TRANSCRIPCIÓN
En la fecha se ha expedido la Resolución siguiente

RESOLUCIÓN RECTORAL Nº 0474-2023-UNHEVAL

Cayhuayna, 10 de julio de 2023

VISTOS, los documentos que se acompañan en doce (12) folios y un (01) ejemplar de la DIRECTIVA N° 002-2023-UNHEVAL/OTI "USO DE LAS TECNOLOGÍAS DE INFORMACIÓN Y DE COMUNICACIONES";

CONSIDERANDO:

Que, el Artículo 18° de la Constitución Política del Perú establece que cada universidad es autónoma en su régimen normativo, de gobierno, académico, administrativo y económico. Las universidades se rigen por sus propios estatutos en el marco de la Constitución y de las leyes; artículo concordado con la Ley Universitaria N° 30220 y el Estatuto de la Unheval;

Que el director de la Oficina de Tecnología de la Información, mediante Oficio N° 000521-2023-OTI, del 12.JUL.2023, dirigido al dirigido al director de la Oficina de Planeamiento y Presupuesto, remite la propuesta de la DIRECTIVA N° 002-2023-UNHEVAL/OTI "USO DE LAS TECNOLOGÍAS DE INFORMACIÓN Y DE COMUNICACIONES", para su consideración y visto bueno para efectos de su posterior aprobación y entrada en vigor, ello con el objetivo de regular la utilización de las tecnologías de información y comunicaciones en la Unheval, por lo que, solicita su evaluación;

Que la coordinadora de la Unidad Funcional de Modernización, con el Oficio N° 000164-2023-UNHEVAL-UFMO, del 22.JUN.2023, remite el Oficio N° 075-2023-UNHEVAL-MGT, del 22.JUN.2023, con el que informa que la DIRECTIVA N° 002-2023-UNHEVAL/OTI "USO DE LAS TECNOLOGÍAS DE INFORMACIÓN Y DE COMUNICACIONES", se encuentra alineada a la estructura establecida en la Directiva N° 001-2022-UNHEVAL/OPP/UPPM "LINEAMIENTOS PARA LA ELABORACIÓN Y APROBACIÓN DE REGLAMENTOS INTERNOS Y DIRECTIVAS DE LA UNHEVAL"; por lo que, emite opinión favorable para su aprobación, previamente debe ser remitido a la Oficina de Asesoría Jurídica para opinión legal, en cumplimiento a lo establecido en el artículo 7°, numeral 7.1.5 de la Directiva N° 001-2022-UNHEVAL/OPP/UPPM, para luego continuar con el trámite respectivo;

Que la jefa de la Oficina de Asesoría Jurídica, mediante el Informe N° 000022-2023-UNHEVAL-OAJ, del 06.JUL.2023, emite opinión legal respecto a la aprobación de la **DIRECTIVA N° 002-2023-UNHEVAL/OTI "USO DE LAS TECNOLOGÍAS DE INFORMACIÓN Y DE COMUNICACIONES"**; y luego de detallar los **ANTECEDENTES** que se hacen referencia en los considerandos anteriores, informa lo siguiente:

II. BASE LEGAL

2.1. La Constitución Política del Perú.
2.2. Ley Nº 30220, Ley Universitaria del Perú
2.3. Texto Único Ordenado de la Ley Nº 27444, Ley del Procedimiento Administrativo General, aprobado mediante Decreto Supremo Nº 004-2019-JUS.
2.4. Estatuto de la Unheval, aprobado con la Resolución Asamblea Universitaria Nº 0006-2022-UNHEVAL.
2.5. Resolución Consejo Universitario Nº 1478-2022-UNHEVAL-Lineamientos para la Elaboración y Aprobación de Reglamentos Internos y Directivas en la Universidad Nacional Hermilio Valdizán.

III. APRECIACIÓN JURÍDICA

3.1. Que, en el cuarto párrafo del artículo 18° de la Constitución Política del Perú, prescribe lo siguiente:
Artículo 18 Educación universitaria
La educación universitaria tiene como fines la formación profesional, la difusión cultural, la creación intelectual y artística y la investigación científica y tecnológica. El Estado garantiza la libertad de cátedra y rechaza la intolerancia.
Las universidades son promovidas por entidades privadas o públicas. La ley fija las condiciones para autorizar su funcionamiento. La universidad es la comunidad de profesores, alumnos y graduados. Participan en ella los representantes de los promotores, de acuerdo con ley.
Cada universidad es autónoma en su régimen normativo, de gobierno, académico, administrativo y económico. Las universidades se rigen por sus propios estatutos en el marco de la Constitución y de las leyes.

3.2. Que, del numeral 1.1 del Articulo IV del título Preliminar del Texto Único Ordenado de la Ley N° 27444 Ley del Procedimiento Administrativo General, se refiere respecto al principio de Legalidad de la siguiente forma:
Artículo IV. Principios del procedimiento administrativo
1.1. *Principio de legalidad.* *- Las autoridades administrativas deben actuar con respeto a la Constitución, la ley y al derecho, dentro de las facultades que le estén atribuidas y de acuerdo con los fines para los que les fueron conferidas.*

Av. Universitaria 601-607 Cayhuayna – Pillco Marca, Apartado 278 - Pabellón Central Block "A" Segundo Piso - Telf. (062)591063, Anexo 0114
correo: secretariageneral@unheval.edu.pe

///... RESOLUCIÓN RECTORAL Nº 0474-2023-UNHEVAL -02-

3.3. Que, del numeral 3) del artículo IV del título Preliminar del Texto Único Ordenado de la Ley N° 27444 Ley del Procedimiento Administrativo General, prescribe lo siguiente:
1.3. Principio de impulso de oficio.- *Las autoridades deben dirigir e impulsar de oficio el procedimiento y ordenar la realización o práctica de los actos que resulten convenientes para el esclarecimiento y resolución de las cuestiones necesarias.*

3.4. Que, el literal b) del Artículo Nº 119° del Estatuto de la Universidad Nacional Hermilio Valdizan, prescribe que:
"El Consejo Universitario tiene las siguientes atribuciones:
(...)
b) Aprobar el reglamento general de la UNHEVAL, el reglamento de elecciones y otros reglamentos internos especiales, así como vigilar su cumplimiento".

3.5. Que, el numeral 7.1 del Artículo 7 de la Directiva Nº 001-2022- UNHEVAL/OPyP/UPPyM, muestra los alcances respecto a la formulación de reglamentos o directivas internas:
7.1. FORMULACIÓN DE REGLAMENTOS O DIRECTIVAS INTERNAS
7.1.1. A iniciativa propia o por recomendación de la Oficina de Planeamiento y Presupuesto a través de la Unidad de Planeamiento, Presupuesto y Modernización; los órganos o unidades orgánicas de la UNHEVAL, formulan proyectos de reglamentos o directivas relacionadas con sus competencias, denominándose "Órganos Proponentes.
7.1.2. El órgano proponente remite a la Oficina de Planeamiento y Presupuesto el expediente conteniendo el proyecto de reglamento o directiva, adjuntando un informe sustentatorio que justifique la necesidad de su aprobación. en caso de que los órganos proponentes sean unidades orgánicas, la remisión del expediente a la Oficina de Planeamiento y Presupuesto se realizará a través de /os órganos de /os que dependen y con su visto bueno.
7.1.3. Previo a ello el órgano proponente debe realizar las coordinaciones necesarias con los órganos de la UNHEVAL que estén vinculados o articulados con el objetivo del reglamento o directiva, con el fin de establecer las responsabilidades y recoger las opiniones y sugerencias que permitan su mejor aplicación o cumplimiento. Como medio probatorio deberá considerarse como anexo al informe sustentatorio el Anexo Nº 04, Acta de reunión que participaron en la formulación del reglamento o directiva.
7.1.4. La Oficina de Planeamiento y Presupuesto a través de la Unidad de Planeamiento, Presupuesto y Modernización revisa el expediente y, de ser el caso observa la misma, debiendo devolver el expediente al órgano proponente, para el levantamiento de las observaciones y de ser el caso entablar las coordinaciones necesarias con el Órgano proponente a fin de que levante las observaciones que se hayan formulado.
7.1.5. Si la Oficina de Planeamiento y Presupuesto a través de la Unidad de Planeamiento, Presupuesto y Modernización no tiene observaciones o estas han sido subsanadas, emite opinión técnica favorable y deriva el expediente, con el proyecto de la directiva debidamente visada, a la Oficina de Asesoría Jurídica. Tanto la devolución del expediente al Órgano Proponente como la emisión de la opinión favorable de la Oficina de Planeamiento y Presupuesto a través de la Unidad de Planeamiento, Presupuesto y Modernización, ser realizan en el plazo máximo de siete (7) días hábiles, contados a partir de la recepción del expediente.
7.1.6. La Oficina de Asesoría Jurídica revisa el expediente y emite opinión legal. Si la opinión es favorable, remite el expediente al órgano que debe aprobar el reglamento o la directiva, para que continúe con el procedimiento para su aprobación, previa visación del documento normativo; en caso de que previa a su aprobación requiera la emisión de resolución de aprobación de propuesta por el órgano proponente remitirá el expediente al mismo.
7.1.7. La Oficina de Asesoría Jurídica, de ser el caso observa el proyecto del reglamento o directiva, debiendo devolver el expediente al órgano proponente, para el levantamiento de las observaciones y de ser el caso entablar las coordinaciones necesarias con el Órgano proponente a fin de que levante las observaciones que se hayan formulado.
7.1.8. La Oficina de Asesoría Jurídica debe emitir su opinión en un plazo máximo de siete (07) días hábiles, contados a partir de la recepción del expediente.
7.2. DE LA APROBACIÓN DE REGLAMETNO Y DIRECTIVAS INTERNAS
7.2.1. El reglamento o la directiva, puede ser aprobada por el Consejo Universitario, Rector, Vicerrector Académico, Vicerrector de Investigación, Consejo de Facultad, Decano, Direcciones o Jefaturas Administrativas, en el marco de su competencia.
(...)

3.6. La presente Directiva tiene por finalidad normar el uso de las tecnologías de información y comunicación en las diversas dependencias de la Universidad Nacional Hermilio Valdizán para que sean utilizadas de manera eficiente y responsable.

3.7. Que, asimismo, es preciso mencionar que la presente directiva tiene un alcance institucional, es decir que abarca a todas las oficinas administrativas y académicas, con ello al personal docente, personal no docente y alumnos de la universidad.

3.8. Respecto a la revisión del expediente administrativo que contiene la DIRECTIVA Nº 002-2023-

MLCB/sec

...///

UNHEVAL-OTI, "USO DE LAS TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES", se puede señalar que el contenido del proyecto se encuentran dentro de las pautas expuestas en la Directiva Nº 001- 2022-UNHEVAL-UOPyP/UPPyM- Lineamientos para la elaboración y aprobación de Reglamentos Internos y Directivas de la Universidad Nacional Hermilio Valdizán, aprobado mediante la Resolución Consejo Universitario Nº 1478-2022- UNHEVAL, en tanto que corresponde emitir acto resolutivo, la misma que sea aprobado por Consejo Universitario.

IV. CONCLUSIÓN

Teniendo en cuenta los considerandos anteriormente expuestos, la Oficina de Asesoría Jurídica opina que se emita acto resolutivo, con cargo a dar cuenta en el Consejo Universitario, conforme a sus atribuciones los siguientes términos:

4.1. APROBAR la DIRECTIVA Nº 002-2023-UNHEVAL-OTI, "USO DE LAS TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES"; que consta de seis (06) numerales, dos (02) disposiciones complementarias y finales y un (01) anexo.

4.2. DAR A CONOCER, el acto resolutivo a las unidades orgánicas y unidades funcionales competentes;

Que el rector remite el caso a Secretaría General, con el Proveído Nº 002348-2023-UNHEVAL-RECT, para que se emita la resolución correspondiente, **CON CARGO A DAR CUENTA AL CONSEJO UNIVERSITARIO**;

Estando a las atribuciones conferidas al rector por la Ley Universitaria N° 30220; por el Estatuto y el Reglamento General de la Unheval; por la Resolución N° 067-2021-UNHEVAL-CEU, del 09.AGO.2021, del Comité Electoral Universitario de la Unheval, que proclamó y acreditó, a partir del 02.SET.2021 hasta el 01.SET.2026, al rector y vicerrectores de la Unheval; asimismo, teniendo en cuenta el Oficio Nº 5224-2021-SUNEDU-02-15-02, emitido por la Unidad de Registro de Grados y Títulos de la Sunedu, a través del cual se informa el registro de datos de las autoridades de la Unheval; la Resolución Rectoral N° 0737-2022-UNHEVAL, del 22.JUN.2022, que encargó las funciones de secretaria general de la Unheval a la Lic. Ninfa Yolanda Torres Munguia, coordinadora de la Unidad Funcional de Archivo Central, a partir del 23.JUN.2022 hasta que se designe al titular;

SE RESUELVE:

1º. APROBAR la **DIRECTIVA N° 002-2023-UNHEVAL/OTI "USO DE LAS TECNOLOGÍAS DE INFORMACIÓN Y DE COMUNICACIONES DE LA UNIVERSIDAD NACIONAL HERMILIO VALDIZÁN"**, la misma que forma parte integrante de la presente Resolución, que consta de seis (06) numerales, dos (02) disposiciones complementarias y finales y un (01) anexo; por lo expuesto en los considerandos precedentes.

2º. DISPONER que el Vicerrectorado Académico, el Vicerrectorado de Investigación, la Dirección de la Escuela de Posgrado, los decanatos de las facultades, la Dirección General de Administración, la Oficina de Tecnología de la Información, y los demás órganos, unidades orgánicas y unidades funcionales competentes adopten las acciones conforme a sus funciones y/o atribuciones.

3º. DAR A CONOCER la presente Resolución a los órganos, unidades orgánicas y unidades funcionales competentes.

Regístrese, comuníquese y archívese.

UNIVERSIDAD NACIONAL HERMILIO VALDIZÁN HUÁNUCO RECTOR

Dr. GUILLERMO A. BOCANGEL WEYDERT
RECTOR

UNIVERSIDAD NACIONAL HERMILIO VALDIZÁN SECRETARIA GENERAL

Lic. NINFA Y. TORRES MUNGUIA
SECRETARIA GENERAL (E)

Lo que transcribo a usted para su conocimiento y demás fines.

Lic. Adm. Ninfa Y. Torres Munguia
SECRETARIA GENERAL (E)

Distribución:
AU-Rectorado
VRAcad
VRInv-OAJ-OCI
Transparencia
DIGA-OGC-OPyP
DAySA-OTI
URH.-UEyC
UnidadesFunctionales
UnidadesÓrganicas
Facultades (14)
Archivo

MLCB/sec

DIRECTIVA N° 002-2023-UNHEVAL-OTI

USO DE LAS TECNOLOGÍAS DE INFORMACIÓN Y DE COMUNICACIONES

Universidad Nacional Hermilio Valdizán
OFICINA DE TECNOLOGÍAS DE LA INFORMACIÓN
HUÁNUCO

DIRECTIVA N° 002-2023-UNHEVAL/OTI

USO DE LAS TECNOLOGIAS DE INFORMACION Y DE COMUNICACIONES

I. OBJETIVO

Normar el uso de las tecnologías de información y comunicación en las diversas dependencias de la Universidad Nacional Hermilio Valdizán para que sean utilizados de manera eficiente y responsable.

II. ALCANCE

La aplicación de la presente normativa es de alcance institucional, es decir abarca todas las oficinas administrativas y académicas, con ello al personal docente, personal no docente y alumnos de la universidad.

III. BASE LEGAL

3.1. Ley N° 27658, Ley Marco de Modernización de la Gestión del Estado.
3.2. Ley N° 30220, Ley Universitaria.
3.3. Decreto Supremo N° 050-2018-PCM, aprueban la definición de seguridad digital en el ámbito nacional.
3.4. Decreto Supremo N° 029-2021-PCM, aprueba el Reglamento del Decreto Legislativo N° 1412, Decreto Legislativo que aprueba la Ley de Gobierno Digital, y establece disposiciones sobre las condiciones, requisitos y uso de las tecnologías y medios electrónicos en el procedimiento administrativo.
3.5. Decreto Legislativo N° 1412, aprueban la Ley de Gobierno Digital.
3.6. Resolución de Consejo Universitario N° 0680-2021-UNHEVAL, dispone la implementación de la estructura orgánica establecido en el Estatuto de la UNHEVAL.
3.7. Resolución de Asamblea Universitaria N° 0006-2022-UNHEVAL, aprueba el Estatuto de la Universidad Nacional Hermilio Valdizán de Huánuco.
3.8. Resolución Consejo Universitario N° 0469-2023-UNHEVAL, aprueba el Reglamento General de la Universidad Nacional Hermilio Valdizán.

IV. RESPONSABILIDADES

4.1. La **Oficina de Tecnologías de la Información** incluso sus unidades funcionales, tiene las siguientes responsabilidades:

4.1.1. Supervisar y asegurar la implementación de los sistemas de información en los servidores de la universidad.

4.1.2. Supervisar el funcionamiento de los sistemas de información.

4.1.3. Asegurar el funcionamiento del servidor en donde se despliegue el sistema de información.

4.1.4. Asegurar la operatividad del cableado de red.

4.1.5. Realizar los mantenimientos preventivos programados de los equipos informáticos con el objetivo de contar con los equipos informáticos operativos.

4.1.6. Realizar los mantenimientos correctivos de los equipos informáticos en cuanto se presente la situación. De acuerdo con el nivel de gravedad de la eventualidad el servicio puede ser tercerizado.

4.1.7. Realizar la gestión de adquisición de repuestos para poner en operatividad los equipos informáticos, ello dependerá de la disponibilidad presupuestal.

4.1.8. Todo trabajo de cableado estructurado deberá ser realizado o verificado por personal técnico informático de la Unidad Funcional de Telecomunicaciones y Sistemas.

4.1.9. Configurar los permisos de acceso a la red y a los archivos compartidos para limitar el acceso solo a las personas que necesitan tenerlo.

4.1.10. Establecer y seguir políticas de uso de la red claras y eficaces, y educar a los usuarios sobre las mejores prácticas de seguridad y uso adecuado de la red.

4.1.11. Limitar el acceso a la red a aquellos que necesiten usarla para su trabajo y establecer políticas claras para el uso de dispositivos personales en la red.

4.1.12. Monitorizar el tráfico de red y establecer alertas para detectar actividad sospechosa o inusual.

4.1.13. Deshabilitar o limitar el acceso a puertos y servicios que no sean necesarios para el trabajo diario, para reducir el riesgo de ataques externos.

4.1.14. Utilizar protocolos de seguridad de red, como WPA2 para redes Wi-Fi, y SSL/TLS para sitios web, para cifrar la información que se transmite por la red.

4.1.15. Configurar los routers y switches de la red para utilizar la última tecnología de seguridad, como la autenticación basada en certificados.

4.2. El personal docente, personal no docente y alumnos de la UNHEVAL, tienen las siguientes responsabilidades:

4.2.1. Cuidar la integridad física de los equipos de cómputo y/o informáticos a su cargo.

4.2.2. Hacer un buen uso de los equipos informáticos (computadoras, impresoras, teléfonos IP, proyectores multimedia y demás accesorios) solo con fines institucionales.

4.2.3. Mantener la configuración inicial de los equipos informáticos y del software involucrado.

4.2.4. Solicitar a OTI el soporte técnico informático cuando sea necesario.

4.2.5. Utilizar solamente los programas instalados en los equipos de cómputo.

4.2.6. No instalar programas informáticos adicionales en los equipos de cómputo.

4.2.7. Salvaguardar oportunamente la información contenida en los equipos informáticos, cuya copia de seguridad es por cuenta de los usuarios.

4.2.8. Salvaguardar las claves y/o contraseñas de los servicios

4.2.9. Navegar con responsabilidad por la web

4.2.10. No utilizar los equipos de cómputo para juegos.

4.2.11. No utilizar para redes sociales con fines personales y otros que no sean los institucionales.

4.2.12. Custodiar los bienes informáticos a cargo del trabajador.

4.2.13. Cada usuario de los equipos informáticos es responsable del correcto encendido y apagado de los mismos con el objetivo de prevenir los deterioros por corte intempestivo de la energía eléctrica.

4.2.14. Ningún usuario se encuentra autorizado a desarmar los equipos informáticos y/o cambiar accesorios a excepción del personal técnico informático de la Unidad Funcional de Mantenimiento y Soporte de Tecnologías de Información o de la Unidad Funcional de Telecomunicaciones y Sistemas.

4.2.15. No compartir las claves personales de acceso a los sistemas de información.

V. DISPOSICIONES GENERALES

5.1. DEFINICIONES

CONFIGURACION: En informática, la configuración es un conjunto de datos que determina el valor de algunas variables de un programa informático o de un sistema operativo. Estas opciones generalmente se cargan durante el inicio del programa y en algunos casos es necesario reiniciarlo para poder ver los cambios.

CONTRASEÑA Una contraseña o clave es una forma de autentificación que utiliza información secreta para controlar el acceso hacia algún recurso. La contraseña debe mantenerse en secreto ante aquellos a quien no se les permite el acceso.

COPIA DE SEGURIDAD: Una copia de seguridad es una copia de los datos originales que se realiza con el fin de protegerlos en caso de pérdida o daño. Las copias de seguridad se pueden realizar en diferentes medios, como discos duros externos, unidades flash USB, discos compactos o DVD. También se pueden realizar copias de seguridad en línea o en la nube.

EQUIPO DE COMPUTO: El equipo de cómputo se refiere a los mecanismos y al material de computación que está adjunto a él. Es un sistema informático de componentes electrónicos que en conjunto proporcionan datos de salida procesados mediante ecuaciones matemáticas. Los principales componentes se dividen en hardware y software. El hardware corresponde a todas las partes físicas de la computadora, como el ratón, el teclado y el monitor. El hardware también puede incluir una impresora, bocinas, micrófono y otros dispositivos periféricos.

EQUIPO INFORMATICO: Un equipo informático es un dispositivo o conjunto de dispositivos electrónicos que permiten procesar información de forma rápida y eficiente mediante programas informáticos. Un equipo informático está compuesto por hardware y software, que son la parte tangible e intangible del ordenador, respectivamente. Los equipos informáticos pueden tener también equipos auxiliares, como impresoras, que se conectan al ordenador y conforman un espacio de trabajo.

HARDWARE: El hardware es la parte física de un sistema informático. Se refiere a las partes físicas, tangibles, de un sistema informático, sus componentes eléctricos, electrónicos, electromecánicos y mecánicos.

MALWARE: El malware es un término que se utiliza para referirse a software malicioso, es decir, programas de computadora diseñados con la intención de dañar, alterar o acceder sin

autorización a un sistema informático o a los datos almacenados en él. El término "malware" es una combinación de las palabras "malicioso" y "software".

MANTENIMIENTO CORRECTIVO: El mantenimiento correctivo de equipos informáticos se refiere a las acciones y procedimientos realizados para reparar y solucionar problemas que han surgido en los equipos informáticos. Estas intervenciones se llevan a cabo después de que se haya producido una avería, fallo o mal funcionamiento en el equipo. El objetivo principal del mantenimiento correctivo es restablecer el funcionamiento normal del equipo y asegurar que vuelva a estar en condiciones óptimas para su uso.

MANTENIMIENTO PREVENTIVO: El mantenimiento preventivo de equipos informáticos se refiere a las acciones planificadas y regulares realizadas para prevenir problemas y mantener el buen funcionamiento de los equipos, con el objetivo de evitar averías y maximizar su rendimiento y vida útil.

PHISHING: El phishing es una forma de ataque cibernético en la que los delincuentes se hacen pasar por entidades legítimas, como bancos, empresas o instituciones, con el objetivo de engañar a los usuarios y obtener información confidencial, como contraseñas, números de tarjetas de crédito o datos personales.

Los atacantes de phishing suelen utilizar técnicas de ingeniería social para engañar a las personas y hacer que revelen sus datos sensibles. Esto se logra mediante el envío de correos electrónicos fraudulentos que parecen legítimos, mensajes de texto, llamadas telefónicas o incluso mediante la creación de sitios web falsos que imitan la apariencia de sitios web auténticos.

PUNTO DE ACCESO: Un punto de acceso es un dispositivo que permite a otros dispositivos conectarse a Internet o a una red local, ya sea por cable o por Wi-Fi. Un punto de acceso recibe, almacena y transmite la información entre la red inalámbrica y la red cableada, y puede soportar varios usuarios y distancias. Un punto de acceso puede formar parte de una red corporativa que se gestiona por un controlador de WLAN que regula la potencia, los canales, la autenticación y la seguridad.

PUNTO DE RED: Un punto de conexión de red (PCR) es un cajetín blanco que se instala en el punto donde se empalma el cable de red interior del edificio, en ella se conecta algún equipo informático que tenga funcionalidad de red.

RANSOMWARE: El ransomware es un tipo de malware malicioso que cifra los archivos y datos de un sistema informático, impidiendo el acceso a ellos y exigiendo un rescate económico

(generalmente pagado en criptomonedas) para proporcionar la clave de descifrado. Este tipo de ataque busca extorsionar a las víctimas, bloqueando el acceso a sus archivos y causando daños significativos a nivel empresarial o personal, ya que los archivos cifrados pueden resultar inaccesibles o incluso borrados si no se paga el rescate.

SEGURIDAD DIGITAL: la seguridad digital en el ámbito nacional es el estado de confianza en el entorno digital que resulta de la gestión y aplicación de un conjunto de medidas proactivas y reactivas frente a los riesgos que afectan la seguridad de las personas, la prosperidad económica y social, la seguridad y los objetivos nacionales en dicho entorno.

SISTEMA DE INFORMACION: Es un conjunto de datos que interactúan entre sí con un fin común. En informática, los sistemas de información ayudan a administrar, recolectar, recuperar, procesar, almacenar y distribuir información relevante para los procesos fundamentales y las particularidades de cada organización.

SOFTWARE: El software es el conjunto de programas de cómputo, procedimientos, reglas, documentación y datos asociados que forman parte de las operaciones de un sistema de computación.

SOFTWARE LIBRE: es aquel cuya licencia de uso garantiza las facultades de:

- Uso irrestricto del programa para cualquier propósito;
- Inspección exhaustiva de los mecanismos de funcionamiento del programa;
- Confección y distribución de copias del programa; y,
- Modificación del programa y distribución libre tanto de las alteraciones como del nuevo programa resultante, bajo estas mismas condiciones.

SOFTWARE PROPIETARIO: es aquel cuya licencia de uso no permite ninguna o alguna de las facultades previstas en la definición anterior.

SOPORTE TÉCNICO: es un grupo de servicios que proveen asistencia técnica para hardware, software u otros bienes electrónicos o mecánicos, ayudando al usuario a resolver cualquier tipo de problema que surja en el uso de este.

SWITCH: Un switch es un dispositivo que permite que la conexión de computadoras y periféricos a la red para que puedan comunicarse entre sí y con otras redes. Switch es una palabra en

inglés usada en el área de informática para referirse al controlador de interconexión entre varios dispositivos.

TELEFONO IP: Un teléfono IP es un teléfono que utiliza la tecnología de voz sobre IP (VoIP) para hacer y recibir llamadas telefónicas. En lugar de utilizar una línea telefónica tradicional, los teléfonos IP se conectan a Internet y utilizan una conexión de banda ancha para enviar y recibir señales de voz. Los teléfonos IP pueden ser hardware o software y se utilizan en entornos empresariales y domésticos.

VI. DISPOSICIONES ESPECIFICAS

a. USO DE EQUIPOS INFORMÁTICOS

El personal docente, personal no docente, alumnos, que hagan uso de los equipos informáticos como computadoras, impresoras, proyectores multimedia y otros equipos informáticos deben cumplir con las siguientes disposiciones:

1. Los equipos informáticos deberán ser utilizados solamente por personal autorizado y que pertenezca a la universidad; en el caso específico de las oficinas administrativas el uso de los equipos informáticos es por parte del personal que tiene a su cargo dichos bienes, en el caso de ambientes académicos los equipos de cómputo son utilizados por los docentes y alumnos en cuanto sea permitido.
2. Los usuarios en general especialmente los que se encuentran a cargo se encuentran obligados a la custodia de los bienes a su cargo.
3. Los usuarios en general deben respetar los correctos encendidos y apagados de los equipos evitando a toda costa utilizar como método de apagado el corte de la energía eléctrica. En caso de deterioro de los equipos de cómputo por inadecuado apagado será de responsabilidad del usuario.
4. Mantener el equipo actualizado con las últimas versiones de software y sistema operativo. Para ello solicitar los servicios de los técnicos informáticos de la Unidad Funcional de Mantenimiento y Soporte de Tecnologías de la Información.
5. Los equipos de cómputo deberán contar con programas antivirus y realizar regularmente escaneos de tu equipo para detectar y eliminar posibles amenazas.
6. Realizar copias de seguridad de los archivos importantes con regularidad.

7. Usar contraseñas seguras para las cuentas y cambiar las contraseñas periódicamente.
8. Evitar descargar archivos o programas de sitios web no confiables o desconocidos.
9. Cerrar sesión de las cuentas en cuando se termine de usarlas y no se debe dejar abierta en dispositivos públicos o compartidos.
10. Limpiar regularmente los archivos temporales, cachés y cookies de tu equipo para liberar espacio de almacenamiento y mejorar el rendimiento.
11. Usar un protector de pantalla y configura la suspensión de pantalla y la hibernación para ahorrar energía y prolongar la vida útil de la batería en laptops y dispositivos móviles.
12. No dejar el equipo expuesto al polvo, la humedad o temperaturas extremas.
13. Ningún usuario no autorizado debe desarmar los equipos informáticos, solo el personal técnico informático de la Unidad Funcional de Mantenimiento y Soporte de Tecnologías de la Información o de la Unidad Funcional de Telecomunicaciones y Sistemas podrá realizar dicha operación.
14. Si se tiene problemas o dudas acerca del equipo, se debe contactar a un profesional de soporte técnico capacitado para ayudarte.
15. No se debe utilizar los equipos informáticos de la universidad con fines particulares.
16. En caso se requiera soporte técnico informático, se debe contactar con la Oficina de Tecnologías de la Información o utilizar el aplicativo Registro de Incidentes y Solicitudes cuyo enlace es https://soporte.unheval.edu.pe

b. USO DE LA RED Y TELEFONÍA

Cada equipo informático con funcionalidad de conexión a red y que se encuentra conectado a la red de la universidad cuenta con una dirección IPv4 única y se encuentra conectado a un punto de red en específico; el personal docente, personal no docente y alumnos deben seguir las siguientes disposiciones:

1. Mantener los equipos actualizados con las últimas versiones de software y sistema operativo, y aplicar los parches de seguridad de manera regular, para ello apoyarse en el personal técnico informático de la Unidad Funcional de Mantenimiento y Soporte de Tecnologías de la Información.

2. Los equipos de cómputo deberán contar con programas antivirus y firewalls para proteger la red y los equipos conectados.
3. Cualquier trabajo de cableado estructurado deberá ser realizado y/o supervisado por personal de la Unidad Funcional de Telecomunicaciones y Sistemas.
4. Ningún usuario deberá cambiar las direcciones IPv4 asignados a los equipos informáticos, el único personal autorizado a realizar dichos cambios es el personal de la Oficina de Tecnologías de la Información.
5. Ningún usuario de la universidad podrá modificar, trasladar, adicionar los puntos de red de la universidad, solo el personal de la Oficina de Tecnologías de la Información puede realizar las modificaciones de ser necesario.
6. Ningún usuario se encuentra autorizado a adicionar dispositivos de red como switches, routers, Access point y/o tarjetas inalámbricas en la red de la universidad, solo lo puede realizar el personal de la Oficina de Tecnologías de la Información.
7. Configurar contraseñas seguras para los equipos y dispositivos conectados, y cambiarlas periódicamente.
8. Realizar copias de seguridad regulares de los datos importantes, preferiblemente fuera de la red, para protegerlos de posibles pérdidas.
9. No compartir información confidencial a través de la red, y encriptar la información que se transmite si es posible.
10. Evitar descargar o instalar software o archivos de fuentes no confiables o desconocidas.
11. No abrir correos electrónicos, enlaces o archivos adjuntos sospechosos, ya que pueden contener virus o malware.
12. Evitar conectarse a redes Wi-Fi públicas no seguras, especialmente al hacer transacciones financieras o ingresar información personal.
13. No compartir contraseñas de la red o de los dispositivos conectados con otros usuarios.
14. Establecer contraseñas seguras para los dispositivos y cambiarlas periódicamente.
15. Evitar descargar archivos sospechosos o de origen desconocido.
16. No compartir información confidencial, como información financiera o de identidad, a través de la red sin asegurarse de que la comunicación esté encriptada.
17. Evitar visitar sitios web no seguros o desconocidos.
18. El uso de la telefonía IP es exclusivamente para fines de carácter institucional.
19. Se debe evitar el cambio constante de la ubicación de los equipos informáticos dado que estos se encuentran

reconocidos y asignados a un punto de red determinado y al hacer estos cambios se va a perder la conexión a la red.

20. Se debe priorizar la ubicación de los equipos que se conectan a la red para que vaya acorde con la ubicación de los puntos de red.

Se debe tener presente que los usuarios finales también pueden contribuir significativamente a la seguridad y el buen uso de la red y los equipos conectados, siguiendo estas recomendaciones y siendo conscientes de los posibles riesgos y amenazas de seguridad.

c. USO DEL SERVICIO DE INTERNET

Todos los equipos informáticos con funcionalidades de red y que se encuentran conectados a la red de la universidad cuenta con acceso al internet o acceso potencial.
El personal docente, personal no docente y los alumnos en general deberán cumplir las siguientes disposiciones:

1. Mantener contraseñas seguras: Es importante utilizar contraseñas fuertes y únicas para cada cuenta. Se recomienda combinar letras mayúsculas y minúsculas, números y caracteres especiales. Además, se aconseja cambiar las contraseñas periódicamente y evitar el uso de información personal obvia.

2. Mantener el software actualizado: Es fundamental mantener el sistema operativo, los navegadores y las aplicaciones actualizadas con las últimas versiones. Esto ayuda a proteger los dispositivos contra vulnerabilidades conocidas.

3. Tener precaución con los correos electrónicos sospechosos: Es importante no hacer clic en enlaces ni descargar archivos adjuntos de correos electrónicos no solicitados o de remitentes desconocidos. Estos correos podrían contener malware o intentar realizar phishing.

4. Utilizar una solución de seguridad confiable: Se recomienda instalar un software antivirus y un firewall en los dispositivos para protegerse contra el malware y los ataques cibernéticos. La Oficina de Tecnologías de la Información a través de su personal técnico informático realizará la instalación de software antivirus en función de su disponibilidad.

5. Verificar la autenticidad de los sitios web: Antes de proporcionar información personal o financiera en un sitio web, es

fundamental verificar su autenticidad. Se debe buscar el candado en la barra de direcciones y utilizar sitios web con conexiones seguras (https://).

6. Ser consciente de la ingeniería social: Los ciberdelincuentes pueden intentar engañar a las personas para obtener información confidencial. Por lo tanto, se debe ser cauteloso al responder a solicitudes de información personal o financiera por teléfono, correo electrónico o mensajes.

7. Evitar el uso de redes Wi-Fi públicas no seguras: Las redes Wi-Fi abiertas en lugares públicos pueden ser inseguras. Se recomienda evitar realizar transacciones financieras o acceder a información confidencial cuando se está conectado a estas redes.

8. Mantener respaldos de los datos: Realizar copias de seguridad regulares de los archivos importantes es una práctica recomendada. Se pueden utilizar servicios en la nube o dispositivos de almacenamiento externos para protegerse en caso de pérdida de datos o ataques de ransomware.

9. Reportar incidentes de seguridad: Si se sospecha de un posible incidente de seguridad o se detecta actividad sospechosa en el dispositivo, informar inmediatamente a la Oficina de Tecnologías de la Información.

10. Participar en la formación en seguridad: Aprovechar las oportunidades de capacitación y educación en seguridad cibernética que brinde la empresa. Mantenerse informado sobre las mejores prácticas de seguridad y contribuir a crear una cultura de seguridad en el entorno empresarial.

11. No se encuentra permitido el acceso a redes sociales con fines particulares durante el horario laboral en los equipos de la institución.

12. No se permite el uso del servicio de internet para juegos en línea, descarga de programas en general; en caso de necesitarlo contactar con la Oficina de Tecnologías de la Información.

d. SANCIONES

1. Los usuarios de los equipos informáticos que tienen la asignación de estos son responsables de la seguridad de su equipo, por lo que un uso incorrecto de su equipo informático

ocasionando daño en el mismo será responsabilidad del usuario y susceptible de ser sancionado y amonestado por el ente correspondiente.

2. Si algún usuario realiza cambios de partes o extrae las partes de un equipo informático sin la autorización y conocimiento de la Oficina de Tecnologías de la Información será considerado sujeto a sanción.
3. Si por negligencia del usuario se deteriora el equipo informático y/o pone en riesgo la seguridad en el entorno de trabajo será sancionado de acuerdo con la gravedad de la falta.
4. En el caso de la pérdida y/o robo de equipos informáticos por negligencia del trabajador responsable será sancionado de forma administrativa además de que es responsable de la reposición del bien.
5. Será motivo de sanción si por las acciones negligentes de un trabajador se pone en riesgo a la red informática y sus componentes de la universidad.

VII. DISPOSICIONES COMPLEMENTARIAS Y FINALES

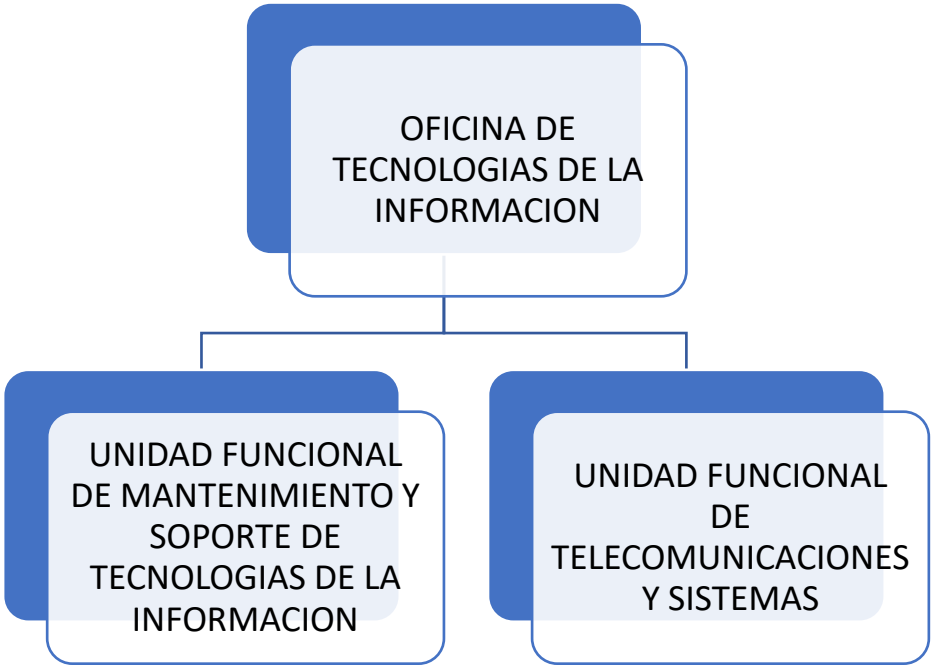
Primera: Con la entrada en vigor de la presente directiva se deroga la Directiva N° 002-2017-UNHEVAL/DI.

Segunda: La Secretaría Técnica es el encargado de precalificar las presuntas faltas, y de realizar todo el proceso de investigación y sanción en coordinación con la Unidad de Recursos Humanos.

VIII. ANEXOS

ANEXO A

ESTRUCTURA DE LA OFICINA DE TECNOLOGIAS DE LA INFORMACION[1]



[1] Se aprueba la creación de las unidades funcionales mediante RESOLUCIÓN CONSEJO UNIVERSITARIO N° 1259-2021-UNHEVAL