
	PROCEDIMIENTO		
	PROCEDIMIENTO DE CONTROL DE ACCESO		
	EDICIÓN: 01	REVISIÓN: 01	PÁGINA 1 DE 11

ÍNDICE

1. Objeto	2
2. Objetivos	2
2.1. General	2
2.2. Específicos.....	2
3. Alcance	2
4. Definiciones y siglas.....	3
5. Control de Acceso Lógico	4
5.1. Creación de roles	4
5.2. Modificación de roles	5
5.3. Eliminación de roles	6
5.4. Política	7
5.5. Identificadores.....	8
5.6. Contraseñas.....	9
5.7. Monitorización de accesos.....	10
5.8. Doble factor de autorización (2FA).....	10
6. Control de acceso a las aplicaciones	11
6.1. Restricción de acceso a las aplicaciones.....	11
7. Segregación de funciones y tareas	11

	PROCEDIMIENTO		
	PROCEDIMIENTO DE CONTROL DE ACCESO		
	EDICIÓN: 01	REVISIÓN: 01	PÁGINA 2 DE 11

1. Objeto

El objeto del presente documento es definir el procedimiento aplicable a la Gestión de Accesos del MINISTERIO DE CIBERSEGURIDAD (a partir de ahora, el Ministerio) a fin de garantizar el seguro funcionamiento del sistema.

2. Objetivos

2.1. General

Controlar y limitar el acceso a la información y recursos de tratamiento de información.


2.2. Específicos

- Garantizar el acceso de usuarios autorizados y evitar el acceso no autorizado a los sistemas de información y servicios.
- Prevenir el acceso no autorizado a los sistemas información y servicios.
- Impedir la suplantación de identidades de usuarios autorizados.
- Asegurar la revisión de accesos periódica.

3. Alcance

Esta normativa se aplica a todas las instalaciones del Ministerio en las que se desarrollen actividades relacionadas al manejo de cualquier tipo de información y de aplicación obligatoria a todo el personal que, ya sea de manera temporal o permanente, preste sus servicios. Inicia con la creación de perfiles y roles generales hasta la correcta segregación de funciones y tareas, además de tener como alcance los siguientes sistemas críticos:

- Active Directory;
- Gmail;
- Sistema de Reporte de Incidentes;

	PROCEDIMIENTO		
	PROCEDIMIENTO DE CONTROL DE ACCESO		
	EDICIÓN: 01	REVISIÓN: 01	PÁGINA 3 DE 11

- Sistema de Gestión de Seguridad de la Información;
- Plataforma de Aprendizaje.

El proceso **no** considera la capacitación relacionada al Control de Acceso e Identidades, el acceso a información en directorios y archivos, el acceso a redes, el acceso al código fuente, la creación de perfiles específicos y transacciones ni la gestión de credenciales de acceso físico.

4. Definiciones y siglas

2FA: Autenticación de dos factores.

Autenticación: Proceso de verificar la identidad de un usuario o sistema antes de concederle acceso a un recurso.


Credenciales: Datos que prueban la identidad de un usuario.

IAM: Gestión de Identidades y Accesos. Es un conjunto de políticas, procesos y tecnologías que permiten a una organización gestionar de forma segura las identidades digitales (usuarios, dispositivos, aplicaciones) y controlar quién puede acceder a qué recursos, en qué momento y en qué condiciones.

Perfiles de usuario: Conjuntos de atributos y permisos asociados a una identidad digital.

Recurso/Activo: Cualquier elemento con valor para el Ministerio. No se tomará en cuenta la gestión de activos físicos de información.

Usuario: Entidad digital identificable (persona, sistema, aplicación) que interactúa con los recursos informáticos del Ministerio.

	PROCEDIMIENTO		
	PROCEDIMIENTO DE CONTROL DE ACCESO		
	EDICIÓN: 01	REVISIÓN: 01	PÁGINA 4 DE 11

5. Control de Acceso Lógico


5.1. Creación de roles

La creación de roles generales para usuarios en el sistema se inicia por parte de una Jefatura de la División (que es el único personal con competencia para autorizar los accesos a los recursos), quien envía el Formulario de Creación de Perfil (de ahora en adelante FOR-022) mediante correo electrónico al Jefe de Recursos Humanos (RRHH a partir de ahora).

