"Año del Fortalecimiento de la Soberanía Nacional"

RESOLUCIÓN DE ALCALDÍA N° 062-2022-MPH/A

Huancayo, 10 de febrero de 2022.

EL ALCALDE DE LA MUNICIPALIDAD PROVINCIAL DE HUANCAYO.

VISTOS:

El Informe Técnico N° 002-2021-MPH/GPP/SGTIC-JJLC de 23 de diciembre del 2021; Informe N° 323-2021-MPH/GPP/SGTIC de 27 de diciembre del 2021; Informe N° 219-2021-MPH-GPP/UR de 29 de diciembre del 2021; Memorando N° 026-2022-MPH/GPP de 06 de enero del 2022; Informe Legal N° 064-2022-MPH/GAJ de 18 de enero del 2022; Memorándum N° 094-2022-MPH/GPP de 25 de enero del 2022; el Informe Técnico N° 001-2022-MPH/GPP/SGTIC-JJLC de 03 de febrero del 2022; y,

CONSIDERANDO:

Que, según el artículo 194° de la Constitución Política del Perú, modificado por la Ley de Reforma de la Constitución Política del Perú, Ley N° 30305, concordante con el Artículo II del Título Preliminar de la Ley Orgánica de Municipalidades Ley N°27972; las municipalidades provinciales y distritales son los órganos de gobierno local, tienen autonomía política, económica y administrativa en los asuntos de su competencia;

Que, la Ley N° 27658 – Ley Marco de Modernización de la Gestión del Estado, declara al Estado Peruano en proceso de modernización en sus diferentes instancias, dependencias, entidades, organizaciones y procedimientos, con la finalidad de mejorar la gestión pública y contribuir con el fortalecimiento de un Estado moderno, descentralizado y con mayor participación de la ciudadanía.

Que, el Decreto Legislativo N° 1412 que aprueba la Ley de Gobierno Digital, dispone que la Presidencia del Consejo de Ministros, a través de la Secretaría de Gobierno Digital, es el ente rector en materia de gobierno digital, que comprende tecnologías digitales, identidad digital interoperabilidad, servicio digital, datos, seguridad digital y arquitectura digital; dictando para tal efecto las normas y procedimientos en dicha materia.

Que, la Política Nacional de Gobierno Electrónico, aprobada mediante Decreto Supremo N° 081-2013-PCM, prevé lineamientos estratégicos para el Gobierno Electrónico en el Perú, sobre Seguridad de la Información, enfatizando la necesidad de velar por la integridad, seguridad y disponibilidad de los datos, y definir lineamientos en seguridad de la información para mitigar el riesgo de exposición de información sensible del ciudadano;

Que, mediante Resolución N° 129-2014/DNB-INDECOPI, se aprobó la nueva versión de la Norma Técnica Peruana NTP ISO/IEC 27001:2014 Tecnología de la Información. Técnicas de seguridad. Sistemas de gestión de seguridad de la Información. Requisitos. 2ª Edición, que tiene por objeto establecer, implementar, operar, monitorear, mantener y mejorar un efectivo Sistema de Gestión de Seguridad de la Información en las organizaciones, que incluye la aprobación de una Política de Seguridad de la Información que dirija y brinde soporte a la gestión de la seguridad de la información.

Que, mediante Resolución Ministerial N° 004-2016-PCM, modificada por la Resolución Ministerial N° 166-2017-PCM, Se aprueban el uso obligatorio de la Norma Técnica Peruana "NTP ISO/IEC 27001:2014 Tecnología de la Información - Técnicas de Seguridad - Sistemas de Gestión de Seguridad de la Información. Requisitos. 2a. Edición", y dispone la creación del Comité de Gobierno Digital en cada entidad integrante del Sistema Nacional de Informática, estableciendo funciones mínimas, debe cumplir. En el artículo 4°, "Del Oficial de Seguridad de la Información, establece *que el titular El Titular de entidad, dentro del plazo de diez (10) días hábiles, contados a partir de la publicación de la presente resolución, debe designar a un Oficial de Seguridad de la Información, quien será responsable de coordinar la implementación del Sistema de Gestión de Seguridad de la Información en la entidad*. Dicha designación debe ser puesta en conocimiento a la Secretaría de Gobierno Digital para las coordinaciones y acciones correspondientes".

