Oficina de Sistemas de Información y Apoyo Tecnológico a la Docencia

MANUAL DE PROCEDIMIENTOS PARA EL USO DE INTERNET Y RECURSOS DE TECNOLOGÍA DEL DEPARTAMENTO DE EDUCACIÓN DE PUERTO RICO

Edward Moreno Alonso, Ed. D.
Secretario

Marie Ortiz Sánchez
Principal Oficial de Informática

Revisado: 17 de diciembre de 2012

P.O. BOX 190759, SAN JUAN, PUERTO RICO 00919-0759 * TEL.: (787) 773-2996 * FAX: (787) 767-6935 **El Departamento de Educación no discrimina por razón de raza, color, sexo, nacimiento, origen nacional, condición social, ideas políticas o religiosas, edad o impedimento en sus actividades, servicios educativos y oportunidades de empleo.**

TABLA DE CONTENIDO

MANUAL DE PROCEDIMIENTOS PARA EL USO DE INTERNET Y RECURSOS DE TECNOLOGÍA DEL DEPARTAMENTO DE EDUCACIÓN DE PUERTO RICO

Página

L VISIÓN GENERAL DE LA POLÍTICA DEL DEPARTAMENTO DE EDUCACIÓN
A, ... introducción 5
B, ... Definiciones....
..... 6
II. PROPIEDAD Y PRIVACIDAD 6
A. ..... Propiedad del Departamento
..... 6
B. ..... Ninguna expectativa de privacidad
..... 7
Iil, SEGURIDAD DE INTERNET... 7
A. ..... Fiitrado de contenido 7
B. ..... Monitoreo y supervisión
..... 8
C. ..... Educación..... 8
D. ..... Limitación de responsabilidad ... 8
IV. "CYBERBULLYING" (Acoso Cibernético)..... 8
A. ..... Visión general de "Cyberbuliying" 8
B. Políticas públicas para prohibir actos de hostigamiento e intimidación
("Bullying")..... 9
V. .....
RESPONSABILIDADES DEL ESTUDIANTE, ESCUELA Y PERSONAL 10
A. .....
Responsabilidades del estudiante 10
B. .....
Responsabilidades de la escuela 11
C. .....
Responsabilidades del profesor..... 11
VI..... CONSECUENCIAS POR NO
CUMPLIR CON EL MANUAL..... 12
A. ..... Disciplina
estudiantil..... 12
B. ..... Disciplina
personal 13
VII. ..... POLÍTICA ESTUDIANTIL ....
..... 13
A. ..... Objetivos
..... 13
B. ..... Principios
..... 14
C.
Condiciones de uso de la red dei Departamento y Recursos de Informática 14
D. ..... Uso
aceptable 14
E. ..... Uso
inaceptable..... 14
F. ..... Correo
electrónico 18
G. .....
Requisitos de informes..... 18
VIII. ..... POLÍTICA DEL PERSONAL..... 19
A. ..... Objetivos
..... 19
B. ..... Uso
aceptable..... 19
C. ..... Uso
inaceptable..... 20

D. ..... Monitoreo y supervisión 23
E. ..... Correo electrónico 24
F. ..... Confidencialidad 24
G. ..... Requisitos de informes 24
IX. LIMITACIONES DE RESPONSABILIDAD 25
X. REFERENCIAS LEGALES 25
APÉNDICE A 26
PÁGINAS DE EXTRACTO DE INFORME FILTRADO DE CONTENIDO 27
APÉNDICE B 30
APÉNDICE C 32
APÉNDICE D 36

17 de diciembre de 2012

Oficina del Secretario

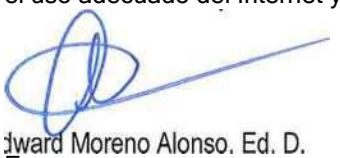
Estimados estudiantes, padres y demás personal:

El Departamento de Educación de Puerto Rico (el "Departamento" o "DE") está orgulloso de ofrecer acceso a recursos de Internet y tecnología de una manera segura y regulada para sus alumnos y su personal. Reconocemos que el Internet se ha convertido en un componente esencial en la educación y en un factor determinante en el éxito de los estudiantes como ciudadanos globales. Los estudiantes pueden utilizar el Internet para perfeccionar sus habilidades en las matemáticas, investigar sobre nuevos temas, colaborar con otros estudiantes de otras partes del mundo, obtener información sobre universidades y oportunidades de trabajo, así como un sinnúmero de otros beneficios educativos y hasta profesionales.

Debido a la conexión integral entre el uso del Internet y el logro estudiantil, el Departamento está comprometido en mantener una red segura y apropiada. Es por esto que hemos adoptado un *Manual de Procedimientos para el Uso de Internet y Recursos de Tecnología* en las escuelas públicas de Puerto Rico. El propósito de este Manual es establecer las normas que rigen el uso del Internet y los recursos de tecnología por parte del personal y los estudiantes. Nuestra meta principal es proteger a los estudiantes y al personal mientras utilizan los recursos disponibles. El uso de estos recursos es un privilegio, no un derecho, que se provee a los estudiantes para alcanzar sus objetivos educativos, para que los educadores optimicen la calidad de sus currículos y para que el personal del Departamento cumpla con sus obligaciones profesionales.

El Departamento tiene una política de cero tolerancias cuando se trata de amenazar, acosar o intimidar a nuestros estudiantes, por cualquier medio, incluyendo el uso de la tecnología en nuestras escuelas. Se recomienda a los estudiantes, padres y al personal a leer la Carta Circular Núm. 5-2012-2013, publicada el 30 de agosto de 2012, y accesible en nuestro Portal electrónico. Se adjunta copia como Apéndice C en este Manual.

Les exhorto a que revisen cuidadosamente este Manual, ya que proporciona las directrices necesarias para el uso adecuado del Internet y la tecnología en nuestro sistema educativo.



:lward Moreno Alonso. Ed. D.
E<
Secretario

MANUAL PARA EL USO DE INTERNET Y RECURSOS DE TECNOLOGÍA DEL DEPARTAMENTO DE EDUCACIÓN DE PUERTO RICO

I. VISIÓN GENERAL DE LA POLÍTICA DEL DEPARTAMENTO DE EDUCACIÓN

A. introducción

El Departamento de Educación de Puerto Rico (el "Departamento" o "DE") provee a sus estudiantes y al personal recursos de informática y acceso a la red del Departamento. La tecnología proporcionada por el Departamento debe ser utilizada únicamente para propósitos educativos y de la agencia, de manera segura, ética, responsable y legal.

El Departamento de Educación reconoce el privilegio de todos los miembros de la comunidad escolar de tener acceso razonable a los diferentes formatos de información que ofrece el internet. Éste debe tener un propósito educativo y se les motiva a utilizarlo responsable y apropiadamente. Debido a la complejidad de las agencias gubernamentales y de la red, los usuarios de la red del Departamento y los recursos informáticos deben someterse a reglas de uso estrictas. Éstas son proporcionadas al personal autorizado y a los estudiantes para que estén conscientes de sus responsabilidades.

El acceso a la red de telecomunicaciones proporciona oportunidades potenciales para beneficio de la educación. El Departamento de Educación tiene un sistema para controlar el contenido de la información difundida por Internet. La información recibida por los estudiantes es controlada y supervisada por un filtrado de contenidos, como es requerido por el estatuto “Children's Internet Protection Act" (CIPA), descrito a continuación.

Gran parte del contenido de difusión de Internet es valioso y educativo, pero hay recursos que pueden ser nocivos. Por esta razón, el estudiante tendrá acceso al mismo en un entorno supervisado y los administradores del sistema no permitirán el uso de materiales nocivos en el ambiente escolar. Los administradores del sistema educativo controlarán el derecho a proporcionar acceso a la red. Los padres deben estar atentos a la existencia de cualquier material perjudicial y controlar el uso de estos recursos en el hogar.

El Secretarlo de Educación ("Secretario") y el Principal Oficia! de Informática ("CÍO") han aprobado este Manual para el Uso de Internet y Recursos de Tecnología con el fin de: (a) establecer procedimientos y normas para el uso aceptable de la red del Departamento y los recursos informáticos, (b) evitar el uso no autorizado e ilegal de los mismos, (c) cumplir con el"*Children’s Internet Protection Act 2000”* (CIPA) y (d) cumplir con la Ley Núm. 267 de 31 de agosto de 2000, para proteger a los niños, niñas y jóvenes en el uso y manejo de 3a Red Internet. Además de cumplir con la Ley Núm. 149 de 15 de julio de 1999, según enmendada, conocida como la Ley Orgánica del Departamento de Educación de Puerto Rico, y la Comisión Federal de Comunicaciones, orden DA 11-125. Este Manual se aplicará a situaciones cuando: (a) la Red del Departamento o Recursos Informáticos se usan tanto en propiedad del Departamento o a través de acceso remoto (como se define en el párrafo b siguiente) y (b) dispositivos personales (como se define en el apartado b siguiente), están conectados a la Red del Departamento o los recursos informáticos con fines educativos tanto dentro como fuera del Departamento o escuela.

El DE se reserva el derecho de suspender o revocar el acceso al personal o estudiantes a la Red del Departamento o sus recursos informáticos, si se determina que hacerlo es necesario o apropiado para proteger estudiantes, personal o propiedad.

El Departamento de Educación puede hacer cambios a este Manual en cualquier momento, cuando la situación lo amerite, publicando las modificaciones a través de la red de información del Departamento en su portal electrónico.

B. Definiciones

"Recursos informáticos" se refiere a todos los equipos existentes y futuros, y la tecnología de información, ya sea fija o portátil, utilizado para realizar tareas y trabajos cotidianos del Departamento, incluyendo pero no limitado a los componentes, espacio de disco, dispositivos de almacenamiento, memoria del sistema, servidores, ordenadores, dispositivos de telecomunicaciones, dispositivos de mano, impresoras, escáner, máquinas de fax, fotocopiadoras, etc., propiedad o arrendado por el DE.

"Red del Departamento" se refiere a la infraestructura existente y futura utilizada para transmitir, almacenar y revisar los datos sobre un medio electrónico e incluye, pero no se limita a, los sistemas de correo electrónico del DE, sistemas de colaboración (por ejemplo, calendario, tableros de mensaje/conferencia, "blogs", conferencias de vídeo, mensajería de "chat' V instantánea de texto, sitios "Web" y "*podcasting**), bases de datos, información, sistemas, servicio de Internet, etcétera, propiedad o arrendado por el DÉ.

"Personal" incluye a funcionarios, empleados permanentes y temporeros, practicantes, proveedores, consultores, contratistas y agentes autorizados, y voluntarios que trabajan bajo la supervisión de personal de la agencia, incluyendo las escuelas.

"Dispositivos personales" se refiere a dispositivos actuales y futuros que son propiedad del Personal cuando se utiliza con fines de negocio del DE, dentro o fuera del Departamento. Ejemplos de dispositivos personales incluyen, pero no se limitan a; asistentes de datos personales (PDA), ordenadores portátiles, tabletas, "IPads" y teléfonos celulares.

"Acceso remoto" se refiere al acceso desde una ubicación fuera de la red del Departamento a porciones del Departamento de Red o sus recursos de informática que están sujetas a los requisitos de acceso autorizado.

II. PROPIEDAD Y PRIVACIDAD

A. Propiedad del Departamento

Todos los documentos, datos e información creados, almacenados, transmitidos y procesados en la Red del Departamento o utilizando Recursos informáticos son y seguirán siendo en todo momento propiedad del DE y estarán sujetos a la búsqueda, modificación, copia, divulgación o eliminación por el DE en cualquier momento y por cualquier razón, sin previo aviso o consentimiento. Los derechos de propiedad del DE permanecerán en pleno vigor y efecto aunque los estudiantes ya no estén matriculados en el sistema de escuelas públicas y sobrevivirán a la terminación de empleo o contrato de personal. Los estudiantes y el personal serán responsables de garantizar que su acceso y uso de cualquier y todos esos documentos, datos e información cumpla con los términos de este Manual.

B. Ninguna expectativa de privacidad

Los estudiantes y el personal autorizado a utilizar la Red del Departamento y sus recursos informáticos no tendrán ninguna expectativa de privacidad con respecto a que sus tareas escolares, registros de empleo, correos electrónicos, uso de internet y archivos, y deben entender que éstos: (1) pueden ser vistos, copiados, transmitidos y divulgados en cualquier investigación del Departamento sobre presuntas violaciones de este Manual y (2) éstos son admisibles en los tribunales según los procedimientos administrativos y de acuerdo a las leyes de registros públicos. Además, el DE puede monitorear y auditar el uso por parte de los estudiantes y el personal que utiliza la Red del Departamento y sus recursos informáticos para cualquier actividad inapropiada o ilegal y expresamente se reserva el derecho, sin previo

aviso o consentimiento, a:

(1) acceder y hacer cambios a la Red o sus recursos de informática para neutralizar amenazas a la seguridad o violaciones a este Manual,

(2) negar o terminar el acceso por parte de los estudiantes o el personal a la Red del Departamento y sus recursos de informática, si hay amenazas a la seguridad o violaciones al Manual,

(3) acciones disciplinarias a estudiantes que lo ameriten, según autorizado o aprobado por el DE,

(4) acceder, buscar, leer, inspeccionar, copiar, supervisar, registrar o utilizar datos y la información almacenada, transmitida y procesada en la Red del Departamento o Recursos Informáticos e

(5) informar cualquier actividad ilegal a las autoridades apropiadas.

III. SEGURIDAD DE INTERNET

A. Filtrado de contenido

Conforme al "C*hiidren's internet Protection Ací 2000"* (CIPA), el Departamento ha implementado el "Forti Analyzer" en computadoras con acceso a internet como el mecanismo para restringir el acceso a sitios que contengan pornografía, representaciones obscenas u otros materiales perjudiciales para menores. La descripción de la solución de filtrado de contenidos se adjunta como Apéndice A. El DE se reserva el derecho de implementar una solución de filtrado diferente, si el Departamento determina que hacerlo así está en su mejor interés.

Un administrador, supervisor o persona autorizada puede desactivar la solución de filtrado de contenidos, con fines de investigación "bona fide" u otros propósitos legales educativos o comerciales, siempre y cuando la persona reciba autorización previa del personal directivo de la Oficina de Sistemas de información y Apoyo Tecnológico a la Docencia (OSIATD).

A pesar de las medidas de protección adoptadas por el DE para proteger a estudiantes de material nocivo, ningún "software" es infalible y todavía hay un riesgo de que los usuarios puedan estar expuestos a material inapropiado. Sin embargo, el DE seguirá tomando las medidas razonables para proteger a sus estudiantes y minimizar el riesgo de acceso intencional o inadvertido por parte de los estudiantes a material inapropiado o dañino mediante el uso de la Red del Departamento y sus recursos informáticos.

