Noray

GDPR - Recomendaciones de seguridad

08/10/2021

Index

Notice

This document is a guide to compliance with the General Data Protection Regulation (GDPR) at the date of publication.

This document contains the most significant aspects of compliance with the GDPR. Therefore, it is provided for informational purposes, and therefore the client is informed so that it can apply in its organization the different actions and/or adaptations to the regulations on Data Protection.

Noray, in order to inform its customers and comply with current regulations, details a series of recommendations that have been made available in Noray's applications in order to assist the customer in such compliance.

Noray does not warrant the continued legality of this document, including Internet web sites and URL references, because they are subject to change or modification at any time without notice.

Noray provides these guidelines to the customer to proceed in conjunction with their advisors or Privacy and Data Protection department of their organization/company to use Noray's applications in a manner consistent with the GDPR. Noray is not responsible for such compliance and disclaims any form of non-implementation of the guidelines displayed and reported in a timely manner in this document.

Introduction

On May 25, 2018, the General Data Protection Regulation (GDPR, EU Regulation 2016/679) comes into force. This European privacy and security regulation sets a new global standard for privacy, security and compliance rights and is primarily about protecting and enabling individuals' privacy rights.

The GDPR establishes strict privacy requirements governing how organizations manage and protect personal data while respecting individual choice, regardless of where the data is sent, processed or stored. To access the full text of the standard you can use the following link: https://www.boe.es/doue/2016/119/L00001-00088.pdf

Objectives of the document

The purpose of this document is, therefore, to give some recommendations about the main milestones to be covered by your organization, as well as to delimit Noray's responsibilities in each of them.

In any case, we encourage you to work with appropriately qualified professionals to discuss the GDPR, to verify how it will apply specifically to your organization, and to determine how best to ensure compliance with the standard in question.

Backup copies

Your organization is responsible for making regular backups, and will make its own backups so that in the event of a loss of information or data, the process of recovering the information can be carried out correctly. Noray recommends that you make such copies periodically and check the contents of the copies to ensure their wholesomeness.

Noray shall not be liable in any case for the loss of information suffered by the customer when it is due to computer failures or lack of proper backups by the customer.

When using a contracted service in the cloud provided by Noray, Noray will require the hosting service provider to guarantee the correct performance of the same. These guarantees will be published on www.noray.com.

Access passwords

Your organization will be responsible for creating access profiles and providing a username and password for your staff, which must be changed by each of them. Noray's application facilitates the control of users and can implement the level of complexity and extension of the same, as well as the periodicity of the change of the same, which must be established by the client.

Noray recommends providing each user with a password and informing them that they must change it, respecting the security parameters defined by the customer. We recommend the use of complex passwords with a minimum length of 8 alphanumeric characters.

Noray shall not be liable in any case for loss of information, nor for access to information by unauthorized personnel, nor for any penalties that the customer may incur for not adopting such security measure.

Noray will provide a tool in its applications so that in case a user enters his password wrongly, the user will be blocked when a limit of attempts established by your organization has been exceeded (it is recommended to block after 3 wrong attempts). You can consult the section 'Bloqueos de Usuarios' of this document where it is described how to activate it in each case. However, if you need assistance in this regard may require the services of Noray not considered within the services included in the maintenance contract signed and therefore will be billed based on the time spent on it and following the rules of displacement of the catalog of services published in www.noray.com.

Audit

Your organization may request from Noray a report on the performance/result of security audits related to GDPR compliance in Noray applications installed in your organization. This report will not be considered within the services included in the maintenance contract subscribed and therefore will be billed according to the time spent on it and following the rules of displacements of the catalog of services published in www.noray.com.

When using a contracted service in the cloud provided by Noray, Noray warrants through its hosting service provider that such system complies with appropriate security requirements and measures. These warranties will be posted on www.noray.com.

Access logs

Noray applications allow the activation of an access log, allowing you to set the period you want to keep this log, so Noray recommends you to activate these access logs in each of the applications to cover this requirement of the standard.

Noray will not be responsible in any case for the loss of information, or access to information by unauthorized personnel, as well as the lack of records of access to the application or penalties that may be incurred by the customer for not adopting this security measure.

You can consult the section 'Activación Log de Accesos' of this document where it is described how to activate it in each case. However, if you need assistance in this regard may require the services of Noray not considered within the services included in the maintenance contract signed and therefore will be billed based on the time spent on it and following the rules of displacement of the catalog of services published in www.noray.com.

Exercise of rights.

The GDPR allows data subjects to exercise various data subject rights (DSR) relating to their personal data. While the Noray applications have current tools and will add other capabilities in upcoming updates to help you respond to DSR requests, the decision to comply with the DSR request and its implementation is your responsibility.

