1. Objeto: Establecer los lineamientos necesarios para la gestión de usuarios en la base de datos SIAU de manera segura y eficiente.

2. Alcance: Aplica desde la solicitud de la creación de usuarios en la base de datos, hasta el bloqueo o caducidad de la cuenta de usuario.

3. Referencias normativas:

- **Resolución 500 de 2021 de Mintic**, *"Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital".*

4. Definiciones:

- **Base de datos (BD):** Es un conjunto de datos estructurados que pertenecen a un mismo contexto y, se usa para administrar de forma electrónica grandes cantidades de información.
- **Contraseña:** Conjunto de caracteres limitados que se establecen para permitir el acceso a los recursos del Sistema de Información.
- **Credenciales de acceso:** Es la asignación de un nombre de usuario y una clave para permitir el acceso al Sistema de Información.
- **DBA:** Administrador de base de datos.
- **SIAU:** Sistema de Información Académico Universitario
- **Sistema de Información:** Es un conjunto de elementos relacionados que almacena, procesa y distribuye información con el fin de facilitar la toma de decisiones en una organización.
- **Usuario:** Es la persona que realiza operaciones en el sistema de información.

5. Condiciones Generales:

- La solicitud de creación de usuarios en la base de datos se debe realizar al DBA mediante el Formato de Gestión de usuarios en la base de datos (FO-GRT-10).
- No se permitirá la creación de usuarios genéricos, salvo excepciones debidamente analizadas y autorizadas por el responsable de seguridad de la información.
- La entrega del usuario de base de datos se realizará a través del formato Acta de entrega usuario y clave de base de datos (FO-GRT-13).
- La entrega de la contraseña de acceso a la base de datos la realizará el DBA directamente al respectivo usuario.
- El usuario es responsable de la custodia y confidencialidad de las credenciales de acceso asignadas y no debe compartirlas puesto que son de uso personal e intransferible.
- El usuario se hace responsable de cualquier acceso y uso de la información que se realice con su cuenta de usuario.
- Se establecerá en la base de datos la política de actualización de contraseña cada 90 días.
- Se establecerá como lineamiento en la base de datos el bloqueo de la cuenta de usuario cuando tenga un período de 15 días sin hacer uso de la misma.
- Se establecerá como lineamiento en la base de datos el cierre de sesión del usuario cada 240 minutos.
- Se establecerá como lineamiento en la base de datos el cierre de la sesión del usuario tras inactividad durante 15 minutos.
- Se establecerá como lineamiento en la base de datos el bloqueo de la cuenta de usuario tras 3 intentos consecutivos de inicio de sesión fallidos.
- Se establecerá como lineamiento en la base de datos, el límite de 3 sesiones simultáneas por cada cuenta de usuario.
- El administrador de la base de datos, deberá llevar un archivo con el registro de la gestión de usuarios para fines de trazabilidad y auditoría.

El registro deberá contener la siguiente información:
- Nombre
- Usuario
- Fecha creación
- Fecha de caducidad
- Fecha de bloqueo
- Estado del usuario (Activo, bloqueado o caducado.)
- Fecha del último inicio de sesión.

Nemotecnia para la creación de usuarios en la base de datos:
- Para el nombre de usuario se usará la siguiente estructura: **primeraletradelnombre. primerapellido**
- En caso de homónimos, se deberá usar la siguiente combinación: **primeraysegundaletradelnombre. primerapellido**

Nemotecnia para la creación de usuarios para aplicación:
Para el nombre de usuario se usará la siguiente estructura: **app_esquemaalqueaplica**

Lineamientos para la creación de contraseñas:
- Las contraseñas a generar deben contener mínimo 8 caracteres mezclando letras mayúsculas, minúsculas, números y caracteres especiales (evitando cualquier referencia de índole personal).
- La contraseña no puede ser una de las cinco últimas contraseñas utilizadas para el mismo nombre de usuario.

6. Contenido:

6.1. Creación de usuarios en la base de datos

No.	ACTIVIDAD	RESPONSABLE	PRODUCTO
1.	El DBA recibe la solicitud para la creación de usuarios en la base de datos.	DBA	**FO-GRT-10** Gestión de usuarios en la base de datos
2.	Verificar que los datos adjuntos en el formato de la solicitud estén completos, de lo contrario solicitar los datos faltantes.	DBA	Datos de usuario a crear
3.	Crear el usuario de la base de datos de acuerdo a lo requerido en la solicitud.	DBA	Usuario creado en la base de datos
4.	Verificar el acceso a la base de datos con la cuenta de usuario creada.	DBA	Permiso de acceso al sistema
5.	Entregar las credenciales de acceso creados (usuario y contraseña) al respectivo usuario.	DBA	**FO-GRT-13** Acta de entrega usuario y contraseña base de datos *-Diligenciado y firmado-*
6.	Archivar en la respectiva carpeta digital los registros generados.	Profesional de la	Soporte de la solicitud y

No.	ACTIVIDAD	RESPONSABLE	PRODUCTO
		Oficina de Sistemas	respuesta

6.2. Bloqueo de usuarios en la base de datos

No.	ACTIVIDAD	RESPONSABLE	PRODUCTO
1.	El DBA recibe la solicitud para bloqueo de un usuario en la base de datos	DBA	**FO-GRT-10** Gestión de usuarios BD
2.	Verificar que los adjuntos de la solicitud estén completos, de lo contrario solicitar los datos faltantes.	DBA	Datos de usuario a bloquear o caducar en la solicitud
3.	Verificar en la base de datos que los datos de la solicitud corresponden a los datos del usuario a bloquear.	DBA	Datos de usuario a bloquear o caducar en la base de datos
4.	Bloquear el usuario en la base de datos, y limitar cualquier recurso asociado como privilegios, roles y conexiones.	DBA oficina de sistemas	Usuario bloqueado o caducado en la base de datos
5.	Informar al solicitante que el usuario fue bloqueado en la base de datos datos, y proporcionarle detalles como la fecha y hora.	DBA oficina de sistemas	Respuesta a la solicitud
6.	Archivar en la respectiva carpeta digital los registros generados.	Profesional de la Oficina de Sistemas	Soporte de la solicitud y respuesta

7. Flujograma:

No aplica

8. Listado de anexos:

- **FO-GRT-10** Gestión de usuarios BD
- **FO-GRT-13** Acta de entrega usuario y contraseña base de datos

9. Historial de Cambios:

Versión	Fecha	Cambios	Elaboró / Modificó	Revisó	Aprobó
01	04/07/2024	Documento nuevo.	Mónica M. Hernández *Prof. Seguridad de la Información*	Adriana Ramos *Prof. de apoyo Planeación/SIG*	Roimán A. Sastoque *Jefe Oficina de Sistemas*