CORRECCIONAL JUVENIL DE OREGON

Declaración de la política

Parte 0: misión, valores y principios

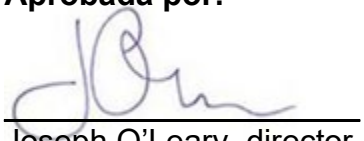
Asunto:

Uso de activos y sistemas de información electrónicos

Sección – Número de política:	*Sustituye a:*	*Fecha de entrada en vigencia:*	*Fecha de la última actualización/revisión:*
0: misión, valores y principios - 7.0	**0-7.0 (12/18)** **0-7.0 (09/16)** **0-7.0 (12/13)** **0-7.0 (09/11)** **0-7.0 (04/09)** **0-7.0 (12/06)** **I-E-3.2 (12/02)**	**10/29/2021**	**Ninguna**

Normas y referencias relacionadas:

- Estatutos Revisados de Oregon (Oregon Revised Statutes (ORS, por sus siglas en inglés)) 164.377 (Delito informático)
- ORS 282.020 (Control de la impresión y de las compras de impresión estatales)
- Servicios de Información Empresarial Políticas estatales de servicios de ciberseguridad
- Reglas administrativas de Oregon (Oregon Administrative Rules (OAR, por sus siglas en inglés)) 416-040 (Uso de las redes electrónicas por parte de los infractores dentro de los centros de la OYA)
- Política del Sistema de Información de Justicia Juvenil (Juvenile Justice Information System (JJIS, por sus siglas en inglés)):
  Seguridad (de usuarios)
  Conceder el acceso al JJIS y a los datos del JJIS
- Acuerdo de seguridad del usuario del JJIS
  Asignación de funciones para el acceso de seguridad de los usuarios del JJIS
- Política de la Correccional Juvenil de Oregon (Oregon Youth Authority (OYA, por sus siglas en inglés)): 0-2.0 (Principios de conducta)
  0-2.1 (Normas profesionales)
  I-B-2.0 (Delegación para los gastos y aprobación de las de pago)
  I-C-9.0 (Dispositivos móviles de comunicación (celulares) y otros dispositivos móviles de almacenamiento de datos)
  I-E-1.4 (Gestión de registros públicos)
  I-E-2.0 (Conservación, destrucción y archivo de registros)
  I-E-2.3 (Solicitudes de información y registros de los jóvenes)
  I-E-3.1 (Gestión de publicaciones)
  I-E-3.2 (Clasificación y protección de activos de información)
- Formularios de la OYA:
  YA 2502 (Formulario de seguridad de la OYA para el acceso a otros sistemas que no le pertenezcan)
  YA 8021 (Acuerdo laboral sobre la comunicación electrónica y activos de información)
  YA 8023 Acuerdo del usuario para dispositivos móviles del Estado
- Preguntas frecuentes (Frequently Asked Questions (FAQ, por sus siglas en inglés)) sobre esta política

Procedimientos relacionados:	▪ Ninguno
Responsable de la política: Director de información	**Aprobada por:**  Joseph O'Leary, director

I. PROPÓSITO:

Esta política proporciona los requisitos y las normas de seguridad para el uso aceptable de la información electrónica, los sistemas informáticos y los dispositivos por parte del personal de la OYA.

II. DEFINICIONES DE LA POLÍTICA:

Control: medios de gestión del riesgo, incluyendo políticas, procedimientos, directrices, prácticas o estructuras organizativas, que pueden ser de naturaleza administrativa, técnica, directiva o jurídica.

Encriptación: uso de un proceso algorítmico para transformar los datos en una forma que los haga ilegibles o inutilizables sin utilizar un proceso o clave confidencial.

Activos de información: cualquier conocimiento que pueda comunicarse o material documental, independientemente de su forma física o de sus características, que tenga valor para la organización.

Información del sistema: computadoras, hardware, software, impresoras, escáneres, fotocopiadoras, medios de almacenamiento, redes, procedimientos y procesos operativos utilizados en la recopilación, el procesamiento, el almacenamiento, el intercambio o la distribución de información dentro de la infraestructura informática y de red compartida del Estado o con cualquier acceso más allá del acceso público ordinario.

Sistema de Información de Justicia Juvenil (JJIS, por sus siglas en inglés): el Sistema de Información de Justicia Juvenil (JJIS) es un sistema de información electrónica integrado a nivel estatal que está diseñado, desarrollado e implementado para apoyar una serie continua de servicios y responsabilidad compartida entre todos los miembros de la comunidad de justicia juvenil. En una asociación de colaboración entre la Correccional Juvenil de Oregon (OYA, por sus siglas en inglés) y los departamentos juveniles de los condados de Oregon, el JJIS es administrado por el estado de Oregon a través de la OYA.

Dispositivo de comunicación móvil (Mobile Communication Device (MCD, por sus siglas en inglés)): es un dispositivo de mensajes de texto o de comunicación inalámbrica bidireccional (celular) que está diseñado para recibir y transmitir mensajes de voz o de texto, incluyendo los Sistemas de Posicionamiento Global (Global Positioning Systems (GPS, por sus siglas en inglés)) móviles, y los teléfonos y relojes inteligentes.

Usuario: son todos los empleados estatales, voluntarios, sus agentes, proveedores y contratistas, incluyendo los usuarios afiliados a terceros que acceden a los activos de información estatales; y todas las demás personas autorizadas a utilizar la tecnología de la información estatal con el propósito de alcanzar los objetivos y procesos comerciales del Estado.

III. POLÍTICA:

La información, los sistemas informáticos y los dispositivos de la agencia se ponen a disposición de los usuarios autorizados para optimizar los procesos comerciales del estado de Oregon. La OYA cumplirá con la política a nivel estatal que esté relacionada con el uso aceptable de los activos de información estatales según las indicaciones de los Servicios de Información Empresarial. Todo uso de la información, de los sistemas informáticos y de los dispositivos debe cumplir con esta política.

La información, los sistemas informáticos y los dispositivos estatales se proporcionan únicamente con fines comerciales y la información de dichos sistemas es propiedad exclusiva del estado de Oregon, sujeta a su control exclusivo, a menos que exista un acuerdo o contrato de anulación que indique lo contrario. Ninguna parte de los sistemas o de la información de la agencia estatal es o puede llegar a ser, propiedad privada de ningún usuario del sistema. El Estado es propietario de todos los derechos legales para controlar, transferir o utilizar toda o cualquier parte o producto de sus sistemas. Todos los usos deben cumplir esta política y cualquier otra política y norma estatal aplicable.

Como agencia estatal, la OYA es responsable de controlar y supervisar sus sistemas, así como de proteger sus activos de información. Toda la información almacenada en las aplicaciones, los sistemas y las redes es propiedad del estado de Oregon. Por lo tanto, los usuarios deben cumplir con las leyes y normas de conservación pública.

El personal de la OYA debe tener acceso a los activos y sistemas de información de manera equitativa, según los requisitos de su trabajo.

IV. NORMAS GENERALES:

El administrador de los Servicios Técnicos de la OYA es responsable de la seguridad de los sistemas de información electrónicos de la OYA.

A. Autorización de seguridad

La OYA es responsable de conceder y supervisar el acceso de los usuarios a los sistemas y a la información necesaria para realizar su trabajo, y de revocar el acceso de los usuarios en el momento oportuno. La OYA puede revocar el permiso para cualquier uso de sus sistemas en cualquier momento sin ninguna causa o explicación.

1. Todos los usuarios deben estar debidamente autorizados y autentificados para utilizar los activos de información estatales.

2. Se le prohíbe al personal permitir que los jóvenes utilicen las computadoras o los dispositivos electrónicos del personal. Las instalaciones de la OYA cuentan con computadoras especialmente diseñadas para el uso de los jóvenes (por ejemplo, quioscos multimedia, Chromebooks, computadoras designadas para la escuela).

   El personal puede permitir que un joven utilice un dispositivo de comunicación móvil de propiedad estatal cuando sea necesario, para apoyar el plan del caso o los objetivos del joven, y el personal debe supervisar directamente al joven todo el tiempo (consulte la política de la OYA I-C-9.0 Dispositivos móviles de comunicación (celulares) y otros dispositivos móviles de almacenamiento de datos).

3. El acceso a la información en las estaciones de trabajo y los servidores requiere un inicio de sesión individual que incluye la identificación del usuario y una contraseña.

4. Aprobación de la autorización de seguridad

   a) Los supervisores son responsables de aprobar el acceso de su personal a la red, los sistemas y los datos de la OYA. El supervisor indicará el tipo de autorización de cada personal o unidad de trabajo y lo notificará al director de seguridad, al administrador de la red local o al servicio de atención al usuario correspondiente para los servicios de información.

   b) Cuando cambie la asignación de trabajo o la situación del personal, el supervisor deberá notificar al director de seguridad correspondiente, los cambios o revocaciones de seguridad necesarios.

B. Contraseñas

1. Las contraseñas deben ser confidenciales y cumplir los requisitos mínimos para las contraseñas que se indican a continuación:

   a) Tener una longitud mínima de 10 caracteres en todos los sistemas;

   b) No debe contener el nombre de la cuenta del usuario o partes del nombre completo del usuario que excedan de dos caracteres consecutivos;

   c) No debe contener espacios;

   d) Contener caracteres de **tres** de las siguientes **cuatro** categorías:

      (1) Caracteres del inglés en mayúsculas (de la A hasta la Z);

      (2) Caracteres del inglés en minúsculas (de la a hasta la z);

(3) Dígitos de base 10 (0 - 9); o

(4) Caracteres no alfabéticos (por ejemplo, !, $, #, %);

e) Expiran en un plazo máximo de 90 días calendario;

f) La vigencia mínima de la contraseña es de siete días;

g) No debe ser idéntica a las 10 contraseñas anteriores;

h) Ser única en diferentes sistemas;

i) No deben ser difundidas abiertamente fuera de una ubicación segura; y

j) No debe mostrarse cuando se introduzca.

2. Almacenamiento de la contraseña en el navegador

El personal no debe almacenar las contraseñas en los navegadores web, ni siquiera cuando el navegador se lo indique.

C. Bloqueo de la cuenta

El bloqueo de la cuenta ocurre cuando el usuario no consigue iniciar sesión después de un número determinado de intentos. El personal de los Servicios de Información (Information Services (IS, por sus siglas en inglés)) aplicará los siguientes componentes de bloqueo de cuentas:

1. El umbral de bloqueo de la cuenta se establece en cinco intentos de inicio de sesión no válidos (tres intentos de inicio de sesión no válidos para las cuentas de acceso privilegiado);

2. La duración del bloqueo de la cuenta debe ser de 30 minutos; y

3. El bloqueo de la cuenta debe restablecerse automáticamente después de 30 minutos.

D. Revocación de la cuenta de usuario

1. El personal de Recursos Humanos debe notificar al IS la situación laboral del miembro del personal (por ejemplo, desvinculación o licencia de ausencia con goce de sueldo) en la fecha en que la cuenta del miembro del personal debe desactivarse o antes.

2. Cuando se termine la relación laboral con la OYA, el personal de IS debe desactivar y eliminar las cuentas de usuario de acuerdo con los procedimientos del IS.

3. El personal del IS debe archivar la cuenta de todos los sistemas electrónicos (por ejemplo, el correo y las carpetas de inicio) en un plazo de 30 días después de la desactivación de la cuenta de usuario.

E. Hardware y software

1. Todo el hardware y el software debe ser aprobado, comprado, descargado e instalado por el personal del IS.

2. El personal no debe utilizar computadoras personales, impresoras o dispositivos móviles (celulares) para asuntos estatales.

3. Consulte la política de la OYA I-C-9.0 Dispositivos móviles de comunicación (celulares) y otros dispositivos móviles de almacenamiento de datos para obtener más información sobre este tema.

F. Uso de activos de información

1. El manejo o el uso de los activos de información debe realizarse de manera que no perjudique la disponibilidad, la fiabilidad o el rendimiento de los procesos y sistemas comerciales estatales, ni contribuya indebidamente al congestionamiento del sistema o de la red.

2. El uso de los activos de información estatales no debe ser falso, ilegal, ofensivo o disruptivo.

3. Las redes y sistemas estatales no deben utilizarse para ver, descargar, almacenar, transmitir o recuperar intencionadamente cualquier información, comunicación o material que:

a) Es acosador o amenazante;

b) Es obsceno, pornográfico o sexualmente explícito;

c) Es difamatorio;

d) Es dañino para la reputación de la OYA;

e) Hace referencia discriminatoria a la raza, la edad, el género, la orientación sexual, las creencias religiosas o políticas, la nacionalidad, la salud o la discapacidad;

f) Es falso o fraudulento;

g) Es ilegal o promueve actividades ilegales;

h) Está destinado al lucro personal;

i) Aprueba el fomento del odio, la intolerancia, la discriminación o los prejuicios;

j) Propicia el juego o las apuestas en Internet; o

k) Contiene humor ofensivo.

4. Cualquier uso de los sistemas de información estatales respetará la confidencialidad de la información de otros usuarios y no intentará:

a) Acceder a sistemas de terceros sin autorización previa de los propietarios del sistema;

b) Obtener los nombres para iniciar sesión o las contraseñas de otros usuarios;

c) Intentar anular o violar las medidas de seguridad de la computadora o de la red;

d) Interceptar, acceder o controlar los archivos electrónicos, o las comunicaciones de otros usuarios o de terceros sin la aprobación del autor o de los propietarios responsables de la empresa;

e) Examinar los archivos o la información de otro usuario sin la necesidad comercial específica de hacerlo y sin la aprobación previa del autor o del propietario responsable de la empresa; o

f) Publicar o difundir datos confidenciales o no autorizados.

G. Acceso a la red

1. El administrador de los Servicios Técnicos de la OYA supervisa la seguridad de la información de la red general de la OYA.

2. El personal de los Servicios Técnicos de la OYA actúan en calidad de directores de seguridad de la red. En esta función, los directores de seguridad de la red tienen la capacidad de crear, eliminar y bloquear cuentas de usuario. También pueden permitir el acceso aprobado a diferentes carpetas en los servidores de la OYA.

3. Todo el personal de la OYA debe firmar un formulario YA 8021 (Acuerdo laboral sobre la comunicación electrónica y activos de información) antes de recibir las credenciales de usuario y posteriormente cada año.

H. Acceso a Internet

El uso de Internet aumenta el riesgo de exponer los activos de información estatales a violaciones de seguridad. La OYA permite al personal un uso personal limitado y casual, siempre que no suponga un costo, o sea insignificante para el Estado y que dicho uso no viole las normas que continuación se indican.

1. Dado que los sistemas estatales son capaces de registrar las pulsaciones del teclado, se aconseja encarecidamente a los usuarios que no lleven a cabo negocios personales que requieran información personal identificable (por ejemplo, banca electrónica o compras en línea). Quienes realicen este tipo de actividades lo hacen bajo su propio riesgo.

2. Solamente la OYA puede determinar si el uso por parte del personal es de carácter personal o comercial.

3. El uso comercial de Internet incluye el acceso a los sistemas estatales alojados en la web, la información relacionada con el empleo en el Estado, incluidos todos los derechos autorizados por los respectivos convenios colectivos de trabajo. Los sitios aprobados para este propósito incluyen, entre otros, la Junta de Beneficios para Empleados Públicos (Public Employees Benefits Board (PEBB, por sus siglas en inglés)), el Sistema de Jubilación de Empleados Públicos (Public Employees Retirement System (PERS, por sus siglas en inglés)), el Programa de Asistencia al Empleado (Employee Assitance Program (EAP, por sus siglas en inglés)), la página Oregon JOBS, el Oregon Savings Growth Plan [Plan de Crecimiento para el Ahorro Universitario de Oregon] e información contractual de los sindicatos.

4. Los sistemas estatales no pueden utilizarse para juegos de computadora, ya sean en Internet o personales, o juegos incluidos en aplicaciones de software aprobados.

5. Los sistemas estatales no pueden utilizarse para alojar o gestionar páginas web personales, o servidor de listas; o para crear, enviar o reenviar cadenas de correo electrónico.

6. Los sistemas estatales no pueden utilizarse para iniciar sesión en cuentas personales de correo electrónico o redes sociales.

7. No está permitido utilizar los sistemas estatales con servidores proxy no autorizados o cualquier otro medio para eludir los sistemas de vigilancia de Internet de la OYA.

8. La OYA permite el uso de los servicios de transmisión por Internet en tiempo real únicamente con fines comerciales.

9. Los dispositivos de propiedad estatal no pueden utilizarse para descargar, almacenar o recuperar cualquier información o material para uso personal.

I. Acceso a la intranet

La intranet de la OYA (OYANet) cuenta con un sistema descentralizado de responsables de sitios que gestionan la seguridad de los mismos. Cada responsable de sitio debe gestionar la seguridad y el acceso a su sitio asignado.

J. Acceso remoto

1. El personal solo puede acceder a las redes y a la intranet de la OYA desde ubicaciones externas con equipos de propiedad estatal, proporcionados por el departamento del IS de la OYA.

2. El personal debe utilizar la autenticación de múltiples factores para acceder de manera remota a los sistemas y las aplicaciones de la OYA.

3. El personal no debe llevar el equipo de propiedad estatal fuera de los Estados Unidos.

K. Acceso inalámbrico

1. Red inalámbrica de la OYA

a) El personal debe conectarse al punto de acceso inalámbrico seguro de la OYA cuando utilice equipos de propiedad estatal, mientras esté en las oficinas de la OYA.

b) El personal puede conectar los equipos de propiedad estatal a las redes inalámbricas públicas cuando se encuentre fuera de las oficinas de la OYA.

2. Red inalámbrica para invitados

a) Las personas que son invitadas en las oficinas de la OYA pueden utilizar la red inalámbrica para invitados.

b) La red inalámbrica para invitados debe estar protegida por una contraseña. La contraseña se puede compartir con los invitados. Se puede encontrar en la página de inicio del sitio de la intranet de la OYA.

c) El personal puede utilizar la red inalámbrica para invitados para su uso casual como se define en esta política.

d) Los equipos de propiedad estatal no deben conectarse a la red inalámbrica para invitados.

L. Mensajería instantánea (Instant messaging (IM, por sus siglas en inglés)) y mensajes de texto

1. La mensajería instantánea (IM), los mensajes de texto y otras alternativas de comunicación/mensajería están destinadas a fines comerciales relacionados con el Estado.

   Sin embargo, la OYA permitirá al personal un uso personal limitado y casual. Las únicas soluciones aprobadas son la plataforma de Teams, Teams IM y la aplicación de mensajes de texto a nivel nacional en los teléfonos móviles proporcionados por el Estado. Toda la comunicación transmitida a través de estos servicios es detectable.

2. Uso aceptable

   a) El personal puede utilizar la mensajería instantánea y la mensajería de texto para comunicar información sobre hechos y logística que no sea parte sustancial de los asuntos oficiales; que haya sido documentada en otra parte o que se registre, documente y conserve como un registro público independiente.

   b) En ausencia de una documentación separada, el personal no debe utilizar la mensajería instantánea o los mensajes de texto para fines oficiales, salvo para comunicaciones regulares que no se ajusten a la definición de “registro público”.

   c) Los mensajes de texto no deben contener información restringida o de nivel crítico.

   d) Algunos ejemplos de usos aceptables de la mensajería instantánea y de texto son:

      (1) Programación;

      (2) Solicitar una llamada o un correo electrónico sobre un asunto, sin discutirlo a fondo;

      (3) Solicitar u ofrecer ayuda logística (“¿Puede ayudarme a llevar estas cajas al almacén?”);

      (4) Reenviar información de contacto de cualquier persona (“Llámeme al 503-123-4567”);

      (5) Explicar su ubicación actual o preguntar por la ubicación de otra persona (“Estamos en la reunión discutiendo el anuncio de esta mañana. ¿Está por aquí?”);

(6) Describir hechos o acontecimientos que no están relacionados con las actividades laborales de la agencia (“¡Se me cayó el café encima justo antes de la reunión!”), o que han sido o serán necesariamente registrados por separado (“El Sr. Jones acaba de testificar ante la comisión que nuestro proyecto de ley le costaría $3 millones a los contribuyentes”); y

(7) Preguntar por acontecimientos como los anteriores (“¿Ha testificado ya el Sr. Jones en el comité?”).

3. Uso inaceptable

a) El personal debe evitar las discusiones sustanciales sobre los asuntos de la OYA a través de la mensajería instantánea y los mensajes de texto. Como se ha indicado anteriormente, los hechos sustanciales solo pueden comunicarse por mensajería instantánea o por mensaje de texto si van a estar, o ya están, documentados en un registro público independiente.

b) Si se producen discusiones importantes relacionadas con los asuntos de la OYA a través de mensajería instantánea o mensajes de texto, dichas discusiones se deben copiar inmediatamente en un formato de registro público independiente (por ejemplo, copiando los mensajes pertinentes en un correo electrónico de la agencia).

M. Uso del correo electrónico

El correo electrónico está destinado a utilizarse únicamente para asuntos relacionados con el Estado. No obstante, la OYA permitirá a los empleados un uso personal limitado y casual.

1. Todo el correo electrónico debe ser profesional.

2. Archivos adjuntos en un correo electrónico

a) Los archivos adjuntos relacionados con asuntos del Estado pueden enviarse con el correo electrónico para asuntos relacionados con el Estado.

b) Los archivos adjuntos personales pueden enviarse con los correos electrónicos personales siempre que su tamaño y frecuencia sean limitados.

3. Se prohíbe el envío de correos electrónicos u otras comunicaciones electrónicas que intenten ocultar la identidad del usuario o que personifiquen a otra persona.

4. No se permite el uso de codificadores, servicios de reenvío, buzones o métodos de supresión de identidad.

5. El correo electrónico puede utilizarse para asuntos sindicales según lo autorizado por los respectivos convenios colectivos de trabajo.

6. Los correos electrónicos son registros públicos, y la OYA y todos los usuarios son responsables de garantizar el cumplimiento de las leyes de archivo y registros públicos. Consulte la política de la OYA I-E-1.4 Gestión de registros públicos para el manejo de registro de correos electrónicos.

7. La información restringida y de nivel crítico que se transmita fuera del sistema de correo electrónico de la OYA, debe encriptarse y protegerse adecuadamente de acuerdo con la política I-E-3.2 Clasificación y protección de activos de información: guía de manejo de la información.

N. Dispositivos de propiedad estatal

1. Las computadoras de trabajo deben bloquearse o desconectarse cuando el usuario se retire del área.

2. El personal no debe conectar dispositivos móviles de almacenamiento de datos personales (es decir, CD, DVD, Blu-ray, unidades de memoria flash) a los dispositivos de propiedad estatal.

O. Sistema de Información de Justicia Juvenil (JJIS, por sus siglas en inglés)

El JJIS contiene información de nivel restringido y confidencial. Consulte las políticas del JJIS de seguridad (usuarios), y concesión de acceso al JJIS y a los datos del JJIS para conocer las directrices sobre la autorización y la revocación del acceso al JJIS.

P. Seguridad del sistema de otras agencias

Las funciones del personal de la OYA pueden requerir el acceso a sistemas ajenos a la OYA, como el Sistema de control de información del cliente (Customer Information Control System (CICS, por sus siglas en inglés)), Unidad de servicios de administración financiera estatal (Statewide Financial Management Systems (SFMS, por sus siglas en inglés)), Sistema de datos de las fuerzas del orden público (Law Enforcement Database System (LEDS, por sus siglas en inglés)) y otros. Estos sistemas requieren que los directores de seguridad de la agencia supervisen los controles internos y autoricen las solicitudes de acceso de seguridad a los sistemas. Comuníquese con el director de seguridad correspondiente para obtener acceso a estos sistemas.

Q. Solicitudes de adquisiciones personales

Los sistemas de información estatales no deben ser utilizados para realizar solicitudes de adquisiciones personales. Por ejemplo, los

sistemas no deben utilizarse para realizar cabildeo, solicitar, reclutar, vender o persuadir a favor o en contra de empresas comerciales, productos, causas religiosas o políticas u organizaciones externas.

R. Cumplimiento legal

El uso de los sistemas de información estatales debe respetar los derechos de autor, las licencias, los contratos, los derechos de propiedad intelectual y las leyes relacionadas con los datos, los programas informáticos y otros materiales disponibles a través de dichos sistemas.

S. Violación

La violación de los términos de esta política puede resultar en la limitación, suspensión o revocación del acceso a las herramientas de información estatales, y puede dar lugar a la adopción de otras medidas disciplinarias que puede incluir y llegar hasta el despido del servicio estatal. La violación de partes a sabiendas de esta política, también puede constituir un “delito informático” según los: ORS 164.377.

T. Supervisión, control y cumplimiento

Los organismos estatales son responsables de supervisar el uso de los sistemas y activos de información. La OYA realizará, como mínimo, una supervisión de forma aleatoria y con causa. El sistema de supervisión se utiliza para crear informes de uso, los cuales la dirección de la agencia revisa para comprobar su cumplimiento.

V. PROTOCOLO DE FUNCIONAMIENTO LOCAL REQUERIDO: NO

Preguntas frecuentes

1. ¿Puede un joven utilizar una computadora del personal de la OYA?

No, no se permite que un joven utilice las computadoras del personal de la OYA. Las computadoras del personal de la OYA son para los asuntos oficiales de la OYA. Los jóvenes del centro tienen acceso a otras computadoras destinadas a su uso.[1]

El personal puede permitir que un joven utilice un MCD de propiedad estatal cuando sea necesario para apoyar el plan del caso o los objetivos del joven, y el personal debe supervisar directamente al joven todo el tiempo.

2. ¿Está bien utilizar una foto de mi familia como fondo de pantalla?

Sí. El personal puede utilizar fotos personales como fondos de pantalla. Sin embargo, el personal debe enviar las fotos a su dirección de correo electrónico del trabajo. Esto permite que nuestro sistema de correo electrónico analice el archivo en busca de posibles virus. El personal debe limitar el número de fotos personales guardadas en su computadora.[2]

3. ¿Puedo utilizar mi memoria USB/unidad de memoria flash personal o cualquier otro dispositivo de almacenamiento de información de conexión USB en mi computadora de trabajo?

No. La OYA no puede permitir que el personal conecte ningún dispositivo multimedia extraíble que no sea de la OYA y que pueda almacenar información a una computadora de escritorio o portátil de propiedad estatal. Solo el director de la OYA puede conceder una excepción a esta norma.[2]

4. ¿Puedo utilizar la computadora de mi casa para leer el correo electrónico del trabajo?

No. El personal solo puede acceder al correo electrónico estatal y a otros recursos desde equipos entregados por el Estado.

5. ¿Puedo utilizar gráficos o animaciones en la línea de la firma de mi correo electrónico o de fondo?

No. El correo electrónico enviado desde el sistema estatal es representativo de la OYA y, como tal, debe ser legible y profesional. Se recomienda al personal que incluya una cuadro de firma en su correo electrónico.

6. ¿Puedo escuchar mi emisora de música favorita en mi computadora?

No. La transmisión de video y audio debe ser exclusivamente para uso comercial.[2]

7. ¿Puedo utilizar una computadora portátil del Estado para consultar mi correo electrónico personal cuando esté de viaje?

No. No se permite el acceso a los correos electrónicos que no pertenecen a la OYA.[2]

8. ¿Puedo almacenar archivos de música personales en mi computadora o en una ubicación o recurso de red?

No. Los archivos musicales personales no se deben almacenar en las computadoras de propiedad estatal.[2,3]

9. ¿Puedo escuchar música en mi computadora?

No. El personal no debe conectar dispositivos móviles de almacenamiento de datos personales (es decir, CD, DVD, Blu-ray, unidades de memoria flash) a los dispositivos de propiedad estatal para su uso personal.[4]

10. ¿Qué categorías de Internet están bloqueadas en la red OYA?

- Drogas de abuso
- Contenido para adultos
- Comando y control
- Violación a los derechos de autor
- Sitios de citas
- Sitios de apuestas
- Hackeo
- Programas maliciosos
- Contenido que incluya desnudez
- Redes de pares
- Ciberestafa
- Evasión de proxy y anonimizadores
- Sitios de armas

Las siguientes categorías no están bloqueadas, pero pueden estar marcadas con una advertencia de que estas categorías del sitio solo pueden ser utilizadas para asuntos autorizados de la OYA.

- Subastas
- Criptomoneda
- Juegos en línea
- Grayware
- Dominios recientemente registrados
- Sitios cuestionables
- Sitios de trajes de baño y ropa íntima

Referencias:

1. Política de la OYA 0-7.0, IV.A.1
2. Política de la OYA 0-7.0, III, p.3
3. Política de la OYA I-C-9.0
4. Política de la OYA 0-7.0, IV.N.2