Your organization will be responsible for processing such a request in accordance with your organization's established data protection protocols.
Noray shall not be liable in any case for the non-existence of records of data protection rights exercised by end customers and/or for any penalties that may be incurred by the customer for not adopting this security measure.

You can consult the section 'Gestión de Ejercicio de Derechos' of this document where it is described how to activate it in each case. However, if you need assistance in this regard may require the services of Noray not considering them within the services included in the maintenance contract signed and therefore will be billed based on the time spent on it and following the rules of displacement of the catalog of services published in www.noray.com.

Data quality

Noray applications allow to know the actions performed by an end customer, so that, based on these statistics, you can keep the data updated and if necessary cancel or delete those that are no longer necessary for the fulfillment of the purpose for which they were collected.

Duty of disclosure

Noray applications allow the inclusion of texts relating to the fulfillment of the duty of information in relation to the processing of personal data of end customers.

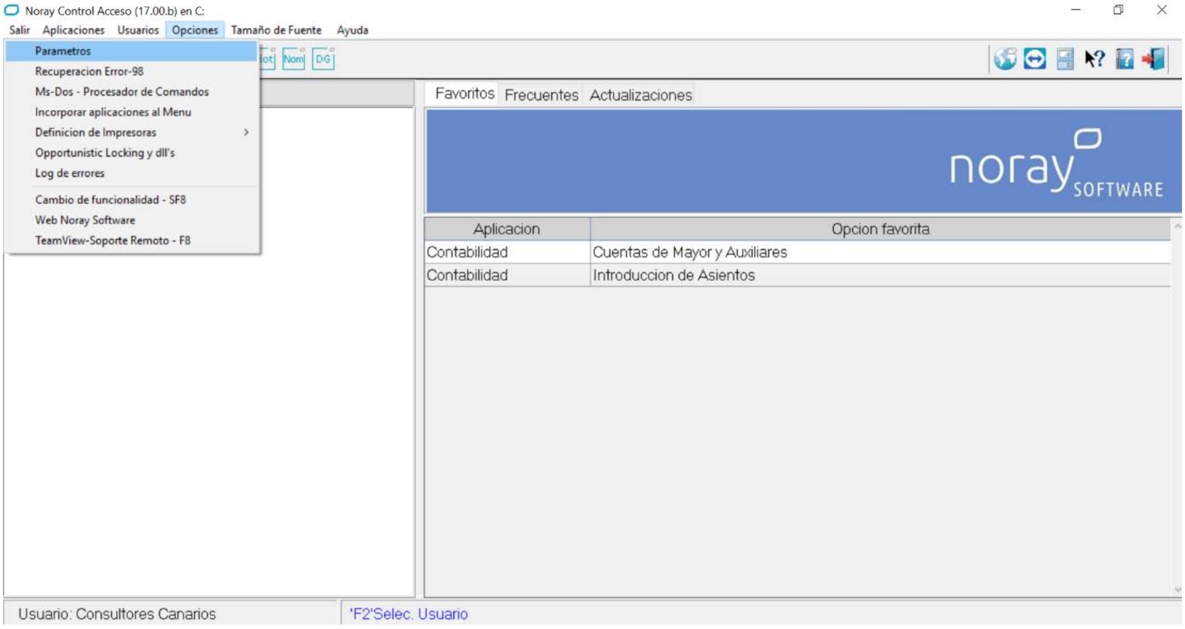
For this purpose, it is advisable to include in the documents to be delivered to customers such as invoices, travelers' entry forms, welcome cards, etc. .the policies and clauses foreseen for the processing of personal data in force for their inclusion, as well as, in compliance with the European Data Protection Regulation, to obtain the express consent for each of the data processing foreseen.

However, if you need assistance in this regard may require the services of Noray not considered within the services included in the maintenance contract signed and therefore will be billed based on the time spent on it and following the rules of displacement of the catalog of services published in www.noray.com.

Access Log Activation.

Noray Access Control.

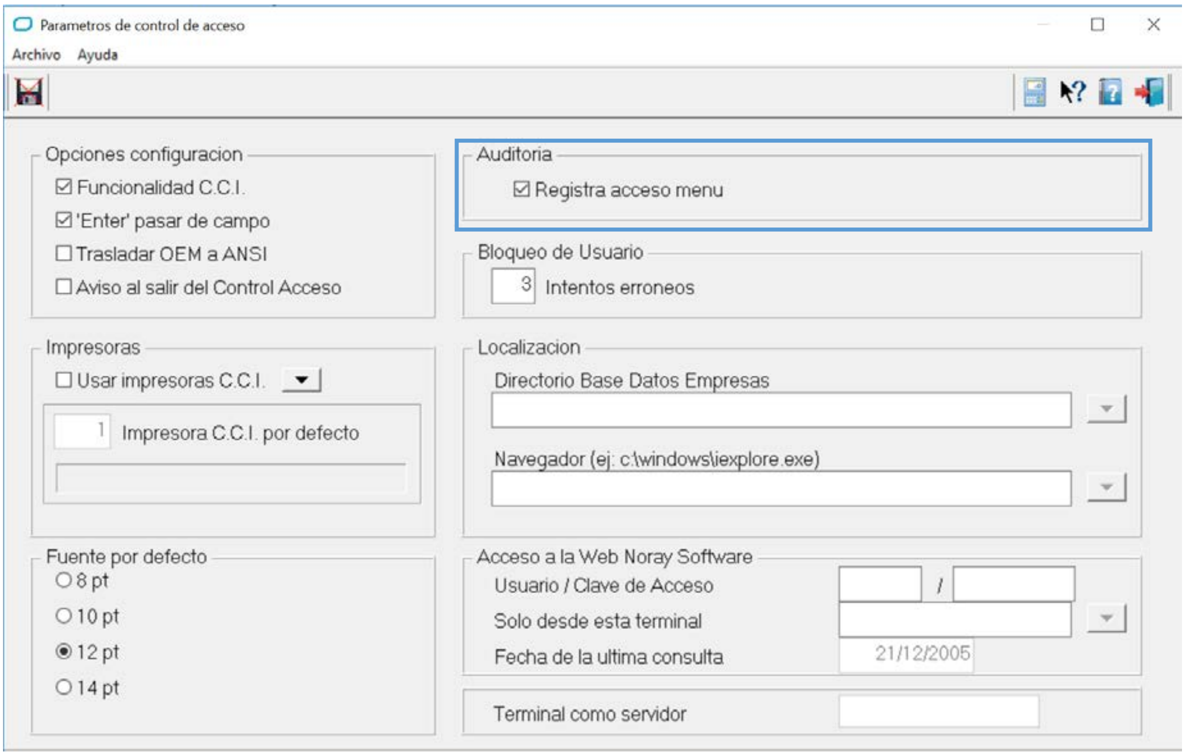
To activate the access control to the different Noray applications, simply access the Parameters through the Options menu and activate the corresponding checkbox shown in the image.



Aplicacion	Opcion favorita
Contabilidad	Cuentas de Mayor y Auxiliares
Contabilidad	Introduccion de Asientos

Usuario: Consultores Canarios

'F2'Selec. Usuario



Opciones configuracion
- ☑ Funcionalidad C.C.I.
- ☑ 'Enter' pasar de campo
- ☐ Trasladar OEM a ANSI
- ☐ Aviso al salir del Control Acceso

Auditoria
- ☑ Registra acceso menu

Bloqueo de Usuario
- 3 Intentos erroneos

Impresoras
- ☐ Usar impresoras C.C.I.
- 1 Impresora C.C.I. por defecto

Localizacion
- Directorio Base Datos Empresas
- Navegador (ej: c:\windows\iexplore.exe)

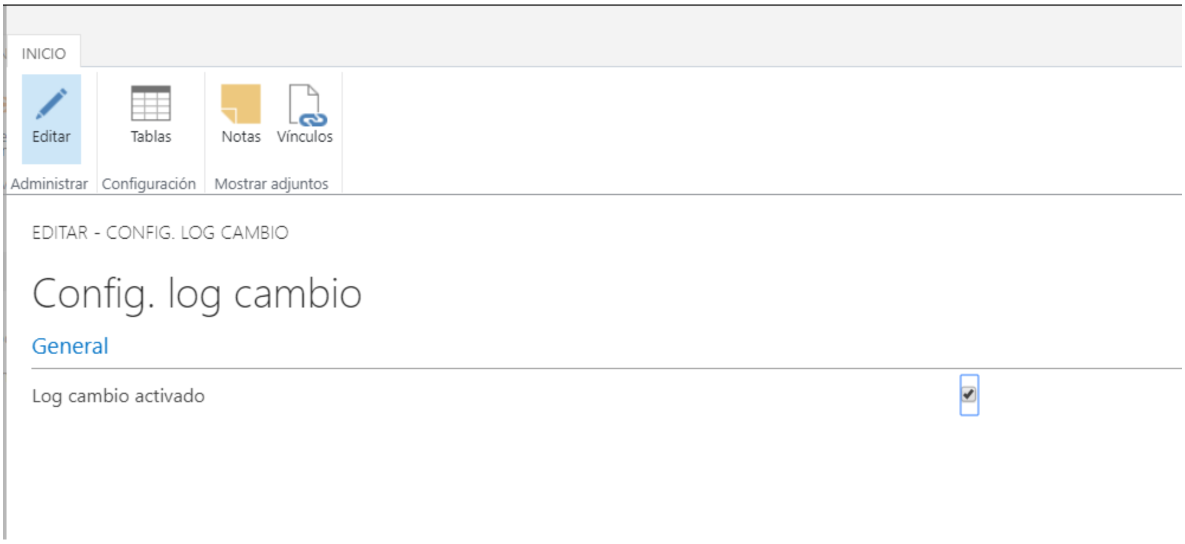
Fuente por defecto
- ○ 8 pt
- ○ 10 pt
- ● 12 pt
- ○ 14 pt

Acceso a la Web Noray Software
- Usuario / Clave de Acceso /
- Solo desde esta terminal
- Fecha de la ultima consulta 21/12/2005

Terminal como servidor

Noray Htl.