Después de verificar la información en un plazo no mayor a 3 días hábiles, el Jefe de RRHH solicitará al Analista de Perfiles la creación del perfil. Si la información no es correcta, se enviará un correo electrónico a la Jefatura de División pidiendo iniciar nuevamente el proceso.

El Analista de Perfiles deberá asegurarse de que los accesos y permisos solicitados sean esenciales para el correcto desempeño de dicho perfil, solicitando a cada Responsable de Sistema una confirmación. El Responsable de Sistema tendrá que informar la esencialidad de estos accesos y permisos en un plazo no mayor a 1 día hábil. En caso de que al menos uno de los accesos o permisos se considere no vital para el desempeño de funciones y objetivos asignados al perfil, deberá ser modificada la solicitud por el Responsable de Sistema (o incluso rechazada).

Una vez que el Analista de Perfiles cuenta con la creación del perfil se enviará al Encargado de Seguridad, quien deberá validar la adecuada segregación de funciones técnicas y al Jefe de Riesgos, quien deberá evaluar la adecuada segregación de funciones operacionales, ambos disponen de un plazo máximo de tres días para responder. En caso de que no cuenten con la debida segregación funcional, el Analista de Perfiles enviará la información al Jefe de la División solicitante, volviendo al primer paso.

	PROCEDIMIENTO		
	PROCEDIMIENTO DE CONTROL DE ACCESO		
	EDICIÓN: 01	REVISIÓN: 01	PÁGINA 5 DE 11

En el caso que el perfil solicitado requiera privilegios de administración, deberá ser validado adicionalmente por el Comité de Ciberseguridad, quienes dispondrán de un plazo máximo de 5 días hábiles para responder. En caso de que el perfil de administración sea rechazado, el Analista de Perfiles enviará la información al Jefe de la División solicitante, volviendo al primer paso.


Si todos los pasos previos han sido exitosos el Analista de Perfiles agregará el perfil en el maestro de perfiles (a partir de ahora REG-025), informando de su creación a la Jefatura de la División Solicitante, al Jefe de Recursos Humanos, al Encargado de Seguridad y al Jefe de Riesgo.

5.2. Modificación de roles

La modificación de roles generales para usuarios en el sistema se inicia por parte de una Jefatura de la División (que es el único personal con competencia para autorizar los accesos a los recursos), quien envía el Formulario de Modificación de Perfil (de ahora en adelante FOR-023) mediante correo electrónico al Jefe de RRHH.

Posterior a ello, el Jefe de RRHH validará la información en un plazo no mayor a 3 días hábiles, si la información provista es correcta entonces solicitará al Analista de Perfiles iniciar la modificación del perfil. En caso contrario se enviará correo a la Jefatura de División volviendo al inicio de este proceso.

Luego, el Analista de Perfiles deberá validar los cambios en los roles y accesos solicitados en los sistemas, solicitando así a cada Responsable de Sistema la creación de esto. El Responsable de Sistema deberá informar la viabilidad de los cambios en un plazo máximo de 1 día hábil. En caso de no ser viable, se enviará al Comité de Ciberseguridad para su evaluación y priorización, siendo cerrado el requerimiento; de otra forma, el Responsable del Sistema modificará el perfil requerido.

	PROCEDIMIENTO		
	PROCEDIMIENTO DE CONTROL DE ACCESO		
	EDICIÓN: 01	REVISIÓN: 01	PÁGINA 6 DE 11

Una vez que el Analista de Perfiles cuenta con la modificación del perfil se enviará al Encargado de Seguridad, quien deberá validar la adecuada segregación de funciones técnicas y al Jefe de Riesgos, quien deberá evaluar la adecuada segregación de funciones operacionales, ambos disponen de un plazo máximo de tres días para responder. En caso de que no cuenten con la debida segregación funcional, el Analista de Perfiles enviará la información al Jefe de la División solicitante, volviendo al primer paso.


En el caso que el perfil solicitado requiera privilegios de administración, deberá ser validado adicionalmente por el Comité de Ciberseguridad, quienes dispondrán de un plazo máximo de 5 días hábiles para responder. En caso de que el perfil de administración sea rechazado, el Analista de Perfiles enviará la información al Jefe de la División solicitante, volviendo al primer paso.

