Academia Nacional de Seguridad Pública

1.0 CONTROL DE CAMBIOS

Revisión:	0	1	2	3	4	5	6	7
Fecha:	13/09/2017							
	Modificación Por ajustes a estructura organizativa							

Elaboró:	Revisó:	Aprobó:
Ing. Hugo Nelson Avilés López	Lic. José Antonio García Hernández	Comisionado Pablo de Jesús Escobar Baños
Jefe Unidad. de Tecnología de Información	Jefe Secretaría Técnica y de Planificación Institucional	Director General

2.0 **INTRODUCCIÓN:**

Las tecnologías de información y comunicación que utiliza la ANSP (Academia Nacional de Seguridad Pública) están orientadas en fortalecer los procesos de formación académica, para ofrecer un mejor servicio a la PNC y a la ciudadanía; por ello, el buen uso y correcto funcionamiento de las tecnologías de información y comunicación es de gran importancia para el cumplimiento de los objetivos estratégicos, y es necesario que se reconozca y comprenda por cada usuario su papel en la protección del patrimonio y servicios de la ANSP.

La ANSP depende en gran medida de sus sistemas de información y comunicación, por cuanto las tecnologías de información son un pilar fundamental para los procesos de formación; almacenando y procesando detalles de alumnos, personal docente y administrativo, así como una serie de registros de transacciones que se realizan con otras instituciones. Una amenaza directa a la seguridad de nuestros sistemas informáticos, significa una amenaza directa a los procesos de formación.

3.0 **MARCO LEGAL:**

Este documento se basa en el cumplimiento de la Ley de Ética Gubernamental de El Salvador, artículos 4 literal l) y 5 literal a), publicado en el diario oficial No. 229, tomo No. 393 de fecha 7 de diciembre de 2011; Ley de Acceso a la Información Pública, publicada en el diario oficial No.70, tomo No. 371, de fecha 8 de abril de 2011; Normas Técnicas de Control Interno Especificas de la ANSP, Art. 38, publicada en el diario oficial No. 160, tomo No. 408, de fecha 3 de septiembre de 2015; Reglamento Interno de Trabajo, artículo 49 literales l), m) y q), emitido en noviembre de 2001. Siendo responsabilidad y compromiso de los usuarios leer, comprender y aplicar el contenido en nuestras funciones diarias dentro de la institución y es responsabilidad del jefe del Unidad de Tecnología de Información la revisión, actualización y divulgación del presente documento, el cual deberá revisarse cada vez que sea necesario debido a modificaciones a las anteriores leyes y reglamentos.

4.0 **POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN**

"En la ANSP estamos comprometidos en formar profesionales en seguridad pública y ciencias policiales, utilizando como las tecnologías de información y comunicación, mediante personal capacitado para la administración y uso de la infraestructura tecnológica institucional, mejorando los procesos y gestionando los riesgos informáticos para brindar información confiable, íntegra y oportuna."

5.0 **OBJETIVOS DE SERGURIDAD DE LA INFORMACIÓN:**

1. Socializar el uso seguro de las TIC´s a todos los empleados, personal en comisión de servicio y estudiantes;

2. Contar con personal capacitado en normas y estándares de mejores prácticas de seguridad de la información que administre las Tecnologías de Información capacitado;

3. Implementar las normas y estándares de mejores prácticas de seguridad de la información en los procesos del Sistema de Gestión de Calidad de la ANSP;

4. Garantizar la seguridad de la información, protegiendo la integridad de la misma a través de la implementación de mejores prácticas basadas en normas y estándares de la industria, las cuales deberán asegurarse que el acceso y disponibilidad sean acordes a las políticas y reglamentos institucionales; aplicando métodos, procesos o técnicas para la protección de los sistemas y plataformas tecnológicas los cuales deberán ser evaluados periódicamente;

5. Implementar un plan de contingencia de todos los servicios informáticos institucionales.

6.0 LINEAMIENTOS PARA LA SEGURIDAD DE LA INFORMACIÓN

6.1 PROCESAMIENTO Y MANEJO DE LA INFORMACIÓN

1. El procesamiento y manejo de la información implica la protección de la información en términos de:

a. Confidencialidad: Divulgar la información sólo a las personas autorizadas.

b. Integridad: Garantiza la exactitud de la información.

c. Disponibilidad: Asegurar el acceso y la utilización oportuna de la información.