Que, con Resolución Ministerial N° 119-2018-PCM modificada con la Resolución Ministerial N° 087-2019-PCM, se dispone la creación y funciones de un Comité de Gobierno Digital en cada entidad de la Administración Pública. Que, con Informe Técnico N° 002-2021-MPH/GPP/SGTIC-JJLC de 23 de diciembre del 2021 e Informe N° 323-2021-MPH/GPP/SGTIC de 27 de diciembre del 2021; la Subgerencia de Tecnologías de la Información y Comunicación, según funciones establecidas en el artículo 35 del Reglamento de Organización y Funciones de la Municipalidad Provincial de Huancayo, aprobado por Ordenanza Municipal N° 522-MPH/CM, presentó el proyecto

244

de Resolución que aprueba las Políticas de Seguridad de la Información de la Municipalidad Provincial de Huancayo, adjuntado el anexo respectivo (Políticas Específicas) y designando al Oficial de Seguridad de la Información. Dichas Políticas tienen por objeto lograr un nivel razonable de seguridad en la información, garantizando su confidencialidad, integridad y disponibilidad;

Que, con Informe N° 219-2021-MPH-GPP/UR de fecha 29 de diciembre del 2021; la Unidad de Racionalización de la Gerencia de Planeamiento y Presupuesto, concluye que el Proyecto de Resolución de Alcaldía y anexo correspondiente están formulados con arreglo al contexto normativo que se sustenta el Informe Técnico N° 002-2021-MPH/GPP/SGTIC-JJLC y se recomienda realizar los cambios sugeridos y proseguir trámite solicitando la opinión legal de la Gerencia de Asesoría Jurídica.

Que, con Memorando N° 026-2022-MPH/GPP de fecha 06 de enero del 2022 e Informe Legal N° 64-2022-MPH/GAJ de 18 de enero del 2022; la Gerencia de Asesoría Jurídica concluye y recomienda: Retorno a la Subgerencia de Tecnologías de la Información y Comunicación, para que corrija la Resolución de Alcaldía a emitirse y Reformule o rectifique el Anexo de Políticas de Seguridad de la Información de la MPH, según el análisis y sustento que antecede y observaciones detalladas en el proyecto; en cumplimiento de la Directiva N° 002-2020-MPH/GM aprobado con Resolución de Gerencia Municipal N° 186-2020-MPH/GM y modificado con Resolución de Gerencia Municipal N° 042-2021-MPH/GM. Cumplido derivar al Despacho de Alcaldía para suscripción del acto resolutivo de Aprobación. Así mismo, no existe ninguna controversia jurídica, siendo factible su aprobación;

Que, con Memorándum N° 094-2022-MPH/GPP de 25 de enero del 2022; el Informe Técnico N° 001-2022-MPH/GPP/SGTIC-JJLC de 03 de febrero del 2022; se comunica que se ha procedido con la corrección de la Resolución de Alcaldía a emitirse y se ha rectificado el Anexo de Políticas de Seguridad de la Información de la MPH, así mismo se ha incluido políticas faltantes. Concluyendo su derivación a Despacho de Alcaldía para su suscripción; con Memorando N° 340-2022-MPH/GM de 09 de febrero de 2022 el Gerente Municipal remite todos los actuados a la Secretaría General para la prosecución del trámite;

Que, en mérito a lo expuesto y de conformidad con las atribuciones establecidas en el numeral 6) del artículo 20° de la Ley N° 27972, Ley Orgánica de Municipalidades.

SE RESUELVE:

ARTÍCULO PRIMERO.- APROBAR las Políticas de Seguridad de la Información de la Municipalidad Provincial de Huancayo, conforme al anexo que forma parte integrante de la presente Resolución.

ARTÍCULO SEGUNDO.- DESIGNAR al **Ing. de Sistemas Raúl Antonio Surichaqui Mari** como Oficial de Seguridad de la Información, cuya responsabilidad es de implementar el Sistema de Gestión de Seguridad de la Información en la Municipalidad Provincial de Huancayo, brindando los servicios de seguridad a través de la planeación, coordinación y administración de los procesos de seguridad informática, así como difundir la cultura de seguridad de la información entre todos los miembros de la Municipalidad Provincial de Huancayo.