Si todos los pasos previos han sido exitosos el Analista de Perfiles actualizará el perfil en el maestro de perfiles REG-025, realizando una anotación con los cambios realizados e informando de su modificación a la Jefatura de la División Solicitante, la Jefe de Recursos Humanos, al Encargado de Seguridad y Jefe de Riesgo.

5.3. Eliminación de roles

La eliminación de roles generales para usuarios en el sistema se inicia por parte de una Jefatura de la División (que es el único personal con competencia para autorizar los accesos a los recursos), quien envía el Formulario de Baja de Perfil (de ahora en adelante FOR-024) mediante correo electrónico al Jefe de RRHH.

Posterior a ello, el Jefe de RRHH revisará la información en un plazo máximo de 3 días hábiles, si la información provista es válida entonces solicitará al Analista de Perfiles iniciar la baja del perfil. En caso contrario se enviará correo a la Jefatura de División volviendo al inicio de este proceso.

	PROCEDIMIENTO		
	PROCEDIMIENTO DE CONTROL DE ACCESO		
	EDICIÓN: 01	REVISIÓN: 01	PÁGINA 7 DE 11


El Analista de Perfiles deberá asegurarse de que los accesos y permisos a eliminar sean reemplazados o asignados a otro perfil si estos son de vital importancia para el funcionamiento correcto del sistema, solicitando a cada Responsable de Sistema una confirmación. El Responsable de Sistema tendrá que informar la validez de esta asignación de accesos y permisos en un plazo no mayor a 1 día hábil. Si se determina que no hay otro usuario que pueda obtener estos permisos, se creará un nuevo perfil que cumpla con los requisitos posterior a la baja del perfil anterior.

En el caso que el perfil eliminado requiera privilegios de administración, deberá ser validado adicionalmente por el Comité de Ciberseguridad, quienes dispondrán de un plazo máximo de 5 días hábiles para responder. En caso de que el perfil de administración sea rechazado, el Analista de Perfiles enviará la información al Jefe de la División solicitante, volviendo al primer paso.

Si todos los pasos previos han sido exitosos el Analista de Perfiles eliminará el perfil en el maestro de perfiles REG-025, informando de su baja a la Jefatura de la División Solicitante, al Jefe de Recursos Humanos, al Encargado de Seguridad y al Jefe de Riesgo.

5.4. Política


- Se deben aplicar controles de acceso en todos los niveles de la arquitectura del sistema. Los atributos de cada uno deben reflejar alguna forma de identificación y autenticación, autorización de acceso, verificación de recursos de información y registro y monitorización de las actividades.
- Los usuarios tendrán acceso solamente a los recursos necesarios para el desempeño de las labores propias de su puesto. Los derechos de acceso a los mismos también serán los menores posibles según las necesidades.

	PROCEDIMIENTO		
	PROCEDIMIENTO DE CONTROL DE ACCESO		
	EDICIÓN: 01	REVISIÓN: 01	PÁGINA 8 DE 11

- c) La implementación de los controles de acceso deberá tener en cuenta los tipos de accesos posibles y sus riesgos, la criticidad de la información que resulta accedida a través de ellos y los requisitos legales aplicables.
- d) El acceso a los Sistemas de Información requerirá siempre de autenticación y una verificación de dos factores según el caso, conforme se detalla en este documento.
- e) Los usuarios siempre deben autenticarse como usuarios no privilegiados del sistema. La única excepción es sólo con fines de administración.
- f) Todas las contraseñas asignadas a las cuentas de usuario deben respetar la política de contraseñas detallada en este documento.
- g) Los usuarios deben en todo momento hacer un uso responsable de la información y los sistemas de información accedidos.
- h) Mensualmente se hará una revisión de los derechos de acceso asignados a los usuarios. Los derechos de acceso privilegiados deben revisarse de forma semanal. Además, se deberá hacer una revisión de los permisos de acceso correspondientes a un usuario siempre que hubiese sufrido modificación significativa en sus responsabilidades dentro del Ministerio.

5.5. Identificadores

- Todos los identificadores personales del Ministerio deben posibilitar la identificación unívoca y personalizada de los usuarios. Deben permitir saber quién ha hecho algo y qué ha hecho, además de encontrarse registrado quién recibe y qué derechos recibe.
- La creación de un identificador de usuario debe estar autorizada por su superior jerárquico, de acuerdo con el proceso. Los derechos de acceso de cada recurso se establecerán según las decisiones de la persona responsable del recurso.
- **No** se permite el uso de identificadores genéricos o de grupo.

