710 - 2015 - MINEDU

DIRECTIVA Nº 003 -2015-MINEDU/SPE-OTIC

DIRECTIVA PARA EL ACCESO Y USO ADECUADO DE LOS RECURSOS INFORMATICOS EN EL MINISTERIO DE EDUCACION

1. FINALIDAD

Normar el acceso y uso adecuado de los recursos informáticos en el Ministerio de Educación, garantizando su disponibilidad e integridad.

2. OBJETIVO

Contar con los lineamientos y controles necesarios que permitan orientar a los usuarios del Ministerio de Educación al buen uso de los recursos informáticos, así como los accesos a los mismos.

3. ALCANCE

Todos los usuarios de los recursos informáticos del Ministerio de Educación independientemente de su régimen laboral y terceros que brinden servicios para la institución.

4. BASE NORMATIVA

4.1. Decreto Ley Nº 25762, Ley Orgánica del Ministerio de Educación.
4.2. Decreto Legislativo Nº 822, Ley sobre el Derecho de Autor.
4.3. Decreto Legislativo Nº 1017, Ley de Contrataciones del Estado.
4.4. Ley Nº 28612, Ley que norma el uso, adquisición y adecuación del software en la administración pública.
4.5. Decreto Supremo N° 024-2006-PCM, que aprueba el Reglamento de la Ley N° 28612.
4.6. Decreto Supremo N° 001-2015-MINEDU, que aprueba el Reglamento de Organización y Funciones del Ministerio de Educación.
4.7. Resolución de Contraloría General de la República Nº 320-2006-CG, que aprueban Normas de Control Interno.
4.8. Resolución Ministerial Nº 073-2004-PCM "Guía para la Administración Eficiente del Software Legal en la Administración Publica".
4.9. Resolución Ministerial Nº 129-2012-PCM, que aprueba el uso obligatorio de la Norma Técnica Peruana "NTP - ISO/IEC 27001:2008 EDI Tecnología de la Información. Técnicas de Seguridad. Sistemas de gestión de seguridad de la Información. Requisitos" en todas las entidades integrantes del Sistema Nacional de Informática.
4.10. Directiva N° 008-95-INEI/SJI "Recomendaciones Técnicas para la protección Física de los Equipos y Medios de Procesamiento de la Información en la Administración Pública", aprobada mediante Resolución de Jefatura N° 090-95-INEI.
4.11. Directiva N° 004-2003-INEI/DTNP "Norma Técnica para la Implementación del Registro de Recursos Informáticos en las Instituciones de la Administración Pública", aprobada por Resolución de Jefatural N° 053-2003-INEI.
4.12. Directiva Nº 005-2003-INEI/DTNP, "Normas para el uso del servicio de correo electrónico en las entidades de la Administración Pública", aprobada mediante la Resolución Jefatural Nº 088-2003-INEI.

MINISTERIO DE EDUCACIÓN - Oficina de Tecnologías de la Información y Comunicación - VISACIÓN

MINISTERIO DE EDUCACIÓN - UNIDAD DE CALIDAD Y SEGURIDAD DE LA INFORMACIÓN - OTIC

5. DISPOSICIONES GENERALES

5.1. GLOSARIO DE TERMINOS

5.1.1. Recursos informáticos: Conforme a la Resolución Jefatural Nº 090-95-INEI, los referidos recursos son los bienes de una organización que se encuentran relacionados directa o indirectamente con la actividad informática; y se denominan también activos informáticos. Entre ellos se encuentran:

a) La información digital o mecanizada (no están incluidos los documentos fuentes que la generan), llámese a toda información almacenada en el hardware o equipamiento físico.

b) Hardware o equipamiento informático, donde se considera las computadoras (monitor, CPU, teclado, mouse, laptops), tablets, impresoras, UPS, servidores, equipos de comunicación (teléfonos IP's, Smartphones, switch), cableado de red, gabinetes, entre otros.

c) Medios de comunicación que se utilizan para la transmisión de datos mecanizados o digitales (redes de computadoras, internet, correo electrónico, etc.).

d) Aplicaciones (Programas software de la Institución, ya sea desarrollados por ésta, adquiridos o alquilados a terceros).

