Aprueba Manual para el uso de Computadora Personal, aplicaciones de escritorio, antivirus, tecnologías móviles y redes de comunicación.

RESOLUCIÓN EXENTA 180

SANTIAGO, 18 DE FEBRERO DE 2021

VISTOS: Lo dispuesto en la Ley N° 20.502, que crea el Ministerio del Interior y Seguridad Pública y el Servicio Nacional para la Prevención y Rehabilitación del Consumo de Drogas y Alcohol; la ley N°19.886 de Bases sobre Contratos Administrativos de Suministros y Prestación de Servicios; el DFL N° 2-20.502, de 2011, del Ministerio del Interior y Seguridad Pública; la ley N°19.880 que Establece Bases de los Procedimientos Administrativos que Rigen los Actos de los Órganos de la Administración del Estado; el Decreto con Fuerza de Ley N° 1-19.653, de 2000, que fijó el texto refundido, coordinado y sistematizado de la Ley N° 18.575, Orgánica Constitucional de Bases Generales de la Administración del Estado; el Decreto con Fuerza de Ley N° 29, de 2004, del Ministerio de Hacienda, que fija texto refundido, coordinado y sistematizado de la ley N° 18.834, sobre Estatuto Administrativo; en el Decreto Supremo N° 1.307, de 2 de octubre de 2018, del Ministerio del Interior y Seguridad Pública; en el Decreto Exento Nº 1.436, de 29 de septiembre de 2020, del Ministerio del Interior y Seguridad Pública, en la Resolución Nº 7, de fecha 26 marzo de 2019, y en la Resolución Nº 16, de fecha 30 de noviembre de 2019, ambas de la Contraloría General de la República, que fijan normas sobre exención del trámite de Toma de Razón; y

CONSIDERANDO:

1.- Que, el Servicio Nacional para la Prevención y Rehabilitación del Consumo de Drogas y Alcohol, en adelante también SENDA, es un servicio público descentralizado, dotado de patrimonio y

NR/CG/PC/RD/NM

DISTRIBUCIÓN

1.- Área de Auditoría Interna
2.- División Jurídica
3.- División de Administración y Finanzas
4.- División Programática- Área de Prevención
5.- Unidad de Gestión Documental
S-1832/21

personalidad jurídica propia, que tiene por objeto la ejecución de las políticas en materia de prevención del consumo de estupefacientes, sustancias psicotrópicas e ingestión abusiva de alcohol, y de tratamiento, rehabilitación y reinserción social de las personas afectadas por dichos estupefacientes y sustancias psicotrópicas. Le corresponde también la elaboración de una estrategia nacional de drogas y alcohol.

2.- Que, en cumplimiento de compromisos adquiridos y acordados entre la jefatura del Área de Administración y Finanzas se hizo necesario, aprobar, mediante acto administrativo, el siguiente documento técnico de la referida área:

-Manual de Procedimiento para el uso de Computadora Personal, Aplicaciones de escritorio, Antivirus, Tecnologías móviles y Redes de Comunicación.

3.- Que, de acuerdo a lo prescrito en el artículo 3 de la ley N°19.880 que Establece Bases de los Procedimientos Administrativos que Rigen los Actos de los Órganos de la Administración del Estado, corresponde que el aludido documento antes individualizado, sea formalizado a través de un acto administrativo, razón por la cual,

RESUELVO:

PRIMERO: Apruébese el Manual para el uso de Computadora Personal, aplicaciones de escritorio, antivirus, tecnologías móviles y redes de comunicación, del Servicio Nacional para la Prevención y Rehabilitación del Consumo de Drogas y Alcohol.

SEGUNDO: El texto íntegro del manual que por medio de este acto administrativo se aprueba, es del siguiente tenor:

Procedimientos Computadora Personal - Aplicaciones de Escritorio - Antivirus - Tecnologías Móviles – Redes de Comunicación

Unidad TI

01 de febrero de 2021

División de Administración y Finanzas

“Trabajemos con impecabilidad y propósito”

1. FINALIDAD

Establecer el procedimiento para proteger los activos físicos e intelectuales utilizados en la **generación de información del Servicio.**

2. ALCANCE

Aplica al nivel central y todas sus áreas y unidades, direcciones regionales. Además, aplica a todos los funcionarios de SENDA.

3. DEFINICIONES

SISTCOM: Plataforma de levantamiento de ticket, dirigidos a la unidad de TI, para la atención de requerimientos.

Requerimiento: solicitudes informáticas realizadas a la unidad de TI mediante canales digitales como SIDOC, correo electrónico, SISTCOM.

