Resolución de Secretaría General

N°710 - 2015 - MINEDU

Lima, 02 SEP 2015

Vistos; el Expediente Nº 0176995-2014; los Informes Nºs 0043-2015-MINEDU/SPE-OTIC-UCSI, 0044-2015-MINEDU/SPE-OTIC-UCSI, 051-2015-MINEDU/SPE-OPEP-UNOME y 591-2015-MINEDU/SG-OGAJ;

CONSIDERANDO:

Que, la Primera Disposición Complementaria del Decreto Ley Nº 25762, Ley Orgánica del Ministerio de Educación, señala que el Ministerio de Educación se encuentra facultado para dictar, en el ámbito de su competencia, las disposiciones complementarias necesarias para perfeccionar su estructura y mejorar su funcionamiento;

Que, la Directiva Nº 138-2004-SPE/OFIN denominada "Normas para el Uso de Computadoras Personales (PC's), Periféricos y Servicios Informáticos en Red en el Ministerio de Educación", tiene como finalidad proporcionar al usuario del Ministerio de Educación los procedimientos y conceptos básicos del uso y cuidado de los equipos de cómputo y periféricos en general, así como optimizar el uso de los recursos informáticos;

Que, a través de la Resolución Ministerial Nº 0076-2006-ED se aprobó la Directiva Nº 017-2006-ME/SPE/OFIN denominada "Normas para el Uso de Computadoras Personales (PC's), Periféricos, Software Institucional y Servicios Informáticos en Red del Ministerio de Educación", cuyo objetivo es normar el uso y cuidado de las computadoras personales y periféricos, así como de los servicios informáticos en Red en las dependencias del Ministerio de Educación;

Que, mediante Resolución Ministerial Nº 0067-2009-ED se aprobó la "Política General de Seguridad de la Información", cuyo artículo 4 establece que el Ministerio de Educación contará, entre otros, con un Comité Operativo de Seguridad de Información (COSI) y un Comité Ejecutivo de Seguridad;

Que, conforme a lo dispuesto por el literal a) del artículo 45 del Reglamento de Organización y Funciones del Ministerio de Educación, aprobado por Decreto Supremo Nº 001-2015-MINEDU, la Oficina de Tecnologías de la Información y Comunicación (OTIC), dependiente de la Secretaría de Planificación Estratégica, tiene entre sus funciones, la de proponer, desarrollar e implementar los documentos normativos y estándares relacionados con el desarrollo de los sistemas de información, adquisición y administración de equipamiento de cómputo, redes y comunicaciones, y el uso de los recursos informáticos del sector Educación, en el marco de la normativa vigente;

Que, el Presidente del COSI y Jefe de la OTIC, mediante Memorándum Nº 1325-2015-MINEDU/SPE-OTIC remite los Informes Técnicos Nºs 0043-2015-MINEDU/SPE-OTIC-UCSI y 0044-2015-MINEDU/SPE-OTIC-UCSI, a través de los cuales sustenta y solicita la aprobación de la Directiva para el Acceso y Uso Adecuado de los Recursos Informáticos en el Ministerio de Educación y de la Directiva para la Administración de los Recursos Informáticos del Ministerio de Educación, las mismas que han sido revisadas por el COSI y aprobadas por el Comité

Ejecutivo de Seguridad, a través del Acta de Reunión Nº 001-2015-CESI; asimismo solicita dejar sin efecto la Directiva Nº 138-2004-SPE/OFIN y la Directiva Nº 017-2006-ME/SPE/OFIN;

Que, la Jefa de la Unidad de Organización y Métodos de la Oficina de Planificación Estratégica y Presupuesto, a través del Informe Nº 051-2015-MINEDU/SPE-OPEP-UNOME, opina que la Directiva para el Acceso y Uso Adecuado de los Recursos Informáticos en el Ministerio de Educación y la Directiva para la Administración de los Recursos Informáticos del Ministerio de Educación, cumplen con las formalidades establecidas en las "Normas para la Formulación y Aprobación de Directivas en el Ministerio de Educación", aprobadas mediante Resolución Ministerial Nº 0036-2012-ED;

De conformidad con lo dispuesto en el Decreto Ley Nº 25762, Ley Orgánica del Ministerio de Educación, modificada por la Ley Nº 26510; el Reglamento de Organización y Funciones del Ministerio de Educación, aprobado por Decreto Supremo N° 001-2015-MINEDU; la Directiva Nº 023-2013-MINEDU/SG-OAJ denominada "Elaboración, Aprobación y Tramitación de Dispositivos Normativos y Actos Resolutivos del Ministerio de Educación", aprobada por Resolución Ministerial N° 0520-2013-ED; las "Normas para la Formulación y Aprobación de Directivas en el Ministerio de Educación", aprobadas por Resolución Ministerial Nº 0036-2012-ED; y, la Resolución Ministerial Nº 021-2015-MINEDU, modificada por la Resolución Ministerial Nº 178-2015-MINEDU, por la que se delegan facultades a diversos funcionarios del Ministerio de Educación, durante el Año Fiscal 2015;