2. El procesamiento y manejo de la información es importante porque nuestro éxito estará amenazado si la seguridad de nuestros sistemas informáticos se viera comprometida. Para entender el procesamiento y manejo de la información el usuario debe de:

a. Saber de cuáles instalaciones y equipo informático son de nuestra responsabilidad.

b. Saber con cuáles sistemas informáticos interactuamos y por qué.

c. Saber las medidas de seguridad y/o políticas que requieres para protegerlos.

3. En esencia, el procesamiento y manejo de la información se refiere al uso apropiado de controles y de la buena aplicación de la tecnología. Por ejemplo, no tiene sentido instalar una alarma contra ladrones si se olvida activarla. Esto mismo cuenta para la seguridad de la información, donde los controles no serán efectivos si los usuarios no los utilizan adecuadamente.

6.2 RESPONSABILIDADES DE LOS USUARIOS

Todos los usuarios empleados, personal en comisión de servicio y estudiantes son responsables de la información almacenada y generada en los recursos tecnológicos asignados; para el caso de usuarios que comparten un recurso tecnológico, son responsables de la información almacenada y generada con sus credenciales de acceso. Asimismo, cada usuario es responsable de la confidencialidad de la información a la cual se tiene acceso.

El usuario debe:

1. Luego de una renuncia, despido o traslado de personal a su cargo, además de realizar el debido proceso con el Departamento de Talento Humano, deberá solicitar al Unidad de Tecnología de Información la cancelación de sus accesos mediante un correo electrónico a soporte.dti@ansp.edu.sv.

2. Reportar a la Unidad de Tecnología de Información eventos que pongan en riesgo la confidencialidad de la información enviando un correo electrónico a soporte.dti@ansp.edu.sv.

3. Evitar la divulgación de información reservada o confidencial, conforme a lo establecido en la Ley de Acceso a la Información Pública.

4. El uso de equipos de cómputo propiedad del usuario como computadoras portátiles para realizar actividades de trabajo institucionales dentro de las instalaciones, deberán ser previamente autorizados por la jefatura inmediata del mismo.

5. El uso de equipos de cómputo propiedad del usuario para realizar actividades de trabajo institucionales de forma remota o teletrabajo, deberán ser previamente autorizados por la Unidad de Tecnología de Información de la ANSP, a solicitud de la jefatura inmediata del usuario.

6.3 ACCESO A SISTEMAS INFORMÁTICOS

6.3.1 CLAVES O CONTRASEÑAS

1. Las cuentas de usuario de acceso a los sistemas informáticos son confidenciales, personales, únicas e intransferibles.

2. Las claves o contraseñas son llaves que permiten acceder a información de la ANSP y son utilizadas para controlar el acceso a sistemas informáticos como: datos de personas, información financiera, sistemas operativos, proyectos, entre otros. Por lo que es deber de cada usuario mantenerlos en la más estricta confidencialidad.

3. Las cuentas de usuario de acceso a sistemas deben ser solicitadas por el jefe del área correspondiente a la Unidad de Tecnología de Información de la ANSP.

4. Toda jefatura institucional será responsable de solicitar las bajas de usuarios o cambios de roles, para que sean aplicados en los sistemas informáticos correspondientes.

5. El usuario debe:

a. Recordar que cada uno es responsable de sus propias contraseñas.

b. Cambiar inmediatamente cualquier contraseña que alguien más la sabe.

c. Bloquear la sesión de usuario (Win+L) al levantarnos de nuestro puesto de trabajo por un tiempo prolongado (más de 15 minutos).

d. Cerrar sesión de usuario al término de nuestra jornada de trabajo.

6.3.2 COMPUTADORAS PERSONALES

Las computadoras son recursos informáticos poderosos y flexibles que procesan una amplia variedad de datos, por lo tanto, es necesario protegerlos al igual que debemos proteger la información que contienen.

El usuario debe:

1. Usar las computadoras sólo en actividades de trabajo.

2. Reportar a la Unidad de Tecnología de Información, todos los casos de robo o pérdida de periféricos o equipo de cómputo.

3. Reportar a la Unidad de Tecnología de Información, cualquier problema o mal funcionamiento del equipo de cómputo.

4. Al compartir información, asegúrese de configurar usuario y contraseña para acceder a la información y evitar así el acceso de cualquier usuario.

5. Evitar el traslado de computadoras de escritorio desde un lugar a otro sin la colaboración de la Unidad de Tecnología de Información.

6. Evitar la conexión de una computadora a la red de datos de la Academia sin la autorización de Unidad de Tecnología de Información.

6.3.3 MANEJO DE DISPOSITIVOS DE ALMACENAMIENTO EXTRAÍBLE

Los dispositivos de almacenamiento extraíble como memorias USB, discos duros externos, CD o DVD se pueden perder, reemplazar, dañar y/o manejar con facilidad, por lo tanto, es esencial que tenga un control sobre ellos.

El usuario debe:

1. Mantener guardados los dispositivos de almacenamiento en lugares cerrados y no al alcance de todos, mientras no se estén utilizando.

2. Tener identificados todos los medios de almacenamiento para evitar pérdida de información.

3. Someter a revisión de antivirus todos los dispositivos de almacenamiento extraíble que se reciban o se envíen a organizaciones externas o personas.

6.3.4 USO DE SOFTWARE

1. Los usuarios no se encuentran autorizados a instalar, ejecutar o usar software (bajo contrato de licencia o no licenciado) en forma personal en las computadoras que son propiedad de la ANSP.

2. Toda instalación y configuración del software deberá realizarse por la Unidad de Tecnología de Información.
3. La Unidad de Tecnología de Información, podrá eliminar todo software instalado que no cumpla con esta norma.

4. En caso de vencimiento de la licencia del software utilizado, el usuario debe informar a la Unidad de Tecnología de Información para su renovación.

5. El usuario es responsable de almacenar adecuadamente los archivos generados de la utilización del software instalado.

6. Queda prohibido:

a. Instalar o usar software que no haya sido autorizado y aprobado por la Jefatura de la Unidad de Tecnología de Información.

b. Abrir o ejecutar archivos de dudosa procedencia.

c. Usar cualquier software que se enlista a continuación:
   i. Software de juegos y recreación de cualquier tipo, excepto aquellos que formen parte de paquetes de software autorizados.
   ii. Cualquier software no autorizado que haya sido obtenido de Internet o de cualquier otro medio externo.
   iii. Copias sin licencia de software autorizado.

6.3.5 CONFIDENCIALIDAD DE LA INFORMACIÓN

1. El manejo de la información será de acuerdo a lo establecido en La Ley de Acceso a la Información Pública, por lo tanto, se considera reservada o confidencial según lo establecido en los artículos 19 y 24 de dicha ley.

2. Los datos reservados y confidenciales deben protegerse, el respeto de la confidencialidad constituye una de las responsabilidades laborales más importantes según lo establecido en la Ley de Acceso a la Información Pública y será sancionado de acuerdo a lo establecido en los artículos 76 y 77 de dicha ley.

3. Cumplir con cualquier lineamiento, instrucción, normativa o legislación aplicable y no contemplada en los puntos anteriores.

4. El usuario debe:
    a. Mantener la confidencialidad de la información aún después de haber salido de ANSP.

    b. No acceder, copiar, divulgar ni transferir datos confidenciales o reservados para los cuales no se le haya proporcionado la autorización correspondiente.

    c. Cuando se transmita información confidencial a personas externas de la institución:
        i. Debe darse aviso al destinatario de la misma antes de transmitirla.
        ii. Siempre que sea posible, el destinatario debe estar presente para recibirla.
        iii. La información debe ser transmitida únicamente a través de los canales institucionales y autorizados para proporcionar dicha información.

iv. Debe investigarse de inmediato cualquier demora en la transmisión.
v. Debe confirmarse la recepción de la información.

6.3.6 USO DE COMPUTADORAS PORTÁTILES

1. Las computadoras portátiles y las telecomunicaciones crean nuevas oportunidades para el trabajo a distancia. Sigue estas reglas para reducir los riesgos asociados a la seguridad de la información.

