GOBIERNO DE PUERTO RICO

DEPARTAMENTO DE EDUCACIÓN

Oficina de Sistemas de Información y Apoyo Tecnológico a la Docencia (OSIATD)

MANUAL DE PROCEDIMIENTOS PARA EL USO DE INTERNET, CORREO ELECTRÓNICO Y RECURSOS DE TECNOLOGÍA

TABLA DE CONTENIDO

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 tecnología y acceso a la red del Departamento. Estos deben utilizarse únicamente para propósitos educativos y funciones administrativas de la agencia, de manera segura, ética, responsable y legal.

El DE reconoce el privilegio de todos los miembros de la comunidad escolar de tener acceso razonable a los diferentes recursos de información que ofrece la Internet, que debe tener un propósito educativo, así, como un uso responsable y apropiado. Los usuarios de la red del Departamento y los recursos informáticos deben cumplir con las reglas de uso de estos recursos.

El acceso a la red de telecomunicaciones proporciona oportunidades potenciales para beneficio de la educación. El DE cuenta con un sistema para controlar el acceso de la información difundida por Internet, mediante el sistema de identificación y filtrado de contenido, según requerido por el estatuto Children's Internet Protection Act, descrito a continuación.

Reconocemos que gran parte de la información y el contenido en la red de Internet apoya el proceso educativo; sin embargo, existen recursos con información y contenido que no son adecuados o que pueden ser nocivos. Por esta razón, el estudiante tendrá acceso en un entorno supervisado y configurado para que no se permita el uso de material nocivo en el ambiente escolar. Los administradores del sistema educativo controlaran 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 secretario de Educación –secretario- y el principal oficial de informática (CIO, por sus siglas en inglés) aprueban el Manual para el uso de Internet, correo electrónico y otros 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 y (c) cumplir con el Children's Internet Protection Act 2000 (CIPA), (d) cumplir con la Ley 267 de 31 de agosto de 2000, Ley para proteger a los niños, niñas y jóvenes en el uso y manejo de la red de Internet, además de cumplir con la Ley 149 de 15 de julio de 1999, según enmendada, conocida como Ley Orgánica del Departamento de Educación de Puerto Rico y con la Comisión Federal de Comunicaciones, orden DA 11-125. Este manual aplica a las siguientes condiciones: (a) la red del DE u otros recursos informáticos que se utilizan tanto en las instalaciones y

equipos del DE como por medio de acceso remoto (como se define en la Sección B: Definiciones) y (b) dispositivos personales (como se define en la Sección B: Definiciones) que se conectan a la red del DE o los recursos informáticos con fines educativos o administrativos tanto dentro como fuera del DE o de la escuela.

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

El DE puede hacer cambios a este manual en cualquier momento, cuando la situación lo amerite, y estará disponible en el portal electrónico.

B. Definiciones

Recursos informáticos- Todos los equipos existentes y futuros, y la tecnología de información, ya sea fija o portátil, que se utiliza para realizar tareas y trabajos cotidianos del DE, que incluye, pero no se limita a, componentes, espacio de disco, dispositivos de almacenamiento, memoria del sistema, servidores, ordenadores, dispositivos de telecomunicaciones, dispositivos de mano, impresoras, escáner, máquinas de fax y fotocopiadoras, entre otros, propiedad o arrendado por el DE.

Red del DE- Infraestructura existente y futura que se utiliza para transmitir, almacenar y ofrecer acceso a los datos por medio electrónico. Esta incluye, pero no se limita a, sistemas de correo electrónico, sistemas de colaboración (tales como calendario, tableros de mensaje, conferencia, blogs, conferencias de video, chat o mensajería instantánea de texto, sitios web y podcasting, bases de datos, información, sistemas y servicio de Internet, entre otros, propiedad o arrendado por el DE.

Personal- Funcionarios, empleados permanentes y temporeros, practicantes, proveedores, consultores, contratistas y agentes autorizados y voluntarios, que trabajan bajo la supervisión de personal de la agencia, incluidas las escuelas.

Dispositivos personales- Equipo existente y futuro propiedad de estudiantes y del personal, que se utiliza para realizar funciones oficiales o educativas, dentro o fuera del DE (tal como: asistentes de datos personales (PDA, por sus siglas en inglés), ordenadores portátiles, tabletas, iPads y teléfonos celulares).

Acceso remoto- Acceso autorizado a los recursos de informática desde una ubicación fuera de la red del DE.

Blogs- Sitios web para la publicación de artículos en secuencia cronológica que pueden contener texto, imágenes y videos, entre otras formas de expresión digital, donde los lectores pueden contribuir a discusiones con sus comentarios.

Chat- Conversación inmediata en forma de texto por medios digitales.

Podcasting- Medio para la difusión y descarga de contenido digital (vídeo, sonido, audio, imágenes) por subscrición a fuentes de transmisión sindicada.

II. PROPIEDAD Y PRIVACIDAD

A. Propiedad del Departamento

Todos los documentos, datos e información creados, almacenados, transmitidos y procesados en la red del DE o por medio de otros recursos informáticos son propiedad del DE y estarán sujetos a 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 o activos en el sistema de escuelas públicas. Esto aplica a personal cuando ocurra una terminación de empleo o contrato, jubilación o cualquier otra causa de separación permanente de las funciones). Los estudiantes y el personal serán responsables de garantizar que su acceso y uso de los 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 DE y sus recursos informáticos no tendrán ninguna expectativa de privacidad con respecto a sus tareas escolares, registros de empleo, correos electrónicos, uso y sitios visitados en la Internet y documentos almacenados. Estos: (1) se pueden acceder, copiar, transmitir y divulgar en cualquier investigación del Departamento sobre presuntas violaciones de este manual y (2) estos son admisibles en los tribunales según los procedimientos administrativos y de acuerdo con 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 por cualquier sospecha de actividad inapropiada o ilegal y se reserva el derecho, sin previo aviso o consentimiento a:

1. realizar cambios a la configuración de la red o sus recursos de informática para neutralizar amenazas a la seguridad o por violaciones a las normas establecidas en este manual,

2. denegar 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 por violaciones a las normas establecidas en este manual,
3. acciones disciplinarias a estudiantes y personal que lo ameriten, según autorizado o aprobado por el DE,
4. acceder, buscar, leer, inspeccionar, copiar, supervisar, registrar o utilizar datos e información almacenada, transmitida y procesada en la red del Departamento o en otros recursos informáticos e
5. informar cualquier actividad ilegal a las autoridades apropiadas.

III. SEGURIDAD DE INTERNET

A. Filtrado de contenido

Con el objetivo de cumplir con el Children's Internet Protection Act 2000 (CIPA), el Departamento instaló el programa FortiAnalyzer en las computadoras con acceso a Internet para restringir el acceso a sitios que contengan material pornográfico, representaciones obscenas u otros materiales no aptos para menores. El anejo A contiene la descripción de la solución de filtrado de contenidos. El DE se reserva el derecho de implementar una solución de filtrado diferente, si se determina que es necesario.

Un administrador, supervisor o persona puede solicitar desactivar la solución de filtrado de contenidos con fines de investigación bona fide u otros propósitos legales educativos o comerciales, y si lo autoriza el 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 existe riesgo de que los usuarios puedan estar expuestos a material inapropiado. Sin embargo, el DE tomará las medidas razonables para proteger a sus estudiantes y minimizar el riesgo de acceso intencional o inadvertido a material inapropiado por parte de los estudiantes.

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 detectar violaciones a las normas establecidas en este manual y (2) revelar, copiar o transmitir documentos

de estudiantes y del personal, datos e información, según el DE lo considere necesario o apropiado, a su entera discreción, o según sea requerido 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 otro tipo
comunicaciones, tal como servicios de mensajería, para fines comerciales, legales o de seguridad cuando el DE, a su entera discreción, lo considere necesario o apropiado.

C. Educación

El DE está comprometido a educar a sus estudiantes sobre la seguridad de la Internet que incluye, pero no se limita a, comportamiento apropiado mientras se está en línea en sitios web de redes sociales y en chat romos. También proporcionará a los estudiantes educación y concienciación sobre el cyberbullying y las 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 DE considere eficaz y apropiado.

A los estudiantes transferidos de otros sistemas educativos se le proporcionará las instrucciones y la información relacionada al comportamiento adecuado en línea.

D. Limitación de responsabilidad

El DE no asume ninguna responsabilidad resultante del abuso intencional o accidental de la red del DE y de 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 cyberbullying

Cyberbullying se define como la crueldad hacia los demás al enviar o publicar material nocivo por medio de la Internet o un teléfono celular Hay varias formas diferentes de cyberbullying:

1. Flaming: peleas en línea 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 usarla para enviar material vicioso o embarazoso para otros.

5. Salida y engaño: comprometer a alguien en mensajería instantánea, engañándole a fin de que revele información sensible y reenvíe 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 para luego compartirlo en línea.
9. Acoso cibernético: Intenso y repetido acoso y denigración que incluye amenazas o la creación de un miedo significativo.

El material de cyberbullying puede publicarse en sitios web personales, blogs o, por medio de correo electrónico, grupos de discusión tablones de mensajes, chats mensajería instantánea (IM, por sus siglas en inglés) o mensajes de texto e imágenes. Un cyberbully puede ser un extraño para la víctima o puede alguien que conoce. Un cyberbully también puede ser anónimo y puede solicitar la participación de otras personas en línea que no conocen a la víctima, también conocido como cyberbullying por proxy.

El cyberbullying puede estar relacionado con intimidación u hostigamiento en que el estudiante victima en la escuela también es objetivo de agresión en línea en la escuela Otras veces, el estudiante victima toma represalias en línea o comparte su enojo o depresión en línea como amenaza o material angustiante. Además, el cyberbullying puede involucrar las relaciones personales. Por ejemplo, si se rompe una relación, una persona puede empezar a acosar a la otra persona y amenazar con la distribución de imágenes. El cyberbullying puede basarse también en odio o prejuicio: intimidando a otros a causa de raza, religión, apariencia física (incluida la obesidad) u orientación sexual.

Es ampliamente conocido que la intimidación puede resultar en danos psicológicos a largo plazo para las víctimas; esto incluye baja autoestima, depresión, ira, fracaso, deserción escolar y, en algunos casos, violencia escolar o suicidio. Aunque hay menos investigaciones sobre cyberbullying, la evidencia creciente sugiere que también se asocia con importantes danos psicológicos como ansiedad, depresión o hasta suicidio. Lamentablemente, es muy generalizado, más de la mitad de los adolescentes ha recibido intimidación en línea o ha participado en cyberbullying y más del 25% de los adolescentes han recibido intimidación repetidamente por medio de sus teléfonos celulares o de la Internet.