B. Monitoreo y supervisión

El DE podrá (1) monitorear las actividades en línea “online" del personal y los estudiantes, inclusive acceder, buscar, leer, inspeccionar, revisar, copiar, almacenar, remover o eliminar comunicaciones electrónicas o archivos de estudiantes para abordar las violaciones de este Manual y (2) revelar, copiar o transmitir documentos de estudiantes y del personal, datos e información, según el Departamento lo considere necesario o apropiado, a su entera discreción, o según sea requerido para cumplir los requisitos de este Manual de Política o cumplir con órdenes judiciales, citaciones e interrogatorios. El DE tendrá derecho a interceptar mensajes de correo electrónico y comunicaciones similares, tales como: correo de Internet y otros servicios de mensajería, para fines comerciales, legales o de seguridad como el Departamento, a su entera discreción, considere necesario o apropiado.

C. Educación

El DE está comprometido a educar a sus estudiantes acerca de la seguridad del internet, incluyendo pero no limitado, al comportamiento apropiado mientras esté en línea, en sitios "web" de redes sociales y en *“chat rooms”* y proporcionará a los estudiantes con educación y concienciación sobre el *“cyberbuliying” y fas* respuestas apropiadas y denuncias. Esta educación puede incluir cursos de seguridad de Internet, “software", folletos informativos, consejería individual o cualesquiera otros métodos de enseñanza que el Departamento considere eficaz y apropiado.

A los estudiantes transferidos de otros sistemas educativos se les proporcionará con instrucciones e información acerca de un comportamiento adecuado en línea.

D. Limitación de responsabilidad

El DE ha tomado medidas razonables para proteger a los estudiantes al acceso a contenido nocivo o inadecuado en internet y no incurrirá en ninguna responsabilidad resultante del abuso intencional o accidental de la Red del Departamento y sus recursos de informática, o de un fallo del "software" de filtrado de material nocivo o inadecuado.

IV. “CYBERBULLYING” (Acoso Cibernético)

A. Visión general de “Cyberbuiiying”

“Cyberbullying” se define como la crueldad hacia los demás al enviar o publicar material nocivo usando el internet o un teléfono celular. Hay varias formas diferentes de “cyberbullying":

1. “Flaming”: peleas en línea “oniine" mediante mensajes electrónicos con lenguaje vulgar y enojado.
2. Acoso: enviar repetidamente mensajes crueles, viciosos o amenazantes.
3. Denigración: enviar o publicar chismes o rumores crueles acerca de una persona para dañar su reputación o amistades.
4. Suplantación: irrumpir en la cuenta de correo electrónico de alguien y usarlo para enviar material vicioso o embarazoso para otros.
5. Salida y engaño: comprometer a alguien en mensajería instantánea, engañando a él o ella en revelar información sensible y reenviar información a los demás.
6. Exclusión: intencionalmente excluir a alguien de un grupo en línea.

7. "Outing": compartir secretos, información e imágenes embarazosas de alguien en línea.
8. Engaño: convencer a alguien de revelar secretos o información embarazosa y, a continuación, compartirlo en línea.
9. Acoso cibernético: Intenso y repetido acoso y denigración que incluye amenazas o crea un miedo significativo.

El material "cyberbullying" puede ser publicado en sitios “web” personales o "blogs" o, transmitido a través de correo electrónico, grupos de discusión, tablones de mensajes, “chai”, “IM" o teléfonos de texto e imágenes. Un “cyberbullying" puede ser un extraño para la víctima o alguien que conoce. Un "cyberbullying” también puede ser anónimo y puede solicitar la participación de otras personas en línea que no conocen la víctima, también conocido como “cyberbullying" por “proxy”.

“Cyberbullying" puede estar relacionado con intimidación u hostigamiento donde el estudiante que es victimizado en la escuela y también es el objetivo de la agresión en línea en la escuela. Otras veces, el estudiante que es victimizado toma represalias en línea o compartirá su enojo o depresión en línea como amenazas o material angustiante. Además, “cyberbullying” puede involucrar las relaciones personales. Por ejemplo, sí se rompe una relación, una persona puede empezar a acosar a la otra persona y amenazar con 1a distribución de imágenes. "Cyberbullying” puede basarse también en odio o prejuicio – intimidando a otros a causa de raza, religión, apariencia física (incluyendo obesidad) o su orientación sexual.

Es ampliamente conocido que la intimidación puede resultar en daños psicológicos a largo plazo para las víctimas, que incluyen la baja autoestima, depresión, ira, fracaso y deserción escolar, y, en algunos casos, la violencia escolar o el suicidio. Aunque hay menos investigación sobre "cyberbullying", la evidencia creciente sugiere que también se asocia con importantes daños psicológicos como ansiedad, depresión o incluso suicidio. Lamentablemente, es muy generalizado, más de la mitad de los adolescentes ha sido intimidada en línea o ha participado en ‘‘Cyberbullying" y más del 25% de los adolescentes han sido intimidados repetidamente a través de sus teléfonos celulares o Internet.

“Cyberbullying” parece ser una epidemia rápida en parte por el código de silencio y quizás vergüenza para la víctima que vive este tipo de abusos. Los adolescentes pueden estar reacios a decir a los adultos lo que está sucediendo en línea o a través de sus teléfonos celulares porque están traumatizados emocionalmente. Creen que es su culpa, tienen miedo a una mayor retribución o a que se les restrinja sus actividades en línea o el uso de teléfono celular. Sólo 1 de cada 10 adolescentes le dice a un padre si ha sido una víctima de "Cyberbullying" y menos de 1 en 5 incidentes de "Cyberbullying" se informan a la policía.

B. Políticas públicas para prohibir actos de hostigamiento e intimidación (Buliying)

La Ley Núm. 49 de 2008, que modifica la Ley Núm. 149 de 1999 o "Ley Orgánica del Departamento de Educación", establece políticas que prohíben los actos de intimidación entre estudiantes de escuelas públicas. La Ley define el "*buliying“* como cualquier acción tomada intencionalmente por cualquier comportamiento, ya sea verbal, escrito o físico, que tiene el efecto de asustar o intimidar a los estudiantes e interfiere con su educación y su desempeño en el salón de clases. La intimidación se considera hostigamiento si es continuo y sistemático. Esta Ley prohíbe el acoso e intimidación de los estudiantes si ocurre dentro de la propiedad o el establecimiento de la escuela, alrededor de las áreas, autobuses escolares y actividades patrocinadas por las escuelas.
Con el fin de determinar si la conducta cumple con la norma de acoso o intimidación, el Departamento tomará en consideración sí la conducta se produce en la propiedad escolar, los alrededores o en actividades

patrocinadas por la escuela, tanto como la gravedad y el impacto de las acciones en la victima.

Con respecto a una acción disciplinaria, el agresor puede ser suspendido hasta quince días, dependiendo de la gravedad de sus acciones, además de otros factores.

Todos los estudiantes o personal que de buena fe denuncien hostigamiento e intimidación están protegidos contra cualquier represalia derivada del informe del incidente. Los directores deben presentar informes mensuales sobre cualquier incidente relacionado con la intimidación o acoso en sus escuelas. Además, el Secretario estará obligado a presentar a la Legislatura de Puerto Rico (no más tarde del 15 de junio de cada año) un informe sobre los incidentes relacionados con el acoso y la intimidación en el Departamento y las acciones que fueron tomadas en respuesta a esos incidentes.

Sin embargo, con el fin de luchar contra el acoso y la intimidación, el foco principal del DE es la prevención y educación de sus estudiantes y personal. El Departamento proporciona a los estudiantes y al personal la oportunidad de participar en programas, actividades y talleres diseñados y desarrollados para educarlos sobre la política pública establecida en el Artículo 308 de la Ley relacionada con el acoso e intimidación entre estudiantes o personal. Además, como parte de su currículo, los trabajadores sociales y consejeros orientan a los estudiantes sobre el tema de hostigamiento e intimidación, utilizando diferentes estrategias de prevención y tratamiento. Finalmente, los estudiantes involucrados en estos incidentes son referidos al director de la escuela, trabajador social, consejero escolar y psicólogo para que la escuela pueda evaluar continuamente los efectos emocionales de la intimidación en los estudiantes.

V. RESPONSABILIDADES DEL ESTUDIANTE, ESCUELA Y PERSONAL

A. Responsabilidades del estudiante

El alumno debe seguir todas las reglas de la escuela al usar el Internet.

1. Los estudiantes tienen acceso al Internet siguiendo las instrucciones, la autorización y la supervisión del maestro.
2. La información personal del estudiante, tal como: fotos, dirección, número de teléfono, nombres de los padres y su lugar de trabajo, no se publican (por los estudiantes o el personal de la escuela), a menos que sea con la aprobación previa de los padres. Esta autorización será solicitada para propósitos educativos solamente.
3. Cualquier estudiante que reciba información o mensajes que le incomoden, debe informarlo inmediatamente al maestro o supervisor.
4. Los estudiantes nunca deben ponerse de acuerdo para reunirse con alguien que conocieron a través de Internet, sin el consentimiento o autorización de sus padres o tutores.
5. Ningún estudiante debe intentar tener acceso a información personal, materiales o documentos de otras personas sin su permiso.
6. El estudiante no dañará o destruirá el trabajo de otras personas u organizaciones.
7. El estudiante no accederá, manipulará, alterará, dañará o destruirá los archivos de material o equipo tecnológico.
8. El estudiante puede imprimir el material autorizado por el maestro.
9. Los estudiantes no pueden acceder, crear, copiar o distribuir material que es amenazante, pornográfico, obsceno, racista, o de connotaciones sexuales.
10. El estudiante utilizará únicamente el acceso a internet a través del equipo de la escuela para fines legales o comerciales autorizados y que están relacionados con las actividades curriculares.

B. Responsabilidades de la escuela

1. Asegúrese de cumplir con las normas establecidas en este Manual.
2. Comunicar claramente a los estudiantes, padres y al resto de la comunidad escolar, los propósitos, beneficios y riesgos asociados con el uso de los recursos de internet, antes de proporcionar acceso a la red.
3. Seleccionar los recursos más adecuados de Internet para apoyar y ampliar el proceso de aprendizaje del estudiante.
4. Designar una persona para administrar la red de área local.
5. Demostrar y ofrecer servicios de Internet a los padres.
6. Revise los términos de licencia entre el distribuidor y la escuela.
7. Proporcionar desarrollo profesional a todos los funcionarios relacionados con el acceso a Internet y la integración de recursos tecnológicos en el currículo.
8. Evidenciar la distribución de este Manual para toda la comunidad escolar (profesores, alumnos, padres, etc.). Además, mantener las hojas de recibo en un lugar seguro y accesible, para presentarlas al ser auditado o monitoreado.
9. Mantener este Manual en un lugar accesible a toda la comunidad escolar (biblioteca, tablón de anuncios o portal, proceso de inscripción electrónico, entre otros).

C. Responsabilidades del profesor

1. Asegurar que los estudiantes cumplan con las normas establecidas en este Manual.
2. Garantizar que el uso de recursos de Internet son coherentes con elcurrículo y las metas de los programas del sistema público.
3. Proporcionar, planificar y monitorear experiencias de aprendizaje basadas en el currículo escolar, para que el estudiante se convierta en un aprendiz permanente, independiente y productivo.
4. Monitorear y evaluar los recursos de aprendizaje, incluyendo sitios de Internet antes de recomendar su uso a los estudiantes.
5. Monitorear el acceso al Internet por el estudiante y proporcionar orientación adecuada para el uso efectivo de recursos de Internet.
6. Informar a los estudiantes que la comunicación a través de la red es de naturaleza pública y rara vez prevalece la privacidad.
7. Proporcionar a los estudiantes que utilizan Internet, dirección y expectativas claras acercade las normas de uso aceptable de la red y el sistema electrónico.
8. Discutir la política de uso aceptable de Internet para todos los estudiantes antes de permitirles acceder a la red y la asignación de trabajos o actividades que impliquen el uso de éste.

9. Proporcionar actividades de aprendizaje estructurado que estén alineadas al currículo.

10. Comprobar que el estudiante está trabajando en el aprendizaje de las actividades asignadas a él.

11. Será responsable de que cada uno de sus estudiantes y padres firmen el formulario de consentimiento de este Manual.

12. Entregar a la Oficina del director los documentos de consentimiento de los padres y estudiantes.

13. Proporcionar evidencia relacionada a la supervisión de los alumnos participantes en el uso y manejo de instalaciones tecnológicas. Se recomienda enumerar los equipos para maximizar el control en la supervisión constante de los aparatos utilizados.

VI. CONSECUENCIAS POR NO CUMPLIR CON ESTE MANUAL

A. Disciplina estudiantil

Los estudiantes que no cumplan con las directrices estipuladas en este Manual pueden estar sujetos a las acciones disciplinarias que van desde la suspensión temporera a la revocación permanente de los recursos informáticos y de la red del Departamento, hasta la suspensión o expulsión de la escuela. Los estudiantes que violen ciertas disposiciones de esta política pueden estar sujetos a responsabilidad civil y penal de acuerdo con las leyes estatales y federales aplicables. Acciones disciplinarias específicas pueden incluir, pero no se limitan a lo siguiente:

1. Advertencia verbal
2. Advertencia escrita
3. Restricción de acceso a Internet
4. Pérdida del privilegiode usarlared del Departamento o recursos informáticos
5. Cobro al violador por gastos de llamadas comerciales, compras no autorizadas y otras obligaciones financieras
6. Rembolsará el costo total de la reparación o el remplazo de los bienes dañados, destrozados, perdidos o robados

1. Audiencia disciplinaria para establecer un plan correctivo que corresponda a la falta y medidas que serán impuestas
2, Suspensión de la escuela por un tiempo definido, de acuerdo con las disposiciones del Reglamento General de Estudiantes

B. Disciplina personal

El personal que no cumpla con las disposiciones emitidas mediante este Manual puede ser sometido a una acción disciplinaria según las políticas y procedimientos del DE relativos a la disciplina del personal; dichas acciones varían desde la suspensión temporera o revocación permanente de los privilegios de acceso de recursos informáticos y de la Red del Departamento, a la terminación de empleo o contrato, Violaciones de ciertas disposiciones de este Manual también pueden someter al personal a la responsabilidad civil y penal de acuerdo con las leyes estatales y federales aplicables. Empleados pueden tener el derecho de solicitar una reconsideración o apelación a la medida prevista bajo cualquier política de quejas o acuerdo.

VII. POLÍTICA ESTUDIANTIL

A. Objetivos

Los estudiantes en las escuelas públicas de Puerto Rico pueden utilizar diversas fuentes, incluyendo internet, con el fin de apoyar y maximizar los recursos disponibles para lograr el óptimo rendimiento académico según el plan de estudios establecido por cada programa educativo.

El acceso y uso de Internet por parte de los estudiantes en las escuelas ofrece la oportunidad para localizar diferentes fuentes de información local, nacional e internacionalmente para ampliar y aclarar el contenido del currículo. El acceso a la información y colaboración son vitales para la investigación intelectual en una sociedad democrática.

El propósito de este Manual es que los estudiantes tengan una guía de comportamiento apropiado en línea y puedan comprender las ramificaciones de lo inadecuado. Nuestro objetivo es que los estudiantes puedan hacer uso educativo de Internet, en específico podrán:

1. Desarrollar destrezas y hábitos para acceder, seleccionar, usar, crear y publicar información para un determinado público.

2. Investigar y resolver problemas que identifiquen por ellos mismos o por el maestro, y que requieran investigación, análisis crítico, evaluación, etc.

3. Reflexionar críticamente para tomar decisiones sobre una base de datos o información basada en sus propios valores y sus necesidades de aprendizaje.

4. Pensar críticamente para reconocer y reflejar los valores, creencias, perspectivas y predisposiciones en diferentes fuentes de información.
5. Obtener oportunidades educativas independientes con el apoyo y la orientación de padres y maestros.

B, Principios

Siguiendo las instrucciones y directrices de sus maestros, los estudiantes podrán; recopilar, procesar, crear, comunicar y evaluar la información a través de bases de datos, correo electrónico, servidores, grupos de noticias y la "World Wide Web", con el fin de alcanzar los objetivos curriculares de los programas educativos.

Las oficinas regionales promoverán el compromiso de los docentes para la evaluación de los recursos de Internet y otros materiales de aprendizaje, tales como: programas educativos y apoyo a la integración efectiva de estos recursos en el currículo. Los estudiantes pueden acceder la información de los sistemas previamente evaluados y recomendados por los profesores.

C. Condiciones para el uso de la red del Departamento y Recursos de Informática

Los estudiantes y sus padres o tutores deben firmar acuse de recibo de este Manual y aceptar que los estudiantes autorizados a utilizar los equipos y la Red del Departamento cumplirán con los términos y condiciones del presente acuerdo. Tal reconocimiento y acuerdo estará expuesto en el Apéndice B. o en cualquier otra forma determinada por el Secretario o su designado. Copias de los acuerdos firmados serán conservados por el DE y deberán permanecer en pleno vigor y efecto hasta que se eliminen los privilegios

de acceso o si el estudiante ya no está inscrito en alguna escuela del DE.

D. Uso aceptable

La Red del Departamento y los recursos informáticos se utilizarán únicamente para tareas y funciones del DE y fines educativos; cualquier uso personal debe ser limitado al mínimo. El "uso aceptable" de la red del Departamento y recursos informáticos se refiere a las actividades apropiadas y legales que promuevan los objetivos educativos del DE, incluyendo pero no limitado a las siguientes: (a) educación y colaboración, (b) académico y (c) comunicación entre maestros, administradores, estudiantes y padres.

E, Uso inaceptable

Ninguna información personal o fotos de cualquier estudiante pueden ser publicados en el Internet o publicados por el DE sin el previo consentimiento por escrito de los padres o tutores. Además, el "uso inaceptable" de la Red del Departamentoy sus Recursos de informáticase refierea actividades que no promueven los objetivos educativosdel DE yque, a criterio exclusivo del DE, carecen de contenido educativo legítimo o propósito. Las actividadesque constituyen inaceptables el uso de la Red del Departamento o sus recursos de informática incluirán, pero no se limitarán a, cualquiera de las siguientes actividades no expresamente aprobadas o relacionadas con la investigación educativa o las asignaciones de tarea o escuela:

1. Violación de las leves. El uso de la Red del Departamento o sus recursos de informática para, o en apoyo de actividades que violen cualquier ley estatal, federal, ordenanza municipal o la política del DE, como la venta de drogas, comprar tabaco o alcohol a un menor.
2. Acceder a Material Inapropiado. Acceder intencionalmente, sin autorización, cargar, descargar, ver, almacenar o distribuir cualquier material sexualmente explícito, profano u obsceno, o material que aboga por actos ilegales o violentos, o promueve la discriminación (por ejemplo, literatura de odio),

3. Propiedad Material. Utilizar materiales con derechos de autor (por ejemplo, “software" comercial, música, archivos de sonido, películas, imágenes) sin el permiso del titular, en violación de las leyes de los derechos de autores estatales, federales o internacionales. Sin embargo, se permite la duplicación y distribución de materiales para propósitos educativos, cuando dicha duplicación y distribución entra dentro de la doctrina de uso justo de la ley de derechos de autor de Estados Unidos (Título 17, USC) y su contenido se cita apropiadamente,

4. “Software” no autorizado. Uso del software en violación de los términos de licencia y condiciones.

5. Lesiones personales. Uso de la Red del Departamento o sus recursos de informática por, o para apoyar actividades que causen daño a otros, incluyendo pero no limitado a los siguientes:

    a. Amenazar, acosar, hacer declaraciones falsas o difamatorias sobre otros (esto incluye “Cyberbullying”, correo de odio, chistes y comentarios discriminatorios);

    b. Amenazar la seguridad de una persona;

    c. Apoyar ¡a violencia o el daño a otras personas o discriminar hacia otras personas (por ejemplo, la literatura de odio);

    d. Hostigar o "acechar" otro individuo;

e. Uso profano, obsceno, abusivo, lascivo, vulgar, grosero, calumnioso, amenazante de lenguaje irrespetuoso, o sexualmente explícito;

f. Lenguaje que generalmente se considera ofensivo para las personas si es basado en raza, herencia étnica, origen nacional, sexo, orientación sexual, edad, físico o enfermedad mental o discapacidad, estado civil, religión u otras características que pueden estar protegidas por leyes de derechos civiles;

g. Promover o participar una relación con otros estudiantes, niños o adultos que no esté relacionado con lo académico o actividades extracurriculares patrocinadas por la escuela, a menos que esté previamente autorizado por escrito por el principal y el padre/tutor (Esto incluye interacción de estudiantes y maestros (amigos, etc.) en sitios de redes sociales);

h. Ponerse en contacto con otros estudiantes, niños o adultos utilizando el correo electrónico de terceros, sobre temas no relacionados con la escuela;

i. Utilizar información publicada, enviada o almacenada en línea que podría poner en peligro a otros (por ejemplo, bombardear la construcción, fabricación de drogas) o

j. Cargar, “postear”, enviar correos electrónicos, transmitir o hacer disponible cualquier contenido que podría interferir con el proceso educativo, sea ilegal, peligroso, y que pueda causar un riesgo de seguridad.

6. Daños a la propiedad. Uso de la Red del Departamento o sus recursos de informática para, o en apoyo de las actividades que causen daños a la propiedad, incluyendo pero no limitado a, los siguientes:

a. “Hacking”, bandalizar, introducir virus, ‘'worms", “Troyans”, bombas de tiempo, así como cambios no permitidos (es decir, instalar o modificar) en el "hardware", “software” y herramientas de supervisión;

b. Hacer uso de acceso autorizado a la Red del Departamento o sus recursos de equipo para falsificar, tergiversar, hacer cambios no autorizados o eliminaciones o de lo contrario, manipular con datos del Departamento;

c. Entrar, cambiar, mover o copiar los datos en la Red del Departamento o en los recursos de equipo cuando el usuario no tiene ningún derecho de autorización de acceso o entrada. Cualquier entrada, modificación o supresión de los datos del Departamento por un usuario no autorizado se consideran manipulación y está prohibido;

d. Ingresar datos falsos en la Red del Departamento o en sus recursos de informática; o

e. Comprometerse en cualquier otra conducta deliberada que interfiera, obstruya o cargue los recursos de la red del Departamento o sus recursos de informática.

7. Violaciones de seguridad de Red. No cumplir con las políticas y directrices establecidas por el Principal Oficial de Informática o su designado o usar la Red de Departamento o sus recursos de informática de una manera que ponga en peligro o atente contra Ja seguridad; facilitar el acceso no autorizado o la divulgación de información confidencial, privilegiada se considerará como violación a la

seguridad de la Red. Las violaciones de seguridad de Red incluyen, pero no se limitan a lo siguiente:

a. Ganar acceso no autorizado a la red del Departamento o sus Sistemas de Información, intentando iniciar una sesión a través de la cuenta de otra persona, códigos de acceso o identificación de Red distintos a los asignados al usuario;

b. Revelar información personal acerca de ellos mismos o de otras personas incluyendo los "logins", contraseñas, direcciones y números de teléfono de otros usuarios;

c. Interferir con la capacidad de otros usuarios para acceder a sus cuentas;

d. Intentar subvertir o eludir la seguridad de la Red de Departamento o restricciones, perjudicar la funcionalidad de la Red de Departamento o equipo recursos; o

e. Revelar, difundir, transmitir, usar o reproducir información confidencial o propiedad del DE (por ejemplo, datos financieros, información, personal, de estudiantes o registros, contraseñas y códigos de acceso, etc.) sin autorización o salvaguardas apropiadas, incluyendo pero no limitado a, información financiera, correspondencia, Informes, códigos de acceso o información personal o estudiante.

8. Uso no educativo. El uso no educativo de la Red del Departamento o sus recursos de informática es inaceptable. Usos inaceptables incluyen, pero no se limitan a lo siguiente:

a. "Social Media". Participar en juegos en línea, sitios de redes sociales o en salas de "chat";

b. Uso comercial, (a) vender o comprar algo por internet para uso persona!, para lucro personal o para hacer una ganancia (es decir, ejecutar un negocio en "eBay" a través de la Red del Departamento),
(b) mediante la Red del Departamento o sus recursos de informática para ofrecer o proveer bienes, servicios, anuncios de productos, promociones o solicitudes no autorizadas o (c) participación en actividades gubernamentales y para recaudar fondos o relaciones públicas relacionadas (por ejemplo, solicitud para fines religiosos); o

c. Otros usos no educativos, Promover o participar en (1) apuestas, correo basura, cartas en cadena, bromas, rifas, actividades (2) actividades religiosas (3) cabildeo político.

9. Uso incorrecto genera Está prohibido el uso de la Red del Departamento o sus recursos de Informática para apoyar actividades que atenten contra la seguridad de la Red del Departamento o sus sistemas de información. El mal uso general incluye, pero no está limitado a lo siguiente:

a. Acceso no autorizado. Obtener o acceder recursos más allá de los autorizados al usuario mientras utiliza la Red del Departamento o sus sistemas de información.

b. Robo de identidad. Suplantar a cualquier persona viva o muerta, organización, empresa u otra entidad mientras usa la Red del Departamento o sus sistemas de información.

c. Uso de sistema de terceros. Utilizar un sistema de terceros para comunicarse cuando se dispone de un sistema similar en el de Red del Departamento o sus sistemas de información.

d. Actividades prohibidas. Participar en actividades prohibidas en este Manual, ya sea a través

de la Red del Departamento o a través de otro proveedor de servicios de internet, cuando esas actividades se realizan como parte de los programas educativos o extracurriculares del DE.

e. Sistema de terceros. En la medida en que un sistema en particular no esté disponible en la Red del Departamento o sus Recursos de Informática, el uso de un sistema de terceros está sujeto a autorización por escrito del DE. Si es aprobado, tal uso está sujeto a los requisitos de este Manual de Política.

f. Datos cifrados "encripted". Cifrar mensajes, archivos y registros en la de Red del Departamento o sus Recursos de Informática sin el permiso de las autoridades escolares administrativas apropiadas.

g. Declaraciones sobre la Política del Departamento. Hacer una declaración sobre dicha Política, ya sea expresa o implícita, salvo los mensajes que citan procedimientos, políticas, reglas, documentos publicados por la DE, u otras fuentes oficiales.

h. Violación de los términos de uso. Violar los términos de uso especificados para un sistema particular de la Red del Departamento o sus Recursos de informática.

F. Correo electrónico

Las actividades aceptables en relación al correo electrónico son aquellas que cumplen el propósito, objetivos y misión del DE y las responsabilidades educativas de cada estudiante. Los estudiantes no tendrán derecho a la privacidad con relación al correo electrónico. Además, cualquier uso personal del correo electrónico debe ser limitado a uso mínimo. Todos los correos electrónicos enviados por los estudiantes durante el día escolar deben enviarse desde sistemas de correo electrónico autorizados por el DE, con las direcciones de retorno autorizadas por el Departamento, a menos que sea autorizado por el personal apropiado de la escuela o del Departamento. Los estudiantes deben ejercer debido cuidado para asegurar que los mensajes de correo electrónico que contengan información confidencial cumplan los requerimientos de transmisión confidencial y que se transmitan sólo a sus destinatarios.

G, Requisitos de informes

Los estudiantes informarán inmediatamente al DE sobre cualquier violación de segundad real, supuesta o cualquier otra violación bajo esta política, incluyendo pero no limitada a los siguientes:

1. Transmisión incorrecta de la información confidencial
2. "*Jailbraker",* contraseñas o claves de acceso
3. Sospecha de recepción de mensajes que posean contenido de virus
4. Robo o pérdida de recursos informáticos o de equipo, incluyendo dispositivos portátiles
5. Acceso inadvertido a material inapropiado o recepción de comunicación inadecuada
6. Recibo de *"spam"* inadecuado, mensajes electrónicos sospechosos (por ejemplo, incluyendo presuntos mensajes de "*phishing*" (pesca cibernética), que son intentos de obtener información personal, como información de tarjeta de crédito o las credenciales de inicio de sesión, o

haciéndose pasar como entidades legítimas y engañosas de los usuarios)

7. Cualquier actividad descrita en la sección anterior de “Uso Inaceptable", así como cualquier otro uso inadecuado de la Red del Departamento y sus Recursos informáticos:

VIII. POLÍTICA DEL PERSONAL

A, Objetivos

El propósito de esta política para el personal del DE es que cuenten con las mismas herramientas que guiarán a los estudiantes en un comportamiento en línea adecuado. Nuestros objetivos son que, mediante la Red del Departamento y sus recursos informáticos, el personal pueda satisfacer plenamente sus obligaciones profesionales, específicamente:

1. Lograr objetivos curriculares de nuestros programas educativos
2. Desarrollar y construir su currículo
3. Colaborar con maestros local y globalmente
4. Continuar desarrollarse profesionalmente
5. Acceder a la información y a una mayor diversidad de ideas a través del Internet, lo cual facilita el aprendizaje dirigido a la consecución de los objetivos establecidos por los planes de estudio del sistema educativo
6. Comunicarse con los demás e identificar expertos para resolver problemas relacionados al contenido del currículo
7. Aprender más información sobre la economía mundial y familiarizarse con oportunidades de empleo en un nuevo contexto y funcionar productivamente en la sociedad
8. Desarrollar habilidades especiales y competencias tecnológicas que le permitan una mejor inserción en el mercado laboral
9. Contribuir con perspectivas dentro de debates para promover una mayor comprensión a nivel personal, comunitario, nacional y mundial
10. Desarrollar habilidades de autocontrol

Las oficinas regionales promoverán el compromiso de los docentes para la evaluación de los recursos de Internet y otros materiales de aprendizaje, tales como: programas educativos y apoyo a la integración efectiva de estos recursos en el currículo. Los alumnos pueden acceder a información de los sistemas previamente evaluados y recomendados por los profesores.

B. Uso aceptable

La Red del Departamento y sus recursos de informática se utilizarán solamente para funciones del DE; cualquier uso personal debe ser limitado a un uso mínimo. El uso aceptable de la Red del Departamento y recursos informáticos se refiere a esas actividades apropiadas y legales que promueven la educación y objetivos del DE, incluyendo pero no limitado a lo siguiente: (a) desarrollo profesional y colaboración, (b)

desarrollo curricular, (c) instrucción en el aula, (d) administración y prestación de servicios, creación de registros y administración, (e) comunicación entre los maestros, administradores, estudiantes y padres o tutores.

C. Uso inaceptable

Ninguna información personal o fotos de cualquier estudiante pueden ser publicadas en internet o publicadas por el personal sin el previo consentimiento por escrito del DE y de los padres del estudiante o tutores. El "Uso inaceptable" de la Red del Departamento y sus recursos de informática se refiere a actividades que no promueven los objetivos educativos, de negocios y objetivos del DE y que, a criterio exclusivo del Departamento, carecen de contenido educativo legítimo o escolar. Las actividades que constituyen el uso inaceptable de la red del Departamento o recursos de equipo incluirán, pero no se limitarán a, cualquiera de las siguientes actividades no expresamente aprobadas o relacionadas con el ámbito escolar:

1. Violación de las leves. El uso de la Red del Departamento y sus recursos de informática para, o en apoyo de actividades que violen cualquier ley federal o del estado, ordenanza municipal o la política del DE como la venta de drogas, comprar tabaco o alcohol a un menor.

2. Acceso a Material Inapropiado. Acceder intencionalmente, sin autorización, cargar, descargar, ver, almacenar o distribuir cualquier material sexualmente explícito, profano u obsceno, material que aboga por actos ilegales o violentos, o que promueva el discrimen (por ejemplo, literatura de odio).

3. Propiedad Intelectual. Uso de materiales con derechos de autor (por ejemplo “software" comercial, música, archivos de sonido, películas, imágenes) sin el permiso del titular de la propiedad intelectual, en violación de las leyes de propiedad intelectual, estatales, federales o Internacionales; sin embargo, se permite la duplicación y distribución de materiales para propósitos educativos cuando dicha duplicación y distribución entre dentro de la doctrina de uso justo de la ley de Propiedad Intelectual de Estados Unidos (título 17, USC) y el contenido se cita apropiadamente.

4. "Software” no autorizado. Uso del “software” en violación de los términos de licencia y condiciones.

5. Daños personales. Uso de la Red del Departamento y sus recursos de informática por, o apoyar actividades que causen daño a otros incluyendo, pero no limitado a, los siguientes:

   a. Amenazar, acosar, hacer declaraciones falsas odifamatorias sobre otros (Estoincluye “Cyberbullying", correo de odio, chistes y comentarios discriminatorios);

   b. Amenazar la seguridad de una persona.

   c. Apoyar la violencia o el daño a otras personas o discriminación hacia otras personas (por ejemplo, la literatura de odio);

   d. Intimidar o "acechar" otro individuo;

   e. Utilizar lenguaje calumnioso, amenazante, Irrespetuoso, o sexualmente explícito;

   f. Utilizar lenguaje que generalmente se considere ofensivo basado en alusiones a la raza,

herencia étnica, origen nacional, sexo, orientación sexual, edad, físico o enfermedad mental o discapacidad, estado civil, religión u otras características que puedan estar protegidas por leyes de derechos civiles;

g. Promover o participar en una relación con un estudiante que no esté relacionado a asuntos académicos o actividades extracurriculares patrocinadas por la escuela, a menos que esté previamente autorizado por escrito por el director (Esto incluye interacción de estudiantes y maestros {amigos, etc.) en sitios de redes sociales);

h. Comunicarse con alumnos utilizando el correo electrónico de terceros sobre temas no relacionados con la escuela.

i. Utilizar información publicada, enviada o almacenadas en línea que podría poner en peligro a otros (por ejemplo, cómo construir una bomba, manufactura de drogas).

j. Subir, publicar, utilizar el correo electrónico, transmitir o de cualquier otra forma, hacer disponible cualquier contenido que podría interferir con el proceso educativo o sea ilegal, peligroso o pueda causar un riesgo de seguridad.

6. Daños a la propiedad. Uso de la Red del Departamento y sus recursos de informática para, o en apoyo de las actividades que causen daños a ¡a propiedad, incluyendo pero no limitado a, los siguientes:

a. "Hacking", “cracking", vandalizar, la introducción de virus, gusanos (worms), caballos de Troya (Trojans), bombas de tiempo, así como cambios no permitidos (es decir, instalar o modificar) en “hardware", "software" y herramientas de supervisión;

b. Utilizar acceso autorizado a la Red del Departamento o recursos de informática para falsificar, hacer informes falsos, tergiversar, hacer cambios no autorizados o eliminaciones o interferir con la data del DE;

c. Entrar, cambiar, mover o copiar los datos en la Red del Departamento o recursos de informática cuando el usuario no tiene ningún derecho de autorización de acceso o entrada. Cualquier entrada, modificación o supresión de datos del DE por un usuario no autorizado se considera manipulación y está prohibido;

d. Ingresar datos falsos en la Red del Departamento o recursos de informática;

e. Incurrir en cualquier otra conducta deliberada que interfiera, obstruya o sobrecargue los recursos de la Red del Departamento o equipo.

7. Violaciones a la Seguridad de la Red. No cumplir con las políticas y directrices establecidas por el Secretario de Educación o su designado o uso de la Red del Departamento y recursos de informática de una manera que pone en peligro o atenta contra la seguridad, facilita el acceso no autorizado o la divulgación de información confidencial, privilegiada o propiedad como resultado, Violaciones de seguridad a la red incluyen, pero no se limitan a lo siguiente:

a. Ganar acceso no autorizado a la Red de Departamento o recursos de informática,

intentando iniciar sesión a través de la cuenta de otra persona, códigos de acceso o identificación de red distintos de los asignados al usuario;

b. Revelar información personal acerca de ellos mismos o de otras personas incluyendo los "logins", contraseñas, direcciones y números de teléfono de otros usuarios;

c. Interferir con la capacidad de otros usuarios para acceder a sus cuentas;

d. Intentar subvertir o eludir la seguridad de la Red del Departamento o restricciones, perjudicar la funcionalidad de la Red del Departamento y sus recursos de informática;

e. Revelar, difundir, transmitir, usar o reproducir información confidencial o propietaria del DE (por ejemplo, datos financieros, información, personal de estudiantes o del Personal o registros, contraseñas y códigos de acceso, etc.) sin autorización o salvaguardias apropiadas, incluyendo pero no limitado a, información financiera, correspondencia, informes, códigos de acceso o información del personal o los estudiantes.

8. Uso no educacional. Uso no-educacional de la de Red del Departamento o de los recursos informáticos es inaceptable. Usos inaceptables incluyen, pero no se limitan a lo siguiente:

a. Medios de comunicación social. Participar en juegos en línea, sitios de redes sociales o en salas
de "chat, salvo los autorizados por el personal escolar;

b. Uso comercial, (a) vender o comprar algo por Internet para uso personal o para lucro personal o para hacer una ganancia (por ejemplo, ejecutando un negocio en “eBay" a través de la red del Departamento), (b) Utilizar la red del Departamento o recursos informáticos para ofrecer o proveer bienes, servicios, anuncios de productos, promociones o solicitudes no autorizadas o participación en actividades no gubernamentales para recaudar fondos o relaciones públicas (por ejemplo, solicitud para fines religiosos);

c. Otros Usos No Docentes. Promover o participar en (1) apuestas, correo basura, cartas en cadena, bromas, rifas, sitios de correo electrónico anónimo, (2) actividades religiosas (3) cabildeo político o solicitud de votos, incluidos las actividades políticas o de elecciones relacionadas a un sindicato u otras organizaciones de empleados.

9. Mala utilización general. Está prohibido el uso de la Red del Departamento y sus recursos de informática para apoyar actividades que atentan contra la seguridad de la Red del Departamento y sus sistemas de información. La mala utilización general incluye, pero no está limitada a lo siguiente:

a. Acceso no autorizado. Obtención o acceso a los recursos más allá de los autorizados para el usuario mientras esté utilizando la Red del Departamento y sus sistemas de información.

b. Robo de identidad. Suplantar a cualquier persona viva o muerta, organización, empresa u otra entidad mientras usa la Red del Departamento y sus sistemas de información.

c. Uso de sistema de terceros. Utiliza un sistema de terceros para comunicarse cuando dispone de un sistema similar en la Red del Departamento y sus sistemas de información.

d. Actividades prohibidas. Participar en actividades prohibidas por este Manual, ya sea a través de la Red del Departamento o a través de otro proveedor de servicios de Internet, cuando esas actividades se llevan a cabo en capacidad oficial de empleado del DE o como parte de los programas de educación, instrucción o extracurriculares del Departamento.

e. Sistemas de terceros. En la medida en que un sistema en particular no esté disponible en la Red del Departamento y sus recursos de informática, el uso de un sistema de terceros está sujeto a autorización por escrito del DE. Si es aprobado, dicho uso estará sujeto a las regulaciones de este Manual.

f. Codificación de Datos. Codificar mensajes, archivos y registros en la Red del Departamento y sus recursos de informática sin el permiso de las autoridades escolares administrativas apropiadas.

g. Declaraciones sobre la Política del Departamento. Hacer una declaración sobre la Política, ya sea expresa o implícita, salvo los mensajes que citan procedimientos, regulaciones del DE, documentos publicados por el DE u otras fuentes oficiales.

h. Violación de los términos de uso. Violando los términos de uso especificados para un sistema particular de la Red del Departamento y sus recursos de informática.

D. Monitoreo y supervisión

El Departamento de Educación utiliza actualmente el "FortiAnalyzer" para monitorear las actividades en línea del Personal y los estudiantes, incluyendo la navegación por el “Web", uso del correo electrónico, participación de la sala de “chat” y otras formas de comunicación electrónica. Una descripción de la solución de filtrado de contenidos se adjunta como Apéndice A. El DE se reserva el derecho de implementar una solución de filtrado diferente sí determina que él así hacerlo está en su mejor interés.
Un administrador, supervisor o persona autorizada puede desactivar la solución del filtrado de contenidos para una investigación "bona fide” u otros propósitos educativos o comerciales, siempre y cuando la persona reciba autorización previa del Secretario o su designado.

El DE podrá (1) supervisar actividades en línea de los estudiantes y el personal; y acceder, buscar, leer, inspeccionar, revisar, copiar, almacenar, extraer o eliminar comunicaciones electrónicas del personal o archivos para verificar las violaciones a este Manual y (2) revelar, copiar o transmitir documentos, datos e información del persona!, según el Departamento lo considere necesario o apropiado, a su entera discreción, o según sea necesario para cumplir los requisitos de este Manual o cumplir con órdenes judiciales, citaciones e interrogatorios. El DE tendrá derecho a interceptar mensajes de correo electrónico y comunicaciones similares, tales como: correo de Internet y otros servicios de mensaje, para tales fines comerciales, legales o de seguridad como el Departamento, a su entera discreción, considere necesario o apropiado.

E. Correo electrónico

Actividades de correo electrónico aceptables son aquellas que conforman a la finalidad, objetivos y misión del DE, a las obligaciones de trabajo y a las responsabilidades de cada usuario. El personal no tendrá derecho a la privacidad en relación al correo electrónico. Además, cualquier uso personal de correo electrónico debe ser limitado a utilización mínima. Todo el correo enviado por personal en su capacidad

como representantes del DE debe enviarse desde sistemas de correo electrónico autorizados por el Departamento, con las direcciones de retorno autorizadas del Departamento. El personal debe ejercer debido cuidado para asegurar que los mensajes de correo electrónico que contengan información confidencial conforman a los requerimientos de transmisión confidencial, señalados aquí y se transmiten sólo a sus destinatarios.

F. Confidencialidad

El personal deberá mantener y proteger la confidencialidad de los registros y la identidad del estudiante al utilizar la Red del Departamento y los recursos de informática. Además, deberá mantener y proteger la confidencialidad de otra información confidencial que esté alojada, procesada o mantenida en la Red del Departamento y sus sistemas de información. Ejemplos de dicha información confidencial incluye, pero no está limitada a, información exenta de divulgación en el Acta de Libertad de Información de Illinois, información protegida de la divulgación bajo el *"Federal Health Insurance Portability*" (HIPAA), otra información personal, información financiera, planes estratégicos, propiedad intelectual de los proveedores e información protegida por los acuerdos de no divulgación intergubernamentales u otros acuerdos de no divulgación.

G. Requisitos de informes

El Personal informará inmediatamente al DE cualquier violación de seguridad real o sospechosa o cualquiera otra violación bajo esta política incluyendo, pero no limitado a los siguientes:

1. Transmisión impropia de la información confidencial;

2. Contraseñas o claves de acceso comprometidas;

3. Recibo de mensajes que contengan contenido sospechoso de portar virus;

4. Robo o pérdida de los recursos informáticos, incluyendo dispositivos portátiles;

5. Acceso inadvertido a material inapropiado o recepción de comunicación inadecuada;

6. Recibo de "*spam*" inapropiado, mensajes electrónicos sospechosos (por ejemplo, incluyendo presuntos mensajes de *"phishing"* (pesca cibernética), que son intentos de obtener información personal, como información de tarjeta de crédito o las credenciales de inicio de sesión o enmascarada como entidades legítimas que confundan a los usuarios); o

7. Actividad descrita en la sección anterior sobre "Uso Inaceptable" así como cualquier otro uso inadecuado de la Red del Departamento o Recursos de informática.

IX. LIMITACIONES DE RESPONSABILIDAD

El DE no será responsable de (1) cualquier reclamación, pérdidas, daños, costos y otras obligaciones derivadas del uso de la Red del Departamento o sus recursos de informática, (2) Obligaciones financieras no autorizadas resultantes del uso de la Red del Departamento o sus recursos de informática o (3) la exactitud o calidad de la información obtenida a través del acceso del usuario a la Red del Departamento o sus recursos de informática.

Cualquier declaración publicada o comunicada a través del uso de la Red del Departamento y sus recursos de informática será el punto de vista individual del autor y no del Departamento.

x REFERENCIAS LEGALES

1. Carta Circular Núm. 5-2012-2013 (30 de agosto de 2012), adjunta como Apéndice C.
2. Carta Circular Núm. 7-2011-2012 (16 de agosto de 2011), adjunta como Apéndice D.
3. "Children's Internet Protection Act of 2000" ("CIPA"), Pub. Law 106-554, enmendada.
4. Las políticas públicas para establecer la prohibición de actos de hostigamiento e intimidación (Bullying) entre los estudiantes en las escuelas públicas, Ley Núm. 149 de 15 de julio de 1999, según enmendada, conocida como la Ley Orgánica del Departamento de Educación de Puerto Rico.
5. Ley Núm. 267 de 2000, Ley para proteger a los niños y jóvenes en el uso ymanejo de la red de Internet.
6. Protección de los niños en el Siglo XXI, Ley Pública Núm. 110-385, Título II,122 estadístico 4096 (2008), enmendada.
7. Orden de la Comisión Federal de Comunicaciones, DA 11-125 (2011)

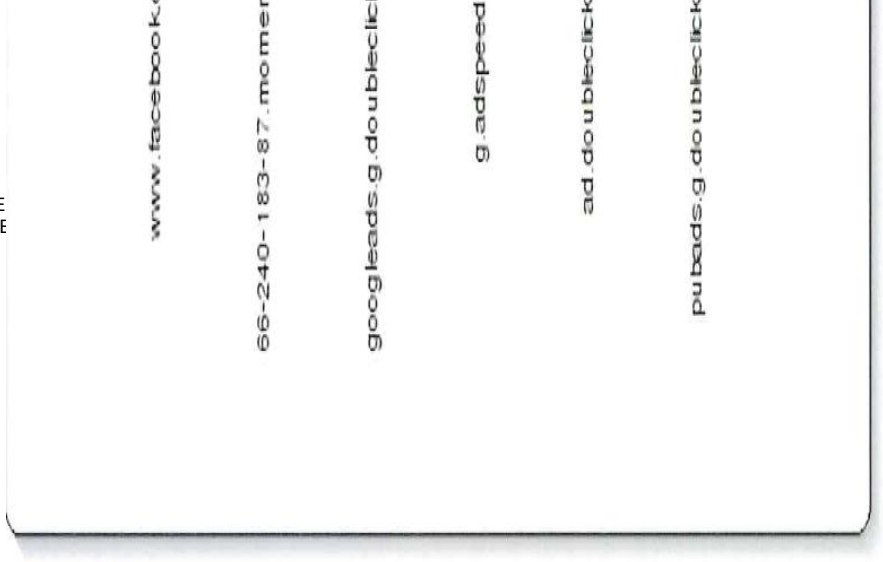
APÉNDICE A

Descripción de “FORTIANALYZER” (solución de filtrado de contenido)

Conforme a la Ley de Protección de Internet para los Niños (CIPA), el DE ha implementado el “FortiAnalyzer" en todos los equipos conectados a Internet como mecanismo para restringir el acceso a sitios que contengan pornografía, representaciones obscenas u otros materiales perjudiciales para los menores. El "software” funciona mediante la búsqueda de palabras o conceptos, según lo determinado por el Departamento, Cuando el “software" identifica tales palabras o conceptos, niega el acceso de usuario basados en el nivel de acceso asignado a la palabra o concepto. En general, los niveles de acceso van desde el nivel menos restrictivo al nivel más restrictivo. El menos restrictivo permite a los usuarios acceso al sitio “web" o documento que contenga la palabra o concepto, mientras que el nivel más restrictivo deniega a los usuarios acceso al sitio "web” o documento que contenga la palabra o concepto. Niveles de acceso intermedio entre estos dos extremos, automáticamente permitirán y denegarán automáticamente el acceso. En su lugar, el “software" pedirá, para realizar una revisión más exhaustiva del sitio "web" o documento y determinará si es objetable, además del nivel apropiado de acceso (por ejemplo, para los estudiantes de secundaria, la palabra o concepto "Mama" caería en este nivel intermedio para que un estudiante que está haciendo la investigación sobre el cáncer de mama se permitiría el acceso a sitios “web" o documentos relacionados con "pechos", pero un estudiante buscando pornografía se le negaría acceso a pornografía relacionada con "senos").

Además, el “FortiAnalyzer” proporciona a los administradores control de micro-aplicaciones en “Facebook" y ‘Twitter”, así como muchas otras plataformas populares y medios de transmisión. Permite a los administradores bloquear o permitir características como "chat, mensajería, video y audio sin bloquear sitios de “Web” en su totalidad. El "FortiAnalyzer” utilizado por los administradores puede establecer políticas de seguridad, controlar el uso de aplicaciones y ver fácilmente las tendencias en su red con la “web" en tiempo real, informes y seguimiento. Puede ser desactivado sujeto a la supervisión de personal y medidas de protección de la tecnología, en el caso de los menores, minimizado sólo para investigación "bona fide" u otros fines lícitos. Las siguientes páginas contienen algunas capturas de pantalla de los informes que produce el "FortiAnalyzer".

A pesar de las medidas de protección incorporadas en la solución de filtrado de contenidos, es importante señalar que ningún “software” es infalible, y todavía hay un riesgo de que un usuario pueda estar expuesto a un sitio o mensajes que contengan materiales inapropiados.

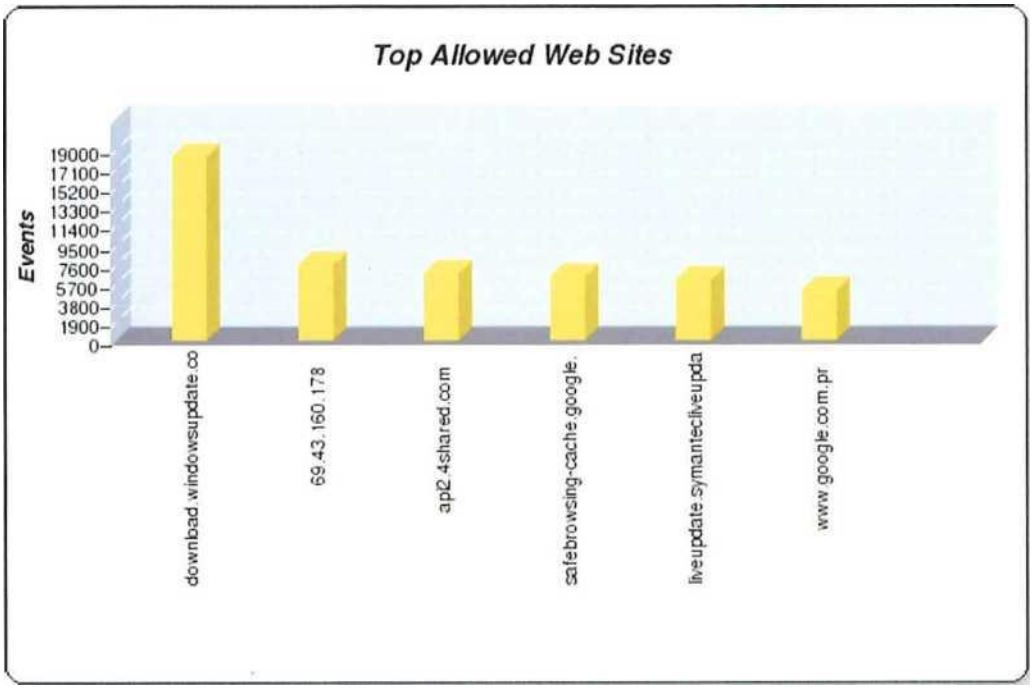


Top Allowed Web Sites

The most frequently allowed web sites over the reporting period.

All FortIGates
Devices: DE-FG-1000, FG-3K6-2_FG3K6A3406605089, FG-3K6-3, FG3K6A-1

Top Allowed Web Sites Destinatíon	Events	% of Total
download.windowsupdate.com	18320	9.43
69.43.160.178	7497	3.86
api2.4shared.com	6758	3.48
safebrowsing-cache.google.com	6383	3.28
liveupdate.symanteclive update.com	5932	3.05
www.google.com.pr	4956	2.55
Other	144499	74.35
Total	194345	100.00

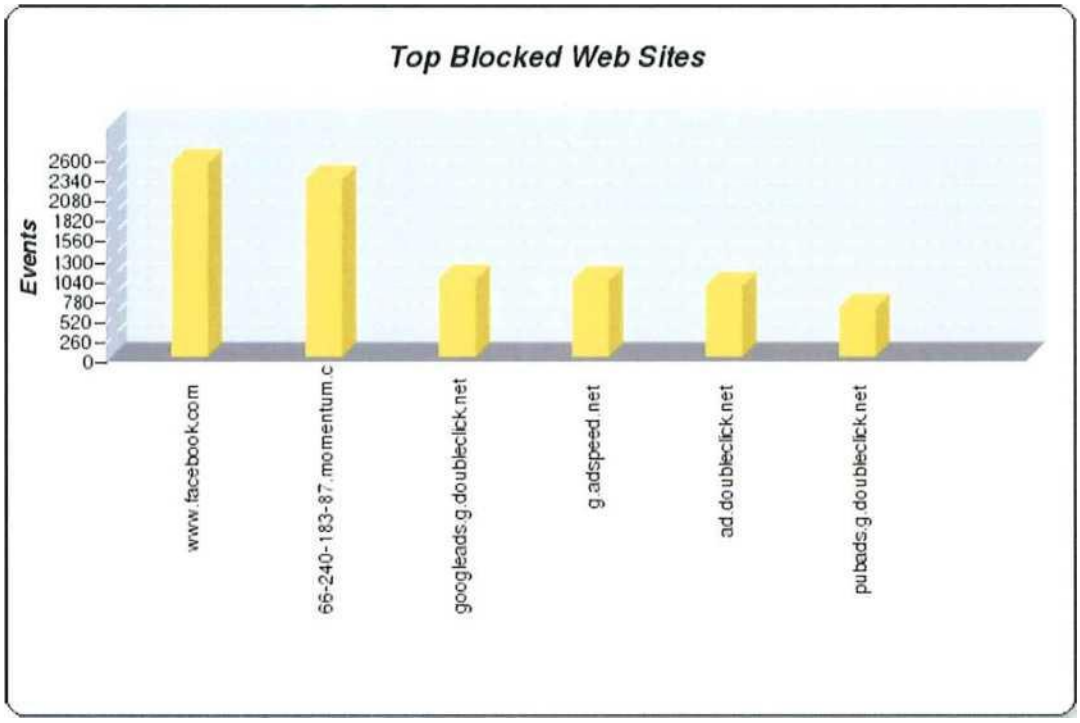


Top Blocked Web Sites

The most frequently blocked web sites over the reporting period.

All FortiGates
Devices: DE-FG-1000, FG-3K6-2_FG3K6A3406605089, FG-3K6-3, FG3K6A-1

Top Blocked Web Sites Destínation	Events	% of Total
www.facebook.com	2518	11.61
66-240-18 3-87. momentum.co m	2285	10.54
googleads.g.doubleclick.net	1008	4.65
q.adspeed.net	978	4.51
ad.doubleclick.net	923	4.26
pubads.q. doubleclick.net	624	2.88
Other	13348	61.56
Total	21684	100.00



Pop Blocked Web Users

The users with the most blocked web site connection attempts over the reporting period.

All FortiGates
Devices: DE-FG-1000, FG-3K6-2_FG3K6A3406605089, FG-3K6-3, FG3K6A-1

Top Blocked Web Users		
User	Events	% of Total
10.13.44.131	4202	19.38
172.18.94.109	2670	12.31
172.26.56.101	1201	5.54
172.18.122.106	1126	5.19
172.28.84.101	1125	5.19
172.26.125.114	926	4.27
Other	10434	48.12
Total	21684	100.00

APÉNDICE B

ACUERDO DE USO DE INTERNET Y TECNOLOGÍA

La persona que firma este documento reconoce que ha leído el Manual para el Uso de Internet y Recursos de Tecnología del Departamento de Educación de Puerto Rico. La(s) firma(s) al final de este documento es (son) jurídicamente vinculantes. Lea los términos y condiciones de esta política cuidadosamente y acate todas las disposiciones de la misma.

ESTUDIANTE

Entiendo y acataré este Manual y cumpliré con las condiciones estipuladas en el mismo. El DE no será responsable de datos perdidos, dañados o no disponibles debido a dificultades técnicas y soy responsable de lo que hago cuando utilizo la tecnología del Departamento. Entiendo que mis privilegios de acceso pueden ser suspendidos o revocados si violo el Manual, y que ciertas violaciones pueden constituir delitos. También entiendo que puedo ser disciplinado, o que en algunos casos, puedo estar sujeto a acciones legales o penales por no cumplir con lo establecido en este Manual.

Nombre del estudiante en letra de molde

Nombre de lapersonaquerecibe elAcuerdo

Firma de estudiante o usuario

Firma delapersona que recibeelAcuerdo

Fecha

PADRE O TUTOR

Si el solicitante es menor de 18 años, también se requiere una firma del padre o tutor.

Como padre o tutor de este estudiante, he leído el Manual. Entiendo que el equipo y recursos tecnológicos del DE, así como el acceso al Internet, debe utilizarse exclusivamente con fines educativos.

Autorizo al DE para que mi hijo utilice recursos de tecnología de la escuela y el Internet con fines educativos y autorizo al Departamento para disciplinar a mi hijo en caso de que él o ella no cumpla con el Manual. Entiendo también que ciertas violaciones del Manual pueden constituir conductas delictivas, que el Departamento puede reportar tales violaciones a las autoridades competentes, y que mi hijo o yo podemos estar sujetos a acciones legales o penales.

Reconozco que es imposible que el DE impida el acceso a material controversial y que no se mantenga al Departamento responsable de materiales adquiridos en la Red. Además, acepto toda la responsabilidad por las acciones de mi hijo usando recursos de tecnología del DE e Internet en la escuela, así como en otros lugares.

También acepto/deniego mi permiso respecto a la publicación de información pertinente a mi hijo en internet por el DE, como sigue:

{Seleccione una de las siguientes casillas)

□ **Opción 1:** Identificación del trabajo del estudiante debe limitarse a nombre y última inicial o un identificador de código confidencial de estudiante. Están permitidas las fotografías individuales o en grupos sin alguna identificación del estudiante,

□ **Opción 2:** Identificación del trabajo del estudiante puede contener su nombre completo. Fotografías individuales o en grupos pueden contener identificación del estudiante.

□ **Opción 3:** Ninguna información, trabajo o fotografías de mi hijo pueden ser publicados.

Nombre del padre o tutor en letra de molde

Firma del padre o tutor

Fecha

APÉNDICE C

Carta Circular Núm. 5-2012-2013 POLÍTICA PÚBLICA PARA LA PREVENCIÓN Y PROHIBICIÓN DE ACTOS DE HOSTIGAMIENTO E INTIMIDACIÓN ENTRE ESTUDIANTES ("BULLYING") EN LAS ESCUELAS PÚBLICAS DE PUERTO RICO

30 de agosto de 2012

OFICINA DEL SECRETARIO

CARTA CIRCULAR NÚM. 5» 2012-2013

Secretaria Asociada, Subsecretarios, Secretaria Asociada de Educación Especial, Secretarios Auxiliares, Directora Ejecutiva del Instituto de Capacitación Administrativa y Asesoramiento a Escuelas, Directora Interina del Instituto para el Desarrollo Profesional del Maestro, Directores de Oficinas, Programas y Divisiones, Directores de las Regiones Educativas, Superintendentes de Escuelas a cargo de los Distritos Escolares, Superintendentes Auxiliares, Facilitadores Docente de Trabajo Social, Directores de Escuela, Trabajadores Sociales Escolares y Maestros

POLÍTICA PÚBLICA PARA LA PREVENCIÓN Y PROHIBICIÓN DE ACTOS DE HOSTIGAMIENTO E INTIMIDACIÓN ENTRE ESTUDIANTES ("BULLYING") EN LAS ESCUELAS PÚBLICAS DE PUERTO RICO

La Ley Núm. 49 del año 2008, enmendó la Ley Núm. 149 del 1999, conocida como "Ley Orgánica del Departamento de Educación", a fin de establecer como política pública la prohibición de actos de hostigamiento e intimidación ("bullying") entre los estudiantes de las escuelas públicas. En este estatuto se declara que el "estudiante es la razón de ser del Sistema de Educación Pública" y reconoce "el derecho de los estudiantes a su seguridad personal". También reconoce "la obligación de los estudiantes de respetar la integridad física y moral de sus compañeros".

El acto de hostigamiento e intimidación entre estudiantes se define como cualquier acción realizada intencionalmente, mediante cualquier gesto, ya sea verbal, escrito o físico que tenga el efecto de atemorizar a los estudiantes e interfiera con la educación de estos, sus oportunidades escolares y su desempeño en el salón de clases.

Este acto, generalmente, deberá ser continuo, sistemático y creciente para considerarse hostigamiento e intimidación. Sin embargo, un solo suceso podría considerarse como "bullying" debido a la severidad del mismo.
La intimidación puede ser:

Verbal: Poner apodos, burlarse o insultar.
Física: Obligar a un compañero (a) a hacer algo que no quiere hacer, estropear, dañar, esconder o robar pertenencias de otro estudiante.
Empujar, agredir, lastimar, pegar o golpear a un compañero(a) o amenazar con hacerlo.

Social: Rechazar al compañero(a) en el grupo; negarse a hablar con el compañero(a).
Difundir rumores o mentiras acerca de algún compañero(a).
Ciberacoso: utilizar las redes sociales, correos electrónicos, "blogs" o mensajería a través de la computadora, tableta, teléfono celular u otro objeto electrónico para dañar la reputación de un compañero(a). Esto incluye, pero no se limita a publicación de información falsa, rumores, amenazas, connotaciones sexuales, etiquetas peyorativas, fotos o videos manipulados.

El Departamento de Educación prohíbe todo acto de hostigamiento e intimidación entre estudiantes que ocurra dentro de la propiedad o predios de las escuelas, áreas circundantes a éstas, o en actividades

auspiciadas por las escuelas y en los autobuses escolares.

El Manual de Protocolos (2011) (Guía para el Director Escolar *y* Personal de Apoyo) y el Reglamento General de Estudiantes (2011), disponen los procesos a seguir y las medidas disciplinarias aplicables ante las situaciones de hostigamiento e intimidación entre los estudiantes. Para minimizar el impacto emocional que esta conducta puede tener en los estudiantes, se referirá a los involucrados, por conducto del director escolar (tanto al bravucón como a las víctimas de éste) al trabajador social, al consejero escolar y/o al psicólogo, de ser necesario, para que trabajen de manera interdisciplinaria, interviniendo a la brevedad posible.

En términos de las medidas disciplinarias, esta falta puede conllevar un periodo de suspensión de hasta 15 días, de acuerdo a la severidad del suceso, la que será impuesta por el director de la escuela una vez examinado los hechos.

Todo lo anteriormente expuesto será ponderado dentro de la perspectiva de lo que sería una situación nociva o de riesgo para los estudiantes o sus propiedades. La conducta del bravucón (bullies) se evaluará con esta misma perspectiva.

Las autoridades concernidas considerarán, dentro de este marco conceptual, la severidad, persistencia o constancia de sus acciones, así como la consecuencia de estas, al crear un ambiente de hostigamiento e intimidante para el o los estudiantes perjudicados (builied).

Cabe señalar que todo estudiante o personal de las escuelas públicas que someta un informe, realizado de buena fe, que contenga algún relato sobre la incidencia de hostigamiento e intimidación contra alguno de los estudiantes por parte de un bravucón (bullies) estará protegido de cualquier acción en daños o represalia que surja como consecuencia de reportar dicho incidente.

Será compulsorio que todos los directores de las escuelas informen mensualmente, a través del módulo de disciplina, cualquier incidente relacionado con un acto de hostigamiento o intimidación en sus escuelas, así como la medida disciplinaria aplicada en cada caso.

Para cumplir con lo que estipula la Ley 49, el Secretario, en coordinación con los superintendentes de escuelas y los consejos escolares, proveerá a los empleados y estudiantes de las escuelas públicas la oportunidad de participar en programas,

actividades y talleres de capacitación diseñados y desarrollados para adquirir conocimiento y herramientas sobre la política pública establecida en el Artículo 3.08ª de esta ley sobre el hostigamiento e intimidación entre estudiantes o el personal escolar.

De la misma manera, los trabajadores sociales y los consejeros escolares incluirán como parte de su plan de trabajo para el núcleo escolar orientar a los estudiantes en torno al problema del hostigamiento e intimidación y utilizarán diferentes estrategias de servicios preventivos o de tratamiento tanto con las víctimas (bullied) de esta conducta como con los bravucones (bullies).

Como parte de la implantación de Ley 49 el Secretario tendrá la obligación de someter anualmente a la Asamblea Legislativa de Puerto Rico no más tarde del 15 de junio de cada año, un informe sobre los incidentes, si algunos de hostigamiento e intimidación dentro del sistema de educación pública y las acciones que fueron tomadas en dichos incidentes.

Agradeceremos que se cumpla con los requerimientos de esta política pública a fin de minimizar la violencia en nuestros planteles escolares.

Esta directriz deroga cualquier otro documento, memorando o carta circular que estén en conflicto, en su totalidad o en parte, con las disposiciones que aquí se establecen.

Co

rdialmente,

Edward Moreno Alonso, Ed. D.
Secretario

APÉNDICE D

Carta Circular Núm. 7-2011-2012 DIRECTRICES Y POLÍTICAS SOBRE LA ADQUISICIÓN Y DESARROLLO DE SISTEMAS, EQUIPO TECNOLÓGICO Y EL USO DE TECNOLOGÍA INFORMÁTICA EN EL DEPARTAMENTO DE EDUCACIÓN

GOBIERNO DE PUERTO RICO DEPARTAMENTO DE EDUCACIÓN

OFICINA DEL SECRETARIO

16 de agosto de 2011

CARTA CIRCULAR NÚM.: 7-2011-2012

Secretaria Asociada, Subsecretarios, Secretaria Asociada Interina de Educación Especial, Secretarios Auxiliares, Directora Ejecutiva del Instituto ele Capacitación Administrativa y Asesoramiento a Escuelas, Director del Instituto para el Desarrollo Profesional del Maestro, Directores de Programas, Oficinas y Divisiones, Directores de las Regiones Educativas, Superintendentes de Escuelas, Superintendentes Auxiliares, Facilitadores Docentes, Supervisores Generales, Supervisores de Zona, Directores de Escuela, Maestros, Maestros Bibliotecarios, Trabajadores Sociales, Orientadores, Consejeros, Padres y Estudiantes

DIRECTRICES Y POLÍTICA SOBRE LA ADQUISICIÓN Y DESARROLLO DE SISTEMAS, EQUIPO TECNOLÓGICO Y EL USO DE LA TECNOLOGÍA INFORMÁTICA EN EL DEPARTAMENTO DE EDUCACIÓN

La Oficina de Sistemas de Información y Apoyo Tecnológico a la Docencia (OSIATD) tiene la obligación de liderar el desarrollo y utilización de los sistemas de información, velar por la adquisición de equipo tecnológico apropiado para las gestiones cotidianas del Departamento de Educación de Puerto Rico (DEPR), los servicios relacionados a estas herramientas y el uso seguro y eficiente de la tecnología informática en la Agencia. El acceso a la tecnología informática permite que tanto los administradores[1], como los docentes tengan la información que necesitan para aumentar su eficiencia y mejorar el aprovechamiento académico de los estudiantes. También, facilita el manejo y análisis de datos a considerarse en la toma de decisiones. Mediante esta Carta Circular se establecen las normas y procedimientos permisibles en el desarrollo de sistemas de información, la adquisición, contratación y uso de la tecnología informática en todas las dependencias y oficinas del DEPR, incluyendo las escuelas.

Esta Carta Circular y el *Manual de Política sobre el Uso Aceptable de Internet en las Escuelas Públicas de Puerto Rico*, revisado en el 2007, establecen las normas y procedimientos para el uso adecuado de este tipo de recurso y las acciones disciplinarias aplicables al utilizarlo indebidamente. Todo usuario de los sistemas computarizados, la red de comunicación y las cuentas de acceso a los sistemas del Departamento está obligado a cumplir rigurosamente con las normas y procedimientos establecidos en ambos documentos. A tales efectos, se establecerá un

Plan de trabajo dirigido a orientar a los usuarios de la tecnología informática del DEPR sobre dicha política.

[1] Pata propósitos de carácter legal en relación con la Ley de Derechos Civiles de 1964, el uso de los términos maestro, director, supervisor, administrador, docente, estudiante, usuario, personal, funcionario y cualquier otro que puede hacer referencia a ambos sexos, incluye tanto el género masculino como el femenino.

Funciones de la OSIATD

La tecnología informática constituye un elemento muy importante en las operaciones administrativas y académicas del DEPR. La OSIATD es la unidad administrativa responsable por la adquisición apropiada y el buen funcionamiento de toda la infraestructura tecnológica del Departamento. También, es responsable de proveer servicios relacionados y el apoyo técnico que necesiten los usuarios, de velar por el cumplimiento de los estándares de instalación establecidos por el Departamento y de maximizar el uso de los recursos tecnológicos disponibles.

La Oficina de Sistemas de Información y Apoyo Tecnológico a la Docencia está ubicada en el 4 piso de la antigua sede del Departamento de Educación, Calle Teniente César González, Esquina Calaf, Urb. Industrial Tres Monjitas en Hato Rey. El número de teléfono es el (787) 773-2696. El número de fax es el (787) 767-6935. Para solicitar servicios técnicos, debe comunicarse a través del Centro de Llamadas al (787) 773-3076 o a través del correo electrónico iielpdesk@de.Robierno.nr.

Directrices en torno a la adquisición de los servicios de desarrollo de sistemas de información

Todas las dependencias del DEPR que interesen adquirir sistemas de información existentes en el mercado o servicios de desarrollo de sistemas específicos para facilitar las funciones de su área deberán cumplir con estas directrices rigurosamente.

1. El director del área deberá presentar a la OSIATD, por escrito, su intensión de contratar servicios de desarrollo o adquirir sistemas existentes de información. En esta comunicación se debe especificar las funcionalidades que se necesitan automatizar, el tiempo dispuesto para poner en función el sistema, la cantidad de usuarios, el presupuesto disponible para el proyecto, el funcionario que estará a cargo del mismo y cualquier otro aspecto relevante.

2. Todo sistema tiene que desarrollarse en plataformas para las cuales el DEPR disponga de licenciamiento. De lo contrario, la unidad interesada debe incluir en su presupuesto la adquisición de las licencias necesarias.

3. El Centro de Cómputos no dispone de servidores para la instalación de aplicaciones o programados adicionales. La unidad interesada debe incluir en su presupuesto una partida para la adquisición de servidores y cualquier otro componente para la instalación de la herramienta. Se requiere para cada proyecto incluir servidores con ambientes de desarrollo, prueba y producción.

4. Los servidores, equipos y cualquier otro elemento necesario tienen que cumplir con los estándares establecidos por el Centro de Cómputos.

5. El Centro de Cómputos designará a mi técnico que estará presente durante todo el proceso de adquisición, desarrollo e instalación de la aplicación.

6. Todo desarrollo o adquisición de sistemas de información incluirá una transferencia de conocimiento efectiva en todos los niveles: administración, mantenimiento, apoyo técnico y usuario final.

7. La unidad interesada participará activamente en la provisión de servicios de apoyo a los usuarios. La OSIATD cuenta con personal limitado en el Centro de Llamadas, Por esta razón, este personal atenderá únicamente el primer nivel de apoyo (contraseñas, accesos y referidos de nivel técnico y comunicación). La unidad interesada debe proveer apoyo a los usuarios de segundo nivel funcional.

8. Todas las aplicaciones o sistemas de información tienen que ser compatibles con los sistemas existentes y la

red de voz y datos del DEPR.

9. Ninguna dependencia del DEPR iniciará gestiones para la adquisición de aplicaciones o desarrollo de sistemas sin el previo conocimiento y aprobación de la OSIATD.

Directrices en torno a la adquisición de equipo tecnológico y servicios relacionados

1. Todas las dependencias del DEPR a cargo de la adquisición de recursos de tecnología (equipo, programados, etc.), la utilización de estos recursos, la transferencia de recursos entre oficinas y la contratación de servicios relacionados, entre otros, deben mantener un estricto inventario sobre cada una de estas actividades, de manera que se faciliten los procesos de moni toreo que realiza la OSIATD.

2. Las siguientes transacciones sólo se tramitarán con la aprobación de la OSIATD, que determinará su compatibilidad con los sistemas existentes. Esta oficina establecerá los estándares y normas que sean necesarios para facilitar la evaluación de compatibilidad.

    a. Adquisición de equipo tecnológico, así como equipo y líneas de comunicación de datos.
    b. Adquisición de servicios de consultoría relacionados con 1a compra de equipo tecnológico y el uso y manejo de la tecnología informática en el DEPR ***{hardware*** y ***software*** no educativos), apoyo y adiestramiento sobre tecnología informática.
    c. Contratación de personal técnico directamente relacionado con la tecnología informática, entiéndase técnicos de sistemas de información, analistas de tecnología, webmaster, programadores, entre otros.
    d. Transferencia de equipo y programación entre las distintas oficinas del Departamento y entre las oficinas centrales, las oficinas regionales, los distritos escolares y las escuelas.
    e. Adquisición de programados de computadoras y aplicaciones educativas.

3. Todo equipo a adquirirse tiene que cumplir con las especificaciones establecidas por la OSIATD y publicadas en el portal electrónico del DE fwww.de.gobierno.pr). Estas especificaciones se revisan anualmente. Si por alguna razón el equipo a adquirirse no apareciera en la lista de especificaciones vigente, la unidad interesada deberá comunicarse con la OSIATD para realizar la consulta correspondiente. Cada suplidor deberá entregar a OSIATD un modelo del equipo a distribuir para que sea preparado con las políticas, aplicaciones programados adquiridos y aprobados por el DEPR.

4. La evaluación y aprobación de los aspectos docentes de las aplicaciones educativas estará a cargo de la Unidad de Tecnología y Currículo (UTC), así como la adquisición de servicios de consultoría, apoyo y adiestramiento relacionados con la integración de la tecnología en las actividades docentes. La UTC deberá asegurarse de que las aplicaciones evaluadas son compatibles con los sistemas operativos actuales y no están en conflicto con los demás programados utilizados.

5. Servidores - En caso de que un área tenga que adquirir servidores para la instalación y funcionamiento de alguna aplicación nueva o la ampliación de una en producción, debe consultarse al Centro de Cómputos para la determinación de las especificaciones del equipo. Estos equipos tienen que ser compatibles con la tecnología en función del Centro de Cómputos. Los servidores se instalarán en el Centro de Cómputos y serán administrados por el personal de éste. Se le aplicarán las políticas del DE y su utilización se planificará de acuerdo a las mejores prácticas en la administración de servidores aprobadas por el DE. Todos los servidores estarán incluidos en la estrategia de resguardo.

6. Cableado Estructurado y Equipos de Comunicación - Toda solicitud para la instalación de cableado

estructurado adicional o nuevo en cualesquiera de las facilidades del Departamento de Educación debe coordinarse directamente con la OSIATD. Se mantendrá fiel al diseño de la Red y se cumplirá con los estándares de instalación, calidad y diseñó establecidos por la OSIATD y publicados en el Manual de Estándares para la Red de Comunicaciones del Departamento de Educación, publicado en el portal electrónico del DE.

Mantenimiento de la red interna

La red interna del DEPR ha sido diseñada para atender las necesidades particulares de la Agencia y facilitar los servicios que ésta ofrece. La red abarca interconexión digital para voz y "data" entre las escuelas, los distritos escolares, las regiones educativas, la Oficina para el Mejoramiento de las Escuelas Públicas (OMEP), la Autoridad Escolar de Alimentos, la Secretaría Asociada de Educación Especial y demás dependencias del Departamento. Esta red debe conservarse fiel a su diseño y construcción original para que se mantenga en condiciones operacionales óptimas y para que no se anule la garantía de los suplidores en los casos en que aplique.

Para mantener el buen estado de la infraestructura de comunicaciones instalada en escuelas y oficinas, es imprescindible que todos velemos por el cuidado de las mismas. Generalmente, en

Las escuelas se realizan trabajos de mantenimiento y mejoras que pueden afectar negativamente la infraestructura de las comunicaciones. Las situaciones más comunes son:

© ***Pintura*** - Los puntos de conexión de la red o "drops" son terminales parecidos a las tomas de conexión telefónica. Estos puntos están debidamente identificados, de manera que pueda hacerse referencia a los mismos para su activación y manejo remoto. Es necesario evitar que los puntos de conexión a la red se pinten, ya que la pintura puede dañarlos o cubrir las etiquetas que los identifican. Los químicos de la pintura aíslan los contactos de cobre y como resultado la comunicación es nula.

® ***Detergentes para limpieza*** - Aplicar directamente cualquier tipo de detergente para limpieza a estos puntos de conexión de la red o "drops", provoca que se oxiden los cables y los contactos de cobre, aislando la conexión entre la red y sus servicios.

© ***Sellado de techos*** - Los cables de comunicación digital están ubicados en los techos de las escuelas. Antes de iniciar un trabajo de sellado de techos, es necesario que éstos sean identificados y protegidos para que no sean afectados por los químicos utilizados para el sellado y por el contacto directo con las antorchas de fuego.

® ***Poda de árboles*** - Los cables que proveen conexión a la escuela se conectan con ésta de forma aérea, en la mayoría de los casos. Es importante identificar los mismos para evitar que sean cortados durante la poda de los árboles,

En los casos de sellado de techos y poda de árboles se debe consultar con la OSIATD para evaluar si los cables aéreos pueden ser afectados.

Algunas de las causas principales de los cambios que se efectúan en la red son la mudanza, remodelación y ampliación de oficinas debido al aumento en el personal, instalación de laboratorios e incorporación de redes locales. A tales efectos, se ha establecido el siguiente procedimiento, que se aplicará cuando sea necesario instalar nuevas conexiones o mover los puntos de conexión ("drops") ya instalados.

1. Notificar por escrito los cambios deseados al Administrador de la Red, ubicado en la OSIATD. Esta notificación debe incluir un diagrama de los cambios a efectuarse y la descripción de los mismos. Además, debe incluir la cantidad de nuevo personal, si ese fuera el caso, y los equipos que interesa conectar.

2. La instalación de puntos de conexión adicionales conlleva un costo directo para la dependencia o escuela. Por lo tanto, se recomienda presupuestar el costo de los cambios como parte del costo de la remodelación o mudanza. El costo estimado fluctúa entre $200.00 a $300.00 por conexión (básico).

3. Informar a la OSIATD antes de efectuar la remodelación, mudanza o cambio en el área, para que se pueda coordinar con el suplidor la instalación de las conexiones ("drops") y

La certificación de éstas, siguiendo los estándares definidos en la Guía de Estándares de Infraestructura del DEPR.

4. Los equipos activos deben tener un mínimo de tres (3) años de garantía y servicio en el lugar, y antes de comprarlos deben ser evaluados por la OSIATD para garantizar que cumplen con los estándares del mercado y con las directrices y políticas sobre tecnología informática del DEPR.

5. Es necesario coordinar con el personal de la OSIATD la instalación de equipos adicionales para ampliar el alcance de la red, entiéndase enrutadores ("routers"), equipos de acceso inalámbrico ("wireless access points"), "hubs", etc. La instalación de estos equipos puede interrumpir el funcionamiento de la red en las escuelas. El personal de la OSIATD removerá cualquier equipo que haya sido instalado sin autorización.

6. Los equipos de comunicación de las escuelas deben estar ubicados en un área en la que se garantice su seguridad y conservación. El director de la escuela deberá velar para que estos equipos sean manipulados únicamente por personal autorizado por la OSIATD.

Servicios de mantenimiento al equipo de computadoras y periferales

La política del DEPR en relación a los servicios de mantenimiento al equipo de computadoras y periferales es que éstos sean ofrecidos por personal de la OSIATD, salvo en situaciones muy especiales. Se podrán utilizar los servicios de mantenimiento para proyectos especiales claramente identificados para los cuales el Departamento no cuente con los recursos especializados necesarios, o en aquellos en los cuales sea costo-efectivo para la Agencia. En estos casos deben especificarse claramente las fechas de comienzo y final del proyecto, así como la intervención del consultor. Además, cada proyecto deberá tener bien definidos y aprobados su meta, objetivos, estrategias y costos. El gerente del proyecto se asegurará de que antes de culminar el mismo, se ejecute una transferencia de conocimiento que asegure que el proyecto podrá tener la continuidad correspondiente con los recursos internos del DEPR.

Adquisición de equipo de computadoras o periferales

Toda compra de equipo de computadoras, laboratorios y periferales deberá cumplir con el siguiente procedimiento:

1. Todo equipo tiene que cumplir con las especificaciones mínimas establecidas y aprobadas por la OSIATD. Estas especificaciones están disponibles en el portal electrónico del Departamento de Educación: www.de.gobierno.pr.

2. Una vez se haya determinado cuál es el equipo que se desea adquirir, la orden de compra será enviada a la Unidad Administrativa de la OSIATD para ser evaluada y aprobada. En ésta el personal técnico autorizado verificará que el equipo que va a adquirirse cumpla con las especificaciones mínimas establecidas como requisito para aprobar la orden.

3. La orden, con ia aprobación correspondiente, será devuelta al comprador para su trámite final. Ninguna compra de equipo de tecnología será procesada sin la previa aprobación de la OSIATD.

4. Para promover la óptima utilización de los recursos de infraestructura tecnológica del DE, se favorecerá la instalación de laboratorios y tecnología de terminales de servicio (Terminal Services). Esta tecnología permite la operación de varios terminales de computadoras con un servidor en común. La configuración de estos laboratorios debe realizarse en coordinación con el personal de la OSIATD.

5. En el caso de que el equipo que se desea adquirir no esté contemplado entre aquellos para los cuales la OSIATD ha establecido especificaciones mínimas, la entidad interesada deberá realizar una consulta a la OSIATD antes de iniciar la gestión de compra.

El DEPR mantiene un contrato de licenciamiento con Microsoft Corp. Este contrato incluye una cantidad específica de licencias para los sistemas operativos Windows y el programado Microsoft Office. Por tanto, las dependencias del DEPR deben abstenerse de adquirir paquetes con estos sistemas operativos y programados, ya que éstos serán instalados por personal de la OSIATD. En el caso de la adquisición de múltiples computadoras, el suplidor deberá comunicarse con la OSIATD para coordinar la instalación de una imagen que contenga el sistema operativo, antivirus, la advertencia legal de uso y el paquete de Microsoft Office correspondiente. Toda compra de computadoras debe realizarse con el sistema operativo en versión sencilla o "Home".

Todas las computadoras del DEPR deben contener la notificación legal de utilización y la política pública desde el principio. Toda dependencia que adquiera equipo de computadoras tiene que coordinar con la OSIATD para que la División de Apoyo al Usuario proceda a la instalación de esta advertencia en todos los equipos.

En el caso de equipo adquirido por el DEPR, a través de propuestas, para su utilización en entidades educativas privadas se aplicarán las mismas directrices establecidas en esta Carta Circular. Los suplidores deben comunicarse con la OSIATD para coordinar la instalación de la imagen correspondiente. Sin embargo, esto no significa que el personal técnico de la OSIATD brindará mantenimiento ni servicios a estos equipos. El personal de la OSIATD no puede ofrecer servicios en entidades privadas. Durante el período de garantía del equipo las llamadas de servicio deben ser tramitadas a través del suplidor. Una vez culmine el período de garantía, la entidad debe procurar la compra de servicios técnicos para los equipos, ya sea mediante un contrato de mantenimiento u órdenes de servicio individuales.

Titularidad y derechos

La computadora, los servicios asociados, tanto internos como externos, el sistema de correspondencia electrónica (E-mail), el intranet, el acceso a Internet y los documentos y programas que existen en la Agencia son propiedad del DEPR y sólo podrán utilizarse para propósitos lícitos, prudentes y responsables dentro de las funciones o poderes de la Agencia. Por

Tal razón, el Secretario de Educación o su representante autorizado tienen la facultad de tomar las medidas necesarias para verificar que el equipo y la programación se utilicen en actividades que estén relacionadas con los fines y propósitos delineados por el DEPR.

Toda información, dato, obra literaria o de arte, escrito, documento, programa, acción, privilegio, patente, derecho de autor o cualquier otro que se cree o modifique mediante el uso de una de las computadoras del DEPR será propiedad de la Agencia, aunque los mismos hayan sido creados mediante el esfuerzo personal del usuario.

La información contenida en todos los equipos y medios tecnológicos provistos, los servicios asociados, tanto

internos como externos, los mensajes de correspondencia electrónica (E-mails), la información de intranet o de Internet, los documentos y los programados existentes podrán utilizarse exclusivamente para los fines de las funciones y poderes del DEPR.

Los programados o recursos para los cuales no exista una licencia o autorización de uso válido a nombre del DEPR no podrán ser utilizados ni instalados en ninguno de los equipos de la Agencia. Los programas del DEPR no podrán ser copiados o instalados en computadoras personales sin la autorización escrita del Director de la OSIATD,

Si algún empleado compra, de forma voluntaria, algún programado de computadoras y desea instalar y utilizar el mismo en los equipos del DEPR, deberá coordinar con la OSIATD la realización del análisis, pruebas e instalación correspondiente. El empleado donará la licencia del programado al DEPR. Ningún empleado instalará programado alguno en las computadoras del DEPR sin la debida autorización de la OSIATD. Toda instalación deberá ser realizada por personal autorizado de la OSIATD.

Los sistemas de computadoras y comunicaciones del DEPR no podrán ser utilizados para propósitos personales, de recreo, para manejo de un negocio o asunto privado del usuario o para la utilización y envío de mensajes en cadena. Además, no se utilizarán los recursos electrónicos del Departamento para tener acceso a compras, juegos, concursos, encuestas, páginas de entretenimiento o cualquier otro servicio ajeno a las funciones de la Agencia.

La utilización y acceso a propiedad intelectual será realizada sin violar los derechos de autor. El Departamento, a través de sus organismos de supervisión, velará por los derechos de propiedad intelectual y derechos de autor. Cualquier usuario que realice acciones en contra de estos derechos estará sujeto a las consecuencias legales correspondientes.

Todo equipo electrónico, incluyendo las computadoras portátiles, que sea propiedad del Departamento debe almacenarse en sitios seguros, preferiblemente bajo llave y en ambientes adecuados. El empleado al que se le entregue este equipo será responsable de éste, por lo que debe tomar medidas para evitar una posible pérdida o daño. El usuario, como custodio del equipo, se compromete a salvaguardarlo, incluyendo los accesorios que acompañan ese equipo. Este compromiso será evidenciado a través de un documento escrito que será firmado en el momento de entrega del equipo. En el caso de pérdida por robo, el usuario deberá presentar

Evidencia de haber denunciado el delito a las autoridades correspondientes mediante la presentación de una querella.

Toda dependencia, oficina, programa, oficina regional, distrito escolar o escuela del DEPR está obligado a mantener un inventario de todo el equipo tecnológico adquirido y utilizado por esa unidad. Este inventario debe cumplir con los requisitos establecidos por la Guía de Procedimientos Fiscales del Custodio de la Propiedad del Departamento de Educación. El inventario debe incluir:

1. Marca, modelo y número de serie del equipo
2. Lugar de ubicación
3. Persona responsable
4. Fecha de adquisición
5. Suplidor
6. Fecha y términos de la garantía
7. Unidad que adquiere el equipo
8. Fondos mediante los cuales fue adquirido

Una copia de este inventario debe ser enviada a la OSIATD. Cualquier cambio en el inventario debe ser notificado a

esta Oficina antes de cumplirse treinta (30) días del mencionado cambio. Esta información se mantendrá en el Sistema de Apoyo al Usuario. Si los equipos no están registrados en el Sistema, la División de Apoyo al Usuario podrá determinar negar el servicio luego de evaluar las circunstancias particulares.

Las computadoras deben estar cubiertas por una garantía de tres (3) años en sus componentes internos. Las pantallas de las computadoras portátiles no están cubiertas por la garantía. Si la pantalla se rompe, el usuario tendrá que costear su reparación o sustitución. La programación y configuración tampoco están cubiertas por la garantía del equipo. Toda entrega o pérdida de equipo será procesada de acuerdo a los estatutos y normas vigentes del Estado Libre Asociado de Puerto Rico y las normas establecidas por el DEPR.

El usuario es responsable de realizar un procedimiento de resguardo (backup) incremental semanalmente de todos sus documentos y asegurarse de haber realizado este procedimiento antes de que cualquier técnico intervenga con el equipo. La OSIATD no es responsable por la pérdida de información contenida en la memoria de las computadoras.

Seguridad

El uso de un código de acceso ("password"), no impedirá que se audite el sistema, y no significa que el usuario albergue expectativa de intimidad alguna con relación a la información almacenada en la computadora que tenga asignada o en cualquiera otra que utilice. Las contraseñas deben mantenerse en estricta confidencialidad. Todo usuario es responsable por cualquier transacción emitida utilizando su contraseña o "password"

El Departamento se reserva el derecho de auditar, vigilar y fiscalizar los sistemas de correspondencia electrónica y todos los servicios computarizados para garantizar que los mismos se utilicen para los propósitos y gestiones relacionadas con el trabajo. Estas auditorías se realizarán periódicamente, o al azar, o cuando exista una investigación sobre la situación en particular. Por estas circunstancias, el personal de DEPR no tiene derecho a la intimidad con relación a cualquier información, documento o mensaje creado, recibido o enviado a través del sistema de correo electrónico al usar las computadoras o el sistema de comunicación digital de la Agencia.

La utilización de equipos de computadoras portátiles privadas de los maestros para acceder al Sistema de Información Estudiantil a través de la red de voz y datos del Departamento se permitirá mediante previa autorización del supervisor inmediato del empleado. Los accesos serán configurados exclusivamente por personal autorizado por la OSIATD con previa verificación de que el equipo cuenta con un sistema de seguridad y antivirus actualizado. El personal de la OSIATD no será responsable por la reparación del equipo personal del empleado. Mientras el empleado esté utilizando su equipo para acceder a la red del DEPR, estará sujeto a las disposiciones de esta Carta Circular y del *Manual de Política sobre el Oso Aceptable de Internet en las Escuelas Públicas de Puerto Rico*. Además, el equipo estará sujeto a una auditoría.

Para salvaguardar la confidencialidad de la información del Departamento, no está permitido el envío fuera de la Agencia de documentos electrónicos o mensajes por medio de correo electrónico que contengan información confidencial del Departamento. Las cuentas personales de servicios de correo electrónico y acceso a Internet (Hotmail, Gmail, Yahoo!!!, etc.) podrán ser utilizadas en los equipos del Departamento, siempre que se cumpla con las normas y procedimientos establecidos mediante esta Carta Circular y el *Manual de Política sobre el Uso Aceptable de Internet en las Escuelas Públicas de Puerto Rico*. Se prohíbe modificar los privilegios de acceso a las redes internas o externas para obtener acceso a dichos recursos.

Ningún usuario podrá codificar, asignar contraseñas o modificar de alguna manera la información, mensajes de correo electrónico o archivos que son propiedad del Departamento con el propósito de impedir que alguien pueda leerlos, entenderlos o utilizarlos, o con el propósito de alterar el nombre del usuario, la fecha de creación o modificación u

otra información que se utilice regularmente para identificar la información, mensajes o archivos, si no se obtiene previamente el consentimiento por escrito de la OSIATD. En el caso de que, por razones de seguridad, se permita codificar, asignar contraseñas o modificar alguna información para evitar que otras personas puedan leerla, el DEPR estará facultado para decodificar la misma o restituirla a su condición original. El usuario será responsable de proveer todos los datos para lograr acceso a la información o archivo.

La modificación de los parámetros o la configuración de las computadoras del Departamento para ampliar las capacidades de acceso a la red de la Agencia sólo podrán ser realizadas por personal asignado y autorizado por la OSIATD. Los medios portátiles de almacenaje de información que sean utilizados en el Departamento deben ser revisados y certificados para garantizar que están libres de virus.

Hacer referencia a ia política de seguridad (de ser necesario) para enfatizar los accesos al área de la Oficina de Sistemas.

Las políticas y disposiciones sobre la seguridad de sistemas y la seguridad física del Centro de Cómputos están contenidas en el documento ***Políticas y Procedimientos de Seguridad Informática del Departamento de Educación***, del cual se incluye una copia con esta Carta Circular.

Políticas anti discrimen

Existe una prohibición absoluta (o de "cero tolerancia") a la utilización de la computadora o del sistema de correspondencia electrónica para enviar, recibir o crear mensajes o documentos de contenido discriminatorio por razón de raza, sexo, credo, ideas políticas, orientación sexual, ideas religiosas, impedimentos físicos u origen social o nacional, o que puedan ser catalogados como hostigamiento sexual.

Está prohibido el manejo o transmisión de material obsceno, profano u ofensivo a través del sistema de computadoras o del sistema de comunicación electrónica del DEPR. Esto incluye, a modo de ejemplo, acceso a materiales eróticos, bromas de cualquier forma o cualquier comentario o chiste que pueda violar la política de discrimen del Departamento o su política de hostigamiento sexual.

Se prohíbe utilizar protectores de monitores ("screen savers") con fotos de personas, artistas, modelos, deportistas, fotos de calendario o cualquier otra imagen que no guarde relación con los fines educativos y/o de las funciones del área de trabajo a la que pertenezca el usuario.

Correo electrónico

Las cuentas de correo electrónico oficiales provistas por el DEPR deberán utilizarse sólo para propósitos exclusivos de las funciones oficiales de cada usuario.

Revisar, leer o interceptar cualquier tipo de comunicación electrónica del Departamento o de cualquier otra persona o entidad, sin el consentimiento expreso del remitente y del destinatario de la comunicación, está prohibido. Los usuarios deberán abstenerse de suscribirse a las listas de correo electrónico o de participar en grupos noticiosos ("newsgroups") que divulguen información o mensajes ajenos a las funciones y deberes del DEPR. El usuario se abstendrá de enviar vía correo electrónico archivos que excedan la capacidad de su cuota en el servidor.

El procedimiento para solicitar una cuenta de correo electrónico está descrito en el documento de ***Políticas y Procedimientos de Seguridad Informática del Departamento de Educación de Puerto Rico*** del cual se incluye una copia con esta Carta Circular.

Acceso a páginas de Internet

El acceso a las páginas de Internet a través de la Red Educativa de Voz y Datos del DEPR está limitado a funciones educativas e inherentes a las funciones de la Agencia. La utilización de esta fuente de información se regirá por las normas establecidas en el *Manual de Política sobre el Uso Aceptable de Internet en las Escuelas Públicas de Puerto Rico.*

El acceso a páginas bloqueadas por los sistemas de filtrado establecidos en la REVD deberá ser solicitado mediante el formulario **Solicitud de Activación de Acceso a Páginas Web en la Red Educativa de Voz** y **Datos.** Este formulario deberá ser enviado a la Unidad de Tecnología y Currículo, donde se realizará la evaluación correspondiente. Una vez evaluada la solicitud, será referida a la OSIATD para proceder a otorgar el acceso al portal a través de la red. Si por alguna razón la solicitud fuera denegada, la Unidad de Tecnología y Currículo notificará al solicitante vía correo electrónico.

Sistema de Información Estudiantil (SIE)

El uso del Sistema de Información Estudiantil (SIE) estará limitado al personal autorizado para ingresar, acceder y modificar información en el mismo. El procedimiento para solicitar una cuenta de acceso al SIE está descrito en el documento de ***Políticas Procedimientos de Seguridad Informática del Departamento de Educación de Puerto Rico.***

Los usuarios del SIE serán responsables de mantener su contraseña en estricta confidencialidad y velar por la privacidad y confidencialidad de los datos ingresados en el SIE. Este compromiso se evidenciará por escrito mediante el documento de autorización y asignación de cuenta al SIE. Este documento deberá mantenerse en archivo en la unidad de trabajo del usuario para fines de auditoría.

Los usuarios del SIE se regirán por las normas y procedimientos establecidos en esta Carta Circular y en el *Manual de Política sobre el Uso Aceptable de Internet en las Escuelas Públicas de Puerto Rico.*

Disposiciones generales

Los programas de charlas (“chais”) serán utilizados únicamente con fines educativos y deberán estar autorizados por la OSIATD. El uso o participación en estos programas será supervisado por los maestros, maestros bibliotecarios o directores escolares, en el caso de que los mismos sean utilizados por los estudiantes.

Las políticas antes mencionadas sobre el uso del correo electrónico y sobre sus auditorías tendrán igual aplicación para los otros recursos de intranet e Internet, tales como; WWW, FTP y chat.

Es responsabilidad de los usuarios cumplir con las **normas de cuotas de espacio en los servidores. El usuario será responsable de la creación de un archivo interno en su computadora, conocido como “PST”, pava archivar los correos electrónicos que entienda**

Necesario mantener. Además, deberá limpiar su buzón de correo electrónico semanalmente, incluyendo la bandeja de salida (“Sent Items”) y los correos borrados (“Deleted Items”).

Las políticas de Internet serán revisadas periódicamente, de ser necesario. Se incorporarán y se harán formar parte de estas advertencias todos los documentos, memorandos, instrucciones, manuales o políticas que se notifiquen de

tiempo en tiempo y que tengan relación con el uso de las computadoras en el DEPR.

Todos los usuarios de Internet, por medio de los equipos electrónicos del Departamento, tienen que cumplir con las normas y procedimientos establecidos en el *Manual de Política sobre el Uso Aceptable de Internet en las Escuelas Públicas de Puerto Rico.*

Aceptación y procedimientos disciplinarios

Se tornarán las medidas disciplinarias, civiles o criminales que correspondan contra los usuarios que violen estas políticas o abusen del acceso al Internet, según sea el caso. En el caso de las medidas disciplinarias, éstas pueden ser tan severas como la destitución de su cargo.

El DEPR se reserva el derecho de denunciar actuaciones que constituyan delito federal o estatal, aunque no estén expresamente prohibidas por estas condiciones de uso de los equipos de computadoras.

Es obligación de cada usuario conocer y seguir todas las políticas o instrucciones del DEPR en relación a las medidas de seguridad para el uso del equipo de computadoras y de las redes disponibles, particularmente las normas adoptadas para la utilización del Internet.

El hecho de que una conducta o actuación relacionada con las computadoras, redes, sistemas y recursos electrónicos del Departamento no esté contemplada en estas advertencias y condiciones de uso de las computadoras, no impide que el usuario pueda ser sancionado, si a juicio de las autoridades de la Agencia se trata de **una conducta o actuación imprudente o irresponsable** con relación a los referidos equipos y recursos electrónicos. A los fines de estas advertencias y condiciones de uso, una conducta o actuación imprudente o irresponsable significa cualquier acción directa o indirecta que ponga en riesgo la seguridad, integridad y confiabilidad de los equipos, las redes, la información, los programas y los sistemas del DEPR. **Uso imprudente o irresponsable** significa, además, cualquier actuación o conducta directa o indirecta que pueda ocasionar daño físico, mental, moral, problemas interpersonales o un menoscabo de la reputación de los usuarios, personas ajenas al Departamento y otros empleados de la Agencia.

Es obligación de todos los usuarios comunicar al Director de la OSIATD o a la persona designada a esos fines, cualquier situación, incidente o problema de seguridad, acceso indebido o violación voluntaria o involuntaria de estas normas, que surja del uso de las computadoras o redes del DEPR.

Esta Caita Circular deroga cualquier normativa establecida anteriormente sobre los sistemas de información del Departamento de Educación de Puerto Rico, incluyendo la Carta Circular Núm. 4-2008-2009: Directrices y Políticas sobre la Tecnología Informática en el Departamento de Educación de Puerto Rico.

Se requiere el fiel cumplimiento de estas directrices.

Cordialmente,

Jesús M. Rivera Sánchez, Eu/D.
Secretario

Anejos

GOBIERNO DE PUERTO RICO

DEPARTAMENTO DE EDUCACIÓN

SOLICITUD DE ACTIVACIÓN DE ACCESO A PÁGINAS WEB EN LA RED EDUCATIVA DE VOZ Y DATOS

Fecha: _____

Entidad que solicita: _____ _____

Persona contacto: ____ _____

Teléfono: _____ Correo electrónico: _____

Dirección de la Página
Web a la cual solicita acceso: _____

Justificación para otorgar el acceso: _____

PARA SER COMPLETADO POR LA UNIDAD DE TECNOLOGÍA Y CURRÍCULO

Aprobado: Sí CU No D

Funcionario que realizó la evaluación: _____

Posición: _____ Firma:

Fecha de la aprobación: _____

PARA SER COMPLEATDO POR LA OFICINA DE SISTEMAS DE INFORMACIÓN

Fecha de apertura de acceso: _____

Funcionario que realiza la programación: _____ _____

Firma:

Anejo B

GOBIERNO DE PUERTO RICO **DEPARTAMENTO DE EDUCACIÓN**

CERTIFICACION

Certifico haber recibido y leído en todas sus partes la Carta Circular Núm. 7-2011-2012: DIRECTRICES Y POLÍTICA SOBRE LA ADQUISICIÓN Y DESARROLLO DE SISTEMAS, EQUIPO TECNOLÓGICO Y EL USO DE LA TECNOLOGÍA INFORMÁTICA EN EL DEPARTAMENTO DE EDUCACIÓN.

Nombre del empleado: _____

Número de identificación: _____

Puesto y posición: _____

Ubicación: _____

Firma del empleado: _____
Fecha: