Servicio de Empleo

CIRCULAR N° 000019

PARA: SERVIDORES PÚBLICOS Y CONTRATISTAS DE LA UNIDAD ADMINISTRATIVA ESPECIAL DEL SERVICIO PUBLICO DE EMPLEO

DE: SECRETARÍA GENERAL

ASUNTO: IMPLEMENTACIÓN POLÍTICAS DE SEGURIDAD Y NAVEGACIÓN

FECHA: 17 AGO 2016

La Secretaría General informa los lineamientos establecidos en relación con la seguridad, navegación y usabilidad de los recursos tecnológicos y servicios de red, los cuales son aplicables y extensivas a los servicios de red proporcionados tanto al interior de la Unidad, así como a los accesos remotos, para todos y cada uno de los usuarios internos y externos, y en los diferentes dispositivos disponibles en el mercado.

Las disposiciones definidas a continuación obedecen a las medidas de austeridad implementadas por el Gobierno Nacional en relación con el recorte de presupuesto en la vigencia actual, fundamentadas en medidas de eficiencia y adecuado uso de los recursos, y acorde con la recomendación efectuada por la Subdirección de Desarrollo y Tecnología en relación la reducción del servicio de internet de 40Mbps a 20Mbps.

Las políticas inician implementación a partir del jueves 18 de agosto de 2016 y se relacionan a continuación:

I. Equipos

1. La Unidad proporcionará a los servidores públicos, que por sus obligaciones o responsabilidades requieran de estos recursos tecnológicos para que puedan desempeñar las funciones u obligaciones encomendadas, por tal motivo no se permite conectar a la red o instalar dispositivos fijos o móviles, tales como: computadores portátiles, tablets, enrutadores, agendas electrónicas, celulares inteligentes, access point, que no sean autorizados por la Secretaría General de la Unidad, solicitud que debe efectuarse a través de correo electrónico por el jefe inmediato.
2. Las claves o contraseñas deben:
   - Poseer algún grado de complejidad y no deben ser palabras comunes que se puedan encontrar en diccionarios, ni tener información personal, por ejemplo: fechas de cumpleaños, nombre de los hijos, placas de automóvil, etc.
   - Tener mínimo diez caracteres alfanuméricos.
   - Cambiarse obligatoriamente la primera vez que el usuario ingrese al sistema.
   - Preferiblemente cambiarla cada 30 días, o cuando lo establezca la Secretaría General. Cada vez que se cambien estas deben ser distintas por lo menos de las últimas tres anteriores. Cambiar la contraseña si ha estado bajo riesgo o se ha detectado anomalía en la cuenta de usuario. No se deben usar caracteres idénticos consecutivos, ni que sean todos numéricos, ni todos alfabéticos.
   - No debe ser visible en la pantalla, al momento de ser ingresada o mostrarse o compartirse. No ser reveladas a ninguna persona, incluyendo al personal de mesa de ayuda tecnológica de la Unidad.
3. Los equipos de cómputo deberán desconectarse de la red eléctrica todos los fines de semana.

Unidad del Servicio Público de Empleo
Carrera 69 No 25B - 44 Piso 7. Bogotá D.C., Colombia
PBX: +57 1 756 0009
www.serviciodeempleo.gov.co

II. Escritorio y pantalla limpia

1. El personal de la Unidad del Servicio Público de Empleo debe conservar su escritorio libre de información, propia de la Entidad, que pueda ser alcanzada, copiada o utilizada por terceros o por personal que no tenga autorización para su uso o conocimiento.
2. El personal del SPE debe bloquear su computador con la pantalla de bloqueo, en los momentos que no esté utilizando el equipo o cuando por cualquier motivo deba dejar su puesto de trabajo, en dado caso que la ausencia del puesto de trabajo sea por un largo de tiempo, se recomienda apagar el equipo.
3. Al imprimir documentos de carácter confidencial, estos deben ser retirados de la impresora inmediatamente y no pueden dejarlos en el escritorio sin custodia.

III. Usuarios

1. La Unidad suministra una cuota de almacenamiento de la información con los permisos necesarios por cada usuario para que guarde la información que considere importante y sobre ella será garantizada la disponibilidad en caso de un daño en el equipo asignado. Sin embargo, es de aclarar que la información es responsabilidad de cada usuario y es quien debe velar por su debida custodia y realización de las copias correspondientes.
2. La Unidad instalará copia de los programas que han sido adquiridos legalmente en los equipos designados y conforme las cantidades disponibles. El uso de programas sin su respectiva licencia y autorización del SPE (imágenes, vídeos, software o música), obtenidos a partir de otras fuentes (internet, dispositivos de almacenamiento externo), puede implicar amenazas legales y de seguridad de la información para la Entidad, por lo que ésta práctica no está autorizada.
3. Todo software usado en la plataforma tecnológica de la Unidad del Servicio Público de Empleo debe tener su respectiva licencia, acorde con los derechos de autor y la normativa al respecto.
4. La Entidad no se hace responsable por las copias no autorizadas de programas instalados o ejecutados en los equipos asignados a sus funcionarios o contratistas, por consiguiente, es responsabilidad de cada usuario el uso dado a los recursos.
5. El uso de dispositivos de almacenamiento externo (dispositivos móviles, DVD, CD, memorias USB, agendas electrónicas, celulares, etc.) pueden ocasionalmente generar riesgos para la Entidad al ser conectados a los computadores, ya que son susceptibles de transmisión de virus informáticos o pueden ser utilizados para la extracción de información no autorizada, por consiguiente, la conexión de cualquier medio magnético y dispositivo de almacenamiento externo a los de la Unidad será responsabilidad de cada usuario, para lo cual, siempre deberá realizar un escaneo de virus.
6. El personal externo que trae sus equipos a la Unidad deberá asegurarse de mantener el antivirus actualizado, así como el sistema operativo legal y actualizado. Es de aclarar, que los equipos del personal externo es responsabilidad única y exclusivamente de ellos y el servicio que presta la Unidad en cuanto a mesa de ayuda está relacionado con actividades estrictamente laborales propias a la Entidad.
7. Los programas instalados en los equipos, son de propiedad de la Unidad Administrativa Especial del Servicio Público de Empleo, la copia no autorizada de programas o de su documentación, implica una violación a la política general de la Unidad. Aquellos funcionarios o personal externo que utilicen copias no autorizadas de programas o su respectiva documentación, quedarán sujetos a las acciones disciplinarias que especifique la ley.
8. La Unidad se reserva el derecho de proteger su buen nombre y sus inversiones en hardware y software, fomentando controles internos para prevenir el uso o la realización de copias no autorizadas de los programas de propiedad de la Entidad. Estos controles pueden incluir valoraciones periódicas del uso de los programas, auditorías anunciadas y no anunciadas.
9. Está prohibido almacenar archivos con contenido que atente contra la moral y las buenas costumbres de la Entidad o las personas, como pornografía, propaganda racista, terrorista o cualquier software ilegal o

malicioso, ya sea en medios de almacenamiento de estaciones de trabajo, computadores de escritorio o portátiles, tablets, celulares inteligentes, etc. o en los recursos compartidos.
10. Se prohíbe extraer, divulgar o publicar información de cualquiera de los equipos asignados a los usuarios y de los recursos compartidos.
11. Los recursos tecnológicos y de software asignados a los funcionarios del SPE son responsabilidad de cada funcionario.
12. Los usuarios son los responsables de la información que administran en sus equipos personales y deben abstenerse de almacenar en ellos información institucional.
13. Los usuarios solo tendrán acceso a los datos y recursos autorizados por la Unidad, y serán responsables disciplinaria y legalmente de la divulgación no autorizada de esta información.
14. Es responsabilidad de cada usuario proteger la información que está contenida en documentos, formatos, listados, etc., los cuales son el resultado de los procesos informáticos; adicionalmente es un deber la protección de los datos de entrada de estos procesos.
15. Los dispositivos electrónicos (computadores, impresoras, fotocopiadoras, escáner, etc.) solo deben utilizarse para los fines autorizados por la Entidad.
16. Cualquier evento o posible incidente que afecte la seguridad de la información, debe ser reportado inmediatamente a la mesa de ayuda a través del aplicativo definido por la Unidad.
17. Los funcionarios a quienes les sean concedidos periodos de vacaciones, deberán asegurarse de re direccionar la cuenta de correo electrónico a quien quede encargado de las labores, para lo cual es necesario habilitar la notificación. En caso de requerir colaboración, se recomienda registrar la solicitud a través del Gestor de Incidentes.

IV. Mesa de ayuda Tecnológica

Los servicios de mesa de ayuda son brindados para servicios estrictamente laborales y de índole institucional, por consiguiente, cualquier servicio requerido deberá realizarlo a través del Gestor de Incidentes en el vínculo: http://app.pbm.com.co/itmanager, ingresando el usuario, que corresponde a la cuenta de correo institucional y la contraseña es Abc-123. En dicho link podrá crear incidencias o requerimientos, categorizarlos, seleccionar el nivel de atención, describir la situación, entre otros aspectos necesarios para conocer la necesidad expuesta.

Toda solicitud de servicio de mesa de ayuda tecnológica será atendida conforme la priorización del servicio y el orden de llegada en el Gestor de Incidentes.

V. Normas que rigen el uso del Internet

1. Es obligación del usuario utilizar el internet de acuerdo a la ética y a la normativa vigente, por consiguiente, la navegación en internet deberá realizarse de forma razonable y con propósitos laborales.
2. En el sistema de acceso a internet a través del servidor de la Unidad, está instalado un filtro de internet y de correo electrónico que permite bloquear el acceso a páginas o sitios de internet que van en contra de la moral o de los propósitos misionales e institucionales. Cuando a través de alguna computadora se pretenda realizar conexión a internet a las páginas con suspensión de acceso, este equipo podrá ser bloqueado en la red. El desbloqueo del equipo deberá realizarse solicitando al responsable de mesa de ayuda a través del aplicativo definido para ello dicha actividad.
3. No está permitido el acceso a las opciones de conversación (chats), salvo que sea de naturaleza institucional y con previa autorización escrita o electrónica al responsable de la mesa de ayuda a cargo del responsable del área indicando de manera expresa los funcionarios y/o contratistas a quienes se les habilita el acceso. Esta solicitud deberá efectuarse con un (1) día hábil de anticipación para disponer del servicio.

4. El uso del chat o de páginas de internet que vayan en contra de la moral, será sancionado de acuerdo con las disposiciones legales vigentes.
5. La clave del servicio de internet inalámbrico para visitantes será cambiada de manera mensual.

VI. Acceso a sitios de Internet

1. El uso de internet es exclusivamente para las actividades institucionales.
2. El administrador de la red o las personas responsables de esta, a través de los equipos de monitoreo y análisis de tráfico detectará a los usuarios que hagan mal uso de los servicios de internet.
3. Las actividades financieras y misionales (video/tele conferencias programadas, manejo de redes sociales por los responsables de las comunicaciones en la Unidad, el manejo de la plataforma, etc.) tienen prioridad, por lo que cualquier usuario utilizando otro servicio (por ejemplo "chat", descarga de software o transferir música) le será solicitado que abandone el sitio o cancele la transferencia de archivos.
4. Cuando se tengan previstos eventos que serán soportados a través de internet, como streaming, video/tele conferencias, entre otros servicios, es necesario informar con anterioridad, como mínimo con dos (2) horas de antelación a la mesa de ayuda tecnológica a fin de asegurar el servicio.
5. Está totalmente prohibido el ingreso a páginas de contenido contrario a la ley o que representen peligro para la Entidad como pornografía, terrorismo, hacktivismo, segregación racial, descarga de programas que permitan realizar conexiones automáticas o visores de sitios clasificados como pornográficos, la utilización de los recursos para distribución o reproducción de este tipo de material ya sea vía web o medios magnéticos.
6. No descargar música y video (especialmente, no emplear servicios como kaZaA, Morpheus, GNUtella, eMule, Ares, Jdownloader, Spotify o similares).
7. No esta permitido participar en juegos de entretenimiento en línea en la Unidad.
8. Verificar que todos los archivos que se copien a su computadora no contengan virus.
9. No utilizar los servicios de Radio y Tv por demanda.
10. Los usuarios utilizarán únicamente los servicios para los cuales están autorizados. No deberán usar la cuenta de otra persona, ni intentar apoderarse de claves de acceso de otros, así como no deberán intentar acceder ni modificar archivos que no son de su propiedad, y mucho menos, los pertenecientes a la administración de la Unidad u otras instituciones.
11. Respetar la privacidad de otros usuarios. Los archivos, discos, USB e información son privados, el usuario no debe intentar leer, copiar o cambiar los archivos de otro usuario, a menos que haya sido autorizado por éste.

VII. Software y licencias

Todo aplicativo informático o software debe ser comprado o aprobado por la Subdirección de Desarrollo y Tecnología y la Secretaria General de manera conjunta, en concordancia con la política de adquisición de bienes de la Entidad.

VIII. Seguridad

1. La Unidad cuenta con un firewall o dispositivo de seguridad perimetral para la conexión a internet.
2. La Unidad en caso de tener un servicio de transferencia de archivos deberá realizarlo empleando protocolos seguros. Cuando el origen sea la Unidad del Servicio Público de Empleo hacia entidades externas, el Entidad establecerá los controles necesarios para preservar la seguridad de la información; cuando el origen de la transferencia sea una entidad externa, se acordarán las políticas y controles de seguridad de la información con esa entidad; en todo caso es necesario revisar y proponer controles en concordancia con las políticas de seguridad de la información de la Unidad; los resultados de la revisión

de requerimientos de seguridad serán documentados y preservados para futuras referencias o para evidenciar el cumplimiento con las políticas y con los controles de seguridad del SPE.

3. Es recomendable configurar los parámetros de seguridad de su computador y navegador de internet para filtrar archivos que puedan dañar a la computadora, en caso de requerir apoyo, podrá solicitarlo a la mesa de ayuda a través del Gestor de incidentes.
4. Cualquier archivo recibido por internet deberá revisarse para asegurar que no contenga virus, ya que existen algunos que pueden destruir toda la información del disco duro del equipo. Antes de abrir cualquier archivo recibido por internet, el usuario debe asegurarse que sea un archivo confiable. Adicionalmente, es necesario, que de manera inmediata se registren los incidentes ocasionados por la recepción de correos sospechosos y/o spam, en el aplicativo definido por la Unidad para el registro de los casos.
5. El usuario no debe interferir en los procesos computacionales de la Unidad mediante acciones deliberadas que disminuyan el desempeño o la capacidad de los equipos instalados. Así mismo, está prohibido el uso de aplicaciones o páginas de internet con el fin de tratar de burlar la seguridad o desempeño de la red interna institucional para acceder a sitios no autorizados y previamente bloqueados.
6. No deje encendida su computadora sin hacer uso de ella por largos periodos de tiempo, si va a dejar de usarla permanentemente, cierre las aplicaciones (navegadores o cuentas de correo) que esté usando.
7. Cambie con frecuencia sus claves de acceso a servicios y no se las comunique a nadie, de preferencia que sus contraseñas incluyan letras, mayúsculas y minúsculas, números y caracteres especiales, que sean de una longitud mínima de ocho (8) caracteres y que no formen palabras o información conocida, por ejemplo: fecha de nacimiento.
8. No desactive el monitor de antivirus de su equipo.

IX. Impresoras y medios de conservación electrónica

1. Los documentos que se impriman en las impresoras de la Unidad del Servicio Público de Empleo deben ser de carácter institucional.
2. Es responsabilidad del usuario conocer el adecuado manejo de los equipos de impresión (escaneo y fotocopiado) para que no se afecte su correcto funcionamiento.
3. Ningún usuario debe realizar labores de reparación o mantenimiento de las impresoras. En caso de presentarse alguna falla, esta se debe reportar a la mesa de ayuda de la Unidad a través del Gestor de incidentes o en la extensión 1605.

X. Excepciones

1. El uso de servicios de mensajería instantánea y el acceso a redes sociales estarán autorizados solo para un grupo reducido de usuarios, teniendo en cuenta sus funciones y para facilitar canales de comunicación con la ciudadanía. De igual manera, estos usuarios exentos deberán usar responsablemente los recursos a los cuales se les permite el acceso para fines laborales, que es para lo que finalmente los utilizarán.
2. No se permite el envío de mensajes con contenido que atente contra la integridad de las personas o instituciones o cualquier contenido que represente riesgo de código malicioso.

La Secretaría General se encuentra dispuesta a atender sus solicitudes, por lo tanto y para implementar la presente circular, serán adelantadas campañas de divulgación por medio electrónico y sistema de sonido a fin de mantener informados a todos quienes integran la Unidad en los aspectos mencionados anteriormente.

CARLOS JAVIER RODRÍGUEZ ORDOÑEZ
Secretario General

17 AGO 2018

Elaboró Nury Maya – Coordinadora Administrativa