El cyberbullying parece ser una epidemia rápida en parte por el código de silencio y quizás vergüenza para la victima que vive este tipo de abusos. Los adolescentes pueden

estar reacios a decir a los adultos lo que está sucediendo en línea o por medio de sus teléfonos celulares porque están traumatizados emocionalmente. Creen que es su culpa, tienen miedo a una mayor retribución o a que se les restrinjan sus actividades virtuales o el uso de teléfono celular. Solo 1 de cada 10 adolescentes le dice a un padre si ha sido 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 (bullying)

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 bullying 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 acoso e intimidación de los estudiantes si ocurre dentro de la propiedad o el establecimiento de la escuela, alrededor de las áreas, en los autobuses escolares y en las 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 si la conducta se produce en la propiedad escolar, los alrededores o en las actividades patrocinadas por la escuela, así como la gravedad y el impacto de las acciones en la víctima.

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 a 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 al 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 mediante 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 estudiantil.

V. RESPONSABILIDADES

A. Responsabilidades del estudiante

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

1. Los estudiantes tienen acceso al Internet solo si siguen las instrucciones, autorización y 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, al personal directivo de la escuela o a sus padres.
4. Los estudiantes nunca deben acordar reunirse con alguien que conocieron por Internet, sin el consentimiento o autorización de sus padres o tutores.
5. 5. Ningún estudiante debe intentar acceder 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 archivos o equipo tecnológico.
8. El estudiante puede imprimir el material para el que tenga el permiso del maestro.
9. Los estudiantes no pueden acceder, crear, copiar, o distribuir material que sea amenazante, con contenido pornográfico, obsceno, racista o de connotaciones sexuales.
10. El estudiante utilizará únicamente el acceso a Internet por medio del equipo de la escuela para fines legales autorizados y que estén relacionados a las actividades curriculares.

B. Responsabilidades del personal directivo de la escuela

El personal directivo de la escuela debe asegurarse que se cumpla con las normas establecidas en este manual y llevará a cabo las siguientes actividades o gestiones:

1. Comunicará 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 del proporcionar acceso a la red y los riesgos asociados con el uso de los recursos de Internet, antes de proporcionar acceso
2. Identificar, recomendar y seleccionar los recursos más adecuados de Internet para apoyar y ampliar el proceso de aprendizaje del estudiante.
3. Designar una persona para administrar la red de área local.
4. Demostrar y ofrecer servicios de Internet a los padres.
5. Cumplir con los términos y condiciones de licencia de programados adquiridos.
6. Coordinar y ofrecer desarrollo profesional a todos los funcionarios sobre el acceso a Internet y la integración de recursos tecnológicos en el currículo.
7. Evidenciar la distribución de este manual para toda la comunidad escolar (maestros, estudiantes, padres, entre otros) y mantener las hojas de recibo en un lugar seguro y accesible, para presentarlas en caso de una auditoria o monitoria.
8. Mantener este manual en un lugar accesible a toda la comunidad escolar (biblioteca, tablón de anuncios o portal, entre otros).

C. Responsabilidades del maestro

El maestro debe velar que los estudiantes cumplan con las normas establecidas en este manual. Llevará a cabo las siguientes actividades o gestiones:

1. Garantizar que el uso de recursos de Internet es coherente con el currículo y con las metas de los programas del sistema.
2. Proporcionar, planificar y monitorear experiencias de aprendizaje basada en el currículo escolar, para que el estudiante se convierta en un aprendiz permanente, independiente y productivo.
3. Monitorear y evaluar los recursos de aprendizaje, incluidos sitios de Internet, antes de recomendar su uso a los estudiantes.
4. Monitorear el acceso al Internet por el estudiante y ofrecer orientación sobre para el uso adecuado de los recursos de Internet.
5. Orientar a los estudiantes que la comunicación en la red es de naturaleza pública y rara vez prevalece la privacidad.
6. Proporcionar a los estudiantes que utilizan Internet, dirección y expectativas claras acerca de las normas de uso aceptable de la red y de los sistemas.

7. Discutir la política de uso aceptable de Internet con los estudiantes antes de permitirles acceder a la red y trabajar con la asignación de trabajos o actividades que impliquen su uso.
8. Proporcionar actividades de aprendizaje estructurado que estén alineadas al currículo.
9. Comprobar que el estudiante está trabajando en el aprendizaje de las actividades que se le asignaron.
10. Asegurarse que cada uno de sus estudiantes y padres firmen el formulario de consentimiento para el uso de los equipos y recursos tecnológicos, que forma parte de este manual.
11. Entregar a la oficina del director los documentos de consentimiento de padres y estudiantes.
12. Proporcionar evidencia relacionada a la supervisión de los alumnos participantes en el uso y manejo de instalaciones tecnológicas (se recomienda identificar los equipos para facilitar su control y supervisión).

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 acciones disciplinarias que van desde la suspensión temporera y la revocación permanente de acceso a los recursos tecnológicos y a la red del DE, 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. Las acciones disciplinarias específicas pueden incluir, pero no limitarse, a lo siguiente:

1. Advertencia verbal,
2. Advertencia escrita,
3. Restricción de acceso a Internet,
4. Pérdida del privilegio de usar la red del Departamento y los recursos informáticos,
5. Gestión de cobro por gastos de llamadas comerciales, compras no autorizadas y otras obligaciones financieras,
6. Rembolso del costo total de la reparación o el remplazo de los bienes dañados, destrozados, perdidos o robados,
7. Audiencia disciplinaria para establecer un plan correctivo que corresponda a la falta y medidas que serán impuestas,
8. 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, revocación permanente de los privilegios de acceso de recursos informáticos y de la red del DE, 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 Los empleados tienen derecho de solicitar una reconsideración o apelación a la medida aplicada.

