POLÍTICA DE PRUEBAS DE SEGURIDAD DEL SISTEMA

FIRMAS DE REVISIÓN Y APROBACIÓN

	Nombre y Apellido / Cargo	Firma
Elaborado por:	Ing. Geovanny Meza, Mg. **Analista de Tecnologías de la Información 3**	Firmado electrónicamente por: JORGE GEOVANNY MEZA MORALES
Revisado y aprobado por:	Ing. Patricio Padrón **Director de Tecnologías de la Información y Comunicación**	Firmado electrónicamente por: NARDO PATRICIO PADRON CORREA

ÍNDICE

1. Notas de Cambio

Versión	Fecha	Detalle de la modificación
1	30/11/2021	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.

Disponer de una política de pruebas de seguridad del sistema que permita garantizar la seguridad de las mismas, sean adquiridas o desarrolladas internamente en el Servicio Ecuatoriano de Capacitación Profesional – Secap, es imprescindible para garantizar la seguridad de la información, por la naturaleza propia de las aplicaciones y la información que se procesará y almacenará a través de dichos sistemas.

3. Alcance

La presente política enfocada exclusivamente a la Dirección de Tecnologías de la Información y Comunicación y sus gestiones a cargo de garantizar la seguridad de los diferentes sistemas con los que cuenta el Secap y que son su responsabilidad.

4. Propósito

Determinar las políticas de pruebas de seguridad del sistema, previo a la puesta en producción.

5. Definiciones

- **Aplicaciones de software:** Programa informático diseñado como una herramienta para realizar operaciones o funciones específicas.
- **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.

- **Internet:** Red mundial de computadores conectadas entre sí que ofrecen acceso y comparten información a través de un lenguaje común.
- **Intranet:** Red informática interna basada en los estándares de internet.
- **Pruebas de seguridad:** Conjunto de métodos, acciones y procedimientos que permiten identificar vulnerabilidades y prevenir amenazas en los sistemas.
- **Red de computadores:** Conjunto de equipos conectados por medio de cables, señales, ondas o cualquier otro método de transporte de datos, que comparten información (archivos), recursos (CD-ROM, impresoras, etc.).
- **Seguridad del sistema:** Conjunto de medidas preventivas y correctivas que permiten resguardar y proteger la información y los sistemas de software que la procesan y almacenan.
- **Servicios:** Conjunto de aplicativos o programas informáticos y de comunicación de datos que apoyan la labor del Secap.
- **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.
- **Sistema de software:** Programas informáticos diseñados con el propósito de facilitar a los usuarios la realización de determinadas tareas.
- **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

- Todo sistema o aplicación adquirido o desarrollado por el Secap, deberá cumplir con los requerimientos de seguridad funcional, esto es: bloqueo de usuario luego de tres intentos fallidos; y, las contraseñas deben tener al menos seis caracteres alfanuméricos.
- Todo sistema o aplicación adquirido o desarrollado por el Secap, deberá cumplir con los requerimientos de seguridad a causa de riesgo, esto es: la aplicación / sistema no debe permitir que los datos sean modificados o destruidos; y, la

aplicación / sistema no debe ser comprometida o mal utilizada para transacciones financieras no autorizadas.

- El gestor de Diseño e Implementación de Soluciones Informáticas se encargará de garantizar que toda aplicación / sistema cuente con las pruebas de seguridad funcional y las de seguridad de causa de riesgo, previo a su aceptación y puesta en producción.
- El gestor de Diseño e Implementación de Soluciones Informáticas se encargará de realizar los procedimientos de pruebas de seguridad funcional y las de seguridad de causa de riesgo, para toda aplicación / sistema que adquiera o desarrolle el Secap.
- Adicionalmente, el gestor de Diseño e Implementación de Soluciones Informáticas se encargará de realizar los procedimientos de pruebas de seguridad del desarrollador, para el caso puntual de las aplicaciones que se desarrollan a la interna del Secap.
- Una vez realizadas las pruebas, el gestor de Diseño e Implementación de Soluciones Informáticas emitirá un informe al director de Tecnologías de la Información y Comunicación a fin de que autorice su puesta en producción, quien podrá autorizar el pedido o disponer la repetición de las pruebas, hasta que sean satisfactorias.
- El director de Tecnologías de la Información y Comunicación, en casos excepcionales como fuerza mayor o urgentes, podrá autorizar el paso a producción de una aplicación / sistema sin el cumplimiento de las pruebas. En dicha autorización, hará constar también un plazo perentorio para la ejecución de las pruebas, mismas que en caso de no ser realizadas, facultará a que el director pueda disponer la suspensión de la ejecución en producción de la aplicación / sistema; así como, requerir las sanciones administrativas por el incumplimiento de una disposición de autoridad superior competente.

7. Anexos

Ninguno.