ARTÍCULO TERCERO.- DISPONER la publicación de la presente resolución y su anexo en el Portal Institucional de la Municipalidad Provincial de Huancayo (www.munihuancayo.gob.pe).

ARTÍCULO CUARTO.- DISPONER que las Políticas de Seguridad de la Información de la Municipalidad Provincial de Huancayo, aprobadas por la presente Resolución, entrará en vigencia a partir del día siguiente de su publicación en el Portal Institucional de la Municipalidad Provincial de Huancayo.

ARTÍCULO QUINTO.- ENCARGAR a todas las Gerencias, Subgerencias y Órganos de la Municipalidad Provincial de Huancayo, el cumplimiento de la presente Resolución de Alcaldía.

REGÍSTRESE, COMUNÍQUESE y PUBLÍQUESE

MUNICIPALIDAD PROVINCIAL DE HUANCAYO
Juan Carlos Quispe Iledesma
ALCALDE

POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN DE LA MUNICIPALIDAD PROVINCIAL DE HUANCAYO

SUB GERENCIA DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES - 2022

POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN DE LA MUNICIPALIDAD PROVINCIAL DE HUANCAYO

Contenido

POLÍTICAS GENERALES DE SEGURIDAD DE LA INFORMACIÓN DE LA MUNICIPALIDAD PROVINCIAL DE HUANCAYO

ENUNCIADO DE LAS POLÍTICAS GENERALES DE SEGURIDAD DE LA INFORMACIÓN

La Municipalidad Provincial de Huancayo es un órgano de Gobierno Local de ámbito provincial el cual tiene como política institucional priorizar el fortalecimiento de la gestión institucional, la lucha frontal contra la corrupción y la inseguridad ciudadana con la finalidad de garantizar una mejor atención al usuario, la igualdad de oportunidades y la seguridad de la población huancaína, teniendo como objetivo asegurar el desarrollo humano, la salud pública, la gestión ambiental y las condiciones habitabilidad para el bienestar de la población. A tal efecto, prevé la seguridad de la información relacionada con sus actividades, metas y programas, en concordancia con la normatividad vigente y los siguientes lineamentos:

- El establecimiento de mecanismos para preservar la confidencialidad, integridad y disponibilidad de la información de la institución, garantizando su transparencia.
- La continua identificación, manejo y mitigación de los riesgos de seguridad de la información que son relevantes para la institución.
- La respuesta efectiva y adopción de acciones correctivas ante incidentes relacionados con la seguridad de la información.
- La comunicación oportuna de las políticas y procedimientos de seguridad definidos, asegurando que sean comprendidos y estén disponibles para todos los interesados.
- El fortalecimiento de los valores y el compromiso de todo el personal de velar por el cumplimiento de las presentes políticas.

CAPÍTULO 1

(GENERALIDADES)

1.1. INTRODUCCIÓN

Las Políticas de Seguridad de la Información de la Municipalidad Provincial de Huancayo han sido elaboradas según la Norma Internacional ISO 27001:2005, y la Norma Técnica Peruana NTP-ISO/IEC 27001:2014 "NTP ISO/IEC 27001:2014 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos. 2a. Edición", aprobada por Resolución Nº 129-2014/DNB-INDECOPI, cuya finalidad principal es asegurar la confidencialidad, integridad y disponibilidad de la información gestionada en la Institución.

Las Políticas de Seguridad de la Información identifican responsabilidades y establecen los objetivos para una protección apropiada y consistente de los activos de información de la Municipalidad Provincial de Huancayo.

1.2. ALCANCE

1.2.1. Las presentes políticas tienen alcance a todas las Gerencias, Sub gerencias y órganos desconcentrados de la Municipalidad Provincial de Huancayo, involucrando a funcionarios y trabajadores bajo cualquier modalidad contractual y terceros que tengan acceso o que desarrollen, adquieran o usen sistemas de información, aplicaciones informáticas y/o datos de la Municipalidad.

1.2.2. Comprende toda la información producida, manejada, transmitida y almacenada en la Municipalidad Provincial de Huancayo, y todos los sistemas y datos asociados con el almacenamiento, procesamiento y transmisión de la información generada por y a favor del Municipio.

1.2.3. En cuanto a las relaciones jurídicas que la Municipalidad Provincial de Huancayo, mantenga con terceros, el presente documento y las disposiciones que en materia de seguridad de la información apruebe la Municipalidad, comprenden la información creada por ellos (los terceros), así como la información propia de la Municipalidad que se les haya otorgado en el marco de dichas relaciones jurídicas.

1.2.4. El presente documento comprende las siguientes políticas específicas:

- Política de seguridad de la información.
- Política de gestión de comunicaciones y operaciones.
- Política de control de accesos.
- Política de adquisición, desarrollo y mantenimiento de aplicaciones informáticas.
- Política de gestión de incidentes.

1.3. OBJETIVO

Las Políticas de Seguridad de la Información tienen por objetivo proteger los recursos de información de la Municipalidad Provincial de Huancayo y la

tecnología utilizada para su procesamiento, frente a amenazas, internas o externas, deliberadas o accidentales, con el fin de minimizar los riesgos de daño y asegurar el cumplimiento de la confidencialidad, integridad y disponibilidad de la información, así como garantizar la continuidad de los sistemas de información. Las Políticas de Seguridad de la Información deben constituirse en parte de la cultura organizacional de la Municipalidad, para lo cual se debe asegurar un compromiso manifiesto de los funcionarios del Municipio, para la difusión, consolidación y cumplimiento de las presentes Políticas.

1.4. DEFINICIONES

Para los fines de las presentes Políticas, se establecen las siguientes definiciones:

a) **Activo:** Todo aquello que presenta valor para la institución, tal como:
   - Información;
   - Software, como un programa de computadora;
   - Físicos, como una computadora;
   - Servicios;
   - Personas y sus calificaciones, habilidades y experiencia;
   - Intangibles, como reputación o imagen.

b) **Aplicación informática:** Es un tipo de software que permite al usuario realizar uno o más tipos de trabajo. Son aquellos programas que permiten la interacción entre un usuario y una computadora (comunicación), brindándole a aquél la opción de elegir entre varias opciones y ejecutar acciones que el programa le ofrece. Las aplicaciones pueden desarrollarse a medida (para satisfacer las necesidades específicas de un usuario) o formar parte de un paquete integrado.

c) **Attachment:** Son aquellos archivos que se incluyen en el correo electrónico, cuya capacidad máxima es de 20MB.

d) **Confidencialidad:** Garantizar que la información sea accesible únicamente a las personas que cuenten con acceso autorizado.

e) **Disponibilidad:** Conseguir que la información esté disponible para los trabajadores de la Municipalidad, dentro de los parámetros de eficacia normales de los sistemas correspondientes, incluidos los Sistemas de Procesamiento de la Información.

f) **Dispositivo BAMBU:** Es el espacio asignado para salvaguardar la información de todos los sistemas de información de la entidad en la nube; siendo estos: Código fuente, Motores de base de datos y repositorios de contenido de información.

g) **Estación de Trabajo:** Equipo de cómputo, también llamado computadora personal que generalmente está conectada a la red informática y es usada por el colaborador como herramienta de trabajo para conectarse a sistemas de información, aplicaciones informáticas, u otros servicios, tales como correo electrónico, internet, etc.

h) **Fileserver:** Servidor destinado para salvaguardar la información de un área a través de unidades lógicas de conexión de red y distribuidas en espacios compartidos por grupos relacionados al área usuaria; cuyo acceso es

configurado por la Sub Gerencia de Tecnologías de la Información y Comunicación.

i) **Incidente de Seguridad de la Información:** Evento no deseado que tiene una probabilidad significativa de comprometer las operaciones de la institución y que genera amenazas a la seguridad de la información.

j) **Información:** Conjunto de datos contenidos en documentos físicos (papel, microfichas, libros, etc.) y medios electrónicos (discos duros, cintas, memorias de tipo USB, disquetes, CD, DVD discos portátiles, entre otros).

