Suprema Corte de Justicia

Provincia de Buenos Aires

VISTO:

La propuesta de implementación de la normativa de contraseñas como parte del Plan Integral de Seguridad Informática, elaborado por la Subsecretaria de Tecnología Informática de esta Suprema Corte de Justicia conforme lo dispuesto en la resolución N° 1649 de fecha 0l de octubre de 2021 y,

CONSIDERANDO:

1°) Que esta Suprema Corte de Justicia ha realizado una tarea continua, orientada a mejorar la gestión por medio del uso intensivo de las tecnologías de la información y la comunicación aplicadas al servicio.

2°) Que deviene necesario actualizar los lineamientos para la creación, administración y modificación de contraseñas para el ingreso a diferentes sistemas, a los efectos de brindar mayor seguridad y reducir el riesgo de accesos no autorizados.

3°) Que los controles internos de seguridad tienen por finalidad garantizar que todos los activos, sistemas, instalaciones, datos y archivos relacionados con el uso de la Tecnología de Información se encuentren protegidos contra accesos no autorizados, daños eventuales y uso indebido o ilegal.

4°) Que, en tal sentido, la Subsecretaría de Tecnología Informática debe velar porque la información solo resulte accesible para quienes están autorizados a tener acceso a ella, y con permisos establecidos para consulta o modificación, según sea el caso.

5°) Que la siguiente Normativa de contraseñas complementa el punto 3.7.1 (Listado de controles) del plan de seguridad de la información de la Suprema Corte de Justicia de la provincia de Buenos Aires.

6°) Que en marco de sus competencias ha intervenido el Comité de Gestión de Seguridad de la Suprema Corte de Justicia

POR ELLO, la Suprema Corte de Justicia, en ejercicio de sus atribuciones y de conformidad a lo dispuesto en el artículo 4 del Acuerdo 3971,

RESUELVE:

Artículo 1°. Aprobar la Normativa de contraseñas elaborada por la Subsecretaría de Tecnología Informática junto al Comité de Seguridad de esta Suprema Corte, que obra como Anexo de la presente resolución.

Artículo 2°. Establecer que las pautas que surgen de la "Normativa de contraseñas" aprobada en el artículo 1° serán de aplicación obligatoria en todo el ámbito de la Jurisdicción Administración de Justicia.

Artículo 3°. Encomendar a la Subsecretaría de Tecnología Informática junto al Comité de Gestión de seguridad de la SCBA, la revisión periódica de la Normativa aprobada por el artículo 1° de la presente y autorizando a los mismos a su actualización, así como a dictar las normas aclaratorias y complementarias que resulten necesarias, debiendo comunicar dichos cambios a la Suprema Corte.

Artículo 4°. Encomendar a la Subsecretaría de Tecnología Informática, la implementación paulatina de la presente política dando difusión de la misma con anticipación suficiente

Artículo 5°. Requerir al Instituto de Estudios Judiciales de la Suprema Corte la difusión de la Jornada de Empleo Seguro, alojada en el canal del Instituto de Estudios Judiciales, a los efectos de que la misma sea realizada por la totalidad del personal de la Jurisdicción Administración de Justicia.

Artículo 6°. Regístrese y comuníquese.

Normativa de contraseñas

Anexo técnico

Subsecretaría de Tecnología Informática

Área de Seguridad y Auditoria

Introducción

La siguiente política de contraseñas complementa el punto 3.7.1 (Listado de controles) del plan de seguridad de la información de la Suprema Corte de Justicia de la provincia de Buenos Aires.

El fin de esta política es establecer el uso correcto de las credenciales de acceso a los sistemas de información de la S.C.B.A.

Antes de establecer cualquier normativa técnica, los usuarios deben comprometerse a mantener las contraseñas en secreto, ya que la contraseña es considerada información secreta y personal, no debiendo ser compartida, ni aún con su personal jerárquico. Cuando existiera indicio que la confidencialidad de la contraseña hubiera sido comprometida, se informará y solicitará el cambio de esta, inmediatamente.

La composición de la contraseña no estará basada en datos que se pudieran prever u obtener fácilmente, mediante información relacionada con la persona, como ser nombres, números de teléfono, número de oficina, fechas de cumpleaños, etc.

El usuario no reutilizará o reciclará viejas contraseñas, como tampoco almacenará contraseñas en papel, archivos de texto, planillas de cálculo o cualquier aplicación cuya función no sea expresamente el almacenamiento seguro de contraseñas.

Aspectos técnicos

Directorio de usuarios: (base de datos y conjunto de servicios que conectan a los usuarios con los recursos de red)

a) USUARIOS BÁSICOS (cualquier usuario cuyos permisos otorgados son el acceso a la red con inicio de sesión de dominio y la usabilidad sobre los sistemas de gestión)

- 12 caracteres
- Letras mayúsculas, minúsculas, números
- No puede tener el nombre de usuario o el nombre completo de la persona
- Historial de contraseñas (5 registros)
- 180 días
- 10 intentos fallidos y bloqueo de cuenta – Se bloquea automáticamente las cuentas durante 10 minutos tras 10 intentos de inicio de sesión no válidos.

b) USUARIOS AVANZADOS (cualquier usuario cuyos permisos otorgados permitan administrar de forma técnica el recurso al que se accede y/o los sistemas de gestión)

- 16 caracteres
- Letras mayúsculas, minúsculas, números y signos
- No puede tener el nombre de usuario o el nombre completo de la persona
- Historial de contraseñas (10 registros)
- 60 días

- 6 intentos y bloqueo de cuenta – Se bloquea automáticamente las cuentas durante 10 minutos tras 10 intentos de inicio de sesión no válidos.

Sistemas de la Suprema Corte de Justicia de Buenos Aires (inicio de sesión fuera del dominio)

a) USUARIOS BÁSICOS (cualquier usuario fuera del dominio con acceso a un sistema de la SCBA)

   - 12 caracteres
   - Letras mayúsculas, minúsculas, números
   - No puede tener el nombre de usuario o el nombre completo de la persona
   - Historial de contraseñas (5 registros)
   - 90 días
   - 10 intentos y bloqueo de cuenta (desbloqueo de cuenta mediante correo electrónico)

b) USUARIOS ADMINISTRADORES (cualquier usuario con permisos de administración a un sistema de la SCBA)

   - 16 caracteres
   - Letras mayúsculas, minúsculas, números y signos
   - No puede tener el nombre de usuario o el nombre completo de la persona
   - Historial de contraseñas (15 registros)
   - 120 días

- 3 intentos y bloqueo de cuenta (desbloqueo de cuenta mediante correo electrónico)
- Doble factor de autenticación

Hardware y otros dispositivos:

- 22 caracteres
- Letras mayúsculas, minúsculas, números y signos
- No puede tener el nombre de usuario o el nombre completo de la persona
- Historial de contraseñas (15 registros)
- 30 días

*NOTA: todas estas características solicitadas quedan sujetas a los atributos técnicos de cada Sistema, Equipamiento o Aplicativo en cuestión. Asimismo, si estas configuraciones pueden ser aplicadas como parámetros dentro de las políticas de seguridad del Directorio de usuarios.

REFERENCIAS:

Funcionario Firmante: 26/10/2022 12:18:00 - GENOUD Luis Esteban - JUEZ

Funcionario Firmante: 26/10/2022 13:25:31 - KOGAN Hilda - JUEZA

Funcionario Firmante: 26/10/2022 16:59:45 - TORRES Sergio Gabriel - JUEZ

Funcionario Firmante: 07/11/2022 12:22:18 - SORIA Daniel Fernando -

JUEZ

Funcionario Firmante: 14/02/2023 15:07:39 - PEREZ VILLAR Carlos Gustavo - SUBSECRETARIO DE LA SUPREMA CORTE DE JUSTICIA

227301732001342172

El presente es impresión del acto dictado conforme Ac. 3971 que obra en el sistema Augusta (arts. 2, 4, 13 del Ac. 3971).

Registrada en la ciudad de La Plata, bajo el número: 000101

MATIAS JOSE ALVAREZ
Secretario
Suprema Corte de Justicia