2. El usuario debe:
    a. Utilizar la VPN institucional para realizar una conexión remota con el equipo informático de la ANSP o personal desde lugares públicos como cibercafés, centros comerciales, restaurantes, entre otros.
    b. No compartir el equipo portátil asignado por la ANSP con personas ajenas a la institución.

    c. Bloquear la sesión de usuario (Win+L) al levantarnos de nuestro puesto de trabajo por un tiempo prolongado (más de 15 minutos).

    d. Cerrar sesión de usuario al término de nuestra jornada de trabajo.

6.3.7 USO DE INTERNET

1. El acceso o uso de Internet es exclusivo para asuntos laborales, y con previa autorización del jefe inmediato. Toda computadora que tiene acceso a internet debe tener antivirus instalado y actualizado, los usuarios deben ser precavidos en los sitios que visitan, ya que el Internet es la principal fuente de virus.

2. EL acceso a internet en las computadoras, vía telefónica por medio de MÓDEMS USB será permitido únicamente usando los módems institucionales provistos por la Unidad de Tecnología de Información.

3. En caso que el empleado haga teletrabajo, la computadora que usa para acceder a la red de la ANSP vía VPN debe contar con antivirus actualizado y no tener instalado programas que no hayan sido aprobados e instalados por el personal de Unidad de Tecnología de Información, por lo que se establece que:
    a. Todas las conexiones y categorías de contenido web que el usuario desee, deben estar justificadas por las necesidades del área y aprobadas por el Jefe inmediato.
    b. Está prohibido el acceso a material pornográfico, frívolo o juegos en Internet.

6.3.8 USO DEL CORREO ELECTRÓNICO

1. El uso del correo electrónico es exclusivamente para fines laborales, la información es confidencial y de uso de la institución.
2. La Unidad de Tecnología de información es la encargada de la administración de los servicios de correo electrónico, Creación de cuentas, cambios de contraseña, desactivar cuentas de correo y demás.

3. Las cuentas de correo electrónico se crearán a petición de la jefatura inmediata del usuario al que se le creará la cuenta.

4. Se establece que:
    a. Está prohibido elaborar y enviar mensajes difamatorios, ofensivos e ilegales para fines perjudiciales, ya sean raciales, sexuales o de cualquier otra clase.

    b. Las cadenas de correos o similares, así como adjuntar archivos ejecutables o que pongan en riesgo el funcionamiento de los equipos.

c. Prohibido compartir correos electrónicos con personal externo con fines de extraer información institucional.

6.3.9 USO DE TELEFONÍA FIJA Y MÓVIL

El uso de telefonía fija y móvil institucional es exclusivamente para fines laborales y no podrán usarse para fines lucrativos y/o comerciales. Toda actividad realizada a través del servicio de telefonía es responsabilidad de la persona a la cual se le ha asignado una línea telefónica, ya sea fija o móvil.

Se establece que:

1. La Dirección General es la encargada de asignar las líneas telefónicas móviles y el monto o plan asignado.

2. Es responsabilidad de la Unidad de Tecnología de Información, controlar la entrega y recepción de líneas telefónicas móviles con su respectivo aparato.

3. La Jefatura de la Secretaría Técnica y de Planificación Institucional es la encargada de asignar las líneas telefónicas fijas y sus restricciones (minutos por llamada, salida a teléfonos móviles y llamadas internacionales).

4. Es responsabilidad de la Unidad de Tecnología de Información controlar la entrega y recepción de las líneas fijas con sus respectivos aparatos, la configuración y monitoreo de las restricciones de las mismas.

5. Es responsabilidad del usuario al cual se le ha asignado un aparato telefónico, conservarlo en buen estado de funcionamiento.

6. En caso de traslado, cese de comisión de servicio, cese de laborales, es responsabilidad del usuario al cual se le ha asignado el aparato de telefonía móvil, entregarlo a la Unidad de Tecnología de la Información.

7. Queda prohibido utilizar los servicios telefónicos de líneas de entretenimiento.

8. Para líneas móviles, en caso de suscripciones a servicios no contratados por la ANSP que generen costos adicionales (backtones, horóscopo, descarga de programas, entre otros), estos deberán ser pagados por el usuario que tiene asignada la línea telefónica móvil.

