POLÍTICA DE ACCESO A REDES Y SERVICIOS DE RED

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
	Ing. Darío Braganza **Analista de Tecnologías de la Información 3**	Firmado electrónicamente por: DARIO JAVIER BRAGANZA SUAREZ
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	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 acceso a las redes institucionales del Servicio Ecuatoriano de Capacitación Profesional – Secap, y a los servicios que se brinda a través de los diversos aplicativos, deben ser manejados con las debidas seguridades, precaución y el cuidado que amerita; razón por la cual, el presente documento establece las políticas relacionadas con el acceso a redes institucionales y los servicios que se brinda a través de las mismas.

3. Alcance

Las presentes políticas son de alcance general; es decir, para todos los servidores, funcionarios, instancias, dependencias, procesos y subprocesos del Secap.

4. Propósito

Normar el acceso a las redes institucionales y los servicios que se brinda a través de las mismas, para garantizar la seguridad de la información.

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.

- 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.
- 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.).
- Servicios: Conjunto de aplicativos o programas informáticos y de comunicación de datos que apoyan la labor del Secap.
- 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.
- VPN: Virtual Private Network o red privada virtual, es una conexión en línea caracterizada por ser segura y estar cifrada (codificada) que permite establecer comunicación desde un equipo remoto a una red empresarial o institucional.

6. Políticas

6.1. Políticas de acceso a la red

- El acceso a la red interna será exclusivo a equipos de computación del Secap; en caso de dispositivos particulares, se podrán conectar a la red excepcionalmente, siempre y cuando se justifique su propósito laboral y cumplan con los requisitos de seguridad y autenticación.
- Cualquier alteración del tráfico entrante o saliente a través de los dispositivos, será motivo de verificación y tendrá como resultado directo la realización de una auditoría a la red de datos del Secap.
- Se registrará todo acceso a los dispositivos de red, mediante archivos de registro o archivos Log de sistemas.
- Será considerado como un ataque informático y una falta grave, cuando un usuario sin autorización, con fines de detectar y explotar una posible vulnerabilidad, realice la exploración de los recursos informáticos o aplicaciones de la red de datos del Secap.
- El director de Tecnologías de la Información y Comunicación autorizará las restricciones de tiempo para las sesiones de trabajo remotos de los usuarios, mientras que al jefe de

Seguridad Informática le corresponderá verificar que el sistema lleve los registros de uso. Las restricciones de tiempo deben revisarse ante cualquier cambio del estado laboral del usuario, como ascenso, remoción o terminación de contrato.

- El director de Tecnologías de la Información y Comunicación autorizará el acceso a la red inalámbrica interna, dependiendo de las características de seguridad del dispositivo con el que se desea conectar el usuario.

6.2. Políticas de servicios de red

- Los funcionarios del Secap deberán tener en cuenta que la identificación del usuario y la contraseña, que les fueron asignados por la Dirección de Tecnologías de la Información y Comunicación, son para el acceso al sistema operativo del computador y a otros servicios de información tales como: correo electrónico, Sisecap, Intranet (NAS), GPR, GLPI, Plataforma Secap Virtual; por lo cual, tomarán las medidas de seguridad necesarias a fin de evitar accesos no autorizados por terceros.
- El acceso a la configuración del sistema operativo de los equipos servidores informáticos, es únicamente permitido a los administradores de sistemas designados por la Dirección de Tecnologías de la Información y Comunicación.
- Los administradores de sistemas tendrán acceso único a los módulos de configuración de las respectivas aplicaciones que tienen bajo su responsabilidad.
- 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).
- 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.

- Se prohíbe la instalación de software que no cuente con la licencia de uso; la responsabilidad que se origine en estos casos recaerá en el usuario que la realizó y la Dirección de Tecnologías de la Información y Comunicación.
- Los usuarios que requieran utilizar un software que no sea propiedad del Secap, deberán solicitarlo a la Dirección de Tecnologías de la Información y Comunicación, justificando su uso e indicando el equipo de cómputo donde se instalará y el período de tiempo que permanecerá dicha instalación.
- Se considera una falta grave que los usuarios instalen cualquier tipo de programa (software), que no esté autorizado por la Dirección de Tecnologías de la Información y Comunicación, en las computadoras a su cargo o cualquier equipo conectado a la red de datos del Secap.
- La Dirección de Tecnologías de la Información y Comunicación será la responsable de proveer las especificaciones técnicas ante la solicitud de adquisición o desarrollo de aplicaciones automatizadas que se requiera en la entidad, así como de evidenciar que la instalación del sistema nuevo no afecte
- adversamente la seguridad general ni los sistemas existentes.
- Todo sistema de información desarrollado o adquirido por el 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.