POLÍTICA DE CONTROL DE ACCESO A LA INFORMACIÓN EN LAS APLICACIONES

Contenido

1. Propósito de la política

Establecer los lineamientos necesarios para el acceso a la información crítica de la organización y a los datos personales de los estudiantes, empleados y proveedores de la UNAB contenidos en los sistemas de información.

2. Alcance

El presente documento aplica a todas las personas que mantienen un vínculo laboral o contractual con la UNAB y a sus asociados de negocios. Cubre la información compuesta por todos los datos personales de estudiantes, empleados, proveedores (personas naturales) o de cualquier otro tipo de información pública, interna, confidencial o secreta que sea almacenada en forma digital en los equipos de cómputo de la UNAB o en los servicios en la nube contratados por la UNAB.

3. Definiciones

- **Dato Personal.** Cualquier información que pueda asociarse a una persona natural, que permite identificar a la persona gracias a la visión conjunta que se logre con la información.
- **Información Pública.** Son aquellos datos personales que pueden ser conocidos sin restricción alguna, datos relativos al estado civil de la persona, a la profesión u oficio entre otros.
- **Información Privada.** Son aquellos datos personales que por su naturaleza íntima o reservada están relacionados con el ámbito privado de las personas y solo es relevante para el titular. Su utilización está sujeta a la autorización del titular.
- **Información Sensible.** Son aquellos datos personales que afectan la intimidad del Titular y su uso indebido puede generar su discriminación. Su utilización está sujeta a la autorización del titular.

4. Requisitos para la creación de usuarios en los sistemas de información UNAB

4.1 Usuario funcional

a) **Establecimiento de vínculo contractual.** Los funcionarios de la UNAB deben contar con algún tipo de vinculación contractual o hacer parte de un convenio con la institución, antes de recibir un usuario para tener acceso a la información. Se prohíbe la creación de usuarios en los sistemas de información sin el cumplimiento de este requisito.

b) **Firma del compromiso de confidencialidad.** Todas las personas que reciban un usuario para acceder a los sistemas de información de la Universidad, deben haber firmado el compromiso frente al uso responsable de la información que la UNAB tenga establecido.

c) **Asignación de Usuario.** Los usuarios en los sistemas de información deben ser asignados a personas naturales o a personas jurídicas plenamente identificadas, para el caso de las personas jurídicas se registra como responsable al representante legal o a la persona designada por la entidad para tal propósito. Se prohíbe la creación de usuarios genéricos que no puedan asociarse a un único responsable.

4.2 Usuario Estudiante

a) **Establecimiento del vínculo académico.** Para que los usuarios estudiantes accedan a los sistemas de información deben haber acreditado un vínculo académico con la UNAB. Se prohíbe la creación de cuentas de estudiantes en los sistemas de información sin el cumplimiento de este requisito.

b) **Firma de la autorización para tratamiento de datos personales**. Todos los estudiantes mayores de edad deben haber autorizado el tratamiento de sus datos personales antes de recibir un usuario para acceder a los sistemas de información. Para el caso de los menores de edad la autorización debe ser firmada por el padre de familia o tutor legal.

5. Asignación de permisos en los sistemas de información

5.1 Usuario funcional

a) **Asignación de permisos.** Los permisos asignados a un usuario funcional en los sistemas de información serán los mínimos necesarios, para que dicha persona pueda realizar las tareas en los sistemas de información de acuerdo a las funciones de su cargo.

b) **Asignación temporal de permisos.** Las personas que reciben nuevas funciones en consideración a un remplazo o que cumplen funciones de otro cargo adicional al suyo, se les asignarán los permisos que se requieran de acuerdo al rol correspondiente al nuevo cargo. Una vez finalizado el remplazo es deber del usuario solicitar la remoción de los permisos que le fueron concedidos.

c) **Cambio de funciones.** Cuando el usuario sea asignado a otro cargo se le deben retirar los permisos actuales y se le deben asignar los permisos de acuerdo a las funciones de su nuevo cargo.

d) **Finalización del contrato**. Una vez finalizado el vínculo laboral o contractual se deben retirar todos los permisos que el usuario tiene asignados en las aplicaciones.

5.2 Usuario estudiante

a) **Asignación de permisos**. Los permisos asignados a un usuario estudiante en los sistemas de información serán los mínimos necesarios para que el mismo pueda realizar las tareas académicas en los sistemas de información.

b) **Finalización del vínculo académico**. Una vez finalizado el vínculo académico del usuario con la UNAB se deben retirar todos los permisos que el usuario estudiante tiene asignados en las aplicaciones académicas.

6. Registro y acceso a la información

6.1 Acceso a la información de uso interno, confidencial o secreta en las aplicaciones. Las aplicaciones que contienen información de uso interno, confidencial o secreta, solo permitirán el acceso a usuarios autenticados con éxito en la aplicación y dichos usuarios deben tener la debida autorización para el acceso a la información. El sistema debe mantener el registro de auditoria de los accesos realizados.

6.2 Registro de información sensible en las aplicaciones. Las aplicaciones que capturan datos personales sensibles no deben obligar al usuario a suministrar un dato sensible, deben indicarle al mismo, cuales son los datos personales sensibles que se están solicitando en la aplicación y deben advertirle al usuario que no está en la obligación de suministrarlos.

6.3 Bases de datos en aplicaciones de ofimática. Las bases de datos que se capturan en aplicaciones de ofimática y que incluyan información confidencial o secreta se deben almacenar con acceso por clave, de tal modo que el archivo no sea visible a cualquier usuario. Estas bases de datos deben ubicarse en el área de almacenamiento de los servidores que la UNAB ha establecido.

7. Asignación y almacenamiento de las contraseñas en los sistemas de información

Todas las aplicaciones deben implementar las directivas de validación de contraseñas establecidas en el documento "Política para creación y manejo de cuentas y contraseñas para usuarios Unab".

8. Conexión de equipos de cómputo a la red

8.1 Conexión de equipos de cómputo a la red de área local. Los equipos de cómputo que se conectan a la red de datos deben permitir al usuario su autenticación en los sistemas de control que habilitan el acceso a los servicios administrativos. Los equipos ubicados en las aulas de informática solo tendrán acceso a los equipos administrativos que contengan aplicaciones académicas o aplicaciones que se utilicen para capacitación administrativa.

8.2 Conexión de los equipos de cómputo a la red Inalámbrica. Los equipos de cómputo que se conectan a la red inalámbrica no tendrán acceso a los equipos administrativo de la Universidad, solo se permitirá el acceso a los servidores ubicados en el área pública de la red de datos de la UNAB.

9. Realización de copias de seguridad

Todos los sistemas de información deberán cumplir con los lineamientos definidos en el documento "Política para las copias de respaldo".

Declaración Final

Esta política fue creada por la Oficina de Seguridad de la Información y revisada por el Comité de Tecnología UNAB. Cada año o en el momento en que se requiera, se verificará la legislación y normas que apliquen en el entorno en el que se desenvuelve la organización para mantener actualizada esta política.