SE RESUELVE:

Artículo 1.- Aprobar la Directiva Nº 003 -2015-MINEDU/SPE-OTIC denominada "Directiva para el Acceso y Uso Adecuado de los Recursos Informáticos en el Ministerio de Educación", la misma que como Anexo I forma parte integrante de la presente Resolución Ministerial.

Artículo 2.- Aprobar la Directiva Nº 004 -2015-MINEDU/SPE-OTIC denominada "Directiva para la Administración de los Recursos Informáticos del Ministerio de Educación", la misma que como Anexo II forma parte integrante de la presente Resolución Ministerial.

Artículo 3.- Dejar sin efecto las Directivas Nºs 138-2004-SPE/OFIN y 017-2006-ME/SPE/OFIN.

Artículo 4.- Disponer la publicación de la presente Resolución y sus Anexos, en el Sistema de Información Jurídica de Educación – SIJE, ubicado en el Portal Institucional del Ministerio de Educación (www.minedu.gob.pe), el mismo día de la publicación de la presente Resolución en el Diario Oficial "El Peruano".

Regístrese, comuníquese y publíquese.

DESILU LEON CHEMPEN
Secretaria General
Ministerio de Educación

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 EDUCACION - Oficina de Tecnologías de la Información y Comunicación - VISACIÓN

MINISTERIO DE EDUCACION - 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.

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.

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.

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

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.

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

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.

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

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.

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

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

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 Tecnología 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.

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

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

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.

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.

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.

_____

FIRMA Y DNI DE LA PERSONA

Fecha: _____

Huella Digital

710-2015-MINEDU

DIRECTIVA Nº 004 -2015-MINEDU/SPE-OTIC

DIRECTIVA PARA LA ADMINISTRACION DE LOS RECURSOS INFORMATICOS DEL MINISTERIO DE EDUCACION

1. FINALIDAD

Establecer los lineamientos técnicos y operacionales que orienten la administración de los recursos informáticos del Ministerio de Educación (MINEDU) por parte de la Oficina de Tecnologías de la Información y Comunicación (OTIC).

2. OBJETIVO

Garantizar la correcta administración de los recursos informáticos del Ministerio de Educación por parte de la Oficina de Tecnologías de la Información y Comunicación, garantizando su uso y disponibilidad.

3. ALCANCE

Todo el personal de la Oficina de Tecnologías de la Información y Comunicación y aquellos que hagan sus veces dentro de las dependencias del Ministerio de Educación.

4. BASE NORMATIVA

4.1. Decreto Supremo N° 001-2015-MINEDU, que aprueba el Reglamento de Organización y Funciones de-l Ministerio de Educación.

4.2. 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.

4.3. Resolución Jefatural Nº 140-95-INEI que aprueba la Directiva Nº 010-95-INEI/SJI denominada "Recomendaciones Técnicas para la Organización y Gestión de los Servicios Informáticos para la Administración Pública".

5. DISPOSICIONES GENERALES

5.1. DE LA OFICINA DE TECNOLOGIAS DE LA INFORMACION Y COMUNICACION

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

- La OTIC o quien haga sus veces, remite las características técnicas para la elaboración de los términos de referencia o especificaciones técnicas necesarias para la adquisición de equipos informáticos.

- El traslado o transferencia de los recursos informáticos es realizado por la OTIC o quien haga sus veces con la Oficina de Logística.

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

- La protección de los Derechos de Autor sobre los aplicativos, software y sistemas de información utilizados por la Institución es brindado por la OTIC o quien haga sus veces.

- La OTIC emite los informes técnicos de evaluación de cumplimiento para estudio de mercado y valorización; obsolescencia tecnológica; mantenimiento oneroso; informe previo de software y de estandarización sobre un recurso informático, en el marco de la asistencia técnica a los usuarios de los servicios informáticos del Ministerio.

6. DISPOSICIONES ESPECIFICAS

6.1. RESPECTO A LA INFORMACION ALMACENADA EN LOS SERVIDORES

La Unidad de Infraestructura Tecnológica (UIT) gestiona el respaldo de la información digital almacenada en los equipos servidores del Centro de Datos. La referida Unidad elaborará e implementará un Plan de Respaldo de los sistemas de información (incluido logs de los sistemas) y la información generada por los servicios propios de UIT, como el correo electrónico, internet, directorio activo, servidores de archivo, entre otros. Asimismo, deberá contemplar la información técnica de configuraciones de los sistemas de seguridad perimetral, enlaces, rutas de los equipos de comunicación y otras necesarias para el adecuado funcionamiento de los servicios que brinda el MINEDU.

El Plan de respaldo contemplará como mínimo los siguientes datos:

- Descripción de la información a respaldar
- Servidor repositorio
- Sistema de información o servicio general que soporta
- Ruta digital de la información
- Periodicidad de la acción del respaldo
- Cronograma del respaldo
- Aplicación con que se respalda o definir si se utiliza script o comandos
- Procedimiento de administración de cintas de respaldo

Esta información será controlada por la OTIC, en el marco de garantizar la seguridad, integridad, disponibilidad y calidad de la información del Ministerio de Educación.

6.2. INFORMACION ALMACENADA EN LAS COMPUTADORAS DEL PERSONAL DE LA OTIC

Todo personal de la OTIC es responsable de la información digital que crea, modifica y almacena en sus computadoras.

LIBRERIAS DE FUENTES DE INFORMACION

Las librerías de fuentes contienen los códigos de los programas fuente, base de datos, manuales y todos los elementos que soportan a los sistemas de información. Estás serán almacenadas en un repositorio digital donde solo tendrá acceso el usuario responsable encargado.

La OTIC encargará en su personal el control de las librerías fuentes quien velará por el respaldo, el registro formal y actualizado de las mismas según el Anexo 01 de la presente Directiva.

El Jefe de la Unidad de Sistemas de Información es el único autorizado para solicitar el acceso a las Librerías de las Fuentes de Información, quien enviará un correo electrónico al responsable encargado, solicitando el acceso a las fuentes necesarias, especificando la justificación de la solicitud y definiendo a la persona que recibirá dichas fuentes bajo el formato de entrega de información según Anexo 02.

Ningún programa en desarrollo o mantenimiento será almacenado en las librerías de las fuentes mientras no sea certificado, ni aprobado su funcionalidad y operatividad, por el Jefe de la Unidad de Sistemas de Información.

6.3. HARDWARE O EQUIPAMIENTO INFORMATICO

La OTIC, a través de la Unidad de Servicios de Atención al Usuario elabora los términos de referencia o especificaciones técnicas de los equipos de las áreas usuarias. Asimismo, establece el plan de renovación del parque informático.

La OTIC en coordinación con la Oficina de Logística del MINEDU, mantendrá un registro de inventario de todos los equipos informáticos a su cargo.

La OTIC a través de la Unidad de Infraestructura Tecnológica elabora los términos de referencia o especificaciones técnicas de los equipos informáticos relacionados al Centro de Datos, tanto a nivel de servidores como equipos de almacenamiento (SAN – NAS), equipos para respaldo, equipo de comunicaciones, equipos para la seguridad perimetral, cableado y otros que la UIT establezca para un mejor funcionamiento del centro de datos. Del mismo modo, establece el Plan Anual de Mantenimiento Preventivo y/o Correctivo del Equipamiento Informático a nivel de centro de datos.

La OTIC, a través de la Unidad de Servicios de Atención a Usuarios, cuenta con un plan anual de mantenimiento preventivo y/o correctivo del equipamiento informático a nivel de usuarios.

La OTIC emite informes técnicos de obsolescencia tecnológica o de mantenimiento oneroso sobre los equipos informáticos que administra.

6.3.1. CENTRO DE DATOS

a) FACTORES AMBIENTALES.-

El Centro de datos contará con las condiciones ambientales (Temperatura/ Humedad) para el adecuado funcionamiento de los equipos informáticos, tomando en cuenta las especificaciones técnicas de los equipos. Deberá mantenerse con la iluminaria bien distribuida y la contingencia de la misma ante posibles cortes de fluido eléctrico. Asimismo, deberá contar con piso y techo técnico.

El Centro de datos deberá poseer sistemas de seguridad física que permitan prevenir o minimizar los riesgos a los que afronta los equipos, considerando como mínimo:

- Sistema de detectores de humo
- Sistema de video vigilancia
- Sistema de autenticación de acceso físico
- Medidores de humedad y Temperatura.
- Extintores para equipos informáticos

b) FACTORES ELECTRICOS.-

El centro de datos contará con un sistema eléctrico independiente al comercial de la sede donde se encuentra, así como todo su sistema de pozo a tierra, para ello se coordinará con la oficina o área encargada del mantenimiento a nivel de infraestructura en general.

