

SERVICIO ECUATORIANO DE CAPACITACIÓN PROFESIONAL	MANUAL DE POLÍTICAS		Página 1 de 6
	MACROPROCESO: Gestión de Tecnologías de la Información y Comunicación	Fecha de Aprobación: 21/12/2020	
	PROCESO: Gestión de Seguridad y Componentes de servicios de TI. SUBPROCESO: Gestión de Seguridad CODIGO: POL-EGSI-5.4.2	VERSIÓN: 3	

POLÍTICA DE PROCEDIMIENTOS SEGUROS DE INICIO DE SESIÓN

SERVICIO ECUATORIANO DE CAPACITACIÓN PROFESIONAL	MANUAL DE POLÍTICAS		Página 2 de 6
	MACROPROCESO: Gestión de Tecnologías de la Información y Comunicación	Fecha de Aprobación: 21/12/2020	
	PROCESO: Gestión de Seguridad y Componentes de servicios de TI. SUBPROCESO: Gestión de Seguridad CODIGO: POL-EGSI-5.4.2	VERSIÓN: 3	

FIRMAS DE REVISIÓN Y APROBACIÓN

	Nombre y Apellido / Cargo	Firma
Elaborado por:	Ing. Geovanny Meza, Mg. Analista de Tecnologías de la Información 3	
Revisado y aprobado por:	Ing. Patricio Padrón Director de Tecnologías de la Información y Comunicación	

SERVICIO ECUATORIANO DE CAPACITACIÓN PROFESIONAL	MANUAL DE POLÍTICAS		Página 3 de 6
	MACROPROCESO: Gestión de Tecnologías de la Información y Comunicación	Fecha de Aprobación: 21/12/2020	
	PROCESO: Gestión de Seguridad y Componentes de servicios de TI. SUBPROCESO: Gestión de Seguridad CODIGO: POL-EGSI-5.4.2	VERSIÓN: 3	

ÍNDICE

1.	Notas del Cambio.....	4
2.	Antecedentes	4
3.	Alcance	4
4.	Propósito.....	4
5.	Definiciones	4
6.	Políticas.....	5
7.	Anexos	6

SERVICIO ECUATORIANO DE CAPACITACIÓN PROFESIONAL	MANUAL DE POLÍTICAS		Página 4 de 6	
	MACROPROCESO: Gestión de Tecnologías de la Información y Comunicación			Fecha de Aprobación: 21/12/2020
	PROCESO: Gestión de Seguridad y Componentes de servicios de TI.			VERSIÓN: 3
SUBPROCESO: Gestión de Seguridad				
CODIGO: POL-EGSI-5.4.2				

1. Notas del Cambio

Versión	Fecha	Detalle de la modificación
1	28/10/2021	Creación de la política

2. Antecedentes

El Esquema Gubernamental de Seguridad de la Información (EGSI), establece una serie de hitos que contemplan la elaboración, implementación y difusión, de políticas, procedimientos, reglamentos, normas y demás instrumentos técnicos, que garanticen el manejo seguro de la información de las instituciones públicas.

El establecer un procedimiento seguro de inicio de sesión, permite garantizar que el servidor o funcionario a quien se le otorgó credenciales de acceso a la red, sistemas y aplicaciones del Secap, sea el correcto y con ello, garantizar la seguridad de la información institucional.

3. Alcance

El presente procedimiento es de alcance general; es decir, para todos los servidores, funcionarios, instancias, dependencias, procesos y subprocesos del Secap.

4. Propósito

Normar el procedimiento seguro de inicio de sesión en la red, sistemas y aplicaciones del Secap, para los servidores y funcionarios institucionales.

5. Definiciones

- **Contraseña:** Código secreto compuesto por una cadena de caracteres que pueden ser especiales y alfanuméricos, que se introduce en un sistema, equipo informático o red para iniciarlo y acceder para operarlo.
- **Credenciales de acceso:** Son el nombre de usuario y contraseña gestionados que dan acceso a un sistema o equipo.
- **Funcionario:** Un funcionario es quien desempeña profesionalmente un empleo público. Los funcionarios participan en la administración pública o de gobierno; y acceden a su condición a través de elección, nombramiento, selección o empleo.

SERVICIO ECUATORIANO DE CAPACITACIÓN PROFESIONAL	MANUAL DE POLÍTICAS		Página 5 de 6
	MACROPROCESO: Gestión de Tecnologías de la Información y Comunicación	Fecha de Aprobación: 21/12/2020	
	PROCESO: Gestión de Seguridad y Componentes de servicios de TI. SUBPROCESO: Gestión de Seguridad CODIGO: POL-EGSI-5.4.2	VERSIÓN: 3	

- Servidor: Persona que presta servicios a la Administración o a nombre y por cuenta de esta, como parte de su organización, en virtud de un acto válido y eficaz de investidura, con entera independencia del carácter imperativo, representativo, remunerado, permanente o público de la actividad respectiva.
- Usuario: Nombre o identificador compuesto por una cadena de caracteres alfanuméricos, que emplea una persona para identificarse en un sistema, equipo o red, previo a ingresar la contraseña.

6. Políticas

- Las credenciales de acceso (usuario y contraseña) para la red de datos, sistemas y aplicaciones del Secap, tiene por objeto garantizar que únicamente el servidor o funcionario, de acuerdo con su perfil y funciones, tenga acceso a la información y a los programas informáticos propios de la Institución, para este efecto se deberá regir a lo establecido en el procedimiento previsto en el Reglamento de Uso de las Tecnologías de la Información y Comunicación que, para el efecto, emitirá el Secap.
- Los servidores y funcionarios serán los únicos responsables del correcto uso y manejo de las credenciales de acceso (usuario y contraseña).
- La autenticación se efectuará a través de la validación de las credenciales de acceso (usuario y contraseña) entregadas al servidor o funcionario, por parte de la red, sistema o aplicación del Secap. Dicha autenticación es un proceso interno e independiente de la red, sistema o aplicación.
- Para la gestión de entrega de las credenciales de acceso y almacenamiento de las mismas, la Dirección de Tecnologías de la Información y Comunicación elaborará los procedimientos o políticas según corresponda.
- La Dirección de Tecnologías de la Información y Comunicación deberá definir y/o estructurar el nivel de permisos sobre las aplicaciones, de acuerdo a la ejecución o gravedad de las aplicaciones o archivos, y haciendo especial énfasis en los derechos de escritura, lectura, modificación, ejecución o borrado de información. Para permitir el ingreso a los sistemas, la dirección solicitante deberá definir previamente los perfiles de acceso, de acuerdo a las funciones y jerarquías de los usuarios, así como rangos limitados de actividades (menús restringidos).

SERVICIO ECUATORIANO DE CAPACITACIÓN PROFESIONAL	MANUAL DE POLÍTICAS		Página 6 de 6
	MACROPROCESO: Gestión de Tecnologías de la Información y Comunicación	Fecha de Aprobación: 21/12/2020	
	PROCESO: Gestión de Seguridad y Componentes de servicios de TI. SUBPROCESO: Gestión de Seguridad CODIGO: POL-EGSI-5.4.2	VERSIÓN: 3	

- La Dirección de Tecnologías de la Información y Comunicación deberá habilitar un equipo servidor de prueba, en el que se realizará el control de calidad de cada programa, con el objetivo de evitar que en los sistemas de producción existan errores de fondo y forma.
- Se deberá llevar un registro mediante Log de aplicaciones, sobre las actividades de los usuarios en cuanto a accesos, errores de conexión, horas de conexión, intentos fallidos, terminal desde donde se conecta, entre otros, de manera que proporcionen información relevante y revisable posteriormente.
- Todo sistema de información desarrollado o adquirido por el Servicio Ecuatoriano de Capacitación Profesional -SECAP- contará con programas, aplicaciones y procedimientos documentados, controles de acceso y seguridades, así como una segregación de funciones según el área y cargo competente, para salvaguardar la confidencialidad, integridad y disponibilidad de los datos.
- Se registrará y archivará toda actividad, procedente del uso de las aplicaciones, sistemas de información y uso de la red, mediante archivos de Log o bitácoras de sistemas.
- Los registros de Log almacenarán nombres de usuarios, nivel de privilegios, IP de terminal, fecha y hora de acceso o utilización, actividad desarrollada, aplicación implicada en el proceso, intentos de conexión fallidos o acertados, archivos a los que se tuvo acceso, entre otros, a fin de conocer las acciones que realizan los usuarios.

7. Anexos

Ninguno.