5.1.2. Área Usuaria: Oficina que requiere y/o utiliza los recursos informáticos de la institución para fines laborales

5.1.3. Usuario: Persona que utiliza los recursos informáticos de la institución para fines laborales.

MINISTERIO DE EDUCACIÓN VISACIÓN Oficina de Tecnologías de la Información y Comunicación

5.1.4. Unidad de red: Directorio compartido a través de las redes de computadoras que permite almacenar información, con límites de acceso y capacidad según las necesidades del usuario.

5.1.5. Software legal: Conforme el Decreto Supremo N° 013-2003-PCM, entiéndase al programa de ordenador, sea propietario o libre, adquirido, obtenido y/o utilizado sin contravenir la legislación sobre el derecho de autor.

5.1.6. Líder usuario: Conforme a la Resolución Ministerial 0164-2010-ED es aquella persona encargada de definir los procesos de negocio según su área de influencia, supervisa y aprueba que las características funcionales del proyecto se implementen y estén disponibles a tiempo, define y prepara la información para las pruebas y ejecuta las pruebas funcionales.

MINISTERIO DE EDUCACIÓN UNIDAD DE CALIDAD Y SEGURIDAD DE LA INFORMACIÓN OTIC

5.1.7. OTIC: Oficina de Tecnologías de la Información y Comunicación. Es responsable de conducir el uso de recurso informáticos a su cargo en el sector Educación, y de proponer las políticas, planes, documentos normativos y estándares pertinentes. Depende de la Secretaría de Planificación Estratégica del MINEDU.

5.1.8. Información digital institucional. Es toda información digital generada, modificada, copiada o almacenada por los usuarios bajo los recursos de la institución y para fines institucionales.

5.2. El traslado y transferencia de los recursos informáticos para su uso dentro de la institución serán autorizados por la Oficina de Logística, donde esta coordinará con la OTIC sobre la factibilidad técnica correspondiente.

5.3. El área usuaria deberá remitir a la OTIC todo requisito y/o especificación técnica relacionada a la adquisición de recursos informáticos, para su revisión y validación antes de remitirlo a la Oficina de Logística.

5.4. La instalación, configuración y desinstalación de los recursos informáticos serán realizados por la OTIC.

5.5. Los usuarios de los recursos informáticos de la institución evitarán poner en riesgo de pérdida, robo o deterioro a los equipos, las redes, la información, los programas y los sistemas de la institución.

5.6. Los usuarios utilizarán los recursos informáticos solo con fines institucionales en el cumplimiento de sus objetivos y son responsables de todas las actividades que realicen con estos recursos.

6. DISPOSICIONES ESPECIFICAS

6.1. GESTION PARA EL ACCESO A LOS RECURSOS INFORMATICOS

- Todo personal que requiera acceso a algún recurso informático, puede solicitarlo a la OTIC, a través del "Formato de Solicitud de Servicio de Acceso a la Red", ubicado en el Intranet del Ministerio de Educación, el mismo que deberá ser firmado por la máxima autoridad de la Dirección, Oficina o Unidad, sea por escrito o a través del correo electrónico institucional.

- El usuario conocerá y aceptará las normas de uso de los recursos informáticos, las cuales serán otorgadas por la OTIC, al momento de la creación de su usuario y clave.

6.1.1. CREACION DE CUENTAS DE USUARIOS

- Las cuentas de usuarios son creadas para acceder a las computadoras, a la red y sus servicios de impresoras e internet, al correo electrónico y a las aplicaciones.

- La máxima autoridad de la Dirección, Oficina o Unidad donde labora el personal solicitante, solicitará mediante documento formal la creación de las cuentas de usuarios especificando los recursos informáticos a donde accederá el personal y el nivel de acceso a otorgar, considerando los fines laborales y el uso racional de los recursos informáticos.

MINISTERIO DE EDUCACIÓN - Oficina de Tecnologías de la Información y Comunicación - VISACIÓN

6.1.2. REGISTRO DE USUARIOS

- Todos los accesos a los recursos informáticos serán registrados por la OTIC de manera sistematizada y automática lo cual permite contar con un control de los registros de accesos (logs), ante cualquier auditoria que se requiera.

- La máxima autoridad de la Dirección, Oficina o Unidad deberá solicitar, a través de un documento formal, el cambio de los privilegios o bloqueo del acceso de los usuarios que cambiaron sus tareas, o de aquellos a los que se les revocó la autorización, se desvincularon de la institución o sufrieron la pérdida o sustracción de sus credenciales de acceso.

