

UNIVERSIDAD NACIONAL HERMILIO VALDIZAN



Plan de Seguridad de la Información

v 1.0

ELABORADO POR
OFICINA DE TECNOLOGÍAS DE LA
INFORMACIÓN

INTRODUCCION

La seguridad de la información es el conjunto de medidas y prácticas diseñadas para proteger la confidencialidad, integridad y disponibilidad de los datos y sistemas de información en cualquier tipo de organización, ya sea una empresa, una institución gubernamental, una universidad o cualquier otro entorno.

El objetivo principal de la seguridad de la información es garantizar que la información esté protegida contra accesos no autorizados, alteraciones malintencionadas o pérdidas accidentales. Para lograr esto, se implementan diferentes controles, políticas, procedimientos y tecnologías que ayudan a prevenir, detectar y responder a amenazas y vulnerabilidades.

La seguridad de la información es de vital importancia en un entorno universitario por diversas razones:

1. **Protección de datos personales:** Las universidades recopilan y almacenan una gran cantidad de datos personales de estudiantes, profesores, personal administrativo y otros miembros de la comunidad académica. La seguridad de esta información es esencial para evitar el robo de identidad, el fraude y otras formas de abuso de datos personales.
2. **Confidencialidad de la investigación:** Las universidades llevan a cabo investigaciones en diversos campos, algunas de las cuales pueden ser sensibles o confidenciales. La seguridad de la información garantiza que los resultados de investigación y los datos asociados estén protegidos de accesos no autorizados y de la divulgación no deseada.
3. **Protección de propiedad intelectual:** Las universidades generan y poseen una gran cantidad de propiedad intelectual, incluyendo patentes, proyectos, tesis, entre otros. La seguridad de la información evita el robo o la apropiación indebida de dichos activos intelectuales.
4. **Continuidad del servicio:** La información es esencial para el funcionamiento diario de una universidad, desde el registro y la gestión académica hasta la administración financiera. La seguridad garantiza que los sistemas y servicios críticos estén disponibles y funcionando adecuadamente, evitando interrupciones y pérdidas de productividad.
5. **Cumplimiento normativo:** Las universidades deben cumplir con regulaciones y leyes relacionadas con la protección de datos y privacidad, como el Reglamento General de Protección de Datos (GDPR) en Europa o leyes de privacidad en otros países. La seguridad de la información es esencial para cumplir con estas regulaciones y evitar posibles sanciones.
6. **Protección contra amenazas cibernéticas:** Las instituciones académicas son objetivos atractivos para los ciberdelincuentes debido a la gran cantidad de información valiosa que manejan. La seguridad de la información ayuda a mitigar el riesgo de ataques cibernéticos, como ransomware, phishing y malware, que podrían tener consecuencias graves para la universidad y sus miembros.
7. **Preservación de la reputación:** Una brecha de seguridad o una filtración de datos pueden dañar la reputación de la universidad y reducir la confianza de estudiantes, profesores y patrocinadores. La seguridad de la información contribuye a mantener una imagen positiva y confiable de la institución.

En resumen, la seguridad de la información en un entorno universitario no solo protege los datos y activos críticos, sino que también garantiza la privacidad y confidencialidad de las personas involucradas, salvaguarda la investigación y propiedad intelectual, y permite un funcionamiento eficiente y confiable de la institución en general.

1. BASE LEGAL

- Ley N° 27658, Ley Marco de Modernización de la Gestión del Estado.
- Decreto Legislativo N° 1412, que aprueba la Ley de Gobierno Digital.
- Decreto Supremo N° 109-2012-PCM, que aprueba la Estrategia para la Modernización de la Gestión Pública.
- Decreto de Urgencia N° 006-2020, que crea el Sistema Nacional de Transformación Digital.
- Decreto de Urgencia N° 007-2020, se aprueba el Marco de Confianza Digital y se dispone medidas para su fortalecimiento.
- 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.

2. OBJETIVO

El presente plan tiene como objetivo establecer políticas, procedimientos, y controles, así como una estructura organizacional para garantizar la integridad, confidencialidad y disponibilidad de los activos de información de la Universidad Nacional Hermilio Valdizán.

3. FINALIDAD

- Planificar las acciones que conduzcan a la implementación de un SGSI.
- Comenzar las acciones a fin de contar con normas, directivas, procedimientos en materia de seguridad de la información.
- Proteger la información de la Universidad Nacional Hermilio Valdizán de las amenazas y peligros a la que se puede encontrar expuesta.
- Proteger contra acceso o uso no autorizado los datos e información, los cuales podrían resultar en un daño significativo a la universidad.

4. ALCANCE

Los Lineamientos de Seguridad de la Información tienen alcance a todos los servidores/as, funcionarios/as y proveedores de servicio bajo contrato que tengan acceso o que desarrollen, adquieran o usen sistemas de información, sistemas y/o datos de la Universidad Nacional Hermilio Valdizán.

Comprende toda la información producida, manejada, transmitida, almacenada y propiedad de la Universidad Nacional Hermilio Valdizán, asimismo, todos los sistemas y datos asociados con el almacenamiento, procesamiento y transmisión de la información, generada por y a favor de la Universidad Nacional Hermilio Valdizán.

5. DEFINICION DE TERMINOS

ACTIVO DE INFORMACIÓN: Un activo es cualquier cosa que tenga valor para una organización. Los activos son los recursos necesarios para que la empresa funcione y consiga los objetivos que se ha propuesto la alta dirección.

AMENAZA: las amenazas son situaciones que desencadenan en un incidente en la empresa, realizando un daño material o pérdidas inmateriales de sus activos de información.

CODIGO MALICIOSO: es un tipo de software diseñado con intenciones dañinas. También conocido como "malware", este código tiene el propósito de causar daño a sistemas informáticos, robar información, propagarse o realizar actividades no autorizadas sin el conocimiento o consentimiento del usuario afectado. Existen diferentes tipos de malware, como virus, gusanos, troyanos, ransomware y spyware, cada uno con características específicas para lograr sus objetivos maliciosos. La presencia de código malicioso en un sistema puede tener consecuencias graves, incluyendo la pérdida de datos, el robo de información confidencial o la afectación del rendimiento del sistema. La prevención y detección temprana de malware son fundamentales para mantener la seguridad y proteger los activos de información.

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 autenticación 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 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.

EVENTO: ocurrencia o cambio de un conjunto de circunstancias en particular. Ocurrencia identificada de un sistema, servicio o estado de la red que indique una posible violación de la seguridad de la información política o falla de los controles, o una situación previamente desconocida que puede ser relevante para la seguridad

GESTIÓN DE INCIDENTES: proceso formal que tiene por finalidad planificar, preparar, identificar, analizar, contener, investigar incidentes de seguridad digital, así como la recuperación y la determinación de acciones correctivas para prevenir incidentes similares, Decreto de Urgencia N° 007-2020.

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.

INCIDENTE DE SEGURIDAD DE INFORMACION: es un evento inesperado o no autorizado que compromete la confidencialidad, integridad o disponibilidad de datos, sistemas o recursos informáticos. Estos incidentes pueden incluir el acceso no autorizado a información confidencial, ataques de malware, intentos de robo de datos, interrupciones del servicio, entre otros. La detección y respuesta oportuna a estos incidentes son esenciales para minimizar el impacto y evitar daños mayores a la seguridad de la información y la continuidad de los servicios. La gestión adecuada de los incidentes de seguridad ayuda a identificar las causas, implementar medidas correctivas y mejorar las defensas para prevenir futuros eventos similares.

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.

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".

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.

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.

VULNERABILIDAD: propiedad intrínseca de algo que deriva en la susceptibilidad a una fuente de riesgo que puede ocasionar un evento con consecuencias. Debilidad de un activo o control que pueden ser explotados por una o más amenazas.

6. ENTORNO DE TI

6.1 Estructura orgánica

La Oficina de Tecnologías de la Información es el órgano de apoyo dependiente del Rectorado; responsable de planificar, implementar y gestionar los sistemas de información, así como la infraestructura tecnológica de informática y comunicaciones de la UNHEVAL.¹

Con RESOLUCIÓN ASAMBLEA UNIVERSITARIA N° 0006-2022-UNHEVAL se aprueba el Estatuto vigente de la UNIVERSIDAD NACIONAL HERMILIO VALDIZAN; en el artículo 203° se indica que la OFICINA DE TECNOLOGIAS DE LA INFORMACION es un órgano dependiente del Rectorado.

Con RESOLUCIÓN RECTORAL N° 0059-2021-UNHEVAL se aprueba el REGLAMENTO DE ORGANIZACIÓN Y FUNCIONES de la UNIVERSIDAD NACIONAL HERMILIO VALDIZAN, en ella se indica el Organigrama de la Institución. En el artículo 56 se establecen las funciones de la oficina.

Por último, con RESOLUCIÓN CONSEJO UNIVERSITARIO N° 1259-2021-UNHEVAL se aprueba la creación de las UNIDADES FUNCIONALES de la UNHEVAL; en lo que concierne a la OFICINA DE TECNOLOGIAS DE LA INFORMACION, se tiene las siguientes Unidades Funcionales²:

¹ Reglamento de Organización y Funciones, artículo 55°. Aprobado mediante Resolución Rectoral N° 0059-2021-UNHEVAL

² Se aprueba la creación de las unidades funcionales mediante RESOLUCIÓN CONSEJO UNIVERSITARIO N° 1259-2021-UNHEVAL.



6.2 Funciones

La Oficina de Tecnologías de la Información es la responsable de planificar, implementar y gestionar los sistemas de información, así como la Infraestructura tecnológica de informática y comunicaciones de la UNHEVAL. Es un órgano de apoyo dependiente del Rectorado y está a cargo de un personal no docente y/o profesional como director, propuesto por el rector y designado por el Consejo Universitario, es cargo de confianza.³

Son funciones y/o atribuciones de la Oficina de Tecnologías de la Información⁴:

- a) formular, evaluar y ejecutar las políticas, planes o documentos de gestión en la entidad en materia de tecnologías de la información y comunicaciones en concordancia con los objetivos institucionales y normativas nacionales;
- b) formular, proponer e implementar planes y políticas de seguridad informática para la protección de las redes, equipos y sistemas de información en la UNHEVAL en concordancia con las políticas de seguridad nacionales;
- c) participar en la formulación del Plan de Gobierno Digital de la UNHEVAL.
- d) formular, dirigir y ejecutar proyectos de implementación/implantación de sistemas de información, así como proyectos de tecnologías de información y comunicaciones;
- e) formular y ejecutar políticas para la administración del equipamiento tecnológico informático institucional que garantice su operatividad, disponibilidad y seguridad;
- f) definir y proponer la arquitectura tecnológica empresarial y el diseño integral para el gobierno digital de la UNHEVAL que mejoren la eficacia y eficiencia de los procesos institucionales;
- g) promover y dirigir la innovación tecnológica de las infraestructuras y sistemas informáticos de la entidad alineado a los avances tecnológicos.

³ Artículo N° 349 del Reglamento de Organización y Funciones aprobado con Resolución Consejo Universitario N° 0469-2023-UNHEVAL.

⁴ Artículo N° 350 del Reglamento de Organización y Funciones aprobado con Resolución Consejo Universitario N° 0469-2023-UNHEVAL.

- h) dirigir el diseño, desarrollo e implantación de los sistemas de información para la gestión digital de la UNHEVAL;
- i) dirigir la administración de la infraestructura tecnológica institucional; y
- j) demás funciones y/o atribuciones que le asigne su superior inmediato en el marco de sus competencias o aquellas que le corresponde por norma expresa.

Por otra parte, La Unidad Funcional de Telecomunicaciones y Sistemas, está a cargo de un personal no docente y/o profesional, como Coordinador, cuyos requisitos se establecen en el respectivo documento de gestión. Es propuesto por el rector y designado por el Consejo Universitario o por la dependencia al cual se le delega dicha atribución, y tiene las siguientes funciones y/o atribuciones:

- a) establecer e implementar políticas de seguridad en el uso de la red por parte de toda la comunidad universitaria;
- b) reportar las fallas presentadas en los equipos y servicios contenidos en el Centro de Datos, además de controlar el tiempo de respuesta del proveedor para la solución del inconveniente y realizar el seguimiento de las reparaciones necesarias;
- c) evaluar las herramientas de software y hardware con la finalidad de optimizar la administración y seguridad de la Red;
- d) elaborar, proponer y aplicar los procedimientos de copias de respaldo y seguridad, de los datos contenidos en los equipos del Centro de Datos;
- e) monitorear el correcto funcionamiento de los diversos servidores que albergan los distintos sistemas informáticos que cuenta la institución;
- f) administrar y velar por la integridad del software base, sistemas operativos y otros componentes de los equipos servidores, así como realizar las coordinaciones con los proveedores que tengan contrato vigente por mantenimiento y soporte de equipo;
- g) proponer y realizar los procedimientos de respaldo y copias de seguridad que garanticen la protección e integridad de los datos procesados por los sistemas de información almacenados en los servidores de la entidad;
- h) implementar estrategias de seguridad para enfrentar con éxito las situaciones de contingencia que garanticen la continuidad de la operatividad de los sistemas de información, seguridad e infraestructura de Base de Datos;
- i) planear los sistemas de información necesarios para implementar con éxito el gobierno digital en la institución;
- j) implementar la infraestructura en la nube (Cloud Computing);
- k) diagnosticar los equipos informáticos necesarios que se encuentran en el Centro de Datos de la UNHEVAL que puedan brindar el adecuado servicio a todos los sistemas informáticos;
- l) realizar el levantamiento de información y análisis para las modificaciones y el diseño de soluciones en equipamiento de telecomunicaciones que permita planificar y administrar eficientemente la infraestructura de red;
- m) verificar el debido cumplimiento de las normas, estándares y directivas, en lo que se refiere a configuración, instalación, mantenimiento de la infraestructura y equipamiento de red (Telefonía, Seguridad, Gestión LAN, WiFi y Control de Acceso);

- n) renovar licencias de equipos informáticos que permita la seguridad de la información y la gestión de los datos;
- o) diseñar y establecer el plano de red de la infraestructura de la UNHEVAL (topología de red física y lógica);
- p) desarrollar y dar soporte a los sistemas de información para lograr la implementación del gobierno digital en la institución;
- q) administrar el sistema de videoconferencia de la UNHEVAL;
- r) apoyo técnico en la revisión de proyectos TIC's o que formen parte de obras de infraestructura, en la fase de perfil, que permita proponer las mejoras del caso;
- s) programar y desplegar los planes de contingencia que garanticen la continuidad de la operatividad de los sistemas de información, seguridad e infraestructura de redes institucional;
- t) actualizar constantemente la página web de la UNHEVAL, con los contenidos más recientes y necesarios para el público y usuario en general;
- u) administrar y mantener operativo los equipos informáticos disponibles en el Centro de Datos de la UNHEVAL y los que forman parte de la red institucional;
- v) administrar y monitorear las herramientas implementadas en el Centro de Datos referente a la seguridad, control de servicios de internet y telefonía;
- w) dirigir y Verificar el mantenimiento preventivo – correctivo del equipamiento e infraestructura de red;
- x) vigilar el debido cumplimiento de las normas y procedimientos del cableado estructurado;
- y) administrar y actualizar los inventarios de Hardware y Software relacionado a la infraestructura y equipamiento de redes;
- z) administrar, gestionar, instalar y mantener los sistemas informáticos y de comunicaciones de los servicios de DNS, DHCP, FTP, Directorio Activo, Proxy, Antivirus y BBDD en los equipos servidores, en las plataformas de Linux y Windows, contenidos en el Centro de Datos;
- aa) administrar y actualizar el inventario de los equipos Servidores y sus respectivas licencias;
- bb) monitorear el acceso al Internet y vigilar el uso correcto por parte de los usuarios de la institución; y
- cc) las demás funciones y/o atribuciones que le asigne el jefe inmediato en el marco de sus competencias o aquellas que le corresponda por norma expresa.

6.3 Infraestructura tecnológica

La infraestructura tecnológica que administra la Oficina de Tecnologías de la Información está compuesta esencialmente por:

- Servidores físicos ubicados en el centro de datos de la universidad.
- Servidores en nube.
- Cortafuegos perimetral de nueva generación.
- Puntos de acceso distribuidos por todo el campus universitario.
- Switches de acceso y switches troncales.

La interconexión de todos los equipos mencionados forma la red UNHEVAL que interconecta los equipos informáticos de las 14 facultades, 27 carreras profesionales, oficinas administrativas, laboratorios de cómputo y otros.

6.4 Sistemas de Información

La universidad cuenta con diversos sistemas de información que apoyan los procesos académicos, de investigación, la gestión administrativa, todos ellos son claves en el desarrollo de las labores universitarias.

NOMBRE DEL SISTEMA INFORMATICO	SISTEMAS DE INFORMACIÓN CON FUNCIONALIDADES DE:	USUARIOS
INTRANET ESTUDIANTE	GESTION ACADEMICA DEL ESTUDIANTE	Estudiantes de la UNHEVAL
INTRANET DOCENTES	GESTION ACADEMICA DEL DOCENTE	Docentes de la UNHEVAL
PAGOS VIRTUALES	GESTION ADMINISTRATIVA	Estudiantes de la UNHEVAL
QUIERO MI DIPLOMA	GESTION ADMINISTRATIVA	Egresados de la UNHEVAL Unidad de Grados y Títulos
SEGUIMIENTO DE EXPEDIENTES	GESTION ADMINISTRATIVA	Trabajadores administrativos de la UNHEVAL, usuarios externos
SISTEMA DE AULA VIRTUAL	GESTION ACADEMICA DE LA UNIVERSIDAD	Estudiantes de la UNHEVAL
SISTEMA DE CALIFICACION PARA ADMISION	GESTION ACADEMICA DE LA UNIVERSIDAD	Trabajadores administrativos de la UNHEVAL
SISTEMA DE CONTROL DE PAGOS DEL CENTRO DE ESTUDIOS INFORMATICOS	GESTION ACADEMICA DE LA UNIVERSIDAD	Centro de Estudios Informáticos
SISTEMA DE ESCALAFON	GESTION ACADEMICA DE LA UNIVERSIDAD	Unidad Funcional de Escalafón y Control
SISTEMA DE GESTION DOCENTE	GESTION ACADEMICA DE LA UNIVERSIDAD	Dirección de Asuntos y Servicios Académicos Docentes de la UNHEVAL
SISTEMA DE RESPONSABILIDAD SOCIAL UNIVERSITARIA	GESTION ACADEMICA DE LA UNIVERSIDAD	Dirección de Proyección Social y Extensión Cultural
SISTEMA INTEGRADO DE GESTION UNIVERSITARIA - MODULO ADMISION	GESTION ACADEMICA DE LA UNIVERSIDAD	Unidad de Admisión
SISTEMA INTEGRADO DE GESTION UNIVERSITARIA - MODULO ASUNTOS ACADEMICOS	GESTION ACADEMICA DE LA UNIVERSIDAD	Dirección de Asuntos y Servicios Académicos Unidad de Procesos Académicos
SISTEMA INTEGRADO DE GESTION UNIVERSITARIA - MODULO CEPRE	GESTION ACADEMICA DE LA UNIVERSIDAD	Centro Preuniversitario
SISTEMA INTEGRADO DE GESTION UNIVERSITARIA - MODULO INGRESOS	GESTION ACADEMICA DE LA UNIVERSIDAD	Unidad Funcional de Ingresos
SISTEMA INTEGRADO DE GESTION UNIVERSITARIA - MODULO POSGRADO	GESTION ACADEMICA DE LA UNIVERSIDAD	Escuela de Posgrado
SISTEMA INTEGRADO DE GESTION UNIVERSITARIA - MODULO REGISTRO CENTRAL	GESTION ACADEMICA DE LA UNIVERSIDAD	Unidad Funcional de Registro Central y Archivo Académico
REPOSITORIO (DSPACE)	GESTION ACADEMICA DE LA UNIVERSIDAD	Dirección de Investigación
SISTEMA DE CMC	GESTION ADMINISTRATIVA	Oficina de Calidad
SISTEMA DE CONVOCATORIAS DE PERSONAL	GESTION ADMINISTRATIVA	Unidad de Recursos Humanos
SISTEMA DE IMPRESIÓN DE CHEQUES	GESTION ADMINISTRATIVA	Unidad de Tesorería
SISTEMA DE SEGUIMIENTO DEL EGRESADO	GESTION ACADEMICA DE LA UNIVERSIDAD	Dirección de Asuntos Académicos
SISTEMA INTEGRADO DE GESTION BIBLIOTECARIA	GESTION ACADEMICA DE LA UNIVERSIDAD	Biblioteca Central
SISTEMA DE PLANILLAS DE PAGO	GESTION ADMINISTRATIVA	Unidad Funcional de Remuneraciones
SEGUIMIENTO DE INVESTIGACIONES	GESTION ACADEMICA DE LA UNIVERSIDAD	Dirección de Investigación

CLOUD UNHEVAL	GESTION ADMINISTRATIVA	Rectorado
OBSERVATORIO TECNOLOGICO DE LA DITT	GESTION ACADEMICA DE LA UNIVERSIDAD	Dirección de Innovación y Transferencia Tecnológica
BOLSA DE EMPLEO	GESTION ACADEMICA DE LA UNIVERSIDAD	Unidad Funcional de Seguimiento al Egresado y Vinculación Laboral Estudiantes de la UNHEVAL
Intranet DITT	GESTION ACADEMICA DE LA UNIVERSIDAD	Dirección de Innovación y Transferencia Tecnológica
Sistema de Bienestar Universitario	GESTION ADMINISTRATIVA	Bienestar Universitario.
SISTEMA DE ADMISION UNHEVAL	GESTION ACADEMICA DE LA UNIVERSIDAD	Unidad de Admisión
LEGAJO PERSONAL	GESTION ADMINISTRATIVA	Trabajadores de la universidad
SISTEMA DE INSCRIPCIÓN EN LINEA DE PROCESOS DE ADMISIÓN PARA LAS SEGUNDAS ESPECIALIDADES	GESTION ADMINISTRATIVA	Postulantes a segundas especialidades
SISTEMA WEB PARA EL TEST DE ORIENTACION VOCACIONAL Y EXAMEN DE APTITUDES Y ACTITUDES	GESTION ACADEMICA DE LA UNIVERSIDAD	Postulantes e ingresantes
SISTEMA DE GRADOS Y TITULOS	GESTION ADMINISTRATIVA	Unidad de Grados y Títulos
SIGA MEF	GESTION ADMINISTRATIVA	Oficinas administrativas
SIAF	GESTION ADMINISTRATIVA	Oficinas administrativas

7. GESTION DE LA SEGURIDAD DE LA INFORMACION

7.1 Objetivo en materia de seguridad

Garantizar la confidencialidad, integridad y disponibilidad de los datos y sistemas de la organización.

Este objetivo se centra en tres aspectos fundamentales de la seguridad de la información:

Confidencialidad: Proteger la información de accesos no autorizados, asegurando que solo las personas autorizadas puedan acceder a la información confidencial.

Integridad: Asegurar que la información no se altere de manera no autorizada o accidental, manteniendo la exactitud y consistencia de los datos.

Disponibilidad: Garantizar que la información y los sistemas estén disponibles y sean accesibles cuando se necesiten, evitando interrupciones no planificadas.

Lograr este objetivo implica implementar medidas de seguridad adecuadas, como sistemas de autenticación robustos, cifrado de datos, firewalls, políticas de acceso y respaldo de información, entre otras prácticas y tecnologías que protejan los activos de información de una organización.

7.2 Seguridad estratégica

La seguridad de la información estratégica se refiere a la protección de los datos e información crítica y confidencial que es vital para la toma de decisiones y el funcionamiento estratégico de una organización o entidad. Esta información puede incluir planes estratégicos, investigaciones, secretos comerciales, propiedad intelectual, datos financieros confidenciales, entre otros.

El objetivo principal de la seguridad de la información estratégica es garantizar que dichos datos y activos cruciales estén protegidos contra accesos no autorizados, manipulación o divulgación indebida. La pérdida o compromiso de esta información podría tener graves consecuencias para la organización, desde la pérdida de ventaja competitiva hasta problemas legales o daño a la reputación. Por lo tanto, implementar medidas de seguridad adecuadas para salvaguardar la información estratégica es fundamental para el éxito y la continuidad del negocio.

La Oficina de Tecnologías de la Información tiene como responsabilidad la implementación del Sistema de Gestión de Seguridad de la Información en la universidad, todo ello de acuerdo con lo establecido en el D.U. N° 007-2020

7.3 Seguridad táctica operacional

En cuanto a la seguridad táctica operacional, es necesario salvaguardar los elementos fundamentales de la infraestructura tecnológica y de comunicación que sostienen el funcionamiento de la institución. Este enfoque se centra en aspectos relacionados con el hardware y software, promoviendo el uso adecuado de las

herramientas informáticas. El análisis de riesgos se orienta hacia la identificación de posibles vulnerabilidades en el hardware y/o software de la infraestructura, con el propósito de reducir y controlar el riesgo a un nivel aceptable mediante acciones preventivas y correctivas.

Además, en el contexto de la seguridad táctica operacional, es fundamental establecer procedimientos y protocolos de respuesta ante incidentes de seguridad que puedan surgir en la infraestructura tecnológica y de comunicación. La rápida detección y mitigación de posibles amenazas y ataques cibernéticos son aspectos esenciales para mantener la continuidad de las operaciones y proteger la información sensible de la organización. Para lograr una seguridad integral, se requiere la colaboración estrecha entre equipos de TI, personal de seguridad, y la sensibilización y capacitación constante de los usuarios para que sean conscientes de las mejores prácticas de seguridad y cómo actuar frente a situaciones de riesgo. Asimismo, la implementación de herramientas de monitoreo y análisis de seguridad en tiempo real permite una gestión proactiva y efectiva de los posibles incidentes, fortaleciendo así la postura de seguridad global de la institución.

8. IMPLEMENTACION DEL SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION

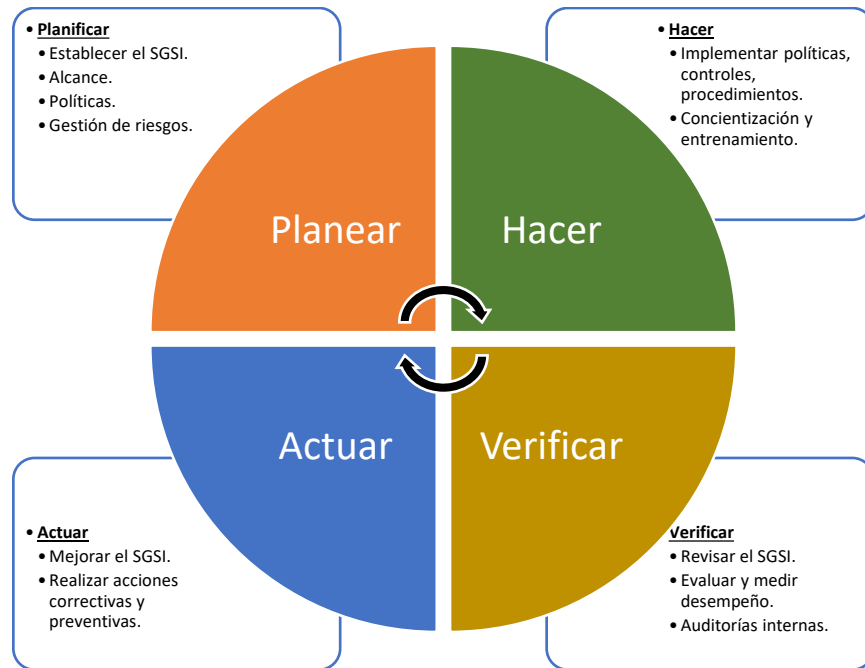
Un Sistema de Gestión de Seguridad de la Información (SGSI) representa un conjunto de políticas de gestión de la información que se enfoca en el diseño, implementación y mantenimiento de procesos eficientes para administrar el acceso a la información. Su objetivo es garantizar la confidencialidad, integridad y disponibilidad de los activos de información, mientras se minimizan los riesgos relacionados con la seguridad de los datos. En otras palabras, el SGSI busca asegurar que la información esté protegida y disponible solo para aquellos que tienen los permisos adecuados, mientras se previenen y mitigan posibles amenazas o incidentes de seguridad.

La implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) conlleva diversos beneficios para una organización. Algunos de ellos son:

1. **Protección de la información sensible:** El SGSI ayuda a salvaguardar los datos confidenciales y sensibles, evitando su acceso no autorizado y asegurando que solo las personas autorizadas puedan acceder a ellos.
2. **Cumplimiento normativo:** Un SGSI bien diseñado puede ayudar a la organización a cumplir con las regulaciones y estándares de seguridad de la información aplicables, lo que puede ser un requisito legal o contractual en muchas industrias.
3. **Continuidad de las actividades:** La gestión efectiva de la seguridad de la información contribuye a reducir la probabilidad de interrupciones y ataques cibernéticos, lo que a su vez mejora la continuidad de las operaciones de la organización.
4. **Mejora de la confianza del cliente:** La adopción de prácticas de seguridad sólidas aumenta la confianza de los clientes y socios comerciales en la organización, lo que puede generar ventajas competitivas y fortalecer las relaciones comerciales.
5. **Reducción de riesgos y costos:** La prevención y mitigación de incidentes de seguridad puede ayudar a evitar costosas brechas de datos y pérdida de información, lo que a largo plazo puede reducir los riesgos y gastos asociados con el manejo de crisis.
6. **Mejora de la eficiencia:** La implementación de procesos bien definidos y tecnologías adecuadas para la seguridad de la información puede mejorar la eficiencia operativa y reducir la probabilidad de errores humanos.
7. **Protección de la reputación:** Un SGSI robusto puede proteger la reputación de la organización al evitar fugas de información o incidentes de seguridad que podrían dañar su imagen pública.
8. **Fomento de la cultura de seguridad:** Al promover la conciencia y la capacitación en seguridad de la información entre los empleados, se crea una cultura de seguridad dentro de la organización que ayuda a prevenir errores y riesgos involuntarios.

8.1 Ciclo Deming para la implementación del SGSI

La implementación del SGSI se desarrolla siguiendo el Ciclo de Deming tal como se puede apreciar en la siguiente ilustración:



9. POLITICAS DE ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACION

9.1 POLITICAS ADOPTADAS ACERCA DEL USO DE DISPOSITIVOS MOVILES

Estas políticas se aplican en los dispositivos móviles adquiridos por la entidad y que se encuentran asignados a los trabajadores de la universidad.

- Se debe reportar la pérdida o extravío de dispositivos propios de la organización de forma inmediata a la toma de conocimiento, siguiendo los pasos detallados en un procedimiento formal.
- Las aplicaciones instaladas en el dispositivo deben ser obtenidas por canales oficiales y con el licenciamiento debido.
- Se debe implementar, para los dispositivos que lo soporten, instrumentos y herramientas técnicas (hardware, software) que permitan bloquear y/o borrar la información de forma remota.
- Se debe contar con procedimientos para la reutilización y/o eliminación de dispositivos (cambio de usuario, equipos en desuso, etc.) que garanticen la eliminación completa y segura de la información previa y sensible anteriormente almacenada.
- Se debe establecer a qué nivel de control y monitorización están sometidos dichos dispositivos y las medidas y posibles sanciones aplicables cuando se produce algún tipo de abuso o infracción por parte de los trabajadores.
- Se debe contar con mecanismos de protección ante código malicioso, en caso de que corresponda.

- Se debe hacer un inventario de los dispositivos móviles propios de la organización.
- Se debe usar controles de acceso (autenticación con contraseñas, doble factor, VPN, entre otros), contar con bloqueo mediante contraseña u otro medio robusto de autenticación.
- No se debe exponer el equipo a altas temperaturas.
- Se debe supervisar el uso de aplicaciones de almacenamiento en la nube.
- Se debe desactivar en el teléfono la búsqueda de redes Wi-fi públicas y dispositivos vías bluetooth.
- Se debe llevar a cabo auditorías periódicas para asegurar el cumplimiento de la política.

9.2 POLITICAS DE GESTION DE SEGURIDAD DE LOS SISTEMAS INFORMATICOS Y ACCESOS A LAS REDES INFORMATICAS

- Política de Autenticación y Acceso:
 - Establecer requisitos de autenticación fuertes, como contraseñas complejas o autenticación de dos factores.
 - Conceder acceso mínimo necesario basado en roles y responsabilidades.
- Política de Actualización y Parches: Implementar actualizaciones y parches de seguridad regularmente en sistemas y aplicaciones.
- Política de Respuesta a Incidentes: Tener un plan detallado para manejar incidentes de seguridad, incluyendo notificaciones y medidas de mitigación.
- Política de Copias de Seguridad: Realizar respaldos periódicos de datos críticos y almacenarlos en ubicaciones seguras.
- Política de Auditoría y Monitoreo: Establecer sistemas de monitoreo continuo para detectar actividad sospechosa y mantener registros de auditoría.
- Política de Educación y Concientización: Capacitar al personal sobre prácticas seguras y riesgos de seguridad informática.
- Política de Control de Dispositivos: Regular el acceso y uso de dispositivos en la red, con medidas de seguridad adecuadas.
- Política de Acceso Remoto: Definir normas para el acceso seguro a la red desde ubicaciones remotas, como a través de VPN.
- Política de Privacidad de Datos: Garantizar el manejo adecuado y la protección de datos personales de acuerdo con las regulaciones pertinentes.
- Política de Eliminación Segura: Establecer procedimientos para la eliminación segura de datos y dispositivos al final de su ciclo de vida.

Estas políticas trabajan en conjunto para mantener la seguridad de los sistemas informáticos y el acceso a redes, protegiendo la integridad, confidencialidad y disponibilidad de la información.

9.3 POLITICAS DE SEGURIDAD DE LAS OPERACIONES EN EL CENTRO DE DATOS

- Control de acceso: Debe haber un control estricto de acceso al centro de datos, tanto físico como lógico. Esto significa que solo las personas autorizadas deben poder ingresar al centro de datos y acceder a los sistemas y datos.
- Seguridad física: El centro de datos debe estar ubicado en un área segura, con medidas de seguridad físicas como cercas, cámaras de seguridad y alarmas.
- Seguridad del sistema: El centro de datos debe estar equipado con sistemas de seguridad de última generación, como firewalls, antivirus y sistemas de detección de intrusiones.
- Seguridad del personal: El personal del centro de datos debe estar capacitado en seguridad de la información y debe seguir las políticas y procedimientos de seguridad.
- Seguridad del medio ambiente: El centro de datos debe estar diseñado para proteger los sistemas y datos de los riesgos ambientales, como incendios, inundaciones y desastres naturales.

9.4 POLITICAS DE SEGURIDAD DE LAS COMUNICACIONES

- Usar contraseñas seguras: Las contraseñas deben ser al menos de 8 caracteres de longitud e incluir una combinación de letras, números y símbolos. No deben ser fácilmente adivinables, como el nombre del usuario, la fecha de nacimiento o el nombre de un ser querido.
- Cambiar las contraseñas con regularidad: Las contraseñas deben cambiarse al menos cada 90 días o después de cualquier incidente de seguridad.
- No compartir contraseñas: Las contraseñas deben mantenerse confidenciales y nunca deben compartirse con nadie.
- Usar autenticación de dos factores (2FA): La autenticación de dos factores (2FA) agrega una capa adicional de seguridad al requerir que los usuarios ingresen un código adicional además de su contraseña al iniciar sesión.
- Ser consciente de los correos electrónicos de phishing: Los correos electrónicos de phishing son correos electrónicos fraudulentos que intentan engañar a los usuarios para que revelen información personal, como contraseñas o números de tarjetas de crédito. Nunca debe hacer clic en enlaces o abrir archivos adjuntos de correos electrónicos de remitentes desconocidos.

- Mantener los sistemas actualizados: Los sistemas operativos y las aplicaciones deben mantenerse actualizados con las últimas versiones de seguridad. Estas actualizaciones a menudo incluyen correcciones de seguridad que pueden ayudar a proteger los sistemas contra ataques.

9.5 POLITICAS DE ADQUISICION Y DESARROLLO DE SISTEMAS⁵

- Cuando se identifique la necesidad de un software para alguna dependencia de la universidad, el área usuaria primero debe evaluar la posibilidad de si la Oficina de Tecnologías de la Información cuenta con recursos para el desarrollo e implementación, para ello el área usuaria debe consultar a la Oficina de Tecnologías de la Información sobre dicha posibilidad.
- Para cumplir con lo descrito en el ítem anterior, se debe referir al Mapa de Procesos y Manual de Procedimientos de la Universidad Nacional Hermilio Valdizán, Procesos Estratégicos E.02 Gestión del Desarrollo y Modernización Organizacional / E.02.03 Desarrollo e Implementación de Sistemas de Información / E.02.03.P.01 Análisis y Diseño de Sistemas de Información y el E.02.03.P.02 Construcción y despliegue de sistemas de información.⁶
- En caso se requiera la adquisición de licencias de software disponibles en el mercado se tomará como marco legal la Ley N° 28612 – LEY QUE NORMA EL USO, ADQUISICIÓN Y ADECUACIÓN DEL SOFTWARE EN LA ADMINISTRACIÓN PÚBLICA, y su reglamento aprobado mediante Decreto Supremo N° 024-2006-PCM.
- Cuando sea necesario realizar la contratación del servicio de planeamiento, desarrollo e implementación de un sistema, los TERMINOS DE REFERENCIA deberá realizarlo el área usuaria y deberá contar con el visto bueno de la Oficina de Tecnologías de la Información.
- La Oficina de Tecnologías de la Información realizará la revisión de los TDR a petición del área usuaria, y formulará las recomendaciones oportunas.
- Los TERMINOS DE REFERENCIA debe considerar además de lo obligatorio (establecido por el OSCE), los siguientes aspectos:
 - Código abierto y código fuente, el sistema informático debe ser de preferencia de código abierto, desarrollo web; y el desarrollador debe proporcionar el código fuente.

⁵ Directiva N° 001-2023-UNHEVAL/OTI – Lineamientos sobre la elaboración y/o adquisición de software en la UNHEVAL.

⁶ Mediante Resolución Rectoral N° 0913-2022-UNHEVAL, se aprueba el MAPA DE PROCESOS V.0.6 de la Universidad Nacional Hermilio Valdizán.

- Documentación, el proveedor del servicio deberá entregar la documentación técnica necesaria tal como el manual de usuario, manual de administrador, manual técnico, diagramas de flujo, diagrama entidad relación, entre otros.
 - Integrado a la base de datos de la universidad, la información ingresada por el aplicativo a desarrollar debe integrarse a la base de datos de la UNHEVAL, de acuerdo con la recomendación de la Oficina de Tecnologías de la Información.
 - Indicar claramente todas las funcionalidades que se desea, el área usuaria conoce perfectamente todos los procesos que desarrolla, para ello debe plasmar en los TDR todo lo que requiere que el aplicativo realice.
 - Garantía y soporte técnico, debe establecer claramente el periodo de garantía por el aplicativo, asimismo el proveedor debe comprometerse a brindar el soporte técnico a la brevedad posible.
 - Instalación e implementación en los servidores, el proveedor del servicio debe realizar el despliegue del código del aplicativo desarrollado en el servidor que la Oficina de Tecnologías de la Información le indique.
 - El producto software final es propiedad de la Entidad, ello incluye los derechos intelectuales.
- El proveedor del servicio debe entregar el sistema implementado e instalado, y demostrar su pleno funcionamiento a satisfacción del área usuaria la cual deberá dar su conformidad.
 - La conformidad a un servicio de planeamiento, desarrollo e implementación de un sistema la dará el área usuaria previa revisión del funcionamiento de todas las funcionalidades requeridas por la dependencia solicitante, dado que ellos son los que conocen mejor sus procesos que desarrollan; asimismo, debe contar con el visto bueno de la Oficina de Tecnologías de la Información que verificará el despliegue en los servidores de la UNHEVAL, la entrega del código fuente, la entrega de la documentación técnica.

9.6 POLITICAS DE SEGURIDAD DE RELACION CON PROVEEDORES

- Todo proveedor que brinde servicios a la UNHEVAL debe suscribir un acuerdo de confidencialidad de la información de la universidad, o debe estar incluido una cláusula de confidencialidad en los contratos a suscribir.
- Los proveedores no tendrán contacto directo con las bases de datos de los sistemas de la universidad, de ser el caso podrán contar con copias de seguridad siempre respetando el acuerdo de confidencialidad de la información.

- Las bases de datos desarrollados por proveedores deberán integrarse a la base de datos principal de la universidad por medio de APIs, para evitar el daño de la base de datos, todo este proceso deberá ser monitoreado por personal de la Unidad Funcional de Telecomunicaciones y Sistemas.
- El proveedor deberá proporcionar los datos completos de la persona de contacto con quien se realizará todas las coordinaciones con respecto a la seguridad de la información.
- Ningún proveedor puede utilizar la información obtenida de la universidad para beneficio propio o de terceros; solamente puede ser utilizado la información proporcionada para los fines y objeto del contrato.
- Toda la información proporcionada por la universidad es propiedad de la universidad, la información generada es propiedad de la universidad de acuerdo con lo establecido en el contrato.
- Cualquier daño a la información o medios físicos ocasionados por el proveedor del servicio serán de responsabilidad del proveedor y será susceptible de iniciar las acciones legales correspondientes.

9.7 POLITICAS DE GESTION DE INCIDENTES DE SEGURIDAD DE LA INFORMACION

- Política de Notificación y Reporte: Establecer procedimientos claros para notificar y reportar incidentes de seguridad a las partes apropiadas dentro de la organización.
- Política de Categorización y Priorización: Definir criterios para categorizar y priorizar los incidentes según su gravedad y posible impacto.
- Política de Respuesta y Recuperación: Detallar pasos específicos a seguir para responder a incidentes, mitigar el impacto y restaurar la operación normal.
- Política de Coordinación: Especificar roles y responsabilidades de los miembros del equipo de respuesta a incidentes y su coordinación durante un incidente.
- Política de Comunicación: Establecer lineamientos para la comunicación interna y externa durante un incidente, incluyendo a las partes afectadas y a las autoridades relevantes.
- Política de Preservación de Evidencia: Definir cómo recopilar, preservar y documentar la evidencia relacionada con el incidente para futuras investigaciones.
- Política de Evaluación de Impacto: Determinar cómo evaluar el impacto potencial de un incidente en los sistemas, datos y operaciones.
- Política de Aprendizaje y Mejora: Establecer un proceso para analizar los incidentes pasados y tomar medidas para mejorar las defensas y la respuesta en el futuro.

- Política de Escalamiento: Definir cuándo y cómo escalar los incidentes a niveles superiores de gestión o a equipos especializados si es necesario.
- Política de Informes y Documentación: Establecer cómo documentar de manera detallada los incidentes, las acciones tomadas y las lecciones aprendidas.
- Política de Simulacros y Ejercicios: Realizar ejercicios de simulacro periódicos para entrenar al equipo de respuesta y probar la efectividad de los procedimientos.

9.8 POLITICAS DE SEGURIDAD SOBRE EL USO DE LOS EQUIPOS INFORMATICOS⁷

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

- 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 estudiantes en cuanto sea permitido.
- Los usuarios en general especialmente los que se encuentran a cargo se encuentran obligados a la custodia de los bienes a su cargo.
- 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.
- 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.
- Los equipos de cómputo deberán contar con programas antivirus y realizar regularmente escaneos de tu equipo para detectar y eliminar posibles amenazas.
- Realizar copias de seguridad de los archivos importantes con regularidad.
- Usar contraseñas seguras para las cuentas y cambiar las contraseñas periódicamente.
- Evitar descargar archivos o programas de sitios web no confiables o desconocidos.

⁷ Directiva N° 002-2023-UNHEVAL/OTI – Uso de las tecnologías de información y de comunicaciones.

- Cerrar sesión de las cuentas en cuando se termine de usarlas y no se debe dejar abierta en dispositivos públicos o compartidos.
- Limpiar regularmente los archivos temporales, cachés y cookies de tu equipo para liberar espacio de almacenamiento y mejorar el rendimiento.
- 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.
- No dejar el equipo expuesto al polvo, la humedad o temperaturas extremas.
- 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.
- Si se tiene problemas o dudas acerca del equipo, se debe contactar a un profesional de soporte técnico capacitado para ayudarte.
- No se debe utilizar los equipos informáticos de la universidad con fines particulares.
- 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>

9.9 POLITICAS DE SEGURIDAD SOBRE LOS CUIDADOS NECESARIOS DE COMPUTADORAS PERSONALES Y PERIFERICOS

- Ubicación adecuada: Colocar la computadora en un lugar limpio y bien ventilado, evitando la exposición directa a la luz solar y fuentes de calor.
- Limpieza regular: Limpiar el polvo y suciedad de la computadora y los periféricos con regularidad utilizando un paño suave y seco o un paño ligeramente humedecido. Evitar el uso de productos químicos agresivos.
- Protección contra sobretensiones: Utilizar protectores contra sobretensiones o reguladores de voltaje para proteger la computadora y los periféricos de picos de electricidad.
- Actualizaciones de software: Mantener el sistema operativo y el software actualizados para asegurar la seguridad y el rendimiento óptimo.
- Antivirus y seguridad: Instalar un programa antivirus confiable y mantenerlo actualizado para proteger la computadora de malware y virus.
- Contraseñas seguras: Utilizar contraseñas fuertes para proteger el acceso a tu computadora y periféricos, y cambia las contraseñas periódicamente.

- Apagado seguro: Apagar la computadora y periféricos de manera adecuada utilizando los comandos del sistema operativo o el botón de apagado, evitando cortar la energía directamente.
- Respaldo de datos: Realizar copias de seguridad periódicas de tus archivos importantes en una unidad externa o en la nube para evitar la pérdida de información en caso de fallos del sistema.
- Actualización de controladores: mantener los controladores de hardware actualizados para un mejor rendimiento y compatibilidad.
- Manipulación adecuada: Al conectar o desconectar periféricos, hazlo con suavidad y asegúrate de seguir las indicaciones del fabricante.
- Transporte seguro: Si se necesita transportar la computadora o periféricos, utilizar bolsas o estuches acolchados para protegerlos de golpes y daños.
- Mantenimiento profesional: Si se experimenta problemas persistentes o sospechas de daños internos, buscar asistencia técnica profesional para reparaciones y mantenimiento.
- Evitar alimentos y líquidos: No consumir alimentos ni bebidas cerca de la computadora y periféricos, para evitar derrames accidentales.
- Actualizaciones de firmware: Si tienes dispositivos periféricos que requieren actualización de firmware, sigue las instrucciones del fabricante para mantenerlos actualizados.
- Descanso periódico: Si utilizas la computadora por períodos prolongados, permite que descanse entre sesiones para evitar el sobrecalentamiento.

9.10 POLITICAS SOBRE EL SOPORTE DE LOS EQUIPOS INFORMATICOS

- Política de mantenimiento preventivo: La Oficina de Tecnologías de la Información establece con anticipación la programación regular de mantenimiento para equipos y sistemas para evitar problemas y mejorar la vida útil de los dispositivos.
- Política de actualización de software: La Oficina de Tecnologías de la Información define el proceso para aplicar parches, actualizaciones y nuevas versiones de software en los equipos informáticos.
- Política de soporte técnico: la Oficina de Tecnologías de la Información a través de su Unidad Funcional de Mantenimiento y Soporte de Tecnologías de Información detalla los canales de comunicación para solicitar asistencia técnica, los tiempos de respuesta esperados y los procedimientos para solucionar problemas.
- Política de adquisición de hardware y software: la Oficina de Tecnologías de la Información define los procedimientos para la adquisición de nuevos equipos y software, incluyendo la

aprobación y la compatibilidad con los sistemas existentes, ello en función de la disponibilidad presupuestal.

- Política de reemplazo de equipos: la Oficina de Tecnologías de la Información establece cuándo y cómo se reemplazarán los equipos obsoletos o que no cumplen con los requisitos mínimos de rendimiento, ello en función de la disponibilidad presupuestal.
- Política de responsabilidad: Establece las responsabilidades de los usuarios en cuanto al cuidado y uso adecuado de los equipos informáticos.⁸
- Política de licencias de software: Asegura que todo el software utilizado en la empresa esté debidamente licenciado y que se cumpla con los términos y condiciones de uso.
- 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>

9.11 POLITICAS DE SEGURIDAD SOBRE EL USO DEL SOFTWARE

- La universidad solo instalará software de fuentes confiables. Esto incluye software comprado en tiendas en línea, instalado desde CD o DVD, o descargado de Internet.
- La universidad mantendrá su software actualizado. Los desarrolladores de software lanzan regularmente actualizaciones de seguridad que pueden corregir vulnerabilidades que pueden ser explotadas por los atacantes.
- La universidad utilizará una contraseña segura para su cuenta de software. Esta contraseña debe ser al menos 8 caracteres de largo y debe incluir una combinación de letras mayúsculas y minúsculas, números y símbolos.
- La universidad no compartirá su contraseña con nadie. La contraseña es personal y no debe compartirse con nadie, ni siquiera con amigos o familiares.
- La universidad habilitará la autenticación de dos factores (2FA) cuando esté disponible. La 2FA agrega una capa adicional de seguridad al requerirle ingresar un código al dispositivo móvil además de su contraseña cuando inicia sesión.
- La universidad instalará un antivirus y lo mantendrá actualizado. Un antivirus puede detectar y eliminar malware, que es un tipo de software dañino que puede robar sus datos o secuestrar su computadora.
- La universidad será consciente de los riesgos de usar software pirata. El software pirata no está autorizado y puede contener

⁸ Directiva N° 002-2023-UNHEVAL/OTI – Uso de las tecnologías de información y de comunicaciones.

malware. También puede violar los términos de servicio de su cuenta de software.

- La universidad evitará usar software que no sea compatible con su sistema operativo. El software incompatible puede causar problemas de seguridad y rendimiento.
- La universidad hará una copia de seguridad de sus datos con regularidad. Esto lo ayudará a proteger sus datos en caso de que su computadora sea pirateada o se pierda.

9.12 POLITICAS DE SEGURIDAD SOBRE EL USO DE SISTEMAS DE INFORMACION

- Política de Uso Aceptable: Establece los términos y condiciones para el uso de los sistemas de información, incluyendo las actividades permitidas y prohibidas, y las consecuencias por violar estas normas.
- Política de Seguridad de la Información: Define las medidas de seguridad que deben implementarse para proteger los datos y sistemas, incluyendo la autenticación, el cifrado, el control de acceso y la detección de amenazas.
- Política de Contraseñas: Establece requisitos para la creación y gestión de contraseñas seguras, incluyendo la frecuencia de cambio y la complejidad de las contraseñas.
- Política de Privacidad de Datos: Define cómo se recopilan, almacenan, procesan y comparten los datos de los usuarios, y establece los derechos y opciones de privacidad de los individuos.
- Política de Copias de Seguridad: Detalla los procedimientos para realizar copias de seguridad de datos críticos y la frecuencia con la que deben realizarse, con el objetivo de garantizar la recuperación en caso de pérdida de datos.
- Política de Acceso Remoto: Establece los requisitos para acceder a los sistemas de información desde ubicaciones externas, incluyendo medidas de seguridad y dispositivos autorizados.
- Política de Actualización de Software: Define cómo se deben mantener actualizados los sistemas operativos y software de aplicaciones para asegurar la protección contra vulnerabilidades conocidas.
- Política de Seguridad en Correo Electrónico: Establece directrices para el uso seguro del correo electrónico, incluyendo la detección de correos electrónicos de phishing y la gestión de archivos adjuntos maliciosos.
- Política de Desconexión de Empleados: Detalla los pasos que se deben seguir cuando un empleado deja la organización para garantizar la seguridad de los datos y el acceso a los sistemas.

9.13 POLITICAS DE SEGURIDAD SOBRE SISTEMAS DE PROTECCION CONTRA VIRUS

- Política de Antivirus y Antimalware: Requerir la instalación y actualización regular de software antivirus y antimialware en todos los dispositivos conectados a la red de la organización.
- Política de Actualización de Software: Exigir la actualización regular de sistemas operativos, aplicaciones y software de seguridad para parchear vulnerabilidades conocidas.
- Política de Uso de Dispositivos Externos: Definir directrices para el uso de dispositivos externos (USB, discos duros externos, etc.) en los sistemas de la organización.
- Política de Acceso a Sitios Web y Correo Electrónico:
 - Restringir el acceso a sitios web y correos electrónicos sospechosos o no relacionados con el trabajo.
 - Implementar filtrado de contenido para bloquear sitios web maliciosos o con contenido potencialmente dañino.
- Política de Educación y Concienciación:
 - Ofrecer capacitación regular a los empleados sobre las mejores prácticas de seguridad cibernética y cómo reconocer correos electrónicos de phishing y enlaces maliciosos.
 - Fomentar la responsabilidad individual en la protección contra virus y malware.
- Política de Copias de Seguridad (Backup): Establecer un programa regular de copias de seguridad de datos críticos y almacenar las copias de seguridad en ubicaciones seguras y aisladas de la red principal.
- Política de Acceso a la Red:
 - Implementar segmentación de red para aislar sistemas críticos de los segmentos de red menos seguros.
 - Requerir autenticación de dos factores para acceder a sistemas y datos sensibles.
- Política de Monitoreo y Detección de Amenazas:
 - Implementar soluciones de monitoreo de seguridad en tiempo real para detectar y responder a actividades sospechosas.
 - Definir procedimientos para la gestión de incidentes de seguridad en caso de infecciones por virus.
- Política de Actualización de Contraseñas:
 - Establecer pautas para la creación y actualización regular de contraseñas seguras en sistemas y cuentas.
 - Recomendar el uso de contraseñas únicas para diferentes servicios y la implementación de una solución de gestión de contraseñas.

9.14 POLITICAS SOBRE EL USO DE REDES LOCALES Y TELEFONIA⁹

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 estudiantes deben seguir las siguientes disposiciones:

- 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.
- Los equipos de cómputo deberán contar con programas antivirus y firewalls para proteger la red y los equipos conectados.
- Cualquier trabajo de cableado estructurado deberá ser realizado y/o supervisado por personal de la Unidad Funcional de Telecomunicaciones y Sistemas.
- 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.
- 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.
- 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.
- Configurar contraseñas seguras para los equipos y dispositivos conectados, y cambiarlas periódicamente.
- Realizar copias de seguridad regulares de los datos importantes, preferiblemente fuera de la red, para protegerlos de posibles pérdidas.
- No compartir información confidencial a través de la red, y encriptar la información que se transmite si es posible.
- Evitar descargar o instalar software o archivos de fuentes no confiables o desconocidas.
- No abrir correos electrónicos, enlaces o archivos adjuntos sospechosos, ya que pueden contener virus o malware.

⁹ Directiva N° 002-2023-UNHEVAL/OTI – Uso de las tecnologías de información y de comunicaciones.

- Evitar conectarse a redes Wi-Fi públicas no seguras, especialmente al hacer transacciones financieras o ingresar información personal.
- No compartir contraseñas de la red o de los dispositivos conectados con otros usuarios.
- Establecer contraseñas seguras para los dispositivos y cambiarlas periódicamente.
- Evitar descargar archivos sospechosos o de origen desconocido.
- No compartir información confidencial, como información financiera o de identidad, a través de la red sin asegurarse de que la comunicación esté encriptada.
- Evitar visitar sitios web no seguros o desconocidos.
- El uso de la telefonía IP es exclusivamente para fines de carácter institucional.
- 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.
- 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.

9.15 POLITICAS SOBRE EL USO DE INTERNET¹⁰

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 estudiantes en general deberán cumplir las siguientes disposiciones:

- **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.

¹⁰ Directiva N° 002-2023-UNHEVAL/OTI – Uso de las tecnologías de información y de comunicaciones.

- 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.
- 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.
- 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.
- 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://>).
- 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.
- 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.
- 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.
- 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.
- 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.

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

9.16 POLITICAS SOBRE EL USO DEL CORREO ELECTRONICO INSTITUCIONAL

- Política de Uso Adecuado:
 - Establecer claramente que el correo electrónico institucional debe utilizarse exclusivamente para asuntos relacionados con el trabajo y actividades empresariales.
 - Prohibir el uso del correo electrónico institucional para fines personales no relacionados con el trabajo.
- Política de Confidencialidad:
 - Recordar a los empleados que el correo electrónico es un medio de comunicación empresarial y que cualquier información confidencial debe ser tratada con precaución.
 - Advertir contra el envío de información confidencial a destinatarios no autorizados o utilizando conexiones no seguras.
- Política de Phishing y Seguridad:
 - Educar a los empleados sobre las amenazas de phishing y cómo identificar correos electrónicos fraudulentos.
 - Establecer procedimientos para informar inmediatamente sobre correos electrónicos sospechosos o enlaces maliciosos.
- Política de Archivos Adjuntos y Enlaces:
 - Desaconsejar la apertura de archivos adjuntos o enlaces de correos electrónicos no solicitados o desconocidos.
 - Implementar soluciones de seguridad para escanear archivos adjuntos en busca de malware antes de entregarlos a los destinatarios.
- Política de Firmas de Correo Electrónico:
 - Definir una plantilla de firma de correo electrónico que incluya información relevante de la organización, como nombre, cargo, empresa y datos de contacto.
 - Prohibir el uso de firmas de correo electrónico que puedan inducir a confusiones sobre la identidad del remitente.
- Política de Retención de Correo Electrónico:

- Establecer pautas para la retención y eliminación de correos electrónicos de acuerdo con las regulaciones y políticas de la organización.
- Especificar períodos de retención para diferentes tipos de correos electrónicos y datos.
- Política de Uso de Correo Electrónico en Redes Públicas:
 - Desaconsejar el uso del correo electrónico institucional en redes Wi-Fi públicas no seguras.
 - Recordar a los empleados la importancia de utilizar una conexión VPN segura cuando accedan al correo electrónico desde ubicaciones remotas.

9.17 POLÍTICAS SOBRE EL USO DEL PORTAL INSTITUCIONAL

- Política de Uso Adecuado:
 - Establecer que el portal web institucional debe utilizarse exclusivamente para fines académicos, administrativos y de comunicación relacionados con la universidad.
 - Prohibir el uso del portal web para actividades personales no relacionadas con la universidad.
- Política de Contenido y Publicación:
 - Definir pautas para la publicación de contenido en el portal web, asegurando que el material sea preciso, actualizado y relevante para la comunidad universitaria.
- Política de Acceso y Privacidad:
 - Definir niveles de acceso y roles para diferentes usuarios dentro del portal web, asegurando que cada usuario tenga acceso solo a la información y recursos relevantes para sus funciones.
 - Establecer medidas de seguridad para proteger la privacidad de los datos personales y académicos de los estudiantes y miembros del personal.
- Política de Contenido Multimedia:
 - Establecer directrices para la inclusión de contenido multimedia, como imágenes y videos, en el portal web.
 - Requerir permisos y derechos de autor adecuados para el uso de contenido multimedia de terceros.
- Política de Interacción en Línea:
 - Establecer reglas de conducta para la interacción en línea en el portal web, incluyendo foros, comentarios y otras áreas de participación.
 - Prohibir el acoso, la discriminación y cualquier forma de comportamiento inapropiado en las plataformas de interacción.
- Política de Actualización y Mantenimiento:

- Definir un proceso regular de actualización y mantenimiento del portal web para asegurarse de que esté funcionando correctamente y que el contenido esté actualizado.
- Designar responsables de supervisar y mantener el portal web.
- Política de Enlaces Externos:
 - Establecer directrices sobre la inclusión de enlaces a sitios web externos desde el portal institucional.
 - Verificar que los enlaces sean relevantes y seguros antes de agregarlos.
- Política de Uso de Datos Analíticos:
 - Informar a los usuarios sobre el uso de herramientas de análisis web para recopilar datos sobre el uso del portal.
 - Garantizar que los datos se utilicen de manera ética y se proteja la privacidad de los usuarios.
- Política de Notificaciones y Anuncios:
 - Definir cómo se mostrarán las notificaciones y anuncios importantes en el portal web.
 - Establecer un equilibrio entre la comunicación efectiva y evitar la saturación de información.

9.18 POLITICAS SOBRE EL ACCESO AL CENTRO DE DATOS

- Política de acceso autorizado: Solo el personal autorizado, debidamente identificado y con las credenciales apropiadas, tiene permitido ingresar al centro de datos.
- Política de autenticación y autorización: Se deben utilizar mecanismos robustos de autenticación, como contraseñas seguras, autenticación de dos factores o biometría, para asegurar que solo los usuarios autorizados tengan acceso.
- Política de acceso basado en roles: El acceso al centro de datos debe ser basado en roles, lo que significa que cada usuario tiene acceso solo a los recursos y áreas necesarios para llevar a cabo sus funciones.
- Política de acompañamiento: Los visitantes o personas no autorizadas deben estar acompañados en todo momento por un personal autorizado mientras se encuentren dentro del centro de datos.
- Política de registro de visitantes: Todos los visitantes deben registrarse en un libro de visitas o sistema de registro antes de ingresar al centro de datos, proporcionando detalles de su visita y tiempo estimado de permanencia.
- Política de supervisión y videovigilancia: El centro de datos debe contar con sistemas de videovigilancia y monitoreo para registrar y supervisar actividades y eventos relevantes.

- Política de acceso físico: Se deben implementar controles físicos adecuados, como puertas con cerraduras, tarjetas de acceso o sistemas de reconocimiento biométrico, para limitar el acceso físico al centro de datos.
- Política de acceso remoto: El acceso remoto al centro de datos debe realizarse a través de conexiones seguras y cifradas, y solo debe permitirse a personal autorizado con fines específicos y previamente aprobados.
- Política de protección contra incendios y desastres: Se deben implementar medidas de protección contra incendios y desastres naturales para preservar la integridad de los equipos y datos en caso de emergencias.
- Política de limpieza y mantenimiento: Las tareas de limpieza y mantenimiento en el centro de datos deben llevarse a cabo bajo supervisión y con precauciones para evitar daños o acceso no autorizado.
- Política de acceso a registros y auditorías: Debe mantenerse un registro detallado de los accesos al centro de datos, así como de las actividades realizadas, y realizar auditorías periódicas para identificar posibles anomalías o violaciones.

9.19 PROHIBICIONES GENERALES

- Queda expresamente prohibido llevar a cabo la utilización de herramientas o métodos de supervisión de la red sin la debida autorización. Además, se encuentra limitado eludir los sistemas de seguridad, autenticación, autorización o auditoría de cualquier servicio de red, aplicación servidor o cuenta de usuario.
- Queda vedado emplear la infraestructura de tecnología de información y redes de la UNHEVAL con el propósito de obtener o compartir contenido con el objetivo de obtener beneficios económicos.
- No se permite el uso de la infraestructura de tecnología de información y redes de la UNHEVAL para llevar a cabo acciones de hostigamiento, difamación, calumnia u otras formas de conducta hostil dirigidas hacia funcionarios, servidores públicos, así como hacia cualquier individuo o entidad en general.
- No está permitida la instalación de puntos de acceso inalámbricos en la Institución que no cuenten con la debida autorización de la Oficina de Tecnologías de la Información.
- Los recursos de tecnología de información proporcionados por la UNHEVAL están destinados exclusivamente para respaldar el desarrollo de los procesos institucionales. Por lo tanto, está prohibido utilizar dichos recursos con propósitos personales.
- Los usuarios no están exentos de enfrentar las consecuencias disciplinarias y legales pertinentes por cualquier acción que no esté

registrada en este documento y que pueda poner en riesgo la seguridad de la información de la Institución.