k) **Integridad:** Asegurar que la información no sea manipulada, destruida o corrompida por accidentes o acciones intencionadas. Ello incluye los elementos que garantizan su procedencia o autenticidad. También se aplica a los equipos y a las personas.

l) **Metadata:** Es el archivo electrónico con contenido de la entidad y editado por el usuario.

m) **Seguridad de la Información:** Es la preservación de la confidencialidad, integridad y disponibilidad de la información.

n) **Sistema de Información:** Es un conjunto de elementos orientados al tratamiento y administración de datos e información, organizados y listos para su uso posterior, generados para cubrir una necesidad u objetivo. Tales elementos se clasifican principalmente en: Personas, datos, actividades o técnicas de trabajo, y recursos materiales en general (como por ejemplo los recursos informáticos y de comunicación).

o) **Sistema de Gestión de Seguridad de la Información:** Considera los riesgos de la Institución para establecer, implementar, operar, monitorear, revisar, mantener y mejorar la Seguridad de la Información.

p) **Usuario:** Trabajador de la Municipalidad Provincial de Huancayo bajo cualquier modalidad de contrato o servicio por terceros, con prescindencia de su nivel o jerarquía, autorizado a utilizar un sistema de información determinado, bajo un nivel de acceso pre-establecido.

q) **Política de Seguridad de la Información en la Municipalidad Provincial de Huancayo:** Conjunto de principios o lineamientos generales, cuya implementación está orientada a asegurar la confiabilidad, integridad y disponibilidad de la información de la Municipalidad. Como documento dinámico del Municipio, debe seguir un proceso de actualización periódica sujeto a los cambios organizacionales relevantes, tales como cambio en la infraestructura tecnológica, alta rotación del personal, desarrollo de nuevos servicios, etc.

Los principales beneficios de la implementación de la referida Política son:

- Contribuir a efectivizar el manejo del riesgo.
- Priorizar el valor de la Información.
- Estandarizar los controles y revisiones de los sistemas de información y aplicaciones informáticas.
- Establecer bases referenciales para el desarrollo de estrategias y planes referidos a la seguridad de la información.

- Brindar un entorno de trabajo seguro a los usuarios.
- Cumplir con los requerimientos regulatorios y legales pertinentes.

1.5. RESPONSABILIDADES GENERALES

1.5.1. Comité de Gobierno Digital de la Municipalidad Provincial de Huancayo:

El Comité de Gobierno Digital de la Municipalidad Provincial de Huancayo vela por la existencia y cumplimiento de las medidas de seguridad de la información del Municipio, salvo en materia informática, en concordancia con el rol de la Institución y los recursos disponibles.

1.5.1.1. Conformación del Comité de Gobierno Digital de la Municipalidad Provincial de Huancayo:

El Comité de Gobierno Digital de la Municipalidad Provincial de Huancayo está conformado de la siguiente manera:

- El Gerente Municipal, quien lo presidirá;
- El Sub Gerente de Tecnologías de la Información y Comunicación, quien será el Secretario Técnico del Comité;
- El Sub Gerente de Gestión de Recursos Humanos;
- El responsable del área de atención al ciudadano de la Gerencia de Secretaría General;
- El Oficial de Seguridad de la Información;
- El Gerente de Asesoría Jurídica;
- El Gerente de Planeamiento y Presupuesto;
- El Analista de Riesgos;

1.5.1.2. Funciones y responsabilidades del Comité de Gobierno Digital de la Municipalidad Provincial de Huancayo:

a. Formular el Plan de Gobierno Digital en coordinación con las Gerencias, Sub Gerencias y órganos desconcentrados de la Municipalidad Provincial de Huancayo.
b. Liderar y dirigir el proceso de transformación digital en la Municipalidad.
c. Evaluar que el uso actual y futuro de las tecnologías digitales sea acorde con los cambios tecnológicos, regulatorios, necesidades de la Municipalidad, objetivos institucionales, entre otros, con miras a implementar el Gobierno Digital.
d. Gestionar la asignación de personal y recursos necesarios para la implementación del Plan de Gobierno Digital, Modelo de Gestión Documental (MGD), Modelo de Datos Abiertos Gubernamentales y Sistema de Gestión de Seguridad de la Información (SGSI) en los Planes Operativos Institucionales, Plan Anual de Contrataciones y otros.
e. Promover y gestionar la implementación de estándares y buenas prácticas en gestión y gobierno de tecnologías digitales, interoperabilidad, seguridad digital, identidad digital y datos en la Municipalidad.
f. Elaborar informes anuales que midan el progreso de la implementación del Plan de Gobierno Digital y evalúen el desempeño del Modelo de Gestión Documental

(MGD), Modelo de Datos Abiertos Gubernamentales y Sistema de Gestión de Seguridad de la Información (SGSI).

g. Vigilar el cumplimiento de la normatividad relacionada con la implementación del gobierno digital, interoperabilidad, seguridad de la información y datos abiertos en la Municipalidad.
h. Promover el intercambio de datos, información, software público, así como la colaboración en el desarrollo de proyectos de digitalización entre entidades.
i. Gestionar, mantener y documentar el Modelo de Gestión Documental (MGD), Modelo de Datos Abiertos Gubernamentales y Sistema de Gestión de la Seguridad de la Información (SGSI) de la Municipalidad.
j. Promover la conformación de equipos multidisciplinarios ágiles para la implementación de proyectos e iniciativas de digitalización de manera coordinada con los Gerentes y Sub gerentes de la Municipalidad.
k. Otras funciones que se le asigne en el ámbito de su competencia y aquellas concordantes con la materia.

1.5.1.3. Funciones Específicas del Presidente del Comité de Gobierno Digital de la Municipalidad Provincial de Huancayo:

El Presidente del Comité de Gobierno Digital de la Municipalidad Provincial de Huancayo asume las siguientes funciones:

a. Mantener una agenda actualizada sobre los temas de seguridad de la información que deba abordar el Comité de Gobierno Digital del Municipio.
b. Coordinar y fijar las fechas para las sesiones del Comité.
c. Revisar y aprobar las Actas del Comité, previa rúbrica de sus integrantes.
d. Conducir y moderar las sesiones del Comité.

1.5.1.4. Funciones Específicas del Secretario Técnico del Comité de Gobierno Digital de la Municipalidad Provincial de Huancayo:

El Secretario Técnico del Comité de Gobierno Digital de la Municipalidad Provincial de Huancayo, asume las siguientes funciones:

a. Realizar las convocatorias para las sesiones del Comité (ordinarias y extraordinarias) conforme al calendario que disponga el Presidente.
b. Redactar las Actas de las sesiones y dar lectura de las mismas ante los integrantes del Comité.
c. Conservar las Actas y la documentación de todas las actuaciones del Comité.

1.5.1.5. Funcionamiento del Comité de Gobierno Digital de la Municipalidad Provincial de Huancayo:

Acerca de las sesiones del Comité:

Las fechas para las sesiones del Comité serán fijadas por el Presidente del Comité, ya sean de carácter ordinario o extraordinario. Se aplicará la siguiente pauta de convocatoria:

a) Para las sesiones ordinarias: Se celebrarán en forma bimensual, previa convocatoria del Presidente con siete (7) días de anticipación. Esta reunión se celebra en forma rutinaria, por lo que la convocatoria sólo constituye una confirmación de fecha, lugar y hora.
b) Para las sesiones extraordinarias: Se celebrarán por libre decisión del Presidente del Comité o a solicitud de uno o más de sus integrantes. Las convocatorias para las sesiones extraordinarias deberán realizarse con el mayor tiempo de anticipación posible, según la urgencia del asunto a tratar.
c) Las convocatorias para las sesiones ordinarias y extraordinarias podrán realizarse por escrito o por correo electrónico, debiendo indicarse el lugar, día y hora de la sesión, y el asunto a tratar en ella.
d) Por cada sesión se levantará un Acta.

Acerca de los acuerdos del Comité:

a) Los acuerdos adoptados en cada sesión quedarán reflejados en las respectivas Actas. Para adoptar el carácter de acuerdos válidos, las actas serán leídas por el Secretario Técnico al final de la sesión y se considerarán aprobadas con su suscripción por parte de todos los integrantes del Comité, creándose el registro necesario. En caso que un integrante del Comité haya sido reemplazado por inasistencia, la persona que lo representó en la sesión deberá informarle sobre los acuerdos adoptados.