MINISTERIO DE EDUCACIÓN - UNIDAD DE CALIDAD Y SEGURIDAD DE LA INFORMACIÓN - OTIC

6.1.3. GESTION DE CLAVES

La OTIC controlará la asignación de claves a través de un procedimiento formal, mediante el cual debe respetarse mínimamente lo siguiente:

- Garantizar que los usuarios cambien las claves iniciales que les han sido asignadas, la primera vez que ingresan al sistema.

- Evitar la participación de terceros o el uso de mensajes de correo electrónico sin protección, en el mecanismo de entrega de la clave.

- Modificar todas las claves predeterminadas por el proveedor, una vez instalado el software y/o hardware (por ejemplo claves de impresoras, routers, etc).

- Configurar los sistemas de autenticación de tal manera que:
  - Se permitan claves que contengan mínimo ocho (08) caracteres y estos sean alfanuméricos.
  - Después de seis (06) intentos de acceso con una clave incorrecta, se debe bloquear el acceso al sistema.
  - Programar para que automáticamente cada cuarenta y cinco (45) días se solicite cambio de la clave.
  - No permitir que, por lo menos, las últimas 3 claves sean reutilizadas.

6.1.4. USO DE CLAVES

Los usuarios seguirán las siguientes buenas prácticas de seguridad en la selección y uso de claves:

- Mantener las claves en secreto.
- Pedir el cambio de la clave siempre que exista un posible indicio de peligro del aplicativo o de las claves.
- Seleccionar claves que: a) Sean fáciles de recordar, b) No estén basadas en algún dato relacionado con la persona, por ejemplo nombres de los hijos, mascotas, números de teléfono, fecha de nacimiento, etc.

6.2. USO DE LOS RECURSOS INFORMATICOS

6.2.1. INFORMACION DIGITAL INSTITUCIONAL

- La información digital que se crea en las computadoras o equipos conectados a la red, debe almacenarse en la unidad de red asignada a cada usuario u oficina para que sea respaldada por la OTIC.

- La OTIC a través de un software legal, administrará el uso de los dispositivos informáticos móviles conectados a las computadoras. Este software permitirá auditar las acciones realizadas sobre estos dispositivos, con el objetivo de minimizar la fuga de la información institucional.

- Si por fines laborales se utilizan dispositivos informáticos móviles como laptops, notebooks, tablets, dispositivos de almacenamiento en USB, CDs, DVDs, entre otros, el usuario evitará almacenar, en forma permanente, la información institucional relevante.

6.2.2. HARDWARE O EQUIPAMIENTO INFORMATICO

- Las computadoras y equipos periféricos designados son de uso exclusivo para el desarrollo de las funciones y responsabilidades establecidas por y para la Institución.

- Todo requerimiento de instalación de hardware o equipamiento informático es solicitado por el Jefe o Director, a la Oficina de Tecnologías de la Información y Comunicación, a través de un documento formal.

- Ninguna oficina mantendrá guardados hardware o equipamiento informático en desuso.

6.2.3. MEDIOS DE COMUNICACIÓN

a) **REDES DE COMPUTADORAS**

Las redes de computadoras son herramientas que permiten la comunicación e intercambio de información, por tanto son de uso exclusivo para las actividades relacionadas con la institución.

Todo usuario poseedor de una cuenta de red es responsable del uso de las redes de computadoras de la institución, no utilizando herramientas y/o software que perjudiquen o pongan en riesgo el buen funcionamiento de las redes.

b) **CORREO ELECTRONICO**

El correo electrónico institucional es una herramienta de comunicación e intercambio de información oficial entre usuarios, de uso exclusivo para las actividades que estén relacionadas con la institución, no constituye un medio de difusión indiscriminada de información.

Todo usuario poseedor de una cuenta de correo electrónico institucional se encuentra obligado a revisarlo de manera diaria, por lo menos una vez al inicio de la jornada laboral y otra antes de retirarse.

Si por necesidades laborales de la Dirección, Oficina o Unidad se requiere crear cuentas genéricas y/o dedicadas de correo electrónico (por ejemplo: logistica@minedu.gob.pe) esta deberá ser solicitada formalmente por la oficina, designando en el documento de solicitud al personal que asumirá la responsabilidad de uso de la cuenta; así como también de la desactivación de la misma.