9. Todo usuario poseedor de una línea móvil institucional deberá utilizar un método de seguridad de acceso al aparato (patrón, pin, contraseña, huella u otro).

10. En caso de robo o extravío o daño irreparable del aparato telefónico móvil, el usuario deberá notificar de inmediato a la Unidad de Tecnología de Información, quien indicará el procedimiento a seguir para el pago del deducible del seguro del aparato y la reposición del mismo.

7.0 **TÉRMINOS Y DEFINICIONES:**

Usuario: Persona que hace uso de los recursos o servicios informáticos o de comunicación, ya sea personal interno o externo a la ANSP.

Sistema de Información o Sistema Informático: sistema computacional que se utiliza para obtener, almacenar, manipular, administrar, controlar, procesar, transmitir o recibir datos, para satisfacer una necesidad de información.

Tecnología de Información y Comunicación: herramientas computacionales e informáticas que procesan, almacenan, sintetizan, recuperan y presentan información.

Computadora: es una máquina electrónica que recibe y procesa datos para convertirlos en información conveniente y útil. Estas pueden ejecutar tareas diversas con suma rapidez y bajo el control de un programa.

Computadora Personal: también conocido como PC (sigla en inglés de personal computer) es una computadora diseñada para ser utilizada por una sola persona a la vez. En cuanto a su movilidad podemos distinguir entre computadora de escritorio y computadora portátil o laptop.

Servidor: computadora en la que se ejecuta un programa que realiza alguna tarea de otras aplicaciones llamadas cliente, ya sea almacenando, procesando o entregando información.

Hardware: se refiere a todas las partes tangibles de un sistema informático; sus componentes eléctricos, electrónicos, electromecánicos y mecánicos; como cables, gabinetes o cajas, periféricos de todo tipo y cualquier otro elemento físico involucrado.

Software: Es el conjunto de los programas de cómputo, procedimientos, reglas, documentación y datos asociados, que forman parte de las operaciones de un sistema informático.

Recurso Tecnológico: Es un medio que se vale de la tecnología para cumplir con su propósito. Los recursos tecnológicos pueden ser tangibles (como una computadora o impresora) o intangibles (sistema o aplicación virtual), incluye a los dispositivos, software o recursos de computación en la nube, que pueden procesar, almacenar y/o transmitir información.

Virus informático: software que tiene por objeto alterar el normal funcionamiento de la computadora.

Antivirus: software que tiene por objeto proteger la computadora de virus informáticos.

Licencia de software: contrato entre la ANSP y el fabricante del software informático para utilizar el software cumpliendo una serie de términos y condiciones establecidas dentro de sus cláusulas.

Software libre: el software libre se refiere a la libertad de los usuarios para ejecutar, copiar, distribuir, y estudiar el mismo, e incluso modificar el software y distribuirlo modificado

Internet: conjunto de redes de comunicación interconectadas de alcance mundial.

Red de comunicación: conjunto de medios de transmisión y conmutación necesarios para el intercambio de información entre los usuarios.

Cifrado de datos: procedimiento que utilizando un algoritmo con cierta clave transforma un mensaje de tal forma que sea incomprensible o al menos difícil de comprender a toda persona que no tenga la clave para poder descifrarlo.

FTP: Protocolo para la transferencia de archivos entre dos o más computadoras por medio de una red de comunicación.

Chat: comunicación escrita realizada de manera instantánea mediante el uso de un software y a través de Internet entre dos, tres o más personas ya sea de manera pública o privada.

Credenciales de acceso: nombre y contraseña asignado por la Unidad de Tecnología de Información para ingresar al equipo informático, sistemas o aplicaciones informáticas.

Representante patronal: personas que ejercen funciones de dirección o de administración en la institución.

VPN: (siglas en inglés de virtual private network) es una tecnología que permite una extensión segura de la red institucional sobre una red pública o no controlada como Internet. Normalmente utilizada para realizar conexiones remotas por medio de Internet a la red institucional.

8.0 MATRIZ DE REGISTRO:

Nombre del formato	Código del formato
FORMATO DE HOJA DE SERVICIO	GT-FR-015