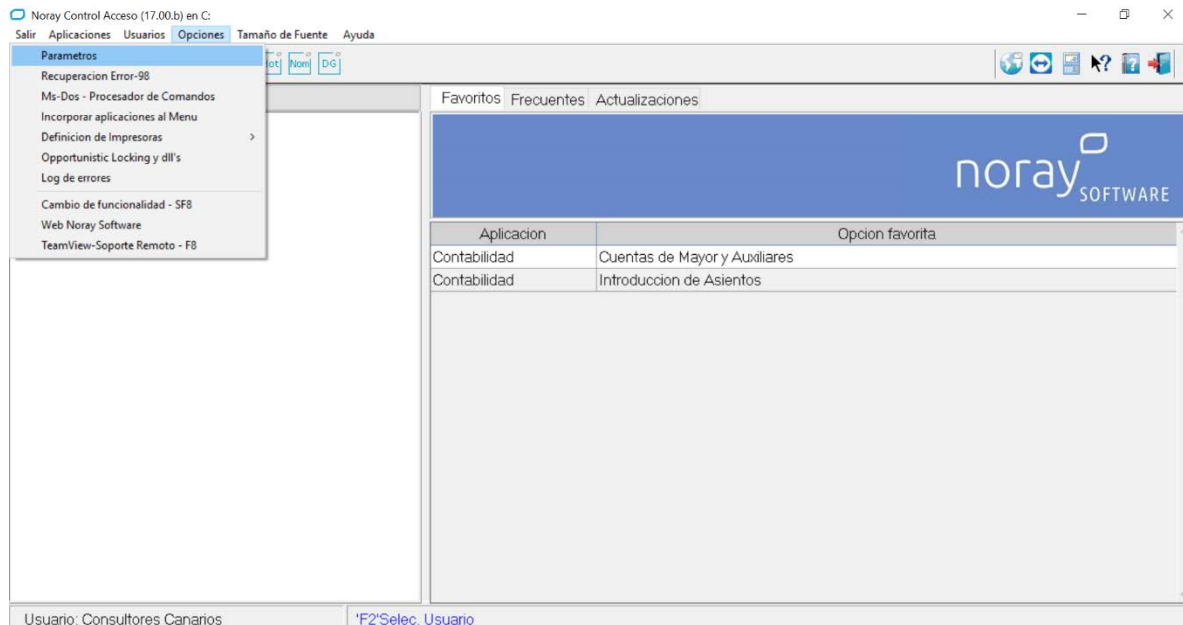
Para a continuación, establecer mediante la opción Tablas, la lista de entidades donde se desea registrar dicho log. Debe incluir aquellas tablas donde se registran datos personales como pueden ser; clientes proveedores, empleados, recursos, usuarios, contactos, huéspedes, documentos donde se incluyan todos los anteriores, etc.

Si bien las aplicaciones Noray proporcionan capacidades para registrar los cambios en determinadas entidades es su responsabilidad asegurarse de que los datos personales y sensibles estén ubicados e incluidos en esta lista, así como clasificados apropiadamente para que su organización cumpla con sus obligaciones bajo el GDPR.

Bloqueos de usuarios.

Noray Control de Acceso.

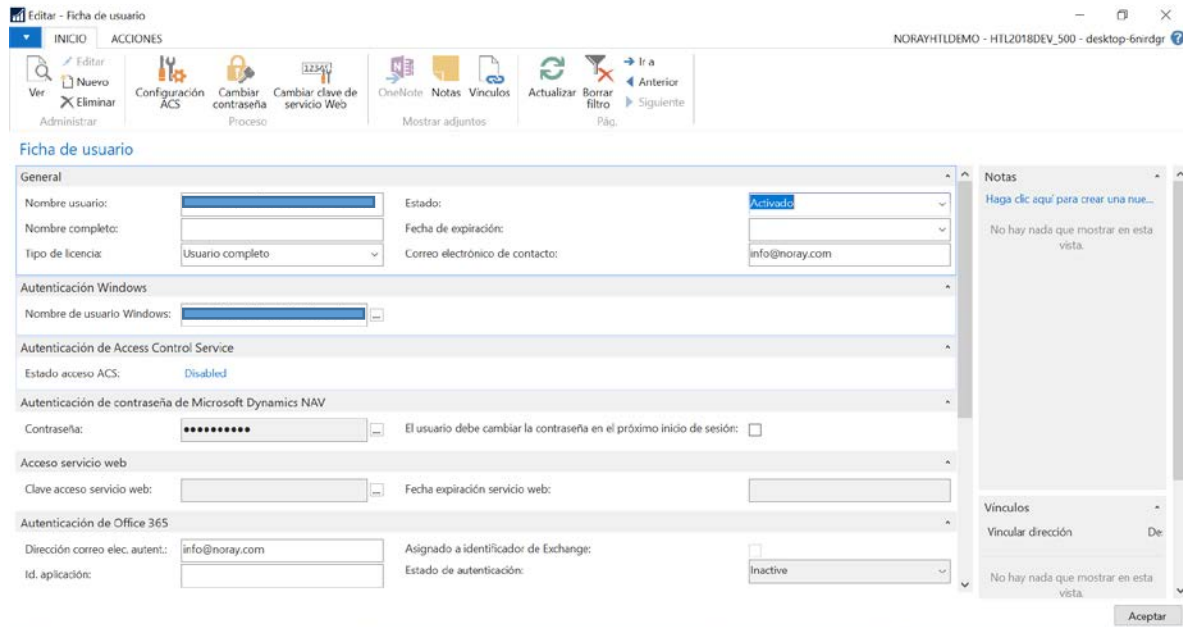
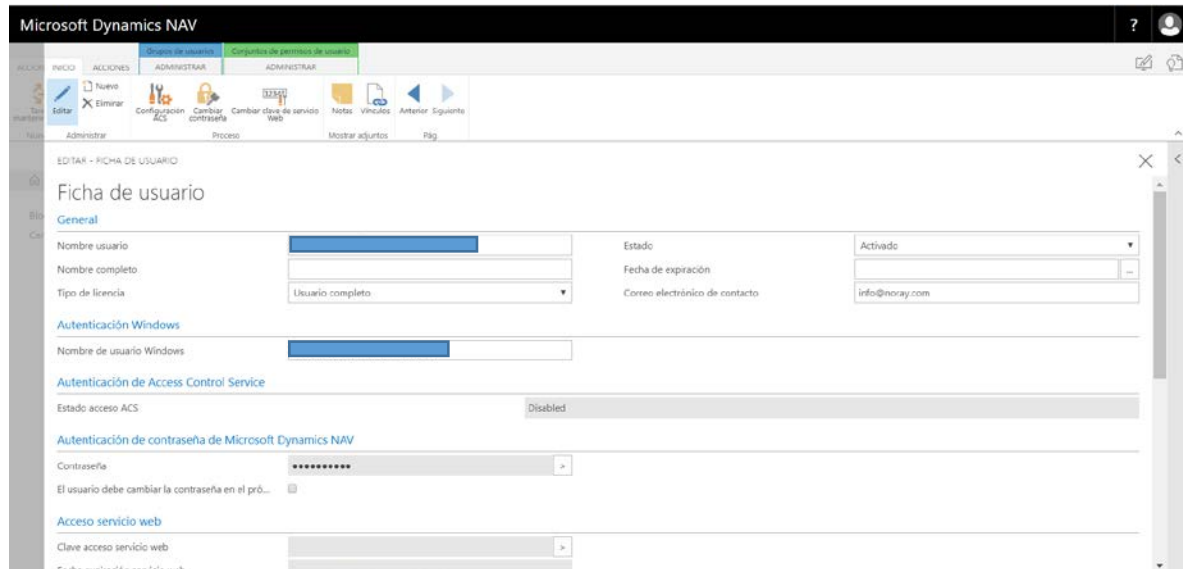
Para configurar el bloqueos de usuarios en las distintas aplicaciones de Noray simplemente debe acceder a los Parámetros a través del menú de Opciones y determinar el número de intentos de introducción de clave errónea que se le pueden permitir al usuario antes de ser bloqueado. Tanto para desbloquear al usuario como para modificarle/recuperar sus claves. Un usuario con privilegios de administrador, podrá acceder al menú de Usuarios y actuar en consecuencia.



Noray Htl.

En Noray Htl no existen restricciones o bloqueos automáticos por intentos de acceso por clave errónea, si bien esto puede ser configurado en el sistema operativo o su cuenta de Office 365 cuando se utilizan los métodos de Usuario Windows o de Office 365 en la autenticación en Noray Htl.

En cualquier caso, en la ficha de usuarios de la aplicación es posible tanto bloquear los usuarios desactivándolos, como establecer fechas de vencimientos de las contraseñas o cambiar las mismas.

Gestión de ejercicio de derechos

Portabilidad de datos

El GDPR permite a una persona realizar una solicitud de portabilidad de sus datos a otra organización, lo que significa, en parte, que usted debe exportar los datos personales del sujeto de datos de sus sistemas y proporcionar los mismos en un formato estructurado, comúnmente usado.

Una vez que se identifican y localizan los datos personales en la aplicación Noray, se puede exportar a un archivo Excel para facilitar una solicitud de portabilidad de datos. Utilizando Excel, puede editar los datos personales que se incluirán en la solicitud y guardar los datos en un formato de uso general, legible por máquina, como. csv o. Xml.

Si bien las aplicaciones Noray proporcionan capacidades para exportar y, por lo tanto, acceder a datos personales, es su responsabilidad asegurarse de que los datos personales y sensibles estén ubicados y clasificados apropiadamente para que su organización cumpla con sus obligaciones bajo el GDPR.

Supresión de datos

El GDPR permite a una persona realizar una solicitud a su organización para que elimine sus datos personales. Las aplicaciones Noray le ofrecen varios métodos para corregir datos personales inexactos o incompletos, o para borrar datos personales con respecto a un sujeto de datos utilizando las capacidades de personalización, pero la decisión y la implementación son su responsabilidad.

En algunos casos, puede optar por utilizar las pantallas de la aplicación para editar directamente sus datos, como modificar o eliminar un contacto.

Si bien las aplicaciones Noray proporcionan capacidades para eliminar datos personales, es su responsabilidad asegurarse de que los datos personales y sensibles estén ubicados y clasificados apropiadamente para que su organización cumpla con sus obligaciones bajo el GDPR.

Modificación de datos

El GDPR permite a una persona realizar una solicitud a su organización para la rectificación de datos personales inexactos concernientes al sujeto de datos.

Las aplicaciones Noray ofrecen a su organización los siguientes métodos para corregir datos personales inexactos o incompletos. En algunos casos, puede exportar datos a Excel para editar rápidamente los registros de múltiples de Noray y, a continuación, reimportar los datos. También puede modificar los datos personales almacenados editando manualmente el campo que contiene los datos personales, como por ejemplo la edición de información sobre un cliente en su ficha.

Ciertos tipos de registros de las aplicaciones, a saber, registros de transacciones de negocios (como general, cliente, movimientos de impuestos) son esenciales para la integridad del sistema de planificación de recursos de la empresa. Así, la modificación de los datos personales en dichos registros es restringida.

Si bien, las aplicaciones Noray ofrecen capacidades para modificar datos personales, es su responsabilidad asegurarse de que los datos personales y sensibles estén ubicados y clasificados apropiadamente para que su organización cumpla con sus obligaciones bajo el GDPR.

Cancelación de datos.

El GDPR permite a una persona realizar una solicitud a su organización para restringir el procesamiento de sus datos personales. Cuando reciba dicha solicitud de un sujeto de datos, puede marcar su registro como bloqueado o con estado inactivo debido a la privacidad. A continuación, las aplicaciones Noray descontinuará el procesamiento de los datos personales de ese sujeto de datos.

Cuando un registro se marca como bloqueado o inactivo, no se pueden crear nuevas transacciones que utilicen ese registro. Por ejemplo, no se puede crear una factura nueva para un cliente, cuando el cliente o el vendedor están bloqueados.

Las aplicaciones Noray ofrecen capacidades para cancelar datos personales, es su responsabilidad asegurarse de que los datos personales y sensibles estén ubicados y clasificados apropiadamente para que su organización cumpla con sus obligaciones bajo el GDPR.

Solicitudes de derechos.

Dado que las personas pueden realizar múltiples solicitudes bajo el GDPR, se espera que realice un seguimiento de todas las solicitudes entrantes y de las acciones que realice como resultado de una solicitud.

Este registro de solicitudes no está contemplado en las aplicaciones Noray, existen múltiples alternativas en herramientas de ofimática, bases de datos, hojas de cálculo, etc. Que ofrecen capacidades para realizar el seguimiento de las solicitudes de rectificación, eliminación o transferencia de datos personales del sujeto de datos. Es su responsabilidad asegurarse de que los datos personales y sensibles estén ubicados y clasificados apropiadamente para que su organización cumpla con sus obligaciones bajo el GDPR.

Detectar y responder a fallos del sistema de seguridad.

Como controlador de datos o de un procesador de datos, el GDPR le obliga a su organización a informar y notificar a la autoridad supervisora pertinente, los sujetos de datos afectados y/o controlador de datos de ciertos tipos infracciones de datos personales.

Cuando ejecute las aplicaciones Noray en sus propias instalaciones o la de un socio, será su responsabilidad supervisar y detectar las brechas de datos para que pueda cumplir los requisitos de notificación aplicables para cualquier incidencia y dentro de los períodos definidos en el GDPR.

Recomendaciones en cumplimiento del RGPD UE art. 32 Seguridad del Tratamiento.

NORAY recomienda a sus Clientes las siguientes normas básicas

- Tener un plan de copias de seguridad.
- Que las copias se realicen de forma automática (preferentemente)..
- Que las copias se realicen todos los días. Es interesante mantener copias separadas de varios días con el fin de tener “varias alternativas” a la hora de recurrir a ellas tras un siniestro.
- Comprobar periódicamente que se están realizando: revisar la carpeta donde se guardan las copias, comprobar que las fechas de los archivos de copias están actualizadas y comprobar que los tamaños de estos archivos son de tamaños más o menos parecidos o van creciendo.

Duplicar periódicamente las copias a un soporte externo (Disco USB, Almacenamiento en la nube, etc.). Con esto evitaremos perder la información en caso de tener un siniestro en nuestras oficinas y perder todo el hardware (copias incluidas).