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 identificar diferentes fuentes de información local, nacional e internacional, con el objetivo de ampliar y aclarar el contenido del currículo. El acceso a la información y recursos de colaboración son vitales para el proceso de investigación.
El propósito de este manual es que los estudiantes tengan una guía del comportamiento apropiado con el uso de los recursos en línea y de las posibles consecuencias de no cumplir con las normas. El objetivo es que los estudiantes puedan hacer uso educativo de Internet y que, en específico, puedan:

1. Desarrollar destrezas y hábitos para acceder, seleccionar, usar, crear y publicar información para un determinado público.
2. Investigar y resolver problemas asignados por el maestro o identificados, que requieran investigación, análisis crítico, evaluación, etc.
3. Analizar datos o información para tomar decisiones que integren valores propios y sus necesidades de aprendizaje.
4. Pensar críticamente para reconocer y reflejar sobre 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 mediante bases de datos, correo electrónico, grupos de noticias y la Word 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 apoyarán la integración efectiva de estos recursos en el currículo. Los estudiantes pueden acceder a información de los sistemas previamente evaluados y recomendados por los profesores.

C. Condiciones para el uso de la red del DE y otros recursos de informática

Los estudiantes y sus padres o tutores deben firmar acuse de recibo de este manual y autorizar los estudiantes a utilizar los equipos y la red del DE bajo los términos y condiciones descritos en el manual. Tal reconocimiento y acuerdo estará expuesto en el Anejo 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 DE 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 otros recursos informáticos se refiere a las actividades apropiadas y legales que promuevan los objetivos educativos del DE, incluido, pero no limitado a lo siguiente: (a) educación y colaboración (b) académico y (c) comunicación entre maestros, administradores, estudiantes y padres.

E. Uso inaceptable

No se podrá publicar ninguna información personal o fotos de los estudiantes 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 DE y sus recursos de informática se refiere a actividades que no promueven los objetivos educativos del DE y que, a criterio exclusivo del DE, carecen de propósito o contenido educativo legítimo. Las actividades

que constituyen inaceptables en el uso de la red del DE o de sus recursos de informática incluirán, pero no se limitarán a, cualquiera de las siguientes actividades no expresamente aprobadas o relacionadas a la investigación educativa o a las asignaciones de tarea o escuela:

1. Violación de las leyes. El uso de la red del DE o de 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 y compra de 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, programas (software) comerciales, música, archivos de sonido, películas e imágenes) sin el permiso del titular, en violación de las leyes de los derechos de autor estatal, federal o internacional. 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 (Titulo 17, USC) y su contenido se cita apropiadamente.
4. Programas (software) no autorizados. Uso del software en violación de los términos de licencia y condiciones.
5. Lesiones personales. Uso de la red del Departamento o de sus recursos de informática para apoyar actividades que causen daño a otros, incluido, pero no limitado a los siguientes:
    a. Amenazar, acosar y hacer declaraciones falsas o difamatorias sobre otros; esto incluye cyberbullying, mensajes de odio, chistes y comentarios discriminatorios;
    b. Amenazar la seguridad de una persona;
    c. Apoyar la 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 de vocabulario profano, obsceno, abusivo, lascivo, vulgar, grosero, calumnioso, amenazante, 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 protegidos por las leyes de derechos civiles;
    g. Promover, o participar en, una relación con otros estudiantes, niños o adultos que no esté relacionada a lo académico o actividades

extracurriculares patrocinadas por la escuela, a menos que esté previamente autorizado por escrito por el director y el padre o tutor (esto incluye interacción de estudiantes y maestros en las redes sociales);

h. Contactar otros estudiantes, niños o adultos, por medio del correo electrónico de terceros, sobre temas no relacionados a 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

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

6. Daños a la propiedad. Uso de la red del DE o sus recursos de informática para, o en apoyo de, actividades que causen daños a la propiedad, incluyendo, pero no limitado a los siguientes:
    a. Hacking, vandalismo, introducción de virus, gusanos (worms), caballos de Troya (Trojans), bombas de tiempo, así como cambios no autorizados (instalar o modificar) al equipo del ordenador (hardware), los programas (software) y las 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, eliminar o añadir información, o manipular datos del DE;
    c. Entrar, cambiar, mover o copiar los datos en la red del DE y sus componentes cuando el usuario no tiene ninguna autorización de acceso o entrada. Cualquier entrada, modificación o supresión de los datos del DE por un usuario no autorizado, se consideran manipulación y están prohibidos;
    d. Ingresar datos falsos en la red del DE o en sus recursos de informática;
    e. Comprometerse en cualquier otra conducta deliberada que interfiera, obstruya o cargue los recursos de la red del DE o sus recursos de informática.
7. Violaciones a la seguridad de la red. No cumplir con las políticas y directrices establecidas por el principal oficial de informática o su designado, o usar la red del DE o sus recursos de informática de una manera que ponga en peligro o atente contra la seguridad; facilitar el acceso no autorizado o la divulgación de información confidencial y 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. Obtener acceso no autorizado a la red del Departamento o sus sistemas de información, por medio de la cuenta de otra persona, códigos de acceso o identificación distinta a la asignada al usuario;

b. Revelar información personal acerca de ellos mismos o de otras personas esto incluyen los códigos de identificación (logins), contraseñas (passwords), direcciones y números de teléfono.
c. Interferir con la capacidad de otros usuarios para acceder a sus cuentas,
d. Intentar subvertir o eludir la seguridad de la red del DE o restricciones, perjudicar la funcionalidad de la red del DE o de otros recursos informáticos;
e. Revelar, difundir, transmitir, usar o reproducir información confidencial o propiedad del DE sin autorización o salvaguardas apropiados, que incluye, pero no se limita a, información financiera, correspondencia, informes, códigos de acceso o información del personal o del estudiante.

8. Uso no educativo. El uso no educativo de la red del DE o sus recursos de informática es inaceptable. Usos inaceptables incluyen, pero no se limitan a, lo siguiente:
    a. Medios sociales. 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 personal, para lucro personal o para hacer una ganancia (es decir, ejecutar un negocio en eBay por medio de la red del Departamento) ofrecer o proveer bienes, servicios, anuncios de productos, promociones o solicitudes no autorizadas; o (c) participar en actividades para recaudar fondos o para relaciones públicas relacionadas (por ejemplo, solicitud para fines religiosos);
    c. Otros usos no educativos. Promover o participar en (1) apuestas, correo basura, cartas en
    cadena, bromas, rifas, entre otros; (2) actividades religiosas; o (3) cabildeo político.
9. Uso incorrecto general. Está prohibido el uso de la red del DE 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 a recursos para los cuales no tiene derecho por no estar relacionado a sus funciones.
    b. Robo de identidad. Suplantar a cualquier persona viva o muerta, organización, empresa u otra entidad.
    c. Uso de sistema de terceros. Utilizar un sistema de terceros para comunicarse cuando se dispone del sistema oficial del DE, o para realizar funciones oficiales sin autorización.

d. Participar en actividades prohibidas en este manual por medio de otro proveedor de servicios de Internet que forme parte de proyectos de apoyo a las escuelas.
e. Sistemas de terceros. En la medida en que un sistema en particular no esté disponible en la red del DE o sus recursos de informática, el uso de este está sujeto a autorización por escrito del DE. Si es aprobado, uso del mismo está sujeto a los requisitos de este manual de política.
f. Datos cifrados encrypted. Cifrar mensajes, archivos y registros en la de red del DE o sus recursos de informática sin el permiso de las autoridades escolares administrativas apropiadas.
g. Declaraciones sobre la Política del DE. 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.

F. Correo electrónico

Las actividades aceptables en relación al correo electrónico son aquellas que cumplen el propósito, los objetivos y la 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 retomo 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 solo a sus destinatarios.

El uso del correo electrónico es una herramienta educativa que debe cumplir con las políticas, las normas y los procedimientos sobre el uso de los sistemas de tecnología del DE (Carta Circular 07-2012-2012).

Uso aceptable- El uso del correo electrónico por los estudiantes debe ser consistente con los objetivos del DE y acorde con las políticas de uso de sistemas y tecnologías. Todo usuario tiene que conocer y entender los estándares de uso de esta herramienta de comunicación. El uso de los estudiantes tiene que ser consistente con los objetivos académicos y para uso académico únicamente.

Uso no aceptable- Los estudiantes con acceso al correo electrónico oficial del DE no podrán transmitir ninguna comunicación que esté prohibida por cualquier medio de la agencia. Los correos electrónicos tienen que seguir las mismas reglas de comunicación presencial y escrita.

Los usos no aceptables incluyen, pero no se limitan, a:

- Uso de palabras obscenas o lenguaje que pueda ser ofensivo, que contenga contenido sexual, político o difamatorio.
- Transmitir cualquier material que viole leyes federales y estatales, estándares, regulaciones o guías, que incluye material que violente los derechos civiles o constitucionales, o constituya hostigamiento; o transmitir material protegido por leyes de derechos de autor, sin el consentimiento expreso del autor.
- Esconder la identidad del usuario, para enviar correos anónimos, a nombre de otro usuario o persona, sin su consentimiento, con el objetivo de esconder su identidad.
- Iniciar correos en cadena,
- Enviar mensajes no solicitados e innecesarios a un grupo de usuarios con el objetivo de realizar actividades de promoción, venta anuncios de eventos de índole privada, social o política, que no tiene relación con eventos propios del DE.

Reglas

1. El sistema de correo electrónico de los estudiantes es propiedad del DE. El DE puede monitorear el uso del sistema. El estudiante que haga uso inapropiado del correo electrónico está expuesto a que se le suspendan los privilegios de tener una cuenta y la acción disciplinara que corresponda.
2. Los estudiantes y padres tienen que solicitar y autorizar, respectivamente, el uso de correo electrónico del DE. Los estudiantes no accederán ni utilizarán el correo electrónico del DE sin la autorización de sus padres o guardianes.
3. Los estudiantes son responsables totalmente de sus cuentas y no compartirán sus claves de acceso con nadie excepto con sus padres o maestros.
4. El estudiante deberá cambiar su contraseña cuando entienda que la confidencialidad está comprometida.
5. El DE bloquea, filtra y monitorea el uso del correo electrónico que contenga material inapropiado.
6. Los estudiantes no podrán enviar información personal y confidencial a personas fuera del sistema educativo sin la supervisión y conocimiento de los padres y maestros.
7. Los estudiantes que reciban material no solicitado de extraños, amenazantes e inapropiados, deberán notificar el incidente inmediatamente al maestro o al director de la escuela y no deberá responder al mismo.

8. Los maestros son responsables de evitar, eliminar y detener cualquier uso inapropiado del correo electrónico, en particular, pero no limitado a: material pornográfico, obscenidad, material protegido, bullying y amenazas, entre otros.
9. El DE puede modificar o borrar correos electrónicos y documentos adjuntos a estos, que puedan contener virus o algún código que pueda causar daño en los sistemas, equipos y componentes de la red.

G. Notificación de incidentes

Los estudiantes informarán inmediatamente al DE sobre cualquier violación de seguridad real, supuesta o cualquier otra violación bajo esta política, que incluya, pero no se límite a lo siguiente:

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, incluidos dispositivos portátiles
5. Acceso inadvertido a material inapropiado o recepción de comunicación inadecuada
6. Recibo de correo basura (spam) inadecuado, mensajes electrónicos sospechosos (por ejemplo, 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.

VIII. POLÍTICA DEL PERSONAL

A. Objetivos

El propósito de esta política para el personal del DE es que cuenten con las herramientas necesarias para ejercer adecuadamente sus funciones y apoyen, directa o indirectamente, al aprovechamiento académico de los estudiantes. El objetivo es que, mediante la red del DE y sus recursos informáticos, el personal pueda realizar lo siguiente:

1. Lograr objetivos auriculares de nuestros programas educativos
2. Desarrollar y construir su currículo

3. Colaborar con maestros local y globalmente
4. Continuar su desarrollo profesional
5. Acceder a la información y a una diversidad de recursos por medio de la Internet, que facilite el proceso de 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. Obtener información sobre temas diversos y globales que amplíen sus conocimientos.
8. Desarrollar habilidades especiales y competencias tecnológicas que les permitan integrarlas al ámbito profesional y social.

Las oficinas regionales promoverán el compromiso de los docentes para la adopción de los recursos de Internet y otros materiales de aprendizaje (programas educativos) y la integración efectiva de estos recursos en el currículo. Los alumnos pueden acceder la información de los sistemas previamente evaluados y recomendados por los maestros.

B. Uso aceptable

La red del DE y sus recursos de informática se utilizarán solamente para funciones oficiales, cualquier uso personal debe ser limitado a un mínimo. El uso aceptable se refiere a esas actividades apropiadas y legales que promueven la educación y objetivos del DE, incluido, 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” se refiere a actividades que no promueven los objetivos educativos, y los objetivos del DE y que, a criterio exclusivo del DE, carecen de contenido educativo legítimo. Las actividades que constituyen el uso inaceptable incluyen, pero no se limitan a, cualquiera de las siguientes actividades no expresamente aprobadas o relacionadas con el ámbito escolar, entre ellas:

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 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. Programas (software) no autorizado. Uso de los programas en violación de los términos de licencia y condiciones.
5. Lesiones personales. Uso de la red del DE y sus recursos de informática para apoyar actividades que causen daño a otros; esto incluye, pero no se limita a, los siguientes:
    a. Amenazar, acosar, hacer declaraciones falsas o difamatorias sobre otros (esto incluye cyberbullying, mensajes con contenido 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); Intimidar o acechar a otro individuo;
    d. Utilizar lenguaje calumnioso, amenazante, irrespetuoso, o sexualmente explícito;
    e. 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 las leyes de derechos civiles;
    f. Promover o participar en una relación con un estudiante que no esté relacionada 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 u otros— en sitios de redes sociales);
    g. Comunicarse con alumnos por medio del correo electrónico de terceros sobre temas no relacionados a la escuela.

h. Utilizar información publicada, enviada o almacenadas en línea que podría poner en peligro a otros (por ejemplo, cómo construir una bomba, manufactura de drogas).
i. 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 la propiedad; esto incluye, pero no se limita a, los siguientes:
    a. Hacking, cracking, vandalismo, la introducción de virus, gusanos (worms), caballos de Troya [Trojans), bombas de tiempo, así como cambios no permitidos (es decir, instalar o modificar) el equipo del ordenador, los programas (software) y las 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 los datos 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 ponga en peligro o atente 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; esto incluye los códigos de identificación (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; esto incluye, pero no se limita a, información financiera, correspondencia, informes, códigos de acceso o información del personal o de 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 por medio de la red del Departamento); (b) utilizar la red del Departamento u otros recursos informáticos para ofrecer o proveer bienes, servicios, anuncios de productos, promociones o solicitudes no autorizadas; o (c) 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, incluidas las actividades políticas o de elecciones relacionadas a un sindicato u otras organizaciones de empelados.
9. Mala utilización general. Está prohibido el uso de la red del Departamento y sus recursos de informática para apoyar actividades que atentan la seguridad de la red del Departamento y de 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 por medio de la red del Departamento o por medio 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. Violar los términos de uso especificados para un sistema particular de la red del Departamento y sus recursos de informática.

D. Monitoreo y supervisión

El DE utiliza FortiAnalyzer para monitorear las actividades en línea del personal y los estudiantes, incluida la navegación por la web, el uso del correo electrónico, la participación en salas de chat y otras formas de comunicación electrónica. Una descripción de la solución de filtrado de contenidos se adjunta como Anejo A. El DE se reserva el derecho de implementar una solución de filtrado diferente
si determina que 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 de 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 personal, 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 la finalidad, los objetivos y la 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 retomo 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; esto incluye, 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, incluidos dispositivos portátiles;
5. Acceso inadvertido a material inapropiado o recepción de comunicación inadecuada;
6. Recibo de correo basura (spam) inapropiado, mensajes electrónicos sospechosos (por ejemplo, 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 legitimas 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 de otros recursos de informática.

IX. LIMITACIONES DE RESPONSABILIDAD

El DE no será responsable de (1) cualquier reclamación, pérdida, daño, costo u otras obligaciones derivadas del uso de la red del Departamento o de 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 por medio del acceso del usuario a la red del Departamento o de sus recursos de informática.

Cualquier declaración publicada o comunicada mediante el 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 5-2012-2013 (30 de agosto de 2012), adjunta como anejo C
2. Carta Circular 7-2011-2012 (16 de agosto de 2011), adjunta como anejo 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 N° 267 de 2000, Ley para proteger a los niños y jóvenes en el uso y manejo de la red de Internet.
6. Protección de los niños en el Siglo XXI, Ley, Publica Núm. 110-385, Título II, 122 estadístico 4096 (2008), enmendada.
7. Orden de la Comisión Federal de Comunicaciones, DA 11-125 (2011)

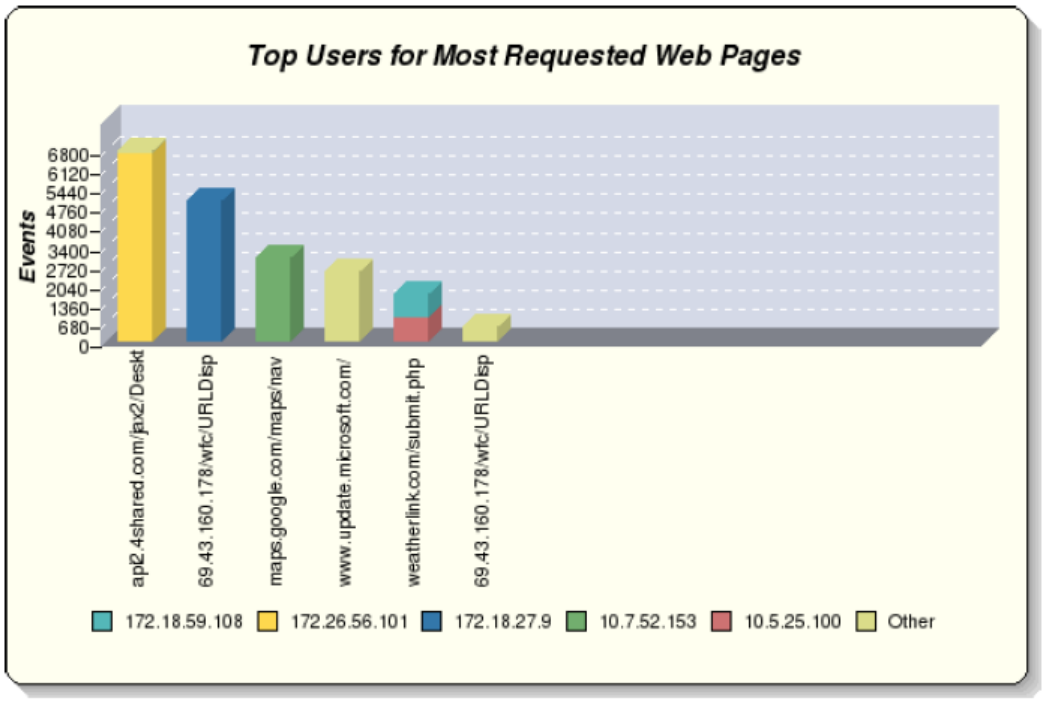
ANEJO A

Descripción de FORTIANALYZER (solución de filtrado de contenido)

Conforme a La Ley de Protección de Internet para los Niños (CIPA, por sus siglas en inglés), el DE ha implementado el FortiAnalyzer en todos los equipos conectados a la Internet como mecanismo para restringir el acceso a sitios que contengan pornografía, representaciones obscenas u otros materiales perjudiciales para los menores. El programa, o software, funciona mediante la búsqueda de palabras o conceptos, según lo determinado por el Departamento. Cuando el programa identifica tales palabras o conceptos, niega el acceso de usuario basado 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 c 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 programa solicitará, 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 un estudiante que investigue 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 solo 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 programa es infalible, y todavía hay un riesgo de que un usuario pueda estar expuesto a un sitio o mensajes que contengan materiales inapropiados.

PÁGINAS DE EXTRACTO DE INFORME DE FILTRADO DE CONTENIDO



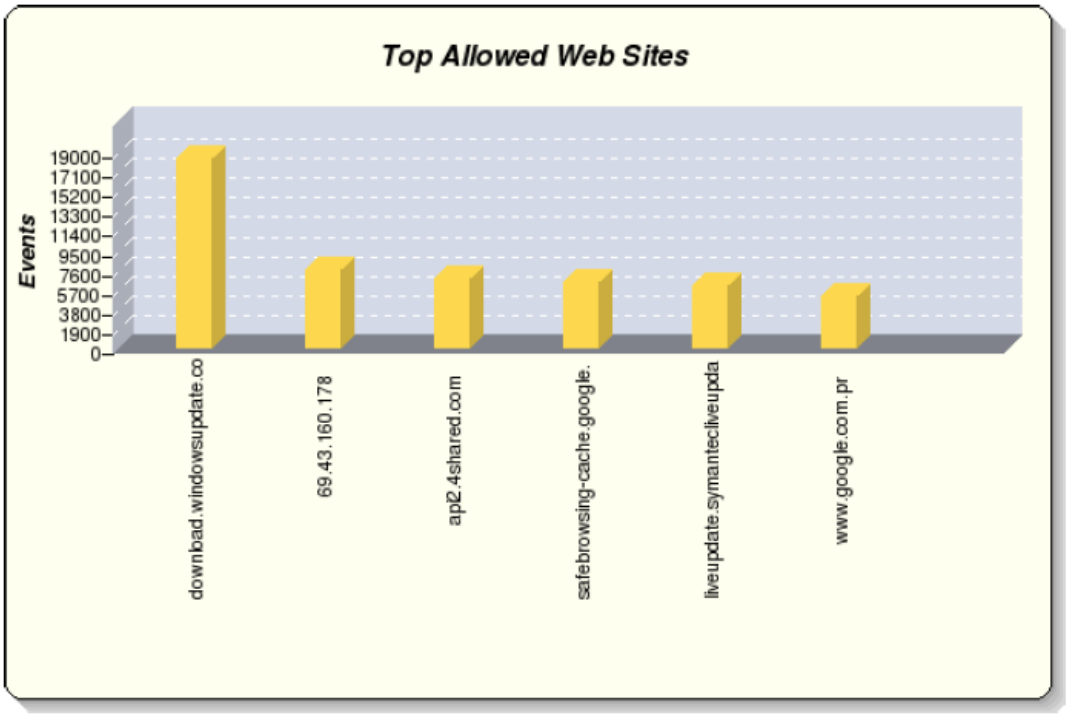
Top Allowed Web Sites

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		
Destination	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**



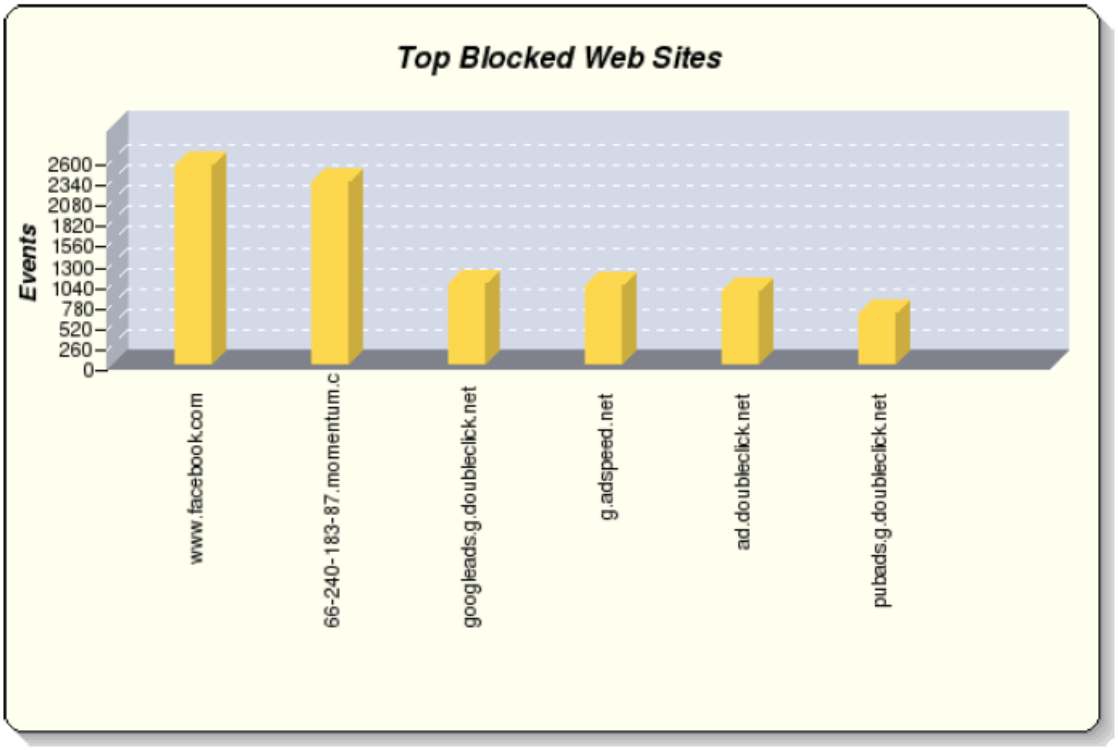
Top Blocked Web Sites

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		
Destination	Events	% of Total
www.facebook.com	2518	11.61
66-240-183-87.momentum.com	2285	10.54
googleads.g.doubleclick.net	1008	4.65
g.adspeed.net	978	4.51
ad.doubleclick.net	923	4.26
pubads.g.doubleclick.net	624	2.88
Other	13348	61.56
Total	**21684**	**100.00**



Top 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**

ANEJO B

GOBIERNO DE PUERTO RICO
DEPARTAMENTO DE EDUCACIÓN

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 la persona que recibe el Acuerdo

_____ _____

Firma de estudiante o usuario | Firma de la persona que recibe el Acuerdo

_____

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

ANEJO C

Carta Circular Núm. 10-2015-2016

POLÍTICA PÚBLICA PARA ESTABLECER EL PROCEDIMIENTO PARA LA IMPLEMENTACION DEL PROTOCOLO DE PREVENCIÓN, INTERVENCIÓN Y SEGUIMIENTO DE CASOS DE ACOSO ESCOLAR (BULLYING) ENTRE ESTUDIANTES EN LAS ESCUELAS PÚBLICAS DE PUERTO RICO

ANEJO D

Carta Circular Núm. 12-2015-2016

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