El centro de datos contará con una estimación de la dimensión del servicio eléctrico necesario para abastecerla, y un sistema de contingencia eléctrica, así como la documentación de la misma (diagrama del cableado, distribución de tableros, circuitos y conexiones, datos de carga, etc.).

El sistema de contingencia eléctrica abarcará redundancia en las estaciones de trabajo y periféricos del centro de datos. Asimismo, los servidores y otros equipos críticos deben estar conectadas a un equipo de contingencia eléctrica y grupos electrógenos con una adecuada estimación de dimensión de su capacidad.

Se realizará revisiones periódicas, al menos una vez al año, sobre el estado del cableado eléctrico en el Centro de datos.

c) CABLEADO DE RED.-

El cableado de red del centro de datos, compuesto por los cables, canaletas, etiquetas y conectores estará instalado considerando los estándares establecidos en el área. Se contará con una guía o manual que identifique los puntos de red en el centro de datos y la distribución del cableado a nivel de sede, desde el equipo de comunicación principal hacia los demás equipos.

d) EQUIPOS DE SERVIDORES Y COMUNICACIÓN.-

Los equipos de comunicación se encuentran inventariados contando con información de su ubicación y distribución dentro y fuera del centro de datos; así como con información de los servidores como: nombre técnico, descripción de uso, ubicación, características técnicas, partición de disco, capacidad de almacenamiento, información que almacena, entre otros.

Los servidores y equipos de comunicación que proporcionen servicios a través de la red e Internet deberán:

- Funcionar 24 horas del día los 365 días del año.
- Recibir mantenimiento preventivo semanal, donde incluye la actualización del sistema operativo y software base del mismo.
- No debe contar con salida a internet directa.
- No debe contar con software libre instalado sin previa revisión y prueba en otro ambiente. Asimismo, debe contar con la autorización del Jefe de la Unidad de Infraestructura Tecnológica.
- Recibir mantenimiento mensual que incluya depuración de logs y eventos, previa copia de seguridad de los mismos.
- Recibir mantenimiento semestral que incluya la revisión de su configuración, limpieza interna y externa de todo el hardware
- Ser monitoreados a través de herramientas que permitan por él o los responsables de dichos servidores y servicios.
- Contar con protección contra descargas eléctricas.
- Contar con mobiliario adecuado que garantice la seguridad de los equipos, evitando alguna posible manipulación indebida, considerando los equipos de comunicación distribuidos en las sedes.
- Todas estas actividades serán registradas en una bitácora respectiva, la cual, de manera tabulada, será presentada mensualmente al Jefe de la Unidad de Infraestructura Tecnológica.

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

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

e) ACCESOS FISICOS AL CENTRO DE DATOS.-

Los equipos informáticos que se encuentren en el Centro de Datos deben de estar en zona restringida.

Los accesos tanto al ingresar y al salir al Centro de Datos serán registrados en una bitácora, la misma que contendrá: Nombre y apellido, DNI, hora inicio y fin, fecha inicio y fin, motivo del acceso, servicio, servidor y/o equipo de comunicación.

Los motivos de accesos se caracterizan por: Instalación, mantenimientos (preventivos y correctivos), eventos, incidencias, problemas, corrección y reparación.

Todo acceso al centro de datos será autorizado por el Jefe de la Unidad de Infraestructura Tecnológica.

El Jefe de la Unidad de Infraestructura Tecnológica es responsable de velar por el correcto registro y la supervisión por lo que se generó el acceso. Los eventos e incidencias serán registrados en una bitácora para la mejora continua.

El monitoreo de los accesos al Centro de Datos será coordinado con la Unidad de Servicios de Atención al Usuario y con la Unidad de Calidad y Seguridad de la Información. El monitoreo de los accesos serán las 24 horas por los 7 días de la semana.

f) ACCESOS A LOS EQUIPOS SERVIDORES Y DE COMUNICACIÓN DEL CENTRO DE DATOS (LOGICO).-

Los equipos informáticos que se encuentren en el Centro de Datos, los cuales pertenecen a distintos segmentos de red, deben tener habilitado y en funcionamiento el control de auditoria para los accesos lógicos a estos equipos.

Los accesos al ingresar y al salir a los equipos servidores y de comunicación del Centro de Datos serán registrados, la misma que contendrá: Nombre y apellido, user, hora inicio y fin, fecha inicio y fin, motivo del acceso, servicio, servidor y/o equipo de comunicación, y quien autorizo.

Los motivos de accesos se caracterizan por: Instalación, configuración, pruebas, migración, apagado, reinicio. Todo acceso será autorizado por el Jefe de la Unidad de Infraestructura Tecnológica.

El Jefe de la Unidad de Infraestructura Tecnológica es responsable de velar por el correcto registro y la supervisión por lo que se generó el acceso lógico a los equipos del Centro de Datos.

El monitoreo de los accesos a los equipos informáticos será coordinado con el gestor de eventos e incidencias y la persona encargada de la seguridad de la información. El monitoreo de los accesos serán las 24 horas por los 7 días de la semana.

Los eventos e incidencias serán reportados a la persona encargada de la seguridad de la información, y serán registrados en una bitácora para la mejora continua, la misma que será remitida al gestor de eventos e incidencias.

g) DOCUMENTACION

El Centro de Datos contará con la siguiente documentación, la cual estará impresa y permanecerá dentro del Centro de Datos:

- Diagrama de la interconexión de red a nivel nacional (visible en el Centro de Datos).
- Diagrama de la interconexión de red a nivel local (visible en el Centro de Datos)
- Manual Técnico de Red donde contemple el inventario del equipamiento existente, tanto hardware y software de todos los equipos y sistemas.
- Correlacion de los elementos de configuración para los servicios internos del Centro de Datos.
- Etiquetado e identificación de los servicios y servidores, así como mantener el detalle de cada uno de ellos.
- Arquitectura de los servicios de tecnologías de información que brinda el Centro de Datos, en la que establece la línea base o versión.
- Cronograma de mantenimiento de los diferentes sistemas y servidores. (visible en el Centro de Datos)
- Información Técnica de todos los equipos, ya sean equipos de red, equipos de alimentación eléctrica, sistemas de aire acondicionado, equipos de seguridad, etc.
- Manuales y Procedimientos de mantenimiento, copias de seguridad, restauración de la información, etc., que puedan servir en caso de una contingencia.
- Registro de Cambios sobre la línea base establecida en la infraestructura del Centro de Datos.
- Un listado de teléfonos de emergencia que puedan servir en caso de una contingencia. (visible en el Centro de Datos).

Una copia de dicha documentación será proporcionada al Jefe de la OTIC como respaldo.

6.3.2. RESPECTO AL EQUIPAMIENTO EN LAS DIRECCIONES, OFICINAS Y UNIDADES

a) COMPUTADORAS

La Unidad de Servicio de Atención al Usuario es la responsable de la instalación y/o desinstalación del equipamiento Informático considerando la adecuada distribución según las necesidades laborales de los usuarios de la OTIC.

Se contará con una guía o manual donde se especifique la ubicación exacta de las computadoras en las sedes y el equipo de comunicación que lo alimenta. Asimismo, la configuración estándar para todos los equipos.

La entrega de las computadoras contará con un acta de recepción por parte del usuario. Toda computadora contará con dos particiones considerando una partición para el almacenamiento de la información que se trabaja, teniendo en cuenta que toda información relevante para la institución se guarde en la unidad de red definido para el usuario u oficina.

La computadora estará debidamente configurada con un antivirus, que se activará para su revisión automáticamente una vez al día, y un antimalware que activa la revisión de los dispositivos móviles conectados. Asimismo, estará asegurada físicamente para prevenir robos o alteraciones de la misma.

Todo traslado y transferencia de los equipos informáticos será autorizado y registrado por la Oficina de Logística del MINEDU.

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

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

Se aplicará como mínimo las siguientes políticas en las computadoras:

- Restricción de acceso al panel de control y sus configuraciones
- Restricción a la administración del antivirus y antimalware
- Restricción a la configuración de internet
- Bloqueo de los puertos USB, salvo las excepciones.

La Unidad de Servicio de Atención al Usuario registrará el software y equipos informáticos alquilados como alta y el tiempo de su prestación.

El recurso informático que no cubra las necesidades del área usuaria para realizar determinadas funciones será declarado en obsoleto tecnológicamente.

El software y licencias de los equipos informáticos que están en proceso de baja, se informará y registrará a través del informe de obsolescencia técnica o de mantenimiento oneroso. Este software será registrado con el estado de ALMACEN para su distribución y asignación posterior.

b) EQUIPOS PERIFÉRICOS

Se contará con una guía o manual donde se especifique la ubicación exacta de los equipos periféricos en las sedes y el equipo de comunicación que lo alimenta. Las impresoras contarán con una herramienta de monitoreo de uso de todos sus servicios, y se bloqueará su acceso a la configuración, evitando que sean manipuladas de manera adecuada. Se contará con un cronograma de mantenimiento de los equipos periféricos.

c) CABLEADO DE RED DE VOZ Y DATOS

La estructura de la red de voz y datos estará documentada, identificando las entradas y salidas de los puntos de red hacia las oficinas o áreas y la interconexión con los equipos de comunicación. Estará tendido mediante canaletas que eviten la manipulación del mismo y separados de las conexiones eléctricas.

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

d) MONITOREO Y SUPERVISIÓN

El personal encargado de la Unidad de Infraestructura Tecnológica monitoreará de manera continua la operatividad y funcionalidad de los equipos y recursos del Centro de Datos, de la red LAN, los enlaces de: Internet, videoconferencia y voz sobre IP.

Cada administrador de los servicios y equipos recursos proporcionará al personal asignado al monitoreo, las herramientas para la gestión de eventos, las métricas e indicadores, para lasalarmas según correspondan.

El personal encargado de la Unidad de Infraestructura Tecnológica configurará en la herramienta de monitoreo avisos de alarma ante posibles eventos de seguridad, entre los tipos de alarmas podríamos considerar:

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

- Congestión de la red.
- Rendimiento degradado
- Pérdida de conectividad.
- Almacenamiento saturado.

El personal encargado de la Unidad de Infraestructura Tecnológica establecerá los parámetros para la generación de los eventos: normal (dentro de los establecido), alerta (alcanzando el límite permitido) y excepción (fuera del rango). Asimismo, evaluará la capacidad de los enlaces de forma periódica, con los administradores de las aplicaciones involucradas.

El monitoreo estará habilitado durante las 24 horas del día y los 7 días de la semana. Se mantendrá evidencia del control que se realiza a través de una bitácora.

6.3.3. MEDIOS DE COMUNICACION

a) Redes de computadoras

El personal de la Unidad de Infraestructura Tecnológica establecerá segmentos de red entre equipos servidores de base de datos, servidores de aplicación, servicios públicos, computadoras internas y la comunicación con Internet.

En los segmentos de red de los equipos servidores establecerá obligatoriamente Listas de Control de Accesos (ACL's) tomando en cuenta el principio del mínimo privilegio. Las computadoras estarán conectadas una red VLAN, si es necesario para el desarrollo de las funciones del usuario.

Se limitará el acceso hacia la red por parte de los usuarios. Se implementará mecanismos como: dominios lógicos separados, implementación de VLANs, evitar saturación en la red, puertas de enlace predeterminadas, entre otros.

El personal de la Unidad de Infraestructura Tecnológica tendrá documentado la asignación de IP públicas y puertos a los servidores, equipos computacionales y de red, tomando en cuenta:

- Justificación del uso de la IP pública y puerto
- Vigencia de la asignación de la IP pública y puerto
- Permisos asignados a dicha IP pública y puerto
- Justificación de los permisos asignados

El tráfico entre la red WLAN y la red del Ministerio de Educación será filtrado. Estos filtros serán aplicados principalmente a la red de servidores, por lo que no se permitirá la administración de servidores desde la red inalámbrica.

El acceso a la administración de los Accesos Point será permitida sólo al personal autorizado a través de una clave de acceso. La clave de la red inalámbrica será cambiada periódicamente para los perfiles necesarios, y se comunicará a las dependencias afectadas.

b) Correo electrónico

El correo electrónico contará con un plan de contingencia que le permita continuar con sus operaciones frente a algún evento que interrumpa la actividad del servicio. Asimismo, tendrá respaldo programado de la información integrado al Plan de Respaldo que ejecuta la Unidad de Infraestructura Tecnológica.

El software de correo electrónico estará configurado de tal manera que no permita el acceso al contenido de los correos sin solicitud de una cuenta de usuario y clave. Contará además con un servicio de Mail Relay ubicado en la zona desmilitarizada (DMZ) de la red, para su contacto con Internet.

Los sistemas de seguridad de la red, limitarán los accesos externos directos hacia los servidores de correo. Se implementará sistemas o software Anti Spam para la minimización de correos masivos no requeridos.

El servidor de correo electrónico estará configurado de tal forma que elimine automáticamente, cada 30 días, los mensajes de la papelera de reciclaje.

c) INTERNET

El servicio de internet institucional contará con un plan de contingencia que le permita continuar con sus operaciones frente a algún evento que interrumpa la actividad del servicio, considerando como prioridad el acceso de los usuarios externos a la página Web del MINEDU. Así como con aplicaciones que permitan filtrar los contenidos Web restringiendo las páginas de adultos, ocio, juegos, descargas masivas, contenido con software malicioso, entre otros.

6.3.4. SISTEMAS DE INFORMACION

Los sistemas de información serán desarrollados en base a la Norma Técnica Peruana "NTP-ISO/IEC 12207:2004 Tecnología de la Información. Procesos de ciclo de vida del software. 1ª Edición" en entidades del Sistema Nacional de Informática, aprobada por Resolución Ministerial Nº 179-2004-PCM.

Todo requerimiento de consumo de un sistema de información desde otro sistema debe ser de conocimiento previo del Líder Usuario.

La clasificación de la información que administra un sistema debe ser definida por el Área Usuaria desde la constitución del proyecto.

El Jefe de la Unidad de Sistemas de Información contará con un inventario actualizado de todos los sistemas de información que administra, considerando como datos mínimos: la descripción del sistema, su arquitectura, estado, fecha de despliegue, servidor donde se ubica, base de datos que alimenta, usuario y nombre del líder usuario.

El equipo de seguridad de la información brindará los lineamientos de seguridad que deben aplicarse en el desarrollo de los sistemas basado en estándares de seguridad de la información.

SOFTWARE

a) DE LA PROTECCION DE LOS DERECHO DE AUTOR

Todo software, aplicativo o sistema de información elaborado por el MINEDU, será desarrollado bajo los estándares establecidos por la OTIC, y será registrado en INDECOPI.

Corresponde a la OTIC encargar en su personal el control y resguardo de las licencias de programas de cómputo, manteniendo actualizado el inventario de las mismas.

Los equipos de cómputo que se alquilen con software contarán con licencias autorizadas, las mismas que serán registradas por la OTIC como alta en calidad de alquiler.

Toda adquisición de equipo informático que incluyan software integrado del tipo OEM o software propietario en general, se documentará por separado la licencia de software y garantía del equipo adquirido, que será registrada por la OTIC.

La OTIC, a través de la persona encargada, tendrá como mínimo de información sobre la adquisición del recurso informático lo siguiente:

- Nombre del Proveedor,
- Fecha de la adquisición,
- Tiempo de soporte y garantía,
- Nombre del Fabricante,
- Nombre del Producto,
- Tipo de licencia,
- Nº de licencia u otra nomenclatura propia del fabricante,
- Cantidad,
- Unidad ejecutora solicitante,
- Dependencia solicitante,
- Contrato, orden de compra y guía de remisión.

Toda adquisición de equipo de cómputo incluye sistema operativo y software de ofimática base.

b) PERFILES DE USUARIO DE SOFTWARE

La OTIC ha definido y registra los perfiles de usuario de software.

Las asignaciones de los perfiles de usuario de software estarán basadas en las funciones del solicitante.

La Unidad de Servicio de Atención al Usuario asignará a cada usuario del MINEDU un perfil de usuario de software según sus necesidades laborales:

Nº	TIPO	SOFTWARE		PERFILES					
				1	2	.	.	.	n
1	SOFTWARE BASE.	1.1	Un Sistema Operativo.	X					
2	OFIMATICA	2.1	Procesador de Texto	X					
		2.2	Hoja de Calculo	X					
		2.3	Presentación de diapositivas	X					
		2.4	Reproductor Multimedia	X					
		2.5	Comprimidor de Archivos	X					
		2.6	Lector de PDF	X					
		2.7	Multigrabador de CD/DVD	X					
		2.8	* Navegador WEB	X					
		2.9	* Correo Electrónico	X					
3	DISEÑO GRAFICO	3.1	Editor de grafico	X					
4	ANTIVIRUS	4.1	Antivirus	X					
5	BASES DE DATOS	5.1	Motor de Base de datos						
6	ESTADISTICA	6.1							
7	GIS	7.1							
8	L. PROG,IDES,REPORT	8.1							
9	MODELAMIENTO	9.1							
10	SISTEMAS DE INFORMACIÓN	10.1							

Todas las estaciones de trabajo tendrá por defecto el perfil 1.

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

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

c) De la administración de licencias

El encargado de la Configuración y Activos de TI coordinará con la Oficina General de Administración para realizar el inventario de Licencias de Software una vez al año.

Las licencias o subscripciones sobre el uso del software deberá identificarse si son perpetuas o solo mientras que dure el contrato de soporte técnico y actualización, por lo que se aclarará en el momento de elaborar las características técnicas del producto.

Toda adquisición de software motivado por una actualización o renovación se mantiene la codificación del software que antecede, registrándolo como actualización o renovación.

Asimismo el encargado de Configuración y Activos de TI registrará el uso de software libre que utilizan los usuarios.

7. PROHIBICIONES EN LA ADMINISTRACION DE LOS RECURSOS INFORMÁTICOS

7.1 Compartir los códigos de acceso físico y lógico que utiliza la Oficina de Tecnologías de la Información y Comunicación.

7.2 Modificar la configuración del hardware y/o software instalado en los equipos servidores o quienes hagan sus veces, sin la autorización respectiva considerando el procedimiento de control de cambios de la OTIC.

7.3 Acceder y utilizar la información para dañar la imagen de la institución, faltas a la moral y a las buenas costumbres o utilizarla para fines personales.

7.4 Conectarse a equipos no autorizados.

7.5 Realizar trabajos con fines de lucro.

7.6 Utilizar cualquier tipo de juego, accesorio o software de entretenimiento.

7.7 Utilizar la infraestructura de la institución para lanzar malware realizar ataques internos o externos.

7.8 Introducir alimentos, bebidas, fumar y tirar basura dentro del centro de datos.

7.9 Introducir cualquier equipo de comunicación o información ajeno a la institución sin la autorización respectiva.

7.10 Mover el equipo de cómputo, mobiliario y cambiar los cables de red, sin la autorización del responsable del centro de datos.

7.11 Introducir al centro de datos cualquier objeto que genere o emita magnetismo o electromagnetismo.

7.12 Ingresar a las áreas exclusivas del Centro de Datos, sin la autorización respectiva.

7.13 Ingresar al Centro de Datos con bultos, mochilas, portafolios, etc., salvo que estén debidamente autorizados por el responsable.

8. RESPONSABILIDADES

8.1 Del Jefe de la OTIC o quien haga sus veces:

8.1.1 Comunicar, informar, velar y exhortar el cumplimiento de la presente norma a todo el personal de dicha oficina.

8.2 Del personal de la OTIC o quien haga sus veces:

8.2.1 Administrar los recursos informáticos que se encuentran bajo su cargo, en el cumplimiento de sus labores.

8.2.2 Utilizar los recursos informáticos que administra y manipularlos solo con fines institucionales.

8.2.3 Reportar o informar a la Unidad de Servicio de Atención al Usuario cualquier incidente, evento o anomalía que surja en los recursos informáticos, así como su solución, para el adecuado registro del mismo.

8.2.4 Desarrollar e implementar del presente documento normativo.

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

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

ANEXO 01

FORMATO DE REGISTRO DE LAS LIBRERIAS FUENTES

Ubicación de la Librería	Nombre del Programa Fuente	Versión	Desarrollador/Fabricante	Fecha creación	Fecha de baja	Versión Manual de Diseño	Versión manual de Usuario	Software de Soporte	ESTADO		
									Operativo en uso	Operativo sin uso	No operativo

VISACION
MINISTERIO DE EDUCACIÓN - Oficina de Tecnologías de la Información y Comunicación
MINISTERIO DE EDUCACIÓN
UNIDAD DE CALIDAD Y SEGURIDAD DE LA INFORMACIÓN
- OTIC -

710 - 2015 - MINEDU

ANEXO 02

Formato de Entrega de Información

PERÚ | Ministerio de Educación | Secretaría de Planificación Estratégica | Oficina de Tecnologías de la Información y Comunicación

Acta de Entrega de Información 001-2015

Información general

Fecha de Entrega	Hora de Entrega	Documento de autorización y/o referencia

Nombre y cargo del responsable de entrega	Nombre y cargo del responsable de recepción

Clasificación de la información

Tipo de Información	Descripción	Elección
Reservada	Información de uso exclusivo por el personal autorizado.	
Confidencial	Información de uso exclusivo para los fines del Ministerio de Educación.	
Pública	Información de uso público	

Medio de entrega

Físico		Digital	X

Físico			Digital		
Cantidad de hojas por documento			Cantidad de archivos por carpetas		
Nombre de documento	Versión	Cantidad	Nombre de carpeta	Fecha de creación	Cantidad
			Base de datos XXXXXX		00 Gb XXXX

Acuerdo de uso

- El uso de la información entregada es de responsabilidad directa del responsable de recepción para lo cual deberá respetar las normas regulatorias que rigen en el Ministerio de Educación y del Sector teniendo en cuenta que la información definida como **confidencial** *es* solo para fines institucionales. Su divulgación, copia y/o adulteración no autorizada está estrictamente prohibida. - La entrega se realiza a través de un CD o USB o copia a una carpeta (ESPECIFICAR)

Los firmantes dan fe del contenido de la presente acta

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

Firma y Sello del Responsable de Entrega NOMBRE COMPLETO	Firma y Sello del Responsable de Recepción NOMBRE COMPLETO

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