POLÍTICAS DE AMBIENTE DE DESARROLLO SEGURO

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: ARMANDO ROBERTO PACHECO PENAFIEL
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 del Cambio

Versión	Fecha	Detalle de la modificación
1	21/10/2021	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.

Las buenas practicas que mantiene la institución, están dirigidas a establecer y proteger correctamente el ambiente de desarrollo, para la actualización e implementación de nuevos sistemas con esfuerzos de integración en el ciclo de vida del desarrollo del sistema, con lo que consecuentemente se garantiza la seguridad de la información que se procesa y almacena en los sistemas institucionales desarrollados.

3. Alcance

Las políticas aquí descritas son de aplicación exclusiva de la Dirección de Tecnologías de la Información y Comunicación; por lo que el alcance de las mismas es a dicha instancia del Secap.

4. Propósito

Normar, a través de políticas, la implementación y operación de un ambiente de desarrollo de aplicaciones seguro, a través del cual se garantice la seguridad de la información institucional.

5. Definiciones

- **Ambiente de desarrollo:** Hardware, software y herramientas utilizadas por los desarrolladores para codificar, generar, depurar, actualizar, integrar, testear, validar y ejecutar programas.
- **Aplicaciones de software:** Programa informático diseñado como una herramienta para realizar operaciones o funciones específicas.
- **Código fuente:** Archivo o conjunto de archivos, que contienen instrucciones concretas, escritas en un lenguaje de programación, que posteriormente compilan uno o varios programas.
- **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.
- **Desarrollador:** Técnico en informática, también conocido como analista programador, que se dedica a uno o más aspectos del proceso de desarrollo de software.
- **Desarrollo de software:** Conjunto de actividades informáticas dedicadas al proceso de creación, diseño, despliegue y compatibilidad de software o aplicaciones.
- **Gestor:** Funcionario, servidor o trabajador del Secap, encargado de dirigir, gestionar o administrar un proceso o subproceso de una dirección.
- **Sistemas 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.
- **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

- La Dirección de Tecnologías de la Información y Comunicación a través del área de Gestión de Administración de Servicios, Componentes de TI y Soporte Técnico a Usuarios, implementará el ambiente de desarrollo cumpliendo todos los requerimientos necesarios, en coordinación con la Gestión de Diseño e Implementación de Soluciones Informáticas.
- El gestor de Diseño e Implementación de Soluciones Informáticas en conjunto con los desarrolladores (analistas), son los responsables del acceso y correcta operación del ambiente de desarrollo.
- Al ambiente de desarrollo únicamente podrán acceder los desarrolladores y analistas de la Gestión de Diseño e Implementación de Soluciones Informáticas, con las credenciales de acceso debidamente asignadas. Las credenciales otorgadas al gestor y analistas de Diseño e Implementación de Soluciones Informáticas, tienen por objeto garantizar que únicamente sean ellos, de acuerdo con su perfil y funciones, quienes tengan acceso al código fuente de las aplicaciones para las cuales han sido designados.
- El gestor y analistas de Diseño e Implementación de Soluciones Informáticas, son los únicos responsables del correcto uso y manejo de las credenciales de acceso (usuario y contraseña).
- En caso de que un analista de otra gestión de la DTIC requiera acceso al ambiente de desarrollo, deberá solicitar autorización al director de TIC, justificando técnicamente el motivo del acceso. En caso de autorizarse el acceso, se emitirán las credenciales de acceso con tiempo de validez específico y los permisos para las tareas que se vayan a efectuar únicamente.
- Durante la fase de desarrollo o codificación de los requerimientos funcionales y no funcionales de las aplicaciones o sistemas que estén desarrollando, los analistas del área de Gestión de Diseño e Implementación de Soluciones Informáticas deberán documentar, archivar y versionar todos los modelos creados y/o actualizados como consecuencia del requerimiento, diseño y desarrollo de los sistemas.

- El código fuente debe residir en el ambiente de desarrollo y se recomienda que mantenga una copia en el computador personal del desarrollador.
- En caso de que el gestor de Diseño e Implementación de Soluciones Informáticas y los desarrolladores requieran tener acceso remoto al ambiente de producción, deberán solicitar autorización al director de TIC y con su aprobación, coordinar con la Gestión de Administración de Servicios, Componentes de TI y Soporte Técnico a Usuarios, el acceso respectivo a través de VPN.

7. Anexos

Ninguno.