La OTIC en caso verifique la no utilización del correo electrónico por más de noventa (90) días, desactivará la cuenta de correo, lo cual será informado al Director o Jefe de la Oficina donde labora el usuario.

El usuario eliminará los mensajes innecesarios, o aquellos que ya fueron leídos en su oportunidad, considerando que la capacidad de almacenamiento de correos es hasta 3 Gb. Excedido dicho tamaño no podrá enviar o recibir correos electrónicos.

El usuario no abrirá correos electrónicos sospechosos y/o con archivos adjuntos no solicitados, teniendo mayor precaución de los correos electrónicos proveniente en idiomas extranjeros.

Los mensajes de correo electrónico institucionales, enviados internamente no deben exceder de 10 Mb, incluyendo el (los) archivo (s) adjuntos que lo acompañen. Los mensajes de correo electrónico enviados o recibidos de correos externos, no deben de exceder de 10 Mb, incluyendo el (los) archivo(s) adjuntos que lo acompañen. Si

por las funciones que realizan algunos usuarios requieran la ampliación de tamaño de los correos, deberá ser solicitado mediante documento formal del Director o Jefe de la Oficina donde labora el usuario, sustentando la necesidad.

Todos los mensajes que se encuentren en la papelera de reciclaje, se eliminan automáticamente cada quince (15) días. Si se desea mantener un mensaje en forma permanente, éste debe almacenarse en el disco duro de su computadora.

La OTIC cuenta con un sistema automático que permite filtrar los correos SPAM en salvaguarda de la seguridad de la información institucional.

c) **SERVICIO DE INTERNET**

Es una herramienta de apoyo e investigación para facilitar las labores de los usuarios que lo requieran, para el cumplimiento de sus funciones. Para ello la OTIC contará con herramientas de filtrado garantizando el uso racional del servicio.

Todo usuario con acceso al servicio de Internet que provee la institución, es responsable de todas las operaciones y/o actividades que realizan con este servicio.

La página inicial del navegador Web será el portal del MINEDU www.minedu.gob.pe y no debe ser cambiada ya que ello muestra el compromiso con la imagen institucional.

d) **TELEFONIA VOZ IP**

El servicio de telefonía por Voz IP del Ministerio de Educación es para fines netamente institucionales, el cual es administrado por la Oficina de Tecnologías de la Información y Comunicación.

El usuario accederá al servicio de telefonía a través de una clave, la cual debe ser solicitada mediante documento formal autorizado por la máxima autoridad de la Dirección, Oficina o Unidad donde labora el solicitante, indicando el tipo de servicio que se requiere como llamadas locales, llamadas nacionales e internacionales y o celulares.

La Oficina de Tecnologías de la Información y Comunicación registrará todas las llamadas realizadas a teléfonos fijos y celulares externos e informará mensualmente a los directores o jefes de oficinas, el reporte de uso del servicio.

MINISTERIO DE EDUCACION
VISACIÓN
Oficina de Tecnologías de la Información y Comunicación

e) **TELEFONIA MOVIL**

El servicio de telefonía móvil es brindado para fines institucionales, siendo la OTIC la encargada de entregar los dispositivos móviles configurados para su uso mediante Acta de entrega y de acuerdo a los perfiles y lista de oficina definida por la Oficina General de Administración:

- Perfil A Alta dirección
- Perfil B para asesores, directores generales, director y jefes.
- Perfil C para trabajadores

MINISTERIO DE EDUCACION
UNIDAD DE CALIDAD Y SEGURIDAD DE LA INFORMACIÓN
OTIC

En caso de pérdida, hurto o robo del dispositivo móvil, el usuario tendrá que hacer la denuncia policial y comunicarlo a la OTIC para el bloqueo del número, el pago correspondiente a la penalidad a cargo del usuario y la reposición del equipo.

6.2.4. APLICACIONES

- Toda aplicación desarrollada o administrada por la OTIC, cuenta con un Líder Usuario, quien realiza los requerimientos del mismo, aprueba la implementación y despliegue del aplicativo, siendo el encargado de solicitar y autorizar posibles cambios que surjan en producción. Asimismo, es quien define los perfiles de los usuarios que podrán acceder a los aplicativos.

- Para acceder a una aplicación, el usuario se comunicará con la Oficina de Tecnologías de la Información y Comunicación, para que según la aplicación, se realice un procedimiento formal de acceso, siendo este autorizado por el Director o Jefe de la Oficina donde labora el usuario solicitante; salvo para aquellas aplicaciones donde la administración de usuarios se encuentre descentralizada.

- El usuario accederá a la aplicación mediante una cuenta de usuario y una clave, la cual debe ser mantenida en total confidencialidad, siendo el usuario responsable del uso que haga con la misma.

- El usuario es responsable de la información que ingresa a la aplicación que accede, por tanto registrará datos válidos y verdaderos, de manera exacta y precisa, teniendo en cuenta que dicha información es para uso institucional.

6.2.5. SOFTWARE

- Toda computadora cuenta con la siguiente lista de software legal base, definida por la OTIC, dando uso adecuado a la administración de los recursos informáticos:

    - Un Sistema Operativo
    - Procesador de Texto
    - Hoja de cálculo
    - Presentación de diapositivas
    - Reproductor Multimedia
    - Comprimidor de archivos
    - Lector de PDF
    - Navegador de Internet
    - Correo electrónico
    - Antivirus

MINISTERIO DE EDUCACIÓN – Oficina de Tecnologías de la Información y Comunicación – VISACIÓN

- Si por necesidades laborales el usuario requiere la instalación de un software legal que no se encuentre en la anterior lista, este debe ser solicitado a la Oficina de Tecnologías de la Información y Comunicación, quien verificará si la Institución cuenta con dicho software y las licencias respectivas.

- Todos los usuarios están en la obligación de informar la existencia de algún software que no está autorizado por la Oficina de Tecnologías de la Información y Comunicación, contribuyendo así al cumplimiento de las normas que protegen los Derechos de Autor sobre softwares y aplicaciones.

MINISTERIO DE EDUCACIÓN – UNIDAD DE CALIDAD Y SEGURIDAD DE LA INFORMACIÓN – OTIC

- La OTIC, es la única autorizada para instalar software legal en las computadoras de los usuarios. Asimismo, es la responsable de administrar el software y las licencias adquiridas.

- La OTIC, está facultada para eliminar el software instalado en las computadoras de la institución que no sea legal, sin mediar aviso previo ni responsabilidad aducida por pérdida de información contenida de ningún tipo.

6.3. ACCESO A LOS RECURSOS INFORMATICOS

El acceso a los recursos informáticos es brindado a todo personal del MINEDU bajo autorización de su jefe directo.

En el caso de terceros (locadores de servicios) tendrán acceso contemplando las limitaciones y permisos que las áreas contratantes les permitan, en razón a la naturaleza de las funciones para las cuales han sido contratados, lo cual deberá estar taxativamente previsto en los términos de referencia para solicitar su contratación. Para ello cada área usuaria es responsable de incluir en los términos de referencia lo siguientes controles de seguridad:

- Determinar los bienes y accesos a los recursos informáticos según la naturaleza de su contrato.
- Definición de acciones ante la ocurrencia de algún incidente de seguridad que comprometa los bienes de la Institución.
- Determinar las obligaciones de las partes y responsabilidades legales.

Asimismo, el Área Usuaria luego de haber recibido la notificación de entrega de la Orden de Servicio al tercero, debe hacer firmar el acuerdo de confidencialidad (Anexo) dentro de las 72 horas y remitirlo a la Oficina de Tecnologías de la Información y Comunicaciones para las atenciones correspondientes a la creación de cuentas de usuarios y accesos a los recursos informáticos.

6.3.1. ACCESO A LA INFORMACIÓN DIGITAL

- De la información digital generada por las aplicaciones

Todo acceso a la información digital administrada por las aplicaciones será realizado a través de la propia aplicación que le corresponde. El acceso será a través de una cuenta de usuario y clave personal.

- <u>De la información digital del usuario o área</u>

La información digital de un usuario o área se encuentra definida en una unidad de red, creada a solicitud formal del usuario, quien define el tipo de acceso de otros usuarios a tal unidad si lo requiere.

Los usuarios pueden almacenar información digital de uso laboral en las computadoras, teniendo en cuenta que, si la información es relevante para la institución se debe almacenar en la unidad de red designada.

El acceso a la información digital en la computadora es a través de un usuario y clave.

La Oficina de Tecnologías de la Información y Comunicación, a través de herramientas tecnológicas, forzará a que, las computadoras en un tiempo de inactividad no menor a 10 minutos, se bloquee automáticamente para evitar el acceso no autorizado por otros usuarios.

- <u>De la información digital del correo electrónico</u>

Todo acceso a la información generada o adjunta dentro del servicio de correo electrónico institucional será realizado a través de una cuenta de usuario y clave personal perteneciente al propietario de dicha cuenta.

Por razones de investigación y a través de una disposición judicial, la Oficina de Tecnologías de la Información y Comunicación, podrá auditar la información digital del correo electrónico institucional del usuario investigado.

6.3.2. ACCESO AL HARDWARE O EQUIPAMIENTO INFORMATICO

- A las computadoras

  El usuario, según sus necesidades, tiene designado solo una computadora para su uso laboral.

  La Oficina de Tecnologías de la Información y Comunicación es la única autorizada para acceder y manipular el hardware de las computadoras por motivos de reparación y mantenimiento de las mismas, bajo conocimiento del usuario.

  La Oficina de Tecnologías de la Información y Comunicación, cuenta con políticas que limitan el acceso a las configuraciones de hardware y software del equipo, para minimizar el mal uso del mismo.

- A las impresoras

  El personal de la Oficina de Tecnologías de la Información y Comunicación es el único autorizado para acceder a la configuración lógica de la impresora.

  La Oficina de Tecnologías de la Información y Comunicación garantiza el acceso a las impresoras a nivel de impresión y otras funcionalidades.

- A otro equipamiento informático

  Los equipos informáticos como equipos servidores, switches, routers, antenas, y cualquier otro equipo que no es de uso diario del personal, es de acceso exclusivo para el personal de la Oficina de Tecnologías de la Información y Comunicación.

6.3.3. ACCESO A LOS MEDIOS DE COMUNICACIÓN

- Acceso a la Red

  Todo acceso a la red es brindado a través de una cuenta de usuario y clave.

  El acceso a la red permite acceder a los servicios de Internet, impresoras y equipos de comunicación de voz y datos si correspondiera.

  El acceso a la red desde locales remotos dependientes de la institución o por necesidades de cumplimiento de convenios con otras instituciones, será configurado por la Oficina de Tecnologías de la Información y Comunicación considerando el uso de sistemas de seguridad que permitan garantizar el uso adecuado de la red.

  La OTIC, a través de herramientas tecnológicas registrará y monitoreará los accesos a la red y así podrá prevenir posibles eventos que perjudiquen la performance de la red.

- Acceso al Correo Electrónico

  Todo acceso al servicio de correo electrónico institucional es habilitado a través de una cuenta de usuario y clave. Ver punto 6.2.3

6.3.4. ACCESO A LAS APLICACIONES

El acceso a las aplicaciones se basa en una cuenta de usuario y clave la cual debe ser solicitada a la OTIC bajo la autorización de la máxima autoridad de la Dirección, Oficina o Unidad donde labora el solicitante.

El líder usuario de una aplicación es el responsable de definir los tipos de permisos de acceso de un usuario.

El usuario con todos los privilegios de uso de una aplicación es el definido como administrador.

Las aplicaciones, sobre todo los que administran información sensible, contará con sistemas de bloqueo automático frente a la inactividad mayor a 10 minutos o según la necesidad requerida.

7. PROHIBICIONES EN EL USO DE LOS RECURSOS INFORMATICOS

Los usuarios cualquiera sea su régimen laboral y/o vínculo contractual con el MINEDU deberán tener en cuenta las siguientes prohibiciones:

7.1. Respecto a la Información digital:

7.1.1. Almacenar música, videos, audio, ejecutables y otra información que no sean de carácter institucional en las unidades de red asignados a cada usuario u oficina, según corresponda.

7.1.2. Utilizar dispositivos informáticos móviles para copiar y almacenar información institucional, sin conocimiento y/o autorización de la máxima autoridad de la oficina donde labora.

7.1.3. Cualquier acceso o intento de acceso a la información digital en mención de una aplicación, sea cual sea su repositorio o archivo, que no sea a través de una cuenta y clave.

