

Manual operacional para usuario final	Página: 1
Obtención, Envío y Grupos de Acceso	Enero 2019
Departamento de operaciones	Versión 5.0



Obtención, Envío y Grupos de Acceso.



INGRESSIO MEXICO S.A DE C.V



+52(55)90000734 a 36



info@ingressio.com



www.ingressio.com

Manual operacional para usuario final	Página: 2
Obtención, Envío y Grupos de Acceso	Enero 2019
Departamento de operaciones	Versión 5.0

Contenido

Introducción	3
Obtención de datos biométricos.....	7
Consideraciones de proceso:	7
Está compuesto por:	9
Grupos de Acceso	10
Creación de Grupos de acceso:	11
Configuración de Grupos de Acceso:	12
Consolidación	13
Consolidación de Lectores.	16



Introducción

En este manual se describen los procesos de configuración y operación de las herramientas de sistema que nos permiten gestionar la transacción de la información entre sistema y los dispositivos biométricos vinculados a cuenta, esta gestión tiene la funcionalidad de “Obtener” y “Enviar” desde sistema los datos de Empleado, los Datos Biométricos y la configuración de parámetros del Tipo de Autenticación de cada empleado, igualmente se describe la lógica de operación para el control de asistencia y control de acceso mediante la configuración de Grupos de Acceso.

A continuar se describe los detalles técnicos sobre los parámetros a interactuar entre sistema y lectores biométricos.

Datos de Empleado:

Se identifica como el Número de Empleado con el cual se registró al empleado mismo en sistema:

Número de Empleado	Nombre Completo	Grupo	Área	Departamento	Puesto	Estatus
2419	Alejandra Lopez Mendoza	001 - Default	001 - Default	001 - Default	001 - Default	1 - Alta

Figura 1. Catálogo de empleados.

La funcionalidad del parámetro se hace visible con el proceso de Consolidación o Envío ya que con el mismo son creados en dispositivos biométricos destino los empleados enviados en dicho proceso, en el caso de ya estar creado el empleado en dispositivo biométrico destino se planchará sobre el número de empleado existente el resto de parámetros enviados en proceso.

Dato Biométrico:

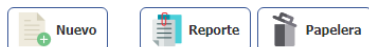
Se identifica con el dato biométrico como huella, rostro, iris o complemento de identificación como código de tarjeta de proximidad o contraseña asociado a un empleado:

Figura 2. Configuración de Datos Biométrico.



Este tipo de dato puede estar almacenado directamente en base de datos si hacemos uso de lectores biométricos del tipo USB, igualmente si en algún momento hemos ejecutado un proceso de obtención de datos biométricos para unificar la información en base de datos o puede estar repartida entre nuestros dispositivos biométricos robustos si el proceso de enrolamiento de datos biométrico se realiza directamente en dichos dispositivos en base a la ubicación física laboral de nuestros empleados, para validar es estado actual en base de datos de nuestros empleados con respecto a este parámetro debemos generar un reporte de Biométricos para identificar dicha asociación.

Catálogo de Empleados



Mostrar Empleados con Estatus Baja Temporal



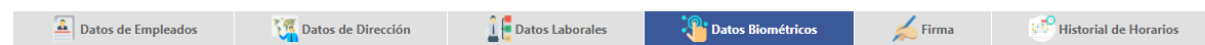
Arrastre una columna aquí para agrupar por esa columna						
Número de Empleado	Nombre Completo	Grupo	Área	Departamento	Puesto	Estatus
00001	Administrador Administrador Administrador	001 - Default	001 - Default	001 - Default	001 - Default	1 - Alta
31	Jorge Sanchez z	403 - Ingressio Queretaro	102 - Operaciones	202 - Operaciones	304 - Ingenieria y Mecatronica	1 - Alta
13	Norberto David Gonzalez Romero	402 - Ingressio México	102 - Operaciones	202 - Operaciones	303 - Gestion de Proyectos	1 - Alta
11	Juan Mendiola Rodriguez	402 - Ingressio México	102 - Operaciones	202 - Operaciones	302 - Sопorte Tecnico	1 - Alta
69	Alfonso Etian Anton Alvarez	402 - Ingressio México	103 - Ventas	203 - Ventas	306 - Ejecutivo de Venta	1 - Alta
10	Yesenia Webber Johnson	403 - Ingressio Queretaro	104 - Administración	204 - Administración	309 - Administrador	1 - Alta

Figura 3. Reportes de Biométricos enrolados.

Tipo de Autenticación:

Se identifica como la regla que define el o los elementos de identificación válidos para el empleado o considerar para su registro exitoso en los dispositivos biométricos robustos:

Catálogo de Empleados



Enrolamiento TCP/IP Viridi - Hanvon

Es Administrador

Tipo de Autenticación AC2100 AC5000 AC6000

Tipo de Autenticación AC7000

Tipo de Autenticación ZK (Huella)

Tipo de Autenticación ZK (Facial)

Contraseña (Solo números)

Código de Tarjeta

Figura 4. Configuración de Datos Biométricos.



Este parámetro es tanto obtenido como enviado con los procesos correspondientes y es de vital importancia su correcta configuración en sistema ya que si la misma no lo es el empleado puede quedar deshabilitado en los dispositivos biométricos robustos por no tener asociado este parámetro de manera funcional acorde a los modelos de dispositivos asociados a nuestra cuenta.

Descripción de escenarios a cubrir.

(A) Obtención de empleados desde dispositivos biométricos a base de datos:

Se presenta cuando el alta y enrolamiento de usuario “empleado” se realiza directamente en dispositivos biométricos robustos y se requiere concentrar la información biométrica del empleado, así como su configuración de Tipo de Autenticación en sistema o base de datos para su resguardo y posterior replica a dispositivos biométrico robustos.

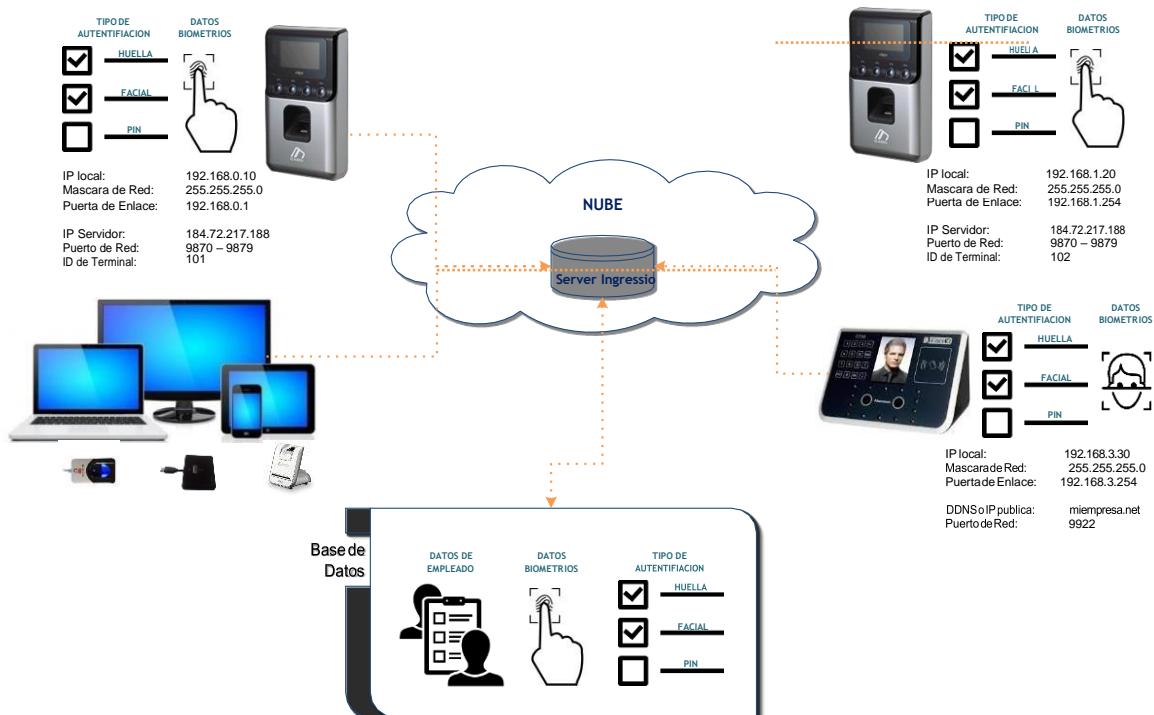


Figura 5. Diagrama de Obtención.

(B) Envío de registros de empleados desde base de datos a dispositivos biométricos:

Se presenta cuando realizamos el alta, enrolamiento y configuración del tipo de autenticación empleados directamente en sistema mediante dispositivos biométricos USB o ya tenemos almacenada la información de empleados obtenida desde otros dispositivos biométricos del tipo robusto y necesitamos replicar la información de empleados a otros dispositivos biométricos robustos de la empresa.

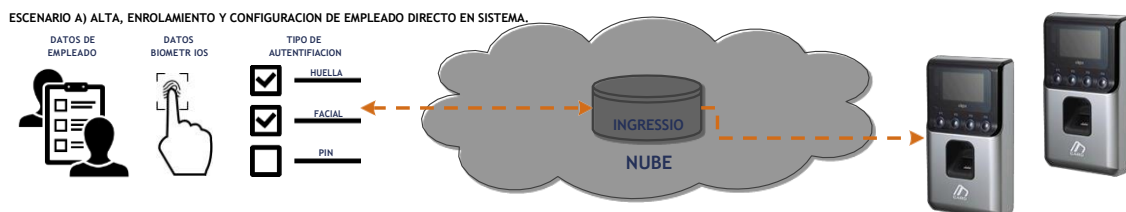


Figura 6. Diagrama de Consolidación/Envío.



(C) Gestión selectiva de envío de datos de empleados para su registro de asistencia y control de acceso para la apertura de puertas o dispositivos de interacción electromecánica:

Se presenta cuando requerimos que no todos los empleados puedan registrar y apertura “accesos” desde todos los dispositivos biométricos de la empresa para lo cual se necesita configurar la relación “**Biométricos<->Empleados Permitidos**” y su posterior envío a través de la lógica de Grupos de Acceso a los lectores biométricos robustos de la empresa.

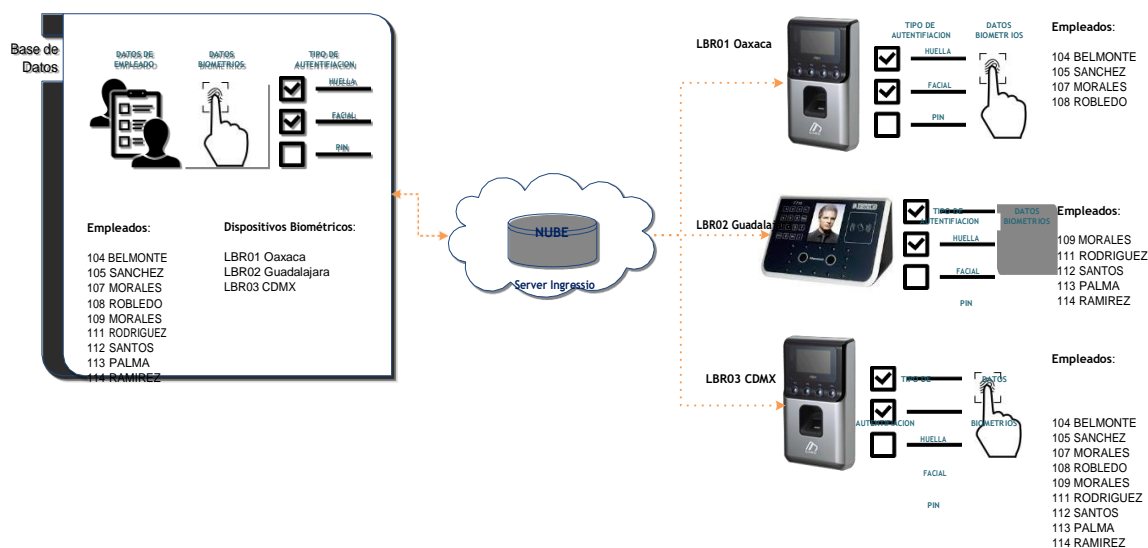


Figura 7. Diagrama de Lógica para Grupos de Acceso.

Glosario:

Dato biométrico: se define como el parámetro de identificación de empleado sea este biométrico (Huella, Rostro, Iris, Venas) o de otro tipo de identificación (Tarjeta de Proximidad o Contraseña).

Enrolamiento: proceso de registro de un dato o combinación de datos biométricos a empleado concreto para su autenticación.

Tipo de Autenticación: configuración de la combinación de datos biométricos enrolados a empleado que le permiten a dicho empleado realizar exitosamente su registro de acceso, esta configuración se basa en una lógica binaria “AND” y “OR” para su ejecución.

Grupo de Accesos: catálogo de la estructura organizacional que nos permite asociar dispositivos biométricos y empleados para su gestión selectiva y permitir o no su registro de asistencia y de acceso en dispositivos biométricos asociados.



Obtención de datos biométricos

En este módulo se describen el procedimiento de configuración de los parámetros para la obtención y orden en que el sistema solicita los datos biométricos almacenados en dispositivos biométricos para finalmente impórtalos o almacenarlos en la base de datos asociada al a cuenta.

Consideraciones de proceso:

- Es importante remarcar la importancia de la columna orden, ya que si existen empleados que se encuentren registrados en más de una terminal los datos de cada terminal se integraran o sustituirán los datos del proceso de obtención de la terminal anterior, es decir la última terminal con el número de orden mayor será la que envíe y finalmente almacene los datos biométricos del empleado en cuestión.
 - Integrará datos si estos son de tipo diferente.
 - Sustituirá si estos son de tipo similar: Huella, Rostro, Iris, Contraseña, Código de Tarjeta de Proximidad, Tipo de Autenticación.
- Para un proceso exitoso previamente debemos validar la correcta sincronización de nuestros lectores biométricos a la cuenta Ingressio relacional.
- El número de empleado debe existir en ambos extremos del proceso Sistema y Dispositivo Biométrico.

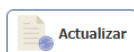
Proceso	Prerrequisitos	Manual
Obtención de Biométricos	Proceso de alta y enrolamiento de empleados en sistema.	INGMTO-102- InicioOperacionesNube
	Proceso de alta de empleados en dispositivo biométrico origen.	INGMTO-100- Instalación Configuración Dispositivos Biométricos

Tabla 1. Prerrequisitos para proceso de obtención.



Para la configuración de este proceso nos ubicamos en la opción de menú **Lectores-> Configuración de Obtención de Biométricos AC/Hanvon.**

Configuración Para la Obtención de Datos Biométricos de Terminales AC



Arrastre una columna aquí para agrupar por dicha columna								
Orden	Habilitar Poleo	Terminal	Puerto	Modelo	Obtener Huellas	Obtener Caras	Obtener Tarjetas	Tipo de Autenticación
1	<input checked="" type="checkbox"/>	2418	9877	Virdi AC-2100 PLUS	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
2	<input checked="" type="checkbox"/>	2437	9872	Virdi AC-7000	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>

Figura 8. Ventana: Lectores-> Obtención de Datos Biométricos AC.

Configuración Para la Obtención de Datos Biométricos Hanvon



Arrastre una columna aquí para agrupar por dicha columna						
Orden Poleo	Habilitar Poleo	Dirección IP	Puerto	Modelo	Obtener Caras	Obtener Tarjetas
1	<input checked="" type="checkbox"/>	187.138.21.153	9922	Hanvon F110	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Figura 9. Ventana: Lectores-> Obtención de Datos Biométricos Hanvon.

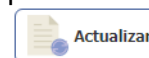


Está compuesto por:

Campo	Descripción
Orden	Puede mover las terminales hacia arriba o hacia abajo para establecer un orden. Este orden se tomará en cuenta a la hora de obtener los datos biométricos de las terminales, si hay varias terminales activas la última tiene prioridad sobre las anteriores, es decir, sustituirá los datos biométricos de las terminales anteriores en caso de que uno o varios usuarios estén registrados en varios lectores.
Habilitar	Indica si la terminal será tomada en cuenta para obtener los datos biométricos que tenga almacenados.
Huellas	Indica si se obtendrán las huellas de los usuarios almacenadas en la terminal.
Caras	Indica si se obtendrán las caras de los usuarios almacenadas en la terminal. (Sólo terminales AC7000 y Hanvon F710).
Tipo de Autenticación	Indicar si se obtiene el parámetro de identidad para el registro de empleado en base a la combinación de datos biométricos con que cuenta el empleado en cada dispositivo (Tecnología Virdi).

Tabla 2. Lectores-> Obtención de Datos Biométricos

Una vez que terminad la configuración sólo deberá dar clic el en botón Actualizar para que los cambios queden almacenados y el proceso se ejecute todos los días a partir de las 21:00 horas en base a nuestra programación estratégica de proceso masivos, por lo cual garantizamos la ejecución exitosa de proceso mismo en las siguientes 24 horas.



Grupos de Acceso

En este módulo se describen los procesos para la configuración de la herramienta que nos permite generar un catálogo de Grupos de Acceso como una estructura organizacional para la asignación de empleados y dispositivos biométricos lo cual nos permite el envío de datos de empleado y datos biométricos desde el sistema a determinados dispositivos biométricos y con esto generar una estructura de seguridad para la restricción de accesos del personal.

Consideraciones de proceso:

- Este proceso implica el conocimiento de operación de la opción de **Consolidación** descrita en un capítulo anterior en este manual ya que el envío de datos de empleado acorde a grupos de acceso se ejecuta desde el sistema Ingressio hacia los dispositivos biométricos mediante la operación mencionada.
- Un grupo de acceso puede contener uno o varios dispositivos biométricos pero un dispositivo biométrico no puede estar asignado a dos o más grupos de acceso.
- Un grupo de accesos puede contener “n” cantidad de empleados asignados a diferentes grupos de acceso.

ESCENARIO C) ESTRUCTURA ORGANIZACIONAL PARA EL CONTROL DE ASISTENCIA Y ACCESO RESTRINGIDO

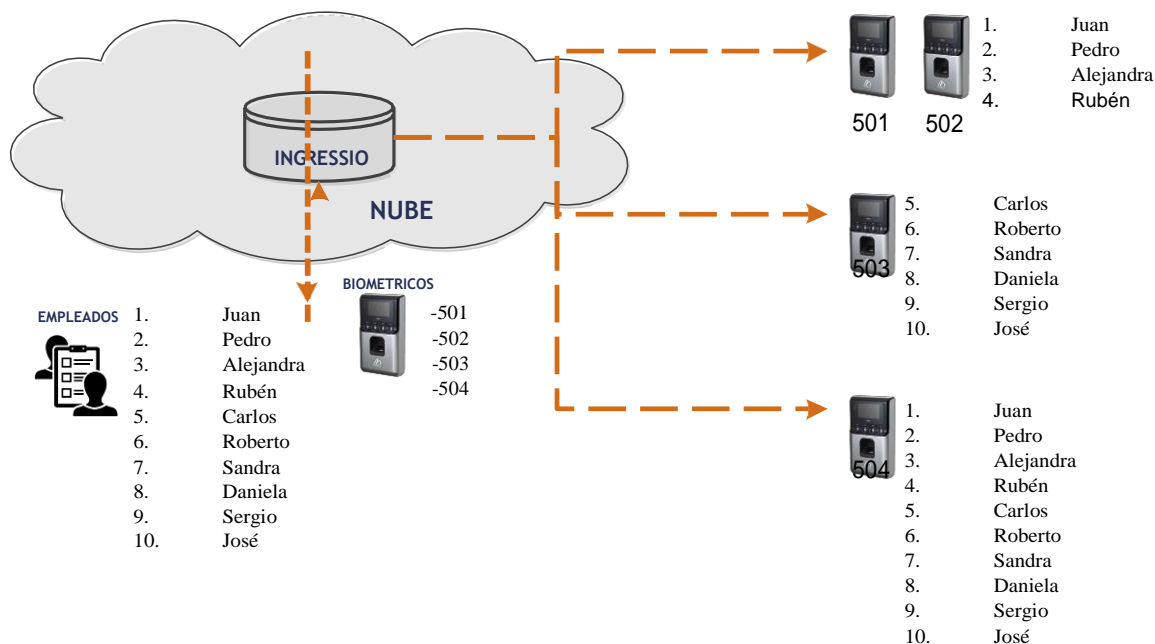


Figura 13. Esquema lógico de configuración de Grupos de Acceso.

Creación de Grupos de acceso:

Ingresamos a esta ventana de configuración a través de la opción de menú **Recursos Humanos -> Catálogos Organizacionales -> Grupos de Acceso.**

Catálogos Organizacionales

G Grupos		A Áreas		D Departamentos		P Puestos		GA Grupos de Acceso	
Reporte PDF		Reporte Grupo de Acceso		Reporte XLSX		Estadística			
+	Clave	Grupo de Acceso	Empleados Asignados	Empleados Activos	Total de Lectores	Lectores Asignados	Comentarios		
	102	Ingreso México	4	4	2	Demo2017 - Demo2017 - ENTRADA PRINC...			
	103	Ingreso Queretaro	2	2	2	_ENROLLLLL - ZKENROLLLLL - ZK - RFID &...			
	104	URU	0	0	1	HJ898GIG - 70980UHJ898 - URU-01			

Figura 14. Consulta de Grupo de Acceso

Agregar un nuevo Grupo de acceso: Para Agregar un nuevo Grupo de acceso desde la pantalla de consulta de clic en el botón (+), enseguida abrirá la pantalla de Edición donde deberá introducir la información correspondiente a cada campo.

Catálogos Organizacionales


G Grupos		A Áreas		D Departamentos		P Puestos		GA Grupos de Acceso	
Reporte PDF		Reporte Grupo de Acceso		Reporte XLSX		Estadística			
+	Clave	Grupo de Acceso	Empleados Asignados	Empleados Activos	Total de Lectores	Lectores Asignados	Comentarios		
Clave:									
Grupo de Acceso:									
Comentarios:									
	102	Ingreso México	4	4	2	Demo2017 - Demo2017 - ENTRADA PRINC...			
	103	Ingreso Queretaro	2	2	2	_ENROLLLLL - ZKENROLLLLL - ZK - RFID &...			
	104	URU	0	0	1	HJ898GIG - 70980UHJ898 - URU-01			

Figura 15. Pantalla alta de Grupo de Acceso

La pantalla tiene una etiqueta "Campos obligatorios *" señalando con un * todos los campos que son obligatorios. Si faltan campos obligatorios estos serán marcados indicando cuales hacen faltan. El sistema informará que los datos se han insertado correctamente, finalmente para guardar el nuevo grupo damos clic en el botón.



Configuración de Grupos de Acceso:

Ingresamos a esta ventana mediante la opción de menú **Humanos -> Catálogos Organizacionales -> Grupos de Acceso** en esta nueva ventana seleccionamos el Grupo de Acceso a Configurar seleccionando el símbolo del engrane  para posteriormente seleccionar e integrar tanto los dispositivos biométricos y grupo de empleados a relacionar en base a las reglas de funcionalidad de nuestro escenario laboral real y criterios de seguridad.

✕

Seleccione los lectores que pertenecerán a este Grupo de Acceso (1 Lector puede pertenecer únicamente a 1 Grupo de Acceso):

<input type="checkbox"/>	Clave	Nombre Lector	Número de Serie	Terminal	Grupo de Acceso Actual
<input checked="" type="checkbox"/>	Demo2017	ENTRADA PRINCIPAL	Demo2017	0	102 - Ingressio México
<input checked="" type="checkbox"/>	oac21i2018	AC2100 PLUS-(1)	001DEMO2018	2418	102 - Ingressio México
<input type="checkbox"/>	1313	Celular Ingressio	1313	0	
<input type="checkbox"/>	_ENROLLLLL	ZK - RFID & Huella & Contraseña (USB)- _ENROLLLLL	ZKENROLLLLL	0	103 - Ingressio Querétaro
<input type="checkbox"/>	1101	TACTIVO Mini-1101	1101	0	

9 Lectores

[Marcar Todos](#) | [Desmarcar Todos](#)
Filtrar Por: Todos los Lectores
 Guardar Configuración de Lectores

Seleccione los empleados que pertenecerán a este Grupo de Acceso (1 Empleado puede pertenecer a 1 o varios Grupos de Acceso):

<input type="checkbox"/>	Número de Empleado	Nombre Completo	Grupo	Área	Departamento	Puesto
<input checked="" type="checkbox"/>	2	Sebastian Altamirano Rodriguez	402 - Ingressio México	102 - Operaciones	202 - Operaciones	305 - Director de Operaciones
<input checked="" type="checkbox"/>	11	Juan Mendiola Rodriguez	402 - Ingressio México	102 - Operaciones	202 - Operaciones	302 - Soporte Técnico
<input checked="" type="checkbox"/>	13	Norberto David Gonzalez Romero	402 - Ingressio México	102 - Operaciones	202 - Operaciones	303 - Gestion de Proyectos
<input type="checkbox"/>			403 - Ingressio			304 - Ingeniería y

21 Empleados

[Marcar Todos](#) | [Desmarcar Todos](#)
Filtrar Por: Todos los Empleados
 Guardar Configuración de Empleados

Figura 16. Configuración de Grupos de Acceso

Debemos de seleccionar los lectores que pertenecerán al grupo de acceso que se este configurando, recordando la siguiente regla: *“1 Lector puede pertenecer únicamente a 1 Grupo de Acceso”* esto quiere decir que cuando un dispositivo se asocia a un grupo de acceso ya no puede ser electo para otro, sin embargo, un grupo de acceso puede tener varios lectores. Una vez realizado esto seleccionamos **Guardar Configuración de Lectores**.

Posteriormente debemos de seleccionar el personal que estará en cada grupo de acceso, los empleados si pueden estar en uno o varios grupos de acceso.



Consolidación

En este módulo se describen los procesos mediante los cuales configuramos y programamos el envío de nuestra carga de datos del tipo empleado, biométricos y autenticación desde nuestro sistema o base de datos hacia uno o varios dispositivos biométricos robustos registrados en nuestra cuenta.

Consideraciones de proceso:

Accedemos a esta herramienta mediante la opción de menú **Lectores-> Administración de Lectores Autónomos-> Nuevo**, las peticiones de consolidación a programar son las siguientes:

Petición	Prerrequisitos	Manual
Consolidación de Grupos de Acceso.	Proceso de alta y enrolamiento de empleados en sistema. Proceso de alta de estructura de grupos de acceso.	INGMTO-102 - Inicio Operaciones Nube
Consolidación de Lectores.	Proceso de alta de empleados en dispositivo biométrico origen.	INGMTO-100 - Instalación Configuración Dispositivos Biométricos

Tabla 3. Prerrequisitos para procedimiento de Consolidación

Consideraciones de proceso:

- Dependiendo de la Petición de "Consolidación" seleccionada, este proceso interactuara con un determinado grupo de dispositivos biométricos robustos.
- El proceso de consolidación se puede configurar para su ejecución de manera continua o única entendiéndose con esto que el proceso mismo se ejecutara todos los días "continuo" o solo una vez "único" a partir la fecha inicio programada.
- Debemos asegurar que los dispositivos biométricos involucrados en un proceso de consolidación cuenten con una correcta interconexión de red y corriente eléctrica durante el proceso mismo.
- Las peticiones de consolidación crean usuarios nuevos en dispositivos biométricos destino si estos no existiesen siempre y cuando el empleado en origen tenga enrolado algún dato biométrico compatible con el dispositivo biométrico destino.
- Es importante analizar y definir en base al grupo de datos biométricos asociados del empleado el tipo de autenticación del empleado como tal acorde al modelo de dispositivo biométrico destino ya que este parámetro está directamente relacionado a la correcta autenticación o registro del empleado en dichos dispositivos.



Accedemos esta herramienta mediante la opción de menú **Lectores-> Configuración de Lectores Autónomos**, en esta ventana podemos observar y monitorear el histórico de procesos de consolidación configurados y su estatus de actividad.

Administración Lectores Autónomos



Arrastre una columna aquí para agrupar por dicha columna				
Clave	Petición	Fecha Inicio	Fecha Fin	Estatus
1	Consolidación de Grupo de Acceso (ZK)	08/11/2018	31/12/2055	Proceso Continuo
2	Consolidación de Grupo de Acceso (VIRDI)	08/11/2018	31/12/2055	Proceso Continuo
3	Limpieza de Lectores (VIRDI)	08/11/2018	31/12/2055	Proceso Continuo

Figura 10. Ventana: Lectores-> Administración de Lectores Autónomos

Está compuesto por:

Campo	Descripción
Nuevo	Opción de acción para la generación de procesos de configuración.
Reporte	Opción de acción para la generación de reporte de consolidaciones configuradas.
Clave	ID de consolidación configurada.
Petición	Tipo de petición configurada en consolidación.
Fecha Inicio	Fecha inicio del proceso configurado.
Fecha fin	Fecha fin del proceso configurado.
Estatus	Validación de proceso realizado o activo.

Tabla 4. Lectores-> Administración de Lectores Autónomos



Consolidación de Grupo de Acceso.

En esta petición se solicita el envío tanto de datos de empleado y dato biométrico desde el sistema a un grupo de dispositivos lectores vinculados a un grupo de acceso, es decir, si se han agregado recientemente nuevos empleados un grupo de acceso, se enviarán los nuevos ID de empleados y actualizan las huellas hacia los lectores compatibles vinculados solo a el grupo de acceso seleccionado.

Administración Lectores Autónomos

*** Previo a esta configuración debemos crear nuestra lógica de Grupos de Acceso descrito en el apartado Grupos de Acceso de este manual operativo.**

Figura 11. Lectores-> Administración de Lectores Autónomos-> Nuevo/Consolidación de Grupos de Acceso

Está compuesta por:

Campo	Descripción
Clave	Este campo se completa automáticamente al realizar la petición, se mostrará el texto "En progreso" lo que indica que la acción está siendo procesada.
Petición	Se selecciona la petición solicitada, en este caso sería "Consolidación de Grupo de Acceso"
Grupo de acceso	Seleccionar el grupo de acceso del cual se desean actualizar las huellas de los lectores.
Estatus	Este campo siempre tendrá el texto "Proceso continuo" lo que indica que siempre se va a estar realizando esta acción, cada que se presenten nuevas huellas, pero también puede elegirse, proceso único (se ejecuta una sola vez) y proceso por rango (se ejecutará en determinadas fechas).
Fecha Inicio	Fecha en la que se dio de alta la petición.
Fecha fin	Última actualización de Huellas.

Tabla 5. Lectores-> Administración de Lectores Autónomos-> Nuevo/Consolidación de Empleados.



Consolidación de Lectores.

En esta petición se solicita actualizar todos los datos de empelado y datos biométricos compatibles de los empleados registrados en cualquier dispositivo biométrico VirDI de la empresa a otro grupo de lector, o bien desde la base de datos en la nube hacia un grupo de dispositivos biométricos seleccionados.

Administración Lectores Autónomos

Clave

Petición

* Próxima Limpieza: 21:00 Hrs

Incluir Empleados con Vacaciones

 Certif2018 - AC7000-01

 oac2112018 - AC2100 PLUS-(1)

Lector Destino

Estatus

Fecha Inicio

Campos Obligatorios *

Figura 12 Lectores-> Administración de Lectores Autónomos-> Nuevo/Consolidación de Lectores Servidor->Lector

Está compuesto por:

Campo	Descripción
Clave	Este campo siempre tendrá por default el texto "En progreso" para indicarle al usuario que su petición está siendo procesada.
Petición	Para este campo es necesario que se indique la opción "Consolidación de Lectores"
Lector	Seleccionar el nombre del lector de donde se va a transferir las huellas.
Lector destino	Seleccionar el nombre del Lector a donde se van a dirigirse las huellas.
Estatus	Este campo siempre tendrá el texto "Proceso continuo" lo que indica que siempre se va a estar realizando está acción, cada que se presenten nuevas huellas, pero también puede elegirse, proceso único (se ejecuta una sola vez) y proceso por rango (se ejecutará en determinadas fechas).
Fecha Inicio	Fecha hasta la cual se quieren las huellas, se recomienda indicar la del día de la petición.
Fecha Fin	Ultima fecha en la que se enviaron las huellas a otro lector.

Tabla 6. Lectores-> Administración de Lectores Autónomos-> Nuevo/Consolidación de Lectores



Manual operacional para usuario final	Página: 17
Obtención, Envío y Grupos de Acceso	Enero 2019
Departamento de operaciones	Versión 5.0

Una vez que termina la configuración sólo deberá dar clic el en botón Actualizar para que los cambios queden almacenados y el proceso se ejecute todos los días a partir de las 21:00 horas con base en nuestra programación estratégica de proceso masivos, por lo cual garantizamos la ejecución exitosa de proceso mismo en las siguientes 24 horas.

La configuración adecuada de estos procesos biométricos es necesaria para envíos en tiempo real, es decir, cuando se llevan a cabo enrolamientos centralizados con lectores USB en tecnologías VIRDI y ZKTeco. Las huellas pueden viajar en el momento a los lectores si se cumple lo siguiente:

- Procesos biométricos de consolidación previamente configurados.
- Lectores en línea al momento de hacer el envío.
- Drivers de lectores USB instalados.
- Permisos a Internet Explorer.

Es importante recordar lo siguiente:

- **Consolidaciones y obtenciones nocturnas:** Solo funcionan en tecnologías VIRDI y HANVON, esto debido a que el peso de los templates no es tan robusto como en la tecnología ZKTeco.
- **Envíos en tiempo real:** Solo está disponible para tecnologías VIRDI y ZKTeco, por lo tanto, la configuración de procesos biométricos en lectores de la marca ZKTeco solo funciona para este apartado.