IP: La dirección IP o simplemente IP, se basa en el protocolo de Internet, que es, además, la base del funcionamiento de Internet. Siendo un conjunto de números que identifica, de manera lógica , inequívoca y jerárquica, a una interfaz en la red (elemento de comunicación/conexión) de un dispositivo (computadora, laptop, teléfono inteligente, servidor o impresora entre otros).

De forma similar a como un número de teléfono es único dentro de una red telefónica. La dirección IP consta de cuatro números separados por puntos y cada número es menor de 256; por ejemplo 192.200.44.69.

Principalmente se distingue entre las direcciones IP dinámicas y las estáticas. Además, también existen direcciones IP “para usos especiales”, de las cuales la mayoría están reservadas para redes privadas.

Asignación de IP: Existen diferentes formas de asignación de dirección IP, como se menciona en la definición anterior, tendremos direcciones dinámicas, estáticas y reservadas.

Dirección IP Dinámica: Una dirección IP dinámica es una IP asignada al usuario, mediante un servidor DHCP (Dynamic Host Configuration Protocol), dentro de un parámetro o intervalo de direcciones, definida por el administrador de la Red.
Esta dirección se proporciona de forma automática al dispositivo que esté configurado de esta forma, y es el caso normalmente utilizado en las conexiones Wifi, o en las redes domésticas, cuando nos conectamos ya sea de forma inalámbrica o cableada y sin hacer mayores configuraciones, ya estamos conectados.

Este tipo de conexiones normalmente suelen ser aleatorias y variables en su asignación, debido a que duran por un tiempo limitado asignado a un determinado dispositivo, es por esto, que en el tiempo, pueden ir cambiando las direcciones que se vayan asignando a este, cada vez que nos conectemos. Dirección IP Manual: Será asignada por el Administrador de la red, a un dispositivo en particular y normalmente es usado, cuando necesitamos saber que la dirección no variara y que los dispositivos serán ubicados a la dirección dada, de forma inequívoca e invariable, de modo que siempre que recurramos a esta, nos encontraremos por ejemplo con: Un Servidor, la impresora de una oficina o piso en particular, un router, etc.

DHCP: (Dynamic Host Configuration Protocol). Protocolo de configuración dinámica de host. Protocolo que usan los ordenadores para obtener información de configuración. El DHCP permite asignar una dirección IP a un ordenador sin requerir que un administrador lo configure en la base de datos de un servidor.

GSUITE: La G Suite (o Google Suite) es un conjunto de herramientas ofimáticas y empresariales que Google provee en la nube a empresas para mejorar la productividad de la operación, abriendo la posibilidad de utilizar aplicaciones web como: Correo electrónico (GMAIL), Chat (HANGOUTS), Calendario (CALENDAR), Documentos (DOCS), Almacenamiento en la nube (DRIVE), entre otros.

Firewall: (Cortafuegos) Es un ordenador o un programa que conecta una red a Internet, pero impide el acceso no autorizado desde Internet. Mecanismo que permite que las comunicaciones entre una red local e Internet se realicen conforme a las políticas de seguridad de quien los instala. Estos sistemas suelen incorporar elementos que garantizan la privacidad, autentificación, etc., con lo que se impide el acceso no autorizado desde Internet.

Virus: Los virus son programas diseñados para infiltrarse en su ordenador y dañar o alterar sus archivos y datos. Los virus tienen la capacidad de corromper o eliminar los

datos de su equipo. Y al igual que los virus naturales, también se replican. Un virus informático es más peligroso de que un gusano informático, ya que modifica o elimina sus archivos, mientras que los gusanos solo se replican sin efectuar cambios en sus archivos o datos.

Ejemplos de virus: W32.Sfc!mod ABAP.Rivpas.A Accept.3773

Los virus pueden infiltrarse en su equipo como archivos adjuntos de imágenes, saludos o archivos de audio/vídeo. Otra de las vías de entrada habituales son las descargas de Internet. Pueden ocultarse en programas gratuitos o de prueba, o en otros archivos descargados.
Por eso, antes de descargarse nada de Internet, debe estar seguro de lo que es. Casi todos los virus llevan adjunto un archivo ejecutable, lo que significa que los virus pueden encontrarse en su equipo pero no pueden afectar a menos que abra o ejecute el programa malicioso. Hay que destacar que los virus no se pueden propagar sin intervención humana, como cuando ejecutamos un programa infectado.

PROCEDIMIENTO COMPUTADORA PERSONAL

Todo funcionario que requiera el uso de una computadora, le será asignada una de acuerdo a la disponibilidad que cuente la unidad de TI, la que evaluará las características técnicas mínimas necesarias para el desarrollo de sus labores.
Esta asignación se realizará mediante la comunicación desde el área de Gestión de Personas que informará el ingreso de nuevos funcionarios y/o requerimientos que provengan desde la Jefatura del área de Operaciones.

El equipo será instalado en la ubicación física que sea informada, el técnico de soporte le asignará una IP al computador para el acceso a la red SENDA, servicio de internet e impresión.
La dirección IP podrá ser dinámica o estática de acuerdo a lo que defina el administrador de sistemas.

Traslado puesto de trabajo

Todo traslado de puesto de trabajo que requiera el movimiento del computador, deberá ser solicitado mediante la plataforma SISTCOM, para que los técnicos de la unidad de TI realicen la tarea, en el caso de las Direcciones Regionales deberán dar aviso al encargado UAF de la región.

Atención de Soporte

Para la atención de solicitudes de soporte técnico el funcionario debe generar un ticket de atención en la plataforma SISTCOM, donde un técnico le asistirá de manera presencial o remota según sea el caso.

Los equipos quedarán bajo responsabilidad del funcionario asignado, entregándoles en buen estado.

Queda totalmente prohibido:

a) Usar software indebido u ocasionar cualquier daño o modificación al computador asignado.

b) El uso de cualquier medio de almacenamiento (USB, celulares, discos duros externos, cámaras fotográficas, memory stick, CD, DVD, etc.), sin antes haberlo analizado con el antivirus institucional instalado en los equipos.

c) Utilizar el equipo para fines no laborales.

PROCEDIMIENTO APLICACIONES DE ESCRITORIO

Todo computador tendrá instalado como mínimo los siguientes programas de escritorio los cuales son la base para desarrollar las labores en el servicio.
Los programas a instalar son: Sistema Operativo, Ofimática, antivirus, winzip, adobe reader, se hace la salvedad que la licencia de ofimática será instalada dependiendo de la disponibilidad de licencias que tenga el servicio, tanto en cantidad como versionamiento, en caso de no contar con una el funcionario deberá utilizar las aplicaciones dispuestas en la plataforma de Gsuite, que se encuentran habilitadas para todos los usuarios.

SOFTWARE ADICIONALES

Si un funcionario para el desarrollo de sus labores requiere de un software en particular, deberá realizar la solicitud a través de la jefatura del área de Operaciones justificando su uso. La unidad de TI verá la disponibilidad de licencia y si no se tuviese, el requirente deberá realizar una solicitud de recursos para su adquisición, esta estará sujeta a la disponibilidad presupuestaria que haya en el momento.

ANTIVIRUS

La unidad de TI cuenta con un antivirus institucional para todos los equipos que son de propiedad del servicio o se encuentran en modalidad de arriendo.
Le compete a la unidad de informática lo siguiente:

Implementar y administrar el programa antivirus institucional que será el único y oficial de la institución.

Establecer una configuración base para la protección de los equipos computacionales, con el fin de evitar la propagación de virus y la instalación de software no deseado por parte de los usuarios.

Mantener una consola de administración centralizada, que permita gestionar usuarios y distribuir actualizaciones a través de la red.

En el caso de los funcionarios, deben verificar que la información almacenada en el computador esté libre de virus y otras amenazas informáticas, para lo cual deberá velar porque el antivirus institucional esté instalado y debidamente actualizado.

PROCEDIMIENTO TECNOLOGÍAS MÓVILES

La unidad de TI debe llevar un registro de asignación y control de todos los dispositivos móviles que posee la Entidad.

El funcionario debe hacer buen uso de los dispositivos móviles que son asignados para el desempeño de sus funciones laborales.

Los dispositivos móviles que son asignados a los funcionarios deben ser protegidos mediante el uso e implementación de los controles apropiados para ello, como son: contraseña de acceso, candado de seguridad para notebook, políticas de restricción en la ejecución de aplicaciones, abstenerse de utilizar redes públicas para conectarse a internet.

Los dispositivos móviles como celulares que almacenan información del Servicio deben contar con un sistema de autenticación, como un patrón, código de desbloqueo o una clave.
El funcionario responsable del dispositivo móvil debe hacer periódicamente copias de respaldo, en caso de los equipos portátiles deberán tener instalado el aplicativo file stream de Drive, con el fin de que se ejecute la copia de respaldo de la carpeta destinada para esta función.

Los funcionarios son responsables de garantizar el buen uso de los dispositivos móviles en redes seguras y con la protección adecuada para evitar acceso o divulgación no autorizada de la información almacenada y procesada en ellos.

PROCEDIMIENTO REDES DE COMUNICACIÓN

Objetivo: Establecer los controles necesarios para proteger la información del Servicio transmitida desde la red interna de SENDA.

La unidad de TI es la responsable de administrar y gestionar la red nacional del Servicio, así también de establecer los controles lógicos para el acceso a los diferentes recursos informáticos, con el fin de mantener los niveles de seguridad apropiados.

La unidad de TI proporciona a los funcionarios tanto del nivel central como de las oficinas regionales todos los recursos tecnológicos de conectividad necesarios para que puedan desempeñar las funciones y actividades laborales, por lo cual no es permitido conectar a las estaciones de trabajo o los puntos de acceso de la red SENDA, elementos de red (tales como switches, enrutadores, entre otros equipos de comunicaciones)

El trabajo a través de medios remotos a la red de datos del SENDA por parte de los funcionarios, sólo se permitirá de acuerdo a la autorización previa de la Jefatura de la División de Administración y Finanzas y/o de la Jefa del área de Operaciones.

Para acceso remoto relacionadas con proveedores externos que se encuentren ejecutando algún proyecto, será el encargado de la unidad de TI, quien concederá las autorizaciones respectivas.

La unidad de TI establecerá un esquema de segregación de redes, con el fin de controlar el acceso a los diferentes segmentos de red y garantizar la confidencialidad, integridad y disponibilidad de la información.

La unidad de TI establecerá una serie de parámetros técnicos para la conexión segura de la red con los servicios de red, así también de establecer mecanismos de autenticación seguros para el acceso a la red.

Las redes inalámbricas de las redes internas estarán separadas lógicamente, para mitigar accesos no autorizados.

Responsabilidades del usuario

Los recursos informáticos, datos, programación (software), redes y sistemas de comunicación electrónica están disponibles exclusivamente para realizar las funciones para la que fueron diseñados e implantados. Los funcionarios son responsables de toda actividad relacionada al uso de su acceso autorizado.

Los funcionarios notificarán a su jefe inmediato y la unidad de TI sobre cualquier incidente que detecten que afecte o pueda afectar a la seguridad de los datos, o por sospecha de uso indebido del acceso autorizado por otras personas.

Todo funcionario es responsable de proteger y no compartir su contraseña. En caso de que algún usuario piense que su contraseña ha sido vulnerada, debe notificar inmediatamente al administrador de sistemas de la unidad de TI. El administrador de seguridad definirá una contraseña provisoria, la cual deberá ser cambiada por el usuario.

El funcionario deberá reportar de forma inmediata cuando detecte algún riesgo real o potencial sobre equipos de computadoras o de comunicaciones, tales como caídas de agua, choques eléctricos, caídas, golpes o peligro de incendio, entre otros. De igual forma, tiene la obligación de proteger las unidades de almacenamiento que se encuentren bajo su responsabilidad y que contengan información confidencial o importante.

Todo usuario que accede a los Sistemas de Información del SENDA debe utilizar únicamente las versiones de los programas autorizados y siguiendo sus normas de utilización.

• Queda prohibido

a) Instalar copias ilegales de cualquier programa, incluidos los estandarizados.

b) Instalar cualquier dispositivo que altere la configuración actual de la red, entiéndase la instalación de: routers, access points, switch, hubs, impresoras, dispositivos alternos para conexión a Internet, entre otros.

c) Destruir, alterar, inutilizar o dañar de cualquier otra forma los datos, programas o documentos electrónicos.

TERCERO: Corresponderá a la División de Administración y Finanzas del Servicio, velar por la difusión y correcta implementación del manual que por medio de este acto administrativo se aprueba.

ANÓTESE Y COMUNÍQUESE

DIRECTOR NACIONAL
SERVICIO NACIONAL PARA LA PREVENCIÓN Y
REHABILITACIÓN DEL CONSUMO DE DROGAS Y ALCOHOL

Documento firmado digitalmente por KATHERINE VERONICA SCHMIED VASQUEZ
Fecha 18-02-2021 09:05:09
Santiago, Chile
Este documento cuenta con una firma electrónica avanzada según lo indica la ley N° 19.799.
Para verificar su validez debe acceder a https://sidoc.senda.gob.cl/consulta e ingresar el siguiente código:
33825031af80824bf36ad0cb0acc4b14e96cbd8c