7.2. Con relación al Hardware o equipamiento informático:

7.2.1. Ingerir y dejar alimentos y/o bebidas cerca y/o encima de los equipos informáticos.

7.2.2. Colocar papeles u otros objetos cerca de las ranuras de ventilación de las computadoras.

7.2.3. Colocar los equipos en el piso, lugares inestables y/o expuestos a ser golpeados involuntariamente o frente a la luz solar o expuestos a polvo.

7.2.4. Mover los equipos y/o periféricos de un lugar a otro, sin autorización correspondiente.

7.2.5. Desarmar los equipos, cuando no corresponde a su función.

7.2.6. Conectar ventiladores, lustradoras, cafeteras, hervidores u otros equipos eléctricos en los mismos enchufes o líneas de los equipos informáticos.

7.3. Respecto a las Redes de datos:

7.3.1. Acceder a la red con computadoras o equipos portátiles que no pertenecen a la institución, sin autorización de la Oficina de Tecnologías de la Información y Comunicación o quien haga sus veces.

7.3.2. Instalar o utilizar herramientas en la red para evitar los controles de seguridad implementados.

7.4. Sobre el Correo electrónico:

7.4.1. Utilizar el correo electrónico institucional para cualquier propósito comercial, financiero o ajeno a la institución y a los fines del Sector.

7.4.2. Enviar correos hacia destinatarios internos o externos en forma masiva, no siendo ello parte de sus funciones.

7.4.3. Distribuir mensajes, signos, figuras, dibujos, fotografías, videos y demás; con contenidos impropios y/o lesivos a la moral o relacionados a la delincuencia o terrorismo.

7.4.4. Enviar de forma masiva publicidad o cualquier otro tipo de correo no solicitado, conocidos como "spam".

7.4.5. Facilitar u ofrecer la cuenta y/o buzón del correo electrónico institucional a terceras personas.

7.4.6. Utilizar la cuenta del correo electrónico institucional para registrarse en empresas u organizaciones con fines personales (foros de estudio, medios de publicación, comercio, etc.)

7.5. Con relación al servicio de Internet:

7.5.1. Acceder a páginas que contengan signos, figuras, dibujos, fotografías, videos u otros con contenidos impropios y/o lesivos a la moral o relacionados a la delincuencia o terrorismo.

7.5.2. Acceder a páginas que vayan en perjuicio o pongan en riesgo la seguridad de las redes y sistemas de la institución.

7.5.3. Transferir información institucional que contravengan las normas legales.

7.5.4. Realizar descargas de software que perjudiquen los recursos informáticos.

7.5.5. Utilizar herramientas y/o software que evadan los controles del servicio de internet.

7.6. Respecto al Software:

7.6.1. Instalar cualquier tipo de software ya sean los de programa de libre uso u otros descargados de internet, o aquellos que son adquiridos de manera personal, aún si contarán con licencia propia.

7.6.2. Desinstalar los software base de la computadora.

7.6.3. La comercialización del software adquirido, instalado o asignado en las computadoras de la institución.

8. RESPONSABILIDADES

8.1. La Oficina General de Recursos Humanos es responsable de:

8.1.1. Comunicar mensualmente a la OTIC, la lista del personal cuyo vínculo laboral y/o contractual ha quedado extinguido, a fin de proceder a la desactivación de las cuentas de acceso a los recursos informáticos.

8.2. La OTIC es responsable de:

8.2.1. Proveer de los recursos informáticos y utilizar herramientas o programas de bloqueo y/o filtro que aseguren tales recursos ante posibles riesgos de la información.

8.2.2. Poner en conocimiento todo mal uso de los recursos informáticos a la Oficina General de Recursos Humanos, con copia al Director o Jefe de la Dirección y/o Oficina donde labora el usuario que realizó tal acción, a fin de que adopten las medidas que correspondan, según las normas institucionales vigentes.

8.2.3. Administrar el acceso a los recursos informáticos de la institución y garantizar la protección de los Derechos de Autor sobre los aplicativos, software y sistemas de información utilizados por la Institución. Asimismo, mantendrá los registros de todos los recursos informáticos en coordinación con la Oficina de Logística.

8.2.4. Efectuar revisiones periódicas con el objeto de cancelar cuentas de usuario repetidas y de bloquear cuentas de usuarios que no hacen uso de las mismas por más de noventa (90) días.

