Política de control de acceso

1. Introducción

El Instituto Dominicano de Aviación Civil, en adelante IDAC, ente público especializado y técnico, con personalidad jurídica, patrimonio propio, poder de reglamentación, de decisión y autoridad para implementar su organización interna, regula el acceso a sistemas y aplicaciones por sus funcionarios y empleados, en el marco de cumplimiento de su Política de Seguridad de Información.

Esta política tiene por objeto:

- Establecer las directrices sobre el control de acceso y las contraseñas.
- Informar de las consecuencias para los empleados y funcionarios en caso de incumplimiento.

2. Alcance

Esta política es aplicable a todos los empleados y funcionarios a los cuáles se conceda acceso a sistemas y aplicaciones del IDAC, en cualquiera de sus instalaciones u operaciones locales o remotas y a través de cualquiera de las redes LAN/WAN de la institución.

3. Instrucciones Generales

Los usuarios y aplicaciones que necesiten tener acceso a los recursos de IDAC son identificados y autenticados.

El sistema de control de acceso mantiene las habilitaciones actualizadas y los registros que permitan la contabilización del uso, auditoria y recuperación en las situaciones de falla.

No es permitido a ningún usuario obtener derechos de acceso de otro usuario.

La información que especifica los derechos de acceso de cada usuario o aplicación es protegida contra las modificaciones no autorizadas.

Las autorizaciones son definidas de acuerdo a la necesidad de desempeño de las funciones (acceso motivado) y considerando el principio de los privilegios mínimos (tener acceso sólo a los recursos o sistemas necesarios para la ejecución de las tareas).

Las claves o contraseñas son individuales, secretas, intransferibles y protegidas con grado de seguridad compatible con la información asociada.

El sistema de control del acceso posee mecanismos que impiden la generación de claves débiles u obvias.

4. Directrices relativas a las contraseñas o claves

Se definen las siguientes características para las claves:

El conjunto de caracteres permitidos debe incluir letras (mayúsculas y minúsculas), números y caracteres especiales;

El tamaño mínimo es de 8 caracteres;

No existe tamaño máximo;

El plazo de validez máximo es de 45 días;

No pueden reutilizarse las últimas 24 contraseñas;

Los cambios son realizados a través de los mecanismos nativos de los sistemas operativos;

Podrán adoptarse restricciones específicas para cada ambiente, aplicación o plataforma, si es necesario.

La distribución de claves (iniciales o no) a los usuarios de TI es manejada de manera segura. La clave inicial, cuando es generada por el sistema, debe ser cambiada por el usuario en su primero acceso.

El sistema de control de acceso permite al usuario cambiar su clave siempre que lo desee. El cambio de una clave bloqueada sólo es ejecutado después de la identificación positiva del usuario. La clave digitada no es exhibida.

Los usuarios son bloqueados después de 180 días sin iniciar sesión.

El sistema de control de acceso solicita nueva autenticación después de 5 minutos de inactividad de la sesión (time-out).

El sistema de control de acceso exhibe, en la pantalla inicial, un mensaje informando que el servicio solamente puede ser utilizado por los usuarios autorizados. En el momento de la conexión, el sistema exhibe para el usuario información sobre el último acceso.

El registro de las actividades (logs) del sistema de control de acceso es definido de manera de auxiliar en el tratamiento de las cuestiones de seguridad, permitiendo la contabilización del uso, auditoria y recuperación en las situaciones de fallas. Los logs deben ser periódicamente analizados.

Todos los consultores y funcionarios temporales son registrados con fecha de vencimiento. La fecha deberá ser igual a la fecha de vencimiento del contrato con la empresa.

5. Consecuencias de incumplimiento

El incumplimiento de las disposiciones contenidas tanto en la presente política como en los documentos relacionados se regirá por el Procedimiento Disciplinario del IDAC, la legislación y/o la normativa OACI, según apliquen.

Román Caamaño Vélez
Director General
Instituto Dominicano de Aviación Civil (IDAC)

Héctor Porcella Dumas
Subdirector General
Instituto Dominicano de Aviación Civil (IDAC)