1.5.2. Responsable de Seguridad de la Información:

Es el representante designado como Oficial de Seguridad de la Información de la Municipalidad Provincial de Huancayo, de acuerdo con lo dispuesto por la Resolución Ministerial N° 004-2016-PCM, modificado por la Resolución Ministerial N°166-2017-PCM. Es el encargado de definir y aplicar los criterios de Seguridad de la Información en la Municipalidad Provincial de Huancayo, en base a la Norma Técnica Peruana "NTP ISO/IEC 27001:2014 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos. 2a. Edición", aprobada por Resolución Nº 129-2014/DNB-INDECOPI. Cumple las siguientes funciones:

a) Establecer y aplicar una metodología de análisis de riesgo, en función de los lineamientos establecidos por el Comité de Gobierno Digital.
b) Proponer ante el Comité de Gobierno Digital las modificaciones de las Políticas de Seguridad de la Información de la Municipalidad, de resultar necesarias.
c) Definir procedimientos para la aplicación de políticas de seguridad informática.
d) Coordinar con todas las Gerencias, Sub Gerencias y órganos desconcentrados, en temas de Seguridad de la Información.
e) Promover la aplicación de auditorías enfocadas en la seguridad, para evaluar las prácticas de Seguridad de la Información en la Municipalidad Provincial de Huancayo.

f) Informar regularmente a los trabajadores/colaboradores de la Municipalidad acerca de los objetivos, medidas y reglamentaciones en materia de seguridad de la información que se encuentren en vigencia.

1.5.3. Personal de la Municipalidad Provincial de Huancayo:

A efectos de las presentes políticas, comprende a todas aquellas personas que prestan servicios en la Municipalidad Provincial de Huancayo.

El personal de la Municipalidad tiene la responsabilidad de cumplir con lo establecido en este documento y de aplicarlo en el entorno en el que desempeña sus funciones. Además, tiene la obligación de alertar de manera oportuna y adecuada al titular del órgano o unidad orgánica en donde o para quien presta sus servicios, sobre cualquier situación que atente contra lo establecido en esta política o pueda poner en riesgo la seguridad de la información del Municipio.

1.5.3.1. Funcionarios:

Se refiere a quienes ostentan cargos de confianza, en las Gerencias, Sub gerencias y órganos desconcentrados de la Municipalidad Provincial de Huancayo, independientemente de su régimen laboral o contractual.

Los Funcionarios; de la Municipalidad deberán garantizar e implementar la seguridad de la información y de los sistemas de información dentro de la Gerencia, Sub gerencia u órgano desconcentrado el cual dirige. Ello implica:

a) Supervisar periódicamente su ámbito de acción a fin de detectar posibles deficiencias en materia de seguridad de la información.
b) Iniciar rápidamente medidas correctivas e informar al Comité de Gobierno Digital y/o Sub Gerencia de Tecnologías de la Información y Comunicación, acerca de las deficiencias y demás incidentes de carácter relevante.
c) Difundir entre el personal a su cargo acerca de la regulación en materia de seguridad de la información que se encuentre en vigencia, y que hayan sido puesta en su conocimiento según Ley.
d) Asegurar los niveles de confidencialidad de la información bajo su ámbito, verificando que las reglas operativas sean cumplidas.
e) Definir al personal bajo su cargo que tendrá acceso a la información, a los sistemas de información y aplicaciones informáticas del Municipio, cuando corresponda.
f) Formular al Comité de Gobierno Digital las recomendaciones que considere pertinentes.
g) Designar a los trabajadores que se encargarán difundir las políticas y su regulación complementaria.
h) Coordinar la activación de planes de contingencia ante eventuales caídas de los sistemas de información, a efectos de asegurar la continuidad de las actividades a su cargo.

1.5.3.2. Servidores públicos bajo el D.L. 276 – D.L. 728 – D.L. 1057 - Ley 30057 así como a los que prestan servicio por terceros:

Comprende a todas las personas que prestan servicios en la Municipalidad, distintas de los funcionarios, independientemente de su régimen laboral o contractual.

Todos los servidores públicos del Municipio deben garantizar activamente la protección de la información. Ello implica:

a) La utilización de la información y de los sistemas de información, aplicaciones informáticas, solo para el cumplimiento de sus funciones.
b) El cuidadoso manejo de la información y de los sistemas de información, especialmente si se trata de información confidencial, asegurando su no divulgación.
c) Observar las reglamentaciones y cumplir cabalmente los procedimientos y estándares en cuanto a la seguridad en materia de información.
d) Informar a los titulares de las Gerencias, Sub gerencias y órganos desconcentrados en donde prestan servicios, sobre las deficiencias e incidentes advertidos en materia de seguridad de la información.
e) Participar en las pruebas e implementación de los planes de contingencia, ante eventuales caídas de los sistemas de información y aplicaciones informáticas.

1.5.3.3. Propietario de la Información:

Para los fines de las presentes Políticas, los funcionarios y servidores públicos son propietarios y responsable de la información y de los procesos que la manipulan, sean manuales, mecánicos o electrónicos. El término "propietario" no significa que la persona tiene algún derecho de propiedad real sobre el activo.

El propietario de la información debe participar activamente en la definición del valor de la información para el Municipio, de manera que se puedan determinar los controles apropiados para protegerla.

1.6. CUMPLIMIENTO DE POLÍTICAS

a) Se verificará el cumplimiento de las políticas generales y específicas a través de varios métodos, incluidos, entre otros, recorridos periódicos, monitoreo de video, informes de herramientas comerciales, auditorías internas y externas.
b) Cualquier excepción a la política debe ser aprobada con anticipación.

1.7. SANCIONES POR INCUMPLIMIENTO

El incumplimiento de las presentes Políticas generales y específicas, dará lugar a inicio del procedimiento administrativo disciplinario con la aplicación de las sanciones correspondientes de hallarse responsabilidad, de conformidad con la normativa vigente, sin perjuicio de las responsabilidades civiles y/o penales que pudieran corresponder.

CAPÍTULO 2

(POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN)

2.1. OBJETIVOS

a) Crear un marco normativo de obligatorio cumplimiento, orientado a gestionar de manera apropiada la seguridad de la información en el Municipio.
b) Establecer las disposiciones con respecto al uso de los activos de información de la Institución, y de las medidas que se deben adoptar para su protección.
c) Establecer planes para la sensibilización y capacitación del personal del Municipio en relación con la importancia y la comprensión de su rol a efectos de mantener la seguridad de la información.
d) Establecer los lineamientos que faciliten la adecuada toma de decisiones en aspectos relacionados con la Seguridad de la Información.

2.2. POLÍTICA

a) Adhesión a la Política:
   i. La presente política y procedimientos asociados deben ser cumplidos por todo el personal de la Municipalidad Provincial de Huancayo.
   ii. El Comité de Gobierno Digital debe monitorear el cumplimiento de la presente política, reportando los resultados al Alcalde Provincial, al menos trimestralmente.

b) Gestión de Riesgos:

El Analista de Riesgos de la Municipalidad Provincial de Huancayo asume las siguientes funciones:

- Apoya a las dependencias de la Municipalidad Provincial de Huancayo en la identificación, cuantificación y priorización de los riesgos de seguridad de la información, de acuerdo con los objetivos de la Institución.
- Propone una metodología de análisis y evaluación de riesgos de seguridad que provea un enfoque sistemático adecuado para identificar, cuantificar y priorizar los riesgos de seguridad de la información.
- Con la elaboración de los propietarios de la información y Sub Gerente de Tecnologías de la Información, o de la dependencia competente del programa, cuando corresponda, utiliza la metodología adoptada para efectuar el análisis de riesgos, a fin de poder establecer los controles apropiados para el tratamiento de cada uno de los riesgos identificados. La evaluación de riesgos debe realizarse como mínimo una vez al año y cada vez que se identifiquen cambios en la estructura, organización y normativa del Municipio.

El Comité de Gobierno Digital del Municipio aprueba la metodología y los resultados de la evaluación de riesgos.

c) Protección de la Información:
   i. La Municipalidad Provincial de Huancayo, reconoce que la seguridad de la información es un objetivo institucional que debe ser impulsado por todo su personