

# Plan de Homologación ENESEM

## Listado de control y acceso a información confidencial

### **INFOCAPT-ENESEM**

**DIRAD-GIAPE**  
INSTITUTO NACIONAL DE ESTADÍSTICA Y CENSOS

Julio 2021

Segundo semestre, 2021

## Índice de Contenido

Índice de Contenido.....	2
1. Antecedentes.....	3
2. Objetivo .....	3
3. Desarrollo .....	3
3.1 Checklist .....	3
3.2 Puntos clave .....	4
4. Conclusiones.....	7
5. Firmas .....	7

## Homologación de la Operación Estadística ENESEM

### 1. Antecedentes

En el año 2020, se planificó la ejecución de la Encuesta Estructural Empresarial (ENESEM) 2019, la cual levanta información de las empresas de los sectores de Manufactura, Minería, Construcción, Comercio y Servicios en el país; esto con el objetivo de satisfacer la necesidad de información sobre variables e indicadores económicos por parte de usuarios internos y externos. El resultado final de esta operación estadística es una publicación que se presenta en la página web del INEC.

La Gestión de Estadísticas Estructurales (GESE) se encarga de realizar la planificación para el levantamiento de la encuesta y publicación, la recolección de la información se lo realiza a través de la plataforma INFOCAPT, que la desarrolla y mantiene la Dirección de Registros Administrativos, adicional a esto la productora establece fechas de cortes de bases de la información ingresada en el aplicativo para proceder con la validación de la información y dar tratamiento de las variables, hasta obtener una base de datos validada.

A continuación, se detalla un listado para verificar el cumplimiento de los procedimientos que rigen el control y acceso a la información confidencial en las fases de recolección y procesamiento.

### 2. Objetivo

Desarrollar un documento de procesos internos de la operación estadística Encuesta Estructural Empresarial (ENESEM) que detalle:

- Establecer quien, como y cuando puede acceder a los activos de información de la empresa y registrar convenientemente dichos accesos

### 3. Desarrollo

#### 3.1 Checklist

A continuación, se incluyen una serie de controles para revisar el cumplimiento de la política de seguridad en lo relativo al **control de acceso al sistema INFOCAPT**.

Los controles se clasificarán en dos niveles de **complejidad**:

- **Básico (B)**: el esfuerzo y los recursos necesarios para implantarlo son asumibles. Se puede aplicar a través del uso de funcionalidades sencillas ya incorporadas en las aplicaciones más comunes. Se previenen ataques mediante la instalación de herramientas de seguridad elementales.

- **Avanzado (A):** el esfuerzo y los recursos necesarios para implantarlo son considerables. Se necesitan programas que requieren configuraciones complejas. Se pueden precisar mecanismos de recuperación ante fallos.

Los controles podrán tener el siguiente **alcance**:

- **Dirección de Estadísticas Económicas (DECON):** aplica a la dirección o al personal que gestiona la información.
- **Dirección de Registros Administrativos (DIRAD):** aplica al personal técnico especializado.
- **Otras Direcciones (OTROS):** aplica a todo el personal.

NIVEL	ALCANCE	CONTROL	
B	DECON	<b>Política de usuarios y grupos</b> Define los roles de usuarios y de grupos en función del tipo de información al que podrán acceder.	<input checked="" type="checkbox"/>
B	DECON	<b>Asignación de permisos</b> Asigna los permisos necesarios para que cada usuario o grupo de usuarios solo puedan realizar las acciones oportunas sobre la información a la que tienen acceso.	<input checked="" type="checkbox"/>
B	DIRAD	<b>Creación/modificación/borrado de cuentas de usuario con permisos</b> Define y aplica un <b>procedimiento</b> para dar de alta/baja o modificar las cuentas de usuario.	<input checked="" type="checkbox"/>
B	DIRAD	<b>Cuentas de administración</b> Gestiona las cuentas de administración de sistemas y aplicaciones teniendo en cuenta su criticidad.	<input checked="" type="checkbox"/>
A	DIRAD	<b>Mecanismos de autenticación</b> Determina e implanta las técnicas de autenticación más apropiados para permitir el acceso a la información de la empresa.	<input checked="" type="checkbox"/>
A	DIRAD	<b>Registro de eventos</b> Establece los mecanismos necesarios para registrar todos los eventos relevantes en el manejo de la información de la empresa.	<input type="checkbox"/>
B	DIRAD	<b>Revisión de permisos</b> Revisa cada cierto tiempo que los permisos concedidos a los usuarios son los adecuados.	<input type="checkbox"/>
B	DIRAD	<b>Revocación de permisos y eliminación de cuentas</b> Desactiva los permisos de acceso y elimina las cuentas de usuario una vez finalizada la relación contractual.	<input type="checkbox"/>

### 3.2 Puntos clave

Los puntos clave de esta política son:

- **Política de usuarios y grupos.** Se define una serie de grupos que tendrán determinados accesos para cada tipo de información establecido. Esta clasificación se puede hacer teniendo en cuenta los siguientes aspectos:
  - en función del área o departamento al que pertenezca el empleado;
  - en función del tipo de información a la que accederá;
  - en función de las operaciones permitidas sobre la información a la que se tiene acceso.

*En función de los criterios anteriores se puede establecer diversos perfiles de usuarios. Los perfiles de usuarios definidos en INFOCAPT-ENESEM son: Informante, Encuestador, Crítico, Revisor y Administrador.*

- **Asignación de permisos.** Una vez establecidos los tipos de información, los perfiles de usuarios y los grupos existentes, se puede concretar los tipos de acceso a la información a los que tienen derecho. Los permisos concretarán que acciones pueden realizar sobre la información (creación, lectura, borrado, modificación, copia, ejecución, etc.). Como norma general siempre se otorgará el **mínimo privilegio** en el establecimiento de los permisos.

*Los permisos que tiene el sistema son los siguientes:*

Perfil	Formulario	Observaciones
<b>Informante</b>	Crear Editar Enviar Imprimir	
<b>Encuestador</b>	Ver	
<b>Crítico</b>	Codificar Editar Enviar Imprimir	Crear
<b>Revisor</b>	Ver	Aprobar
<b>Administrador</b>	Ver	Aprobar

- **Creación/modificación/borrado de cuentas de usuario.** Para permitir el acceso real a los sistemas de información, se debe tener un **procedimiento** que permita gestionar la creación/modificación/borrado de las cuentas de acceso de los usuarios (por ejemplo: cuenta de correo, acceso al INFOCAPT, etc.) indicando quién debe autorizarlo. Se detalla los datos identificativos de las mismas, las acciones que se permiten y se dotará de las credenciales de acceso correspondientes que deberán ser entregadas de forma confidencial a sus dueños. Se incluirán asimismo parámetros tales como la caducidad de las contraseñas y los procedimientos de bloqueo oportunos. Se debe informar al usuario de estos requisitos al entregarle las credenciales, así como de la Política de contraseñas.

*Ese procedimiento se lo realiza solicitando por correo la creación o modificación de la cuenta de usuario.*

- **Cuentas de administración.** Las cuentas de administración permiten realizar cualquier acción sobre los sistemas que administran, por lo que deben ser gestionadas con la máxima precaución. Se tendrá en cuenta los siguientes aspectos:

- utilizar este tipo de cuentas únicamente para realizar labores que requieran permisos de administración;
- implantar un control de acceso basado en un doble factor de autenticación;
- registrar convenientemente todas sus acciones (registro de *logs*);
- cuando se accede a un sistema en modo administrador, este debe indicarnos claramente tal situación a través de su contexto;
- el acceso como administrador debería ser notificado convenientemente;
- evitar que los privilegios de las cuentas de administrador puedan ser heredados;
- las claves de acceso deben ser lo más robustas posibles y ser cambiadas con frecuencia;
- pueden ser sometidas a auditorías periódicas;

*En INFOCAPT la administración de cuentas solo lo puede hacer el usuario que tenga el perfil de administrador.*

- **Mecanismos de autenticación.** Se define e implanta los mecanismos de autenticación más adecuados para permitir el acceso a la información de la empresa. Se tendrá en cuenta aspectos tales como:

- utilizar mecanismos de autenticación internos o basados en servicios de autenticación de terceros (como la federación de identidades o el *social-login*)
- las tecnologías que utilizaremos:
  - autenticación vía web
  - servicios de directorio
  - LDAP
- factores de los mecanismos de autenticación (uno o varios):
  - algo que somos (a través de técnicas biométricas)
  - algo que sabemos (a través de contraseñas)
  - algo que tenemos (a través de dispositivos personales, *tokens* criptográficos)

*En base a lo escrito a este punto, el sistema INFOCAPT usa la autenticación vía web.*

- **Registro de eventos.** Se establece los mecanismos necesarios para registrar todos los eventos relevantes en el manejo de la información de la empresa. Se Registrará convenientemente quién accede a la información, cuando, cómo y con qué finalidad.

*El sistema INFOCAPT cuenta con un registro de fecha de última modificación así como de datos del funcionario que codificó la información.*

- **Revisión de permisos.** Se revisa periódicamente que los permisos concedidos a los usuarios son los adecuados.

*No se hace una revisión periódica de los permisos concedidos a los usuarios.*

- **Revocación de permisos y eliminación de cuentas.** Al finalizar la relación contractual con el empleado es necesario revocar sus permisos de acceso al sistema. Se elimina sus cuentas de correo, sus cuentas de acceso a los repositorios, servicios y aplicaciones. Además, se exige la devolución de cualquier activo de información que se le hubiese asignado (tarjetas de acceso, equipos, dispositivos de almacenamiento, *tokens* criptográficos, etc.).

*El sistema INFOCAPT permite la inhabilitación de la cuenta de usuario previa solicitud de la Dirección productora.*

## 4. Conclusiones

- El sistema INFOCAPT ENESEM cuenta con perfiles de usuario para restringir el acceso a la información según el estado del formulario.
- El sistema INFOCAPT ENESEM usa el sistema de autenticación vía web el cual es usado como una capa de seguridad para que no todos tengan acceso al sistema, sino solo los que tienen una cuenta de usuario habilitada.

Quito, 19 de julio de 2021

## 5. Firmas

Elaborado por:	Revisado por:	Aprobado por:
Marcel Chasiguasín <b>Técnico 2 DIRAD</b>	Marcelo Mora <b>Responsable GIAPE</b>	Paúl Benavides <b>Director DIRAD</b>