To activate the change log in Noray Htl you must access the Change Log Configuration option and activate it.



EDITAR - CONFIG. LOG CAMBIO

Config. log cambio

General

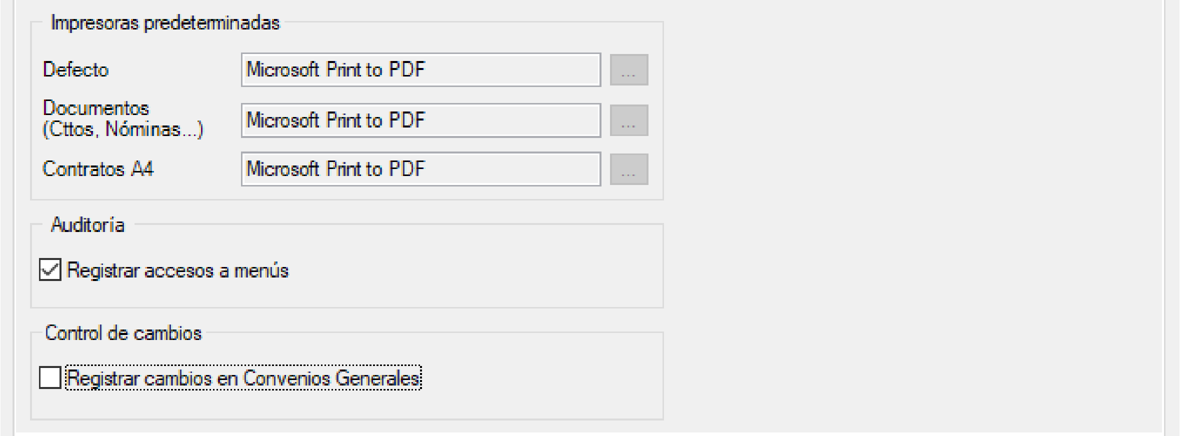
Log cambio activado ☑

Then, by means of the option Tables, establish the list of entities where you want to register this log. It must include those tables where personal data is recorded, such as: clients, suppliers, employees, resources, users, contacts, guests, documents where all of the above are included, etc.

While the Noray applications provide capabilities to record changes to certain entities it is your responsibility to ensure that personal and sensitive data is located and included in this list, as well as appropriately classified for your organization to meet its obligations under the GDPR.

Noray Nomina.

The Noray Nomina application includes the possibility of keeping a record of the modifications of some data made in the program. To do this you must access the general parameters and activate, next to the Logs field in the menu accesses, the change log flag.



Impresoras predeterminadas

Defecto	Microsoft Print to PDF
Documentos (Cttos, Nóminas...)	Microsoft Print to PDF
Contratos A4	Microsoft Print to PDF

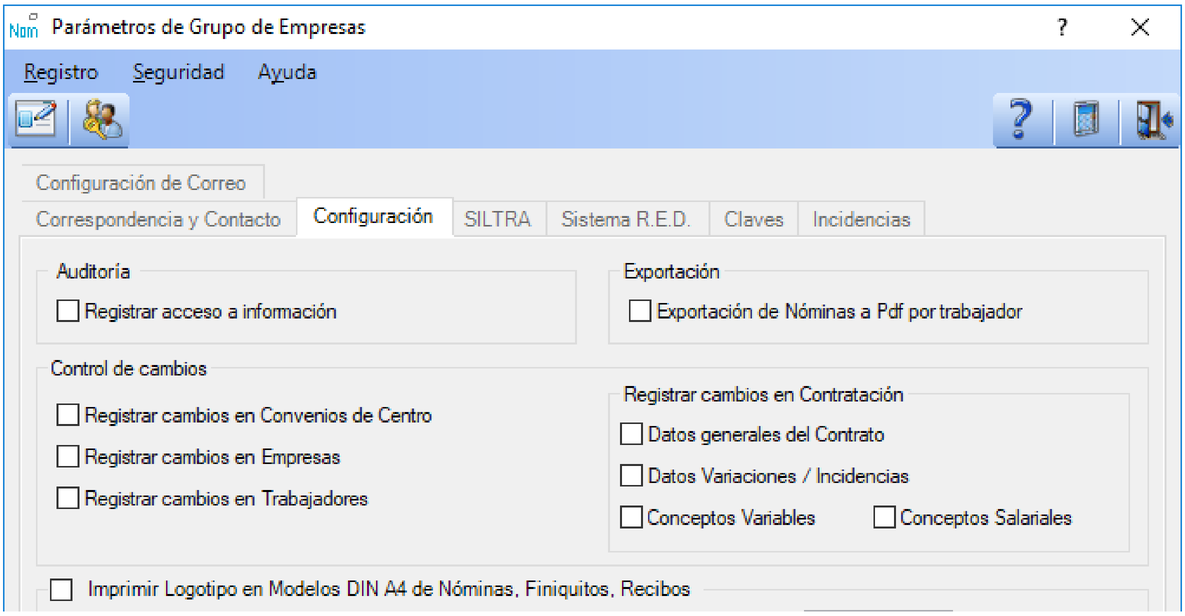
Auditoría

☑ Registrar accesos a menús

Control de cambios

□ Registrar cambios en Convenios Generales

In addition to these fields, there are also other fields within the group parameters for recording changes to other group data.



Parámetros de Grupo de Empresas

Auditoría

□ Registrar acceso a información

Exportación

□ Exportación de Nóminas a Pdf por trabajador

Control de cambios

□ Registrar cambios en Convenios de Centro

□ Registrar cambios en Empresas

□ Registrar cambios en Trabajadores

Registrar cambios en Contratación

□ Datos generales del Contrato

□ Datos Variaciones / Incidencias

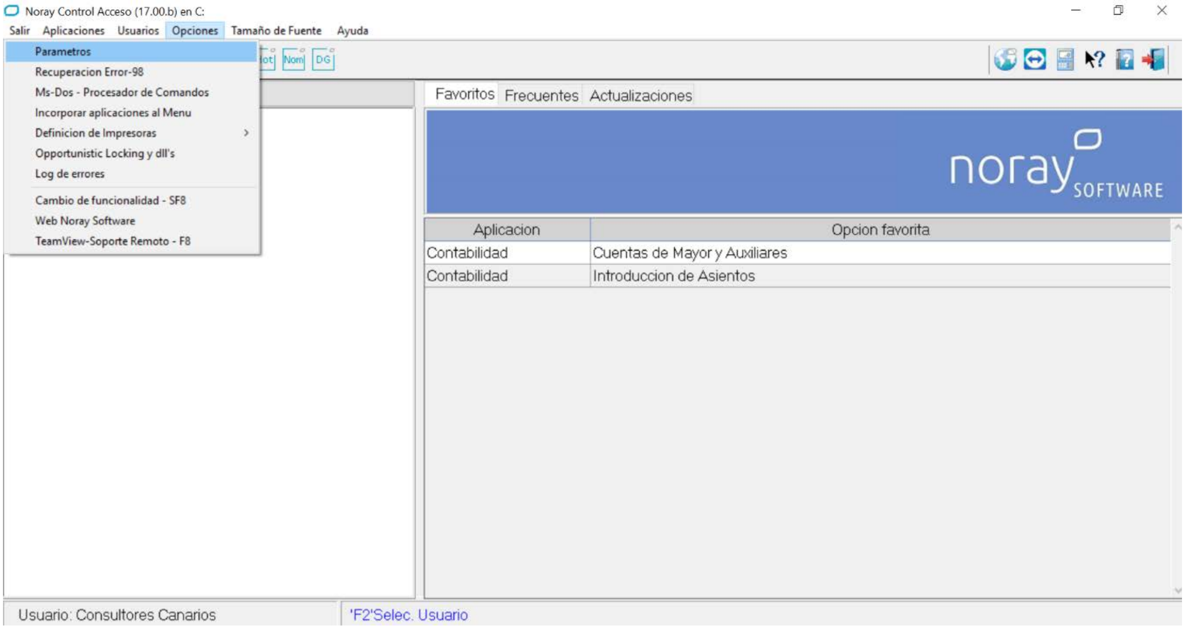
□ Conceptos Variables □ Conceptos Salariales

□ Imprimir Logotipo en Modelos DIN A4 de Nóminas, Finiquitos, Recibos

User lockouts.

Noray Access Control.

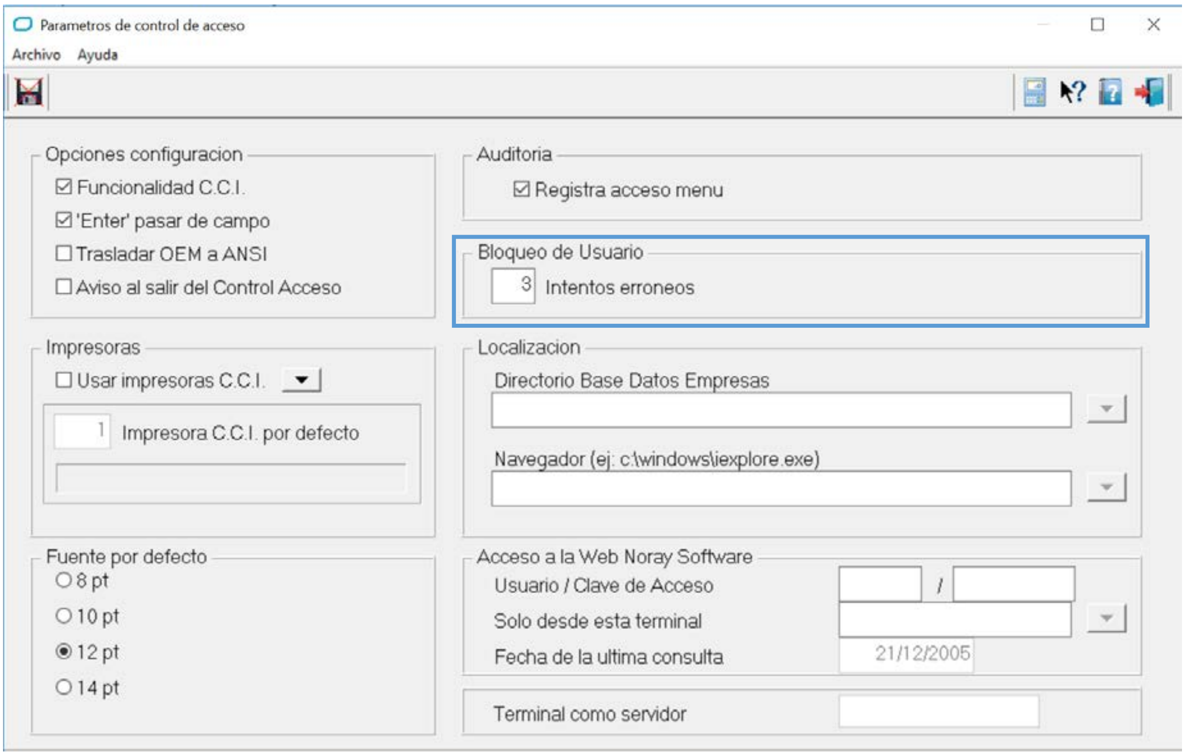
To configure the blocking of users in the different Noray applications, simply access the Parameters through the Options menu and determine the number of wrong password entry attempts that the user can be allowed before being blocked. Both to unlock the user and to modify/recover the user's passwords. A user with administrator privileges will be able to access the Users menu and act accordingly.



Aplicacion	Opcion favorita
Contabilidad	Cuentas de Mayor y Auxiliares
Contabilidad	Introduccion de Asientos

Usuario: Consultores Canarios

'F2'Selec. Usuario



Opciones configuracion

☑ Funcionalidad C.C.I.
☑ 'Enter' pasar de campo
☐ Trasladar OEM a ANSI
☐ Aviso al salir del Control Acceso

Auditoria

☑ Registra acceso menu

Bloqueo de Usuario

3 Intentos erroneos

Impresoras

☐ Usar impresoras C.C.I.

1 Impresora C.C.I. por defecto

Localizacion

Directorio Base Datos Empresas

Navegador (ej: c:\windows\iexplore.exe)

Fuente por defecto

○ 8 pt
○ 10 pt
● 12 pt
○ 14 pt

Acceso a la Web Noray Software

Usuario / Clave de Acceso /

Solo desde esta terminal

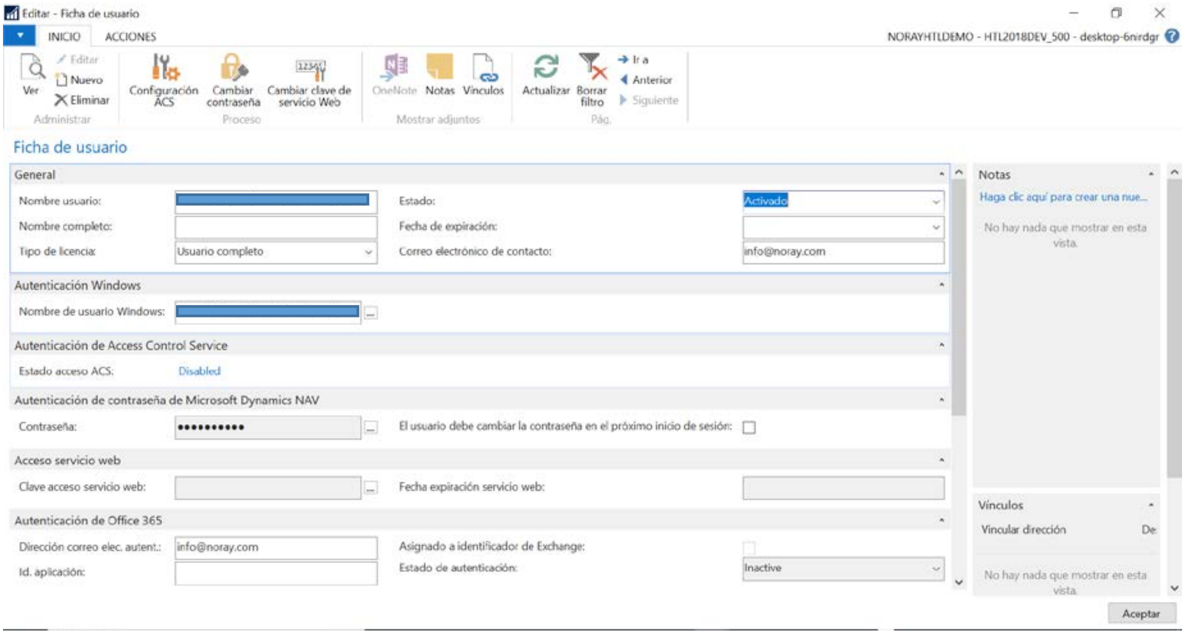
Fecha de la ultima consulta 21/12/2005

Terminal como servidor

Noray Htl.

In Noray Htl there are no restrictions or automatic lockouts for wrong password access attempts, although this can be configured in the operating system or your Office 365 account when using the Windows User or Office 365 methods for authentication in Noray Htl.

In any case, in the users tab of the application it is possible to block users by deactivating them, set password expiration dates or change passwords.



Ficha de usuario

General

Nombre usuario: [redacted]

Nombre completo:

Tipo de licencia: Usuario completo

Estado: Activado

Fecha de expiración:

Correo electrónico de contacto: info@noray.com

Autenticación Windows

Nombre de usuario Windows: [redacted]

Autenticación de Access Control Service

Estado acceso ACS: Disabled

Autenticación de contraseña de Microsoft Dynamics NAV

Contraseña: ••••••••••

El usuario debe cambiar la contraseña en el próximo inicio de sesión: ☐

Acceso servicio web

Clave acceso servicio web:

Fecha expiración servicio web:

Autenticación de Office 365

Dirección correo elec. autent.: info@noray.com

Id. aplicación:

Asignado a identificador de Exchange: ☐

Estado de autenticación: Inactive

Notas

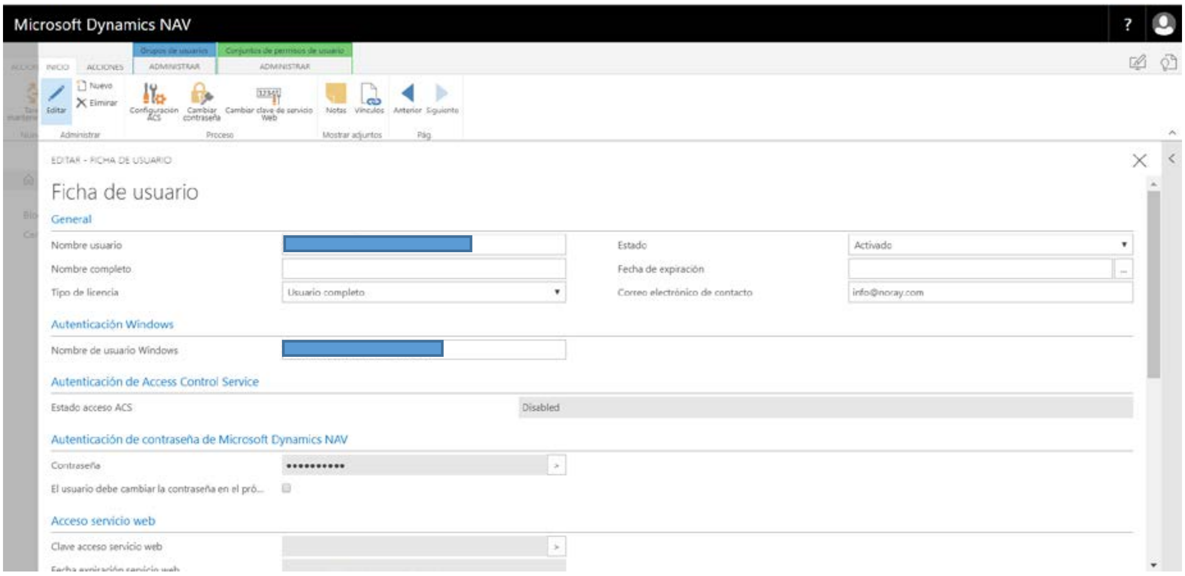
Haga clic aquí para crear una nue...

No hay nada que mostrar en esta vista.

Vínculos

Vincular dirección De

No hay nada que mostrar en esta vista.



EDITAR - FICHA DE USUARIO

Ficha de usuario

General

Nombre usuario	[redacted]	Estado	Activado ▾
Nombre completo		Fecha de expiración	...
Tipo de licencia	Usuario completo ▾	Correo electrónico de contacto	info@noray.com

Autenticación Windows

Nombre de usuario Windows	[redacted]

Autenticación de Access Control Service

Estado acceso ACS	Disabled

Autenticación de contraseña de Microsoft Dynamics NAV

Contraseña	••••••••••• >
El usuario debe cambiar la contraseña en el pró...	□

Acceso servicio web

Clave acceso servicio web	>
Fecha expiración servicio web	

Exercise of rights management

Data portability

The GDPR allows an individual to make a request for portability of their data to another organization, which means, in part, that you must export the data subject's personal data from your systems and provide it in a structured, commonly used format.

Once personal data is identified and located in the Noray application, it can be exported to an Excel file to facilitate a data portability request. Using Excel, you can edit the personal data to be included in the request and save the data in a general-purpose, machine-readable format, such as. csv or. Xml.

While Noray applications provide capabilities to export and therefore access personal data, it is your responsibility to ensure that personal and sensitive data is appropriately located and classified for your organization to meet its obligations under the GDPR.

Data deletion

The GDPR allows an individual to make a request to your organization to delete his or her personal data. Noray applications offer you several methods to correct inaccurate or incomplete personal data, or to delete personal data with respect to a data subject using the personalization capabilities, but the decision and implementation is your responsibility.

In some cases, you may choose to use the application screens to directly edit your data, such as modifying or deleting a contact. You should be aware that deleting some data from Noray applications may cause them to not be able to perform processes correctly, such as payroll calculation in Noray Payroll if employee data is deleted.

Certain types of application records, namely business transaction records (such as general, customer, tax transactions) are essential to the integrity of the enterprise resource planning system. Therefore, modification of personal data in such records is restricted.

While Noray applications provide capabilities to delete personal data, it is your responsibility to ensure that personal and sensitive data is located and classified appropriately for your organization to meet its obligations under the GDPR.

Modification of data

The GDPR allows an individual to make a request to your organization for the rectification of inaccurate personal data concerning the data subject.

Noray applications offer your organization the following methods to correct inaccurate or incomplete personal data. In some cases, you can export data to Excel to quickly edit multiple Noray records and then re-import the data. You can also modify stored personal data by manually editing the field containing the personal data, such as editing information about a customer in their record.

Certain types of application records, namely business transaction records (such as general, customer, tax transactions) are essential to the integrity of the enterprise resource planning system. Therefore, modification of personal data in such records is restricted.

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.

Cancellation of data.

The GDPR allows an individual to make a request to your organization to restrict the processing of their personal data. When you receive such a request from a data subject, you can mark his or her record as blocked or with inactive status due to privacy. Noray Applications will then discontinue processing that data subject's personal data.

When a record is marked as locked or inactive, you cannot create new transactions using that record. For example, you cannot create a new invoice for a customer when the customer or salesperson is locked.

While Noray applications offer capabilities to cancel personal data, it is your responsibility to ensure that personal and sensitive data is located and classified appropriately for your organization to meet its obligations under the GDPR.

Rights applications.

Since individuals can make multiple requests under the GDPR, you are expected to keep track of all incoming requests and actions you take as a result of a request.

Although this record of requests is not contemplated in the Noray applications, there are multiple alternatives in office automation tools, databases, spreadsheets, etc. That offer capabilities to track requests for rectification, deletion or transfer of personal data of the data subject. It is your responsibility to ensure that personal and sensitive data is appropriately located and classified for your organization to meet its obligations under the GDPR.

Detecting and responding to security system failures.

As a data controller or data processor, the GDPR obliges your organization to inform and notify the relevant supervisory authority, the affected data subjects and/or data controller of certain types of personal data breaches.
When running Noray applications on your own premises or that of a partner, it will be your responsibility to monitor and detect data breaches so that you can meet the applicable notification requirements for any incidents and within the periods defined in the GDPR.

Recommendations on compliance of GPRD UE Art. 32 "Security of processing"

NORAY recommends the following basic rules to its Customers

- Have a backup plan.
- That the backups are performed automatically (preferably).
- That the copies are made every day. It is interesting to maintain separate copies of several days in order to have "several options" at the time of resorting to them after a loss.
- Periodically check that they are being made: check the folder where the copies are stored, check that the dates of the copy files are up to date and check that the sizes of these files are of more or less similar sizes or are growing.

Periodically duplicate the copies to an external support (USB disk, cloud storage, etc.). With this we will avoid losing the information in case of having an accident in our offices and losing all the hardware (copies included).