8.3. Los usuarios de los recursos informáticos son responsables de:

8.3.1. Todas las operaciones que realizan con su cuenta de usuario.

8.3.2. Reportar cualquier incidente, daño o perjuicio voluntario o involuntario, sobre los recursos informáticos a la OTIC, para su pronta atención y resolución.

8.3.3. Conservar en secreto, toda clave de acceso de la que es propietario, no pudiendo compartirla ni transferirla a otros usuarios.

8.4. El Responsable de Seguridad de la Información de la Oficina de Tecnologías de la Información y Comunicación del Ministerio de Educación realizará auditorías de forma periódica, que permitan evaluar el cumplimiento de la presente normativa.

ANEXO

ACUERDO DE CONFIDENCIALIDAD

Yo, , identificado con DNI N° ,
como persona natural (de aquí en adelante conocido como La "Persona") conoce y acepta que la confidencialidad de la información, datos, registros, productos, estudios, equipos, estándares, procesos, procedimientos, políticas, guías, documentos, topología de red, números telefónicos, direcciones Internet Protocol ("IP"), asignaciones de puertos, licencias de software, configuraciones, comunicaciones electrónicas, prácticas de comercio y passwords (claves o credenciales) de la ***institución*** (de aquí en adelante conocido como la "Entidad") y su oficio (de aquí en adelante conocido como "Información"), podrán ser de conocimiento de la Persona para el desarrollo de la ejecución de los servicios de levantamiento de información para la Entidad y que dicha Información, junto con cualquier Información preliminar o divulgación, son otorgadas en estricto secreto y confidencia y serán usados para el único propósito de desarrollar negocios, proyectos y/o servicios de la Entidad y dentro de sus instalaciones.

Dicha Información abarca e incluye a los actuales clientes y/o prospectos de clientes y/o Entidades y/o instituciones y/o personas naturales con las cuales la Entidad inicia y mantiene cualquier tipo de relación.

Este instrumento expresa el compromiso por parte de la Persona respecto a que la Información es un activo valioso de la Entidad y que el acceso y conocimiento de la misma son esenciales para el logro de los propósitos de la Entidad y que una divulgación sin control de dicha Información podría ser dañina para los fines y metas de la Entidad. La Persona conoce y acepta que no divulgará o usará bajo ninguna circunstancia, parte o toda, la Información a ningún personal, corporación u otra entidad y que será responsable por los daños que se originen frente a tal incumplimiento. Asimismo, declara conocer y cumplir con la Política General de Seguridad de la Información y la Directiva de Uso de los Recursos Informáticos del Ministerio de Educación.

La Persona no está afiliado o representa a ninguna entidad gubernamental, administrativa o entidad de investigación, pública o privada, y que la información provista u obtenida por la Entidad, no deberá ser usada para ningún fin que no sea relacionada para los fines que fueron entregados, creados, diseñados u obtenidos.

MINISTERIO DE EDUCACIÓN – Oficina de Tecnologías de la Información y Comunicación – VISACIÓN

En consideración a la no divulgación de la información, a la cual La Persona se adhiere y reconoce; La Persona se compromete a que este acuerdo se mantendrá en estricta ejecución mientras preste servicios a la Entidad y al finalizarlo, por un período de cinco (05) años para adelante y que este compromiso será interpretado y respaldado por las leyes y regulaciones del Estado Peruano.

Este compromiso contiene la manifestación de voluntad de La Persona con respecto la materia del mismo y no da garantías ni hacen representaciones, promesas o acuerdos respecto a otras materias que no sean las señaladas explícitamente en este compromiso.

MINISTERIO DE EDUCACIÓN – UNIDAD DE CALIDAD Y SEGURIDAD DE LA INFORMACIÓN – OTIC

LAS CONDICIONES DESCRITAS ARRIBA SON APROBADAS Y ACEPTADAS: LA MANIFESTACION DE LA VOLUNTAD EXPRESADA MEDIANTE LA FIRMA QUE VIENE A CONTINUACIÓN CONFIRMA QUE ESTE DOCUMENTO HA SIDO LEIDO Y ENTENDIDO EN FORMA COMPLETA.

Huella Digital

_____

FIRMA Y DNI DE LA PERSONA

Fecha: _____