	PROCEDIMIENTO		
	PROCEDIMIENTO DE CONTROL DE ACCESO		
	EDICIÓN: 01	REVISIÓN: 01	PÁGINA 9 DE 11


- Los identificadores de usuarios anónimos y los identificadores por defecto siempre estarán **deshabilitados**.
- Los identificadores deben tener asignada una fecha de validez tras la cual se deshabilitarán. En dado caso se entiende que el usuario dejó el Ministerio, terminó la función que requería dichos permisos o que fue autorizado en sentido contrario por la persona que lo autorizó.
- Los usuarios son responsables de **todas** las actividades realizadas con sus identificadores, contraseñas y dispositivos de acceso.
- Las credenciales se activarán una vez que estén bajo el control del propio usuario, y éste reconocerá su recepción junto con el conocimiento y aceptación de las obligaciones que implica su tenencia.
- Se registrarán los accesos realizados con éxito y los fallidos.

5.6. Contraseñas

Es esencial que las contraseñas que se usen como mecanismo de autenticación sean robustas: difícilmente vulnerables. Así, se han definido las siguientes **reglas** que deben ser seguidas por todos los usuarios a la hora de la definición o creación de contraseñas:

- Longitud mínima de 12 caracteres.
- No debe contener el nombre del usuario.
- Debe contener al menos:
 - una mayúscula,
 - una minúscula,
 - un número, y
 - tres caracteres especiales.
- No debe ser igual a ninguna de las últimas tres contraseñas usadas.

Se inicializará el usuario con una contraseña inicial aleatoria que será comunicada verbalmente al usuario, informándole que debe ser cambiada en el primer acceso al

	PROCEDIMIENTO		
	PROCEDIMIENTO DE CONTROL DE ACCESO		
	EDICIÓN: 01	REVISIÓN: 01	PÁGINA 10 DE 11

sistema. Las contraseñas deben renovarse al menos cada 2 meses; en caso de tener privilegios especiales la periodicidad deberá ser mensual.

5.7. Monitorización de accesos

Se deben realizar labores periódicas de monitorización en el sistema a fin de detectar acceso no autorizados, registrando eventos que suministren evidencias en caso de producirse incidentes relativos a la seguridad. Así, al menos se deberán registrar los siguientes eventos:

- Intentos de acceso fallidos,
- bloqueos de cuenta,
- cuentas inactivas,
- cuentas deshabilitadas,
- últimos accesos a cuentas, y
- uso de privilegios.


5.8. Doble factor de autorización (2FA)

Uno de los siguientes mecanismos de autenticación debe combinarse con las credenciales de acceso (usuario y contraseña) para reforzar la seguridad de cada cuenta:

- “algo que se tiene”: como dispositivos físicos (tokens), o
- “algo que es”: elementos biométricos (huella digital, reconocimiento de iris).

Los mecanismos de autenticación se adecuarán al nivel del sistema dadas las siguientes consideraciones:

- Para controles de acceso a subsistemas de Nivel Bajo, se admitirá el uso de cualquier mecanismo de autenticación sustentado en un solo factor (como usuario y contraseña).

	PROCEDIMIENTO		
	PROCEDIMIENTO DE CONTROL DE ACCESO		
	EDICIÓN: 01	REVISIÓN: 01	PÁGINA 11 DE 11

- Para los controles de acceso para niveles superiores, se exigirá de al menos dos factores de autenticación (por ejemplo, usuario, contraseña y huella digital).

6. Control de acceso a las aplicaciones

6.1. Restricción de acceso a las aplicaciones

Deben tenerse en cuenta los siguientes aspectos de seguridad:

- El acceso a aplicaciones y bases de datos debe ser independiente del acceso al sistema operativo.
- El acceso lógico a las aplicaciones y a la información estará restringido solo a los usuarios autorizados.
- Los usuarios recibirán el mínimo nivel de acceso a las aplicaciones según sus funciones dentro del Ministerio.

7. Segregación de funciones y tareas

El sistema de control de acceso exigirá la concurrencia de dos o más personas para realizar tareas críticas, eliminando la posibilidad de que un solo individuo autorizado pueda abusar de sus derechos para cometer alguna acción malintencionada.

Además, la responsabilidad de la supervisión y auditoría debe recaer en personal o entidades que no intervengan en ninguna otra función.