PERÚ | Ministerio de Educación | Viceministerio de Gestión Institucional | Proyecto Especial de Inversión Pública Escuelas Bicentenario | BICENTENARIO PERÚ 2021

DIRECTIVA
"NORMAS PARA EL ACCESO Y USO DEL SERVICIO DE CORREO ELECTRÓNICO INSTITUCIONAL DEL PROYECTO ESPECIAL DE INVERSION PUBLICA ESCUELAS BICENTENARIO - PEIP EB"

Resolución de Aprobación			
Resolución Directoral Ejecutiva N° 00050-2021-MINEDU/VMGI-PEIP EB/DIEJE			
Código	**Versión**	**Páginas**	**Fecha de Aprobación**
DI-016-01-MINEDU/PEIP-EB	1.0	16	03/09/2021

Firmado digitalmente por:
ALVARADO LIZARME Patricia
FAU 20131370998 hard
Motivo: Soy el autor del
documento
Fecha: 14/09/2021 23:43:12-0500

I. OBJETIVO

Establecer disposiciones y controles que permitan orientar a los usuarios del Proyecto Especial de Inversión Pública - Escuelas Bicentenario (en adelante PEIP-EB), en el acceso y buen uso del servicio de correo electrónico institucional.

II. FINALIDAD

Normar el acceso y uso aceptable del servicio de correo electrónico institucional en el PEIP-EB, a fin de garantizar la comunicación interna y externa y fortalecer los niveles de seguridad de la información.

III. ALCANCE

La presente directica es de alcance y aplicación obligatoria para todo el personal de la entidad del PEIP-EB, independientemente del régimen laboral o vínculo contractual al que se encuentren sujetos, a los que se les asigne y autorice el uso del servicio de correo electrónico institucional.

IV. BASE NORMATIVA

4.1. Ley N° 27269, Ley de Firmas y Certificados Digitales.
4.2. Ley N° 27291, Ley que permite el uso de medios electrónicos para la manifestación de voluntad y la utilización de la firma electrónica.
4.3. Ley N° 27309, Ley que incorpora los delitos informáticos al Código Penal.
4.4. Ley N° 27658, Ley Marco de Modernización de la Gestión del Estado.
4.5. Ley N° 27815, Ley del Código de Ética de la Función Pública.
4.6. Ley N° 28493, Ley que regula el uso del correo electrónico comercial no solicitado (SPAM).
4.7. Ley N° 28612, Ley que Norma el Uso, Adquisición y Adecuación del Software en la Administración Pública.
4.8. Ley N° 29733, Ley de protección de datos personales.
4.9. Ley N° 30096, Ley de Delitos Informáticos
4.10. Decreto Legislativo N° 1412, que aprueba la Ley de Gobierno Digital
4.11. Decreto Supremo Nº 052-2008-PCM, que aprueba el Reglamento de la Ley N° 27269, Ley de Firmas y Certificados Digitales.
4.12. Decreto Supremo N° 072-2003-PCM, que aprueba el Reglamento de la Ley N° 27806, Ley de Transparencia y Acceso a la Información Pública, y su modificatoria, Ley 27927.
4.13. Decreto Supremo Nº 031-2005-MTC, que aprueba el Reglamento de la Ley Nº 28493 que regula el envío del correo electrónico comercial no solicitado.
4.14. Decreto Supremo N° 004-2019-JUS, que aprueba el Texto Único Ordenado de la Ley N° 27444, Ley de Procedimiento Administrativo General.
4.15. Decreto Supremo N° 021-2019-JUS, que aprueba el Texto Único Ordenado de la Ley N° 27806, Ley de Transparencia y Acceso a la información Pública.

Jefe de la Oficina de Tecnologías de la Información(e)
V°B°
Luis Antonio Arrasco López

Firmado digitalmente por:
RODRIGUEZ SANCHEZ Marina
FAU 20131370998 soft
Motivo: Soy el autor del
documento
Fecha: 26/08/2021 09:58:48-0500

Firmado digitalmente por:
MENDOZA DE LA CRUZ Israel
Miguel FAU 20131370998 hard
Motivo: Doy V° B°
Fecha: 27/08/2021 08:35:56-0500

4.16. Resolución Ministerial N° 073-2004-PCM, que aprueba la "Guía para la Administración Eficiente del Software Legal en la Administración Pública".

4.17. Resolución Ministerial N° 004-2016-PCM que aprueba el uso obligatorio de la Norma Técnica Peruana "NTP-ISO-IEC 27001:2014, Tecnología de la Información. Requisitos 2da Edición" en todas las entidades integrantes del Sistema Nacional de Informática.

4.18. Resolución Ministerial N° 338-2020-MINEDU, que aprueba el Manual de Operaciones del Proyecto Especial de Inversión Pública Escuelas Bicentenario.

4.19. Resolución de Secretaría de Gobierno Digital Nº 001-2018-PCM/SEGDI, "Lineamientos para el uso de servicios en la nube para entidades de la Administración Pública del Estado Peruano".

4.20. Resolución Directoral Ejecutiva N° 021-2021-MINEDU/VMGI-PEIP ESCUELAS BICENTENARIO, que aprueba la Directiva N° 001 -2021-MINEDU/PEIP EB "Normas para formulación, aprobación y actualización de documentos normativos u orientadores en el Proyecto Especial de Inversión Pública Escuelas Bicentenario – PEIP EB".

4.21. Resolución de Secretaria General N° 073-2019-MINEDU, que aprueba la Directiva N° 005-2019-MINEDU/SPE-OPEP-UNOME denominada "Elaboración, aprobación y derogación de actos resolutivos, así como elaboración y modificación de documentos de gestión, normativos y orientadores del Ministerio de Educación.

4.22. Resolución de Secretaria General N° 090-2020-MINEDU, que suspende la aplicación de la Directiva N° 005-2019-MINEDU/SPE-OPEP-UNOME denominada "Elaboración, aprobación y derogación de actos resolutivos, así como elaboración y modificación de documentos de gestión, normativos y orientadores del Ministerio de Educación.

4.23. Resolución Jefatural N° 207-2002-INEI, que aprueba la Directiva N° 010-2002-INEI/DTNP "Normas Técnicas para la Asignación de Nombres de Dominio de las Entidades de la Administración Pública"

4.24. Resolución Jefatural N° 053-2003-INEI, que aprueba la Directiva N° 004-2003-INEI/DTNP "Norma Técnica para la Implementación del Registro de Recursos Informáticos en las Instituciones de la Administración Pública".

4.25. Resolución Jefatural N° 088-2003-INEI, que aprueba la Directiva N° 005-2003-INEI/DTNP, "Normas para el uso del servicio de correo electrónico en las entidades de la Administración Pública".

Jefe de la Oficina de Tecnologías de la Información(e) V°B° Luis Antonio Arrasco López

Las normas señaladas incluyen sus respectivas modificatorias.

V. GLOSARIO DE TÉRMINOS:

5.1. **Activo**: de acuerdo a la Norma ISO 27000, un activo se refiere a cualquier información o elemento relacionado con el tratamiento de la misma, que tenga valor para la organización.

5.2. **Activos Informáticos:** está referido a los datos, dispositivos, hardware, software u otro componente del entorno relacionado con la información, que debe ser protegido de acceso ilícito, revelación, robo, alteración o destrucción, lo cual significaría una pérdida para la organización.

5.3. **AntiSpam:** aplicación o herramienta informática que se encarga de detectar y eliminar los correos no deseados

5.4. **Área usuaria:** Oficina que requiere y/o utiliza las comunicaciones de la institución para fines laborales.

5.5. **Backup:** copia de seguridad que contiene un duplicado de los datos contenidos en un correo electrónico y que se realizar para poder recuperarlos ante un incidente.

5.6. **Dominio**: es la denominación que identifica a la institución en Internet a fin de que pueda ser ubicada rápidamente, correspondiendo al PEIP-EB el nombre de dominio peip.gob.pe.

5.7. **Información Digital:** toda aquella información que es almacenada o transmitida empleando los sistemas de información y/o sistemas de comunicación institucionales.

5.8. **Internet Message Access Protocol (IMAP):** protocolo de acceso a mensajes de Internet. Es un método de acceso a correos electrónicos en un servidor sin tener que descargarlos al disco duro local.

5.9. **Post Office Protocol (POP):** protocolo que se encarga de establecer una conexión entre un cliente y un servidor de correo electrónico para poder gestionar el envío de mensajes.

5.10. **Secure Sockets Layer (SSL):** tecnología estándar para mantener segura una conexión a Internet, así como para proteger cualquier información confidencial que se envía. Utiliza algoritmos de cifrado para codificar los datos que se transmiten e impedir acceso a hackers.

5.11. **Servicio de Correo Electrónico:** servicio que permite el intercambio de mensajes que contienen archivos, imágenes y/o texto, utilizando sistemas de comunicación electrónicos.

5.12. **Simple Mail Transfer Protocol (SMPT):** es un protocolo de mensajería empleado para mandar un email de un servidor de origen a un servidor de destino. Este procedimiento es indispensable en el proceso de envío de emails.

5.13. **Software:** componentes lógicos de programas y rutinas que permiten a un computador realizar determinadas tareas.

Jefe de la Oficina de Tecnologías de la Información(e)
V°B°
Luis Antonio Arrasco López

5.14. **Spam:** comunicaciones no solicitadas que se envían de forma masiva por internet o mediante sistemas de mensajería electrónica. Estos mensajes no deseados suelen ser publicidad.

5.15. **Transport Layer Security (TLS** protocolos criptográfico que encriptan los datos y autentifican una conexión cuando se mueven los datos en Internet. Es una versión más reciente de SSL, corrige vulnerabilidades de seguridad en los protocolos SSL.

5.16. **Usuario:** Persona que utiliza los activos informáticos de la institución para fines laborales.

VI. DISPOSICIONES GENERALES

6.1. La Oficina de Tecnologías de Información (en adelante OTI), es la encargada de definir el software de servicio de correo electrónico institucional, teniendo en cuenta la solución tecnológica que permita una comunicación efectiva entre los trabajadores del PEIP-EB tanto de manera interna como externa.

6.2. La OTI es la encargada de administrar los accesos a las comunicaciones del PEIP-EB.

6.3. Las unidades funcionales del PEIP-EB, deben de cumplir en el ámbito de su competencia; los lineamientos establecidos en la presente Directiva.

6.4. Los servidores civiles, proveedores de servicio y/o terceros que para el cumplimiento de sus funciones o la prestación del servicio requieran el acceso a los activos informáticos del PEIP-EB, deben de cumplir los lineamientos de seguridad de la información establecidos en la presente Directiva.

6.5. La OTI garantiza el soporte técnico necesario para que las comunicaciones institucionales se realicen mediante correo electrónico conforme la normativa vigente.

VII. DISPOSICIONES ESPECÍFICAS:

7.1. Del servicio de correo electrónico institucional

7.1.1. El sistema de correo electrónico institucional proporciona al usuario los siguientes servicios:

a) Envío y recepción de correo electrónico
b) Herramientas de colaboración integradas como: Calendario, Mensajería Instantánea (chat, voz, video), grupos (listas de distribución)

Jefe de la Oficina de Tecnologías de la Información(e)
V°B°
Luis Antonio Arrasco López

7.1.2. Además, el sistema de correo electrónico debe contar con las siguientes funcionalidades:

a) La solución debe permitir las funciones habituales de envío, recepción, envío con copia, copia oculta, formato, adjuntar documentos y compartir archivos.
b) Permitir implementar políticas restrictivas de seguridad respecto a direcciones IP y dominios de correo desde los cuales los usuarios pueden recibir mensajes legítimos.
c) Permitir enviar correos de auto-respuesta ante la ausencia del usuario.
d) Disponer de registros de auditoría de la actividad de usuarios y administradores.
e) Debe permitir generar una firma personal para envío de correos
f) Debe permitir recuperar correos electrónicos eliminados del buzón de correo.
g) Debe contener funcionalidades operativas de antivirus.
h) Debe garantizar el respaldo de la información.
i) La solución incluye el servicio permanente de AntiSpam que alerte sobre los mensajes sospechosos de correos no deseados y maliciosos.
j) Permitir el acceso a los usuarios para que puedan ingresar al sistema de mensajería mediante la conexión por protocolos estándar POP, IMAP, SMTP, SSL/TLS.
k) Debe incorporar una solución de doble factor de autenticación para el acceso a servicios provistos, la misma que permitirá validar el acceso al usuario que cuente con un teléfono móvil o Smartphone.
l) Posibilidad de importar/exportar backups de la información por usuario de mensajería de correo electrónico en un medio de almacenamiento externo a la solución de correo electrónico.
m) El servicio de correo electrónico institucional en la nube debe permitir la administración de funcionalidades mediante consola descentralizada.

7.2. Del acceso al servicio de correo electrónico institucional

7.2.1. Para acceder a la información contenida en el correo electrónico institucional, se requiere una cuenta de usuario y contraseña perteneciente al propietario de dicha cuenta.

7.2.2. De la creación, actualización y desactivación de cuentas de correo electrónico

Jefe de la Oficina de Tecnologías de la Información(e)
V°B°
Luis Antonio Arrasco López

a) El acceso a los activos informáticos requerido para un usuario, debe ser solicitado a la OTI mediante el *Formato de Altas y Bajas de Usuarios* (cuyo contenido se detalla en el Anexo N°1 de la presente Directiva). Dicho formato debe ser firmado por el Director de Sistema Administrativo III, o Director de Sistema Administrativo II, de acuerdo a

la unidad funcional donde labora el personal, y remitirlo a la OTI por correo institucional al correo helpdesk@peip-eb.gob.pe, administrado por el área de Infraestructura Tecnológica de la OTI.

b) El personal de la OTI responsable de la configuración de los accesos al correo electrónico institucional, antes de otorgar el acceso debe validar que el usuario haya sido capacitado y/o concientizado sobre las normas de uso de los activos informáticos. De no ser así debe de realizar la capacitación y/o concientización correspondiente al momento de realizar la entrega de las credenciales de correo electrónico mediante el *Acta de Entrega de Correo Institucional* (cuyo contenido se detalla en el Anexo N°2 de la presente Directiva).

c) Para la creación de las cuentas de correo electrónico institucional para el personal bajo régimen laboral en el PEIP-EB, se tendrá en cuenta el siguiente formato:

Primera letra del primer nombre	Apellido paterno	Caracter	Nombre del dominio PEIP-EB
a	bbbb*	@	peip-eb.gob.pe

** en casos de duplicidad se incluirán las letras del apellido materno*

d) En los casos de que ya exista una cuenta con el mismo nombre, la OTI procederá a incluir tantas letras del segundo apellido como sea necesario, a fin de crear una cuenta con un nombre único.

e) La OTI realizará un control centralizado y automático de los accesos a los activos informáticos, lo cual le permitirá contar con registros de actividad de los usuarios en casos de auditoría.

f) La desactivación de cuentas de usuario, cambios de privilegios para una cuenta, bloqueo de accesos a usuarios que cambiaron de funciones, o de aquellos que ya no cuentan con autorizaciones para determinadas tareas, así como de los que se desvincularon de la institución o han sufrido robo de credenciales de acceso o prácticas de *phishing*; deben ser solicitados a la OTI mediante documento formal y/o *Formato de Altas y Bajas de Usuarios* remitido por el Director de Sistema Administrativo III o Director de Sistema Administrativo II, de acuerdo a la unidad funcional en la que labora el usuario.

Jefe de la Oficina de Tecnologías de la Información (e)
V°B°
Luis Antonio Arrasco López

g) La OTI podrá crear cuentas de correo electrónico genéricas previo requerimiento formal del Director de Sistema Administrativo III o Director de Sistema Administrativo II de una unidad funcional, quien deberá designar un responsable de la cuenta.

h) Durante los periodos de ausencia de un usuario (por motivos de vacaciones, descanso médico, licencia u otros), el correo electrónico institucional deberá ser configurado por el usuario para emitir una respuesta automática a los mensajes, y/o reenvío a otro correo institucional para que los mensajes sean atendidos durante su ausencia, salvo disposición contraria.

7.2.3. De la generación de la contraseña de acceso

a) La OTI asigna las contraseñas a través de un procedimiento que considera como mínimo:

a.1) Garantizar que los usuarios cambien las contraseñas iniciales que les han sido asignadas, la primera vez que ingresan al sistema.

a.2) Evitar la participación de terceros o el uso de mensajes de correo electrónico sin protección, en el mecanismo de entrega de la contraseña.

a.3) Configurar los sistemas de autenticación de tal manera que:

- Se permita establecer contraseñas que contengan como mínimo ocho (08) caracteres, debiendo ser estos una combinación de letras mayúsculas, minúsculas y caracteres alfanuméricos.
- Se permita alertar al usuario sobre intentos fallidos de acceso al sistema con una contraseña incorrecta.
- No se permita reutilizar, por lo menos, las últimas tres (03) contraseñas.
- Se permita bloquear el acceso al sistema, después de seis (06) intentos de acceso con una contraseña incorrecta.
- Sea posible programar para que automáticamente cada cuarenta y cinco (45) días se solicite cambio de la contraseña.

a.4) La contraseña de acceso es personal e intransferible, por lo tanto, es responsabilidad de cada uno de los usuarios de los servicios informáticos y de comunicaciones del PEIP-EB, proteger la confidencialidad de sus respectivas contraseñas de acceso.

7.2.4. Del acceso y limitaciones a terceros

Jefe de la Oficina de Tecnologías de la Información(e)
V°B°
Luis Antonio Arrasco López

a) En el caso de que se requiera brindar acceso a terceros (locadores de servicios), se otorgará el 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 de su contratación. Para ello cada área usuaria es responsable de

incluir en los términos de referencia lo siguientes controles de seguridad:

a.1) Determinar los accesos a los activos informáticos según la naturaleza de su contrato.
a.2) Definición de acciones ante la ocurrencia de algún incidente de seguridad que comprometa los activos informáticos de la Institución.
a.3) Determinar las obligaciones de las partes y responsabilidades legales.

b) Asimismo, el área usuaria luego de haber recibido la notificación de entrega de la orden de servicio al tercero, debe gestionar la firma del Acuerdo de Confidencialidad dentro de las setenta y dos (72) horas y remitirlo a la OTI para las atenciones correspondientes a la creación de cuentas de usuarios y accesos a los activos informáticos, de corresponder.

7.2.5. Del acceso a información digital del correo electrónico institucional

a) El acceso a la información generada o adjunta dentro del servicio de correo electrónico institucional, se realiza a través de una cuenta de usuario y contraseña personal perteneciente al propietario de dicha cuenta.

b) Las solicitudes de acceso a información contenida en correos electrónicos institucionales, serán atendidas en el marco de las disposiciones establecidas en el Texto Único Ordenado de la Ley N° 27806, Ley de Transparencia y Acceso a la Información Pública.

c) La OTI podrá generar backups del correo electrónico institucional de un usuario en particular, a solicitud expresa del Director de Sistema Administrativo III o Director de Sistema Administrativo II de la unidad funcional al que pertenece el usuario.

d) La OTI guardará copias de respaldo de la información digital contenida en los correos electrónicos siempre que se cuente con la capacidad de almacenamiento necesaria y se cuente con la cantidad suficiente de licencias.

e) La información digital contenida en el servicio de correo electrónico institucional y de los backups generados, serán custodiados por la OTI durante la vigencia del PEIP-EB.

Jefe de la Oficina de Tecnologías de la Información (e)
V°B°
Luis Antonio Arrasco López

7.3. Del uso del servicio de correo electrónico institucional

7.3.1. El servicio de 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.

7.3.2. Toda la información que se transfiera a través del correo institucional, es considerada información confidencial.

7.3.3. La cuenta de correo electrónico institucional es personal e intransferible, siendo responsabilidad del usuario las acciones que se podrían derivar del uso indebido.

7.3.4. El usuario debe proteger la confidencialidad de la contraseña requerida para hacer uso del servicio de correo electrónico institucional.

7.3.5. 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.

7.3.6. En caso de que el usuario utilice una foto para su perfil de correo electrónico institucional, debe incluir una fotografía personal apropiada y acorde con los fines de la institución.

7.3.7. La OTI, en caso verifique la no utilización del correo electrónico institucional por más de noventa (90) días, desactivará la cuenta de correo, lo cual será posteriormente informado al Director de Sistema Administrativo III o Director de Sistema Administrativo II de la unidad funcional donde labora el usuario.

7.3.8. El usuario debe eliminar los mensajes que ya no utilizará, o aquellos que ya fueron leídos en su oportunidad, considerando que la capacidad de almacenamiento de correos es hasta treinta (30) Gigabytes (GB). Excedido dicho tamaño no podrá enviar o recibir correos electrónicos.

7.3.9. En caso de que el usuario reciba correos sospechosos, de destinatarios desconocidos o que contengan archivos adjuntos que no hayan sido solicitados, se sugiere que no sean abiertos y se reporte el evento a la OTI.

7.3.10. Los mensajes de correo electrónico institucionales, enviados internamente no deben exceder de veinticinco (25) Megabytes (MB), incluyendo el (los) archivo(s) adjuntos que lo acompañen. En los casos en que los archivos adjuntos en un mensaje de correo electrónico superen esta capacidad, el servicio de correo generará un link de acceso al OneDrive de la institución

Jefe de la Oficina de Tecnologías de la Información(e)
V°B°
Luis Antonio Arrasco López

desde el cual se podrá descargar los archivos.

7.3.11. Todos los mensajes que se encuentren en la papelera de reciclaje, se eliminan automáticamente cada veinticinco (25) días.

7.3.12. El usuario podrá solicitar al área de Infraestructura Tecnológica de la OTI, el servicio de respaldo de la información almacenada en la cuenta de correo electrónico institucional.

7.3.13. La OTI debe implementar los controles que permitan filtrar los correos SPAM en salvaguarda de la seguridad de la información institucional.

7.3.14. Del buen uso de las contraseñas

a) Los usuarios deben seguir las siguientes buenas prácticas de seguridad en la selección y uso de contraseñas:

a.1) Mantener la confidencialidad de las contraseñas.
a.2) Solicitar a la OTI el cambio de la contraseña ante un indicio de pérdida de confidencialidad de la contraseña o un evento que ponga en riesgo la seguridad del servicio de correo electrónico institucional.
a.3) Seleccionar contraseñas que:
- Sean fáciles de recordar;
- No guarden relación con datos relacionados del usuario, por ejemplo año y fecha de nacimiento, nombres de los hijos, mascotas, números de teléfono, etc.
- Resulten de la combinación de letras mayúsculas, minúsculas y caracteres alfanuméricos.

7.3.15. Estandarización y uso de la firma personal

a) La firma de correo electrónico debe incluir el logo institucional nombres y apellidos del usuario, cargo, Dirección, Oficina o Unidad a la que pertenece, número de celular, cuenta de correo electrónico y página web de la institución.

b) La OTI pondrá a disposición de los usuarios la plantilla para generación de la firma personal, así como el manual con las instrucciones para su creación y configuración a fin de que la firma sea agregada a los mensajes.
c) Para mantener homogeneidad, el usuario debe realizar un uso correcto de la firma, conforme a los lineamientos de la institución,

7.4. Prohibiciones en el uso del servicio de correo electrónico institucional

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. De existir necesidad deberá utilizarse la opción de copia oculta o una lista de distribución.

7.4.3. Responder a los correos SPAM. Para estos casos reportar al área OTI a fin de que se realice la inspección de seguridad. Así mismo está prohibido enviar mensajes en cadena.

7.4.4. 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.

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

7.4.6. Registrar la cuenta de correo corporativo en páginas ajenas a la institución.

7.4.7. Enviar información o enlaces a sitios que puedan considerarse inapropiados por su contenido que promueva actos de xenofobia, discriminación, comportamiento agresivo u ofensivo.

7.4.8. Utilizar el correo electrónico institucional para ejercer hostigamiento o acoso laboral. De evidenciarse estos casos serán remitidos a la Unidad de Recursos Humanos para las acciones correspondientes.

7.4.9. Distribuir mensajes con contenidos impropios y/o lesivos a la moral, o que afecten la imagen de terceros o de la institución u otras entidades públicas.

7.4.10. Acceder y utilizar una cuenta de correo institucional diferente a la asignada.

7.4.11. Difundir por correo electrónico dentro o fuera del PEIP-EB, documentos o información clasificada como SECRETA, RESERVADA o CONFIDENCIAL, sin contar con la autorización correspondiente.

Jefe de la Oficina de Tecnologías de la Información (e)
V°B°
Luis Antonio Arrasco López

7.4.12. Abrir archivos adjuntos recibidos sin analizarlos previamente con la herramienta corporativa contra código malicioso. De encontrarse algún virus o archivo sospechoso se debe comunicar a la OTI para su inspección.

7.4.13. Los permisos de envío y recepción de correos gratuitos deben estar debidamente autorizados.

VIII. RESPONSABILIDADES

8.1. La Unidad de Recursos Humanos es responsable de:

8.1.1. Poner en conocimiento de la OTI cuando notifique a las unidades funcionales correspondientes, la incorporación de nuevo personal a sus dependencias. Esto con el fin de que se gestione la creación de sus cuentas de correo electrónico de acuerdo a lo señalado en el numeral 7.2.2 literal a).

8.1.2. Remitir mensualmente a la OTI, la lista de los servidores civiles cuyo vínculo laboral con el PEIP-EB ha quedado extinguido, a fin de proceder a la desactivación de las cuentas de acceso a los activos informáticos. Esta lista será complementaria a la información que oportunamente remitirán las unidades funcionales de acuerdo a lo señalado en el numeral 7.2.2 literal g).

8.2. La Unidad de Abastecimiento es responsable de:

8.2.1. Verificar la lista de terceros (locadores de servicios) remitida mensualmente por la OTI, e identificar aquellos cuyo contrato ha quedado extinguido, a fin de que la OTI pueda proceder a la desactivación de las cuentas de acceso a los activos informáticos.

8.3. La OTI es responsable de:

8.3.1. Proveer los activos informáticos e implementar controles de seguridad de la información que permitan mitigar los riesgos a los cuales se encuentran expuestos.

8.3.2. Administrar el acceso a los activos informáticos de la institución.

8.3.3. Mantener el registro de los activos informáticos en coordinación con la Unidad de Abastecimiento.

Jefe de la Oficina de Tecnologías de la Información (e)
V°B°
Luis Antonio Arrasco López

8.3.4. Actualizar las funcionalidades y características del servicio de correo electrónico institucional de acuerdo a las nuevas tecnologías emergentes que sean útiles para la gestión del PEIP-EB.

8.3.5. Efectuar revisiones periódicas de las cuentas de correo electrónico institucional con la finalidad de bloquear aquellas cuentas que no fueron utilizadas por más de noventa (90) días. Asimismo, informará posteriormente al Director de Sistema Administrativo III o Director de Sistema Administrativo II de la unidad funcional correspondiente.

8.3.6. Poner en conocimiento todo mal uso de los activos informáticos, a la Unidad de Recursos Humanos, con copia al Director de Sistema Administrativo III o Director de Sistema Administrativo II de la unidad funcional donde labora el usuario que realizó tal acción, a fin de que se adopten las medidas que correspondan, según las normas institucionales vigentes.

Jefe de la Oficina de Tecnologías de la Información(e)
V°B°
Luis Antonio Arrasco López

8.4. Los usuarios de los activos informáticos son responsables de:

8.4.1. Preservar la confidencialidad de la contraseña de acceso de la que es propietario, no debiendo transferirla a otros usuarios.

8.4.2. Asumir la responsabilidad sobre las acciones que se realicen con la cuenta de usuario (cuenta de usuario y contraseña) de su propiedad, salvo que dichas acciones hayan sido realizadas como consecuencia de la vulneración de la seguridad de las cuentas de usuario.

8.4.3. Reportar a la OTI, a través de los procedimientos establecidos; cualquier incidente, daño o perjuicio voluntario o involuntario y/o vulnerabilidad sobre los activos informáticos, para las acciones correspondientes.

IX. DISPOSICIONES COMPLEMENTARIAS:

Las disposiciones no previstas en la presente Directiva serán resueltas por la OTI, conforme lo establecido en el Manual de Operaciones del PEIP-EB, y normatividad vigente aplicable al caso.

Anexo N° 01
FORMATO DE ALTAS Y BAJAS DE USUARIOS

PERÚ | Ministerio de Educación | Viceministerio de Gestión Institucional | Proyecto Especial de Inversión Pública Escuelas Bicentenario

FORMATO DE SOLICITUD DE CREACIÓN, ACTUALIZACIÓN O ELIMINACIÓN DE CUENTAS DE USUARIOS PARA SERVICIOS DE RED

DIA	MES	AÑO

I. SOLICITANTE

Dirección (X) Oficina ( ) Unidad ( )		

II. RELACION DE USUARIO(S)

N°	RESPONSABLE DE LA CUENTA		DNI	TELÉFONO	CARGO O SERVICIO	CAS	Crear(C) Actualiza(A) Eliminar(E)	ACCESO A										
	APELLIDOS Y NOMBRES (Deberá de consignar los 02 Apellidos)	CORREO PERSONAL / INSTITUCIONAL						RED	INTERNET	CORREO ELECTRÓNICO	Servicio de telefonía				Sistemas de Información (colocar número de lista)			Otros
											Fijos	Celulares	Nacionales	Internacionales	Operador	Administrador	Consulta	
1							C			X								
2																		
3																		
4																		
5																		

Observaciones:

III. FIRMA Y SELLOS

A traves de la siguiente firma autorizo la creación, actualización o eliminación del usuario a los servicios de red especificados

Firma
Jefe de la Unidad / Oficina

Jefe de la Oficina de Tecnologías de la Información (e)
V°B°
Luis Antonio Arrasco López

Anexo N° 02
ACTA DE ENTREGA DE CORREO INSTITUCIONAL

PERÚ | Ministerio de Educación | Viceministerio de Gestión Institucional | Proyecto Especial de Inversión Pública Escuelas Bicentenario

"Decenio de la Igualdad de oportunidades para mujeres y hombres"
"Año del Bicentenario del Perú: 200 años de Independencia"

ACTA DE ENTREGA DEL CORREO INSTITUCIONAL PEIP EB

INFORMACION DE CUENTA DE CORREO ELECTRONICO

Dirigido a	:	Nombres y Apellidos
Area	:	Dirección, Oficina o Unidad
Dirección de correo electrónico	:	nombreusuario@peip-eb.gob.pe
Contraseña inicial	:	contraseñaXXX

Para ingresar al de correo institucional, deberá dirigirse a la siguiente dirección https://mail.google.com/ la cual le pedirá los siguientes datos en primer lugar, el **"Usuario"** y luego **"Contraseña"**, estos datos son los proporcionados en este documento.

Una vez ingresado al correo institucional por primera vez, la contraseña podrá ser cambiada, esta opción le solicitara ingresar información en dos casilleros, la primera **"Crear Contraseña"**, es para la contraseña que nueva que deberá ingresar, luego la otra casilla **"Confirmar Contraseña"**, serán para confirmar su nueva contraseña, y para ello deberá utilizar como mínimo 6 caracteres, utilizando para esto la combinación de números y letras (Mayúsculas y Minúsculas).

Cualquier consulta o comentario, favor de reportarlo a la Oficina de Tecnología de Información del PEIP-EB.

Atte.

Oficina de Tecnología de la Información – PEIP-EB

Lima, XX de mayo de 2021

---------- Entregue Conforme

---------- Recibí Conforme

1 de 1

Proyecto Especial de Inversión Pública

Jefe de la Oficina de Tecnologías de la Información(e)
V°B°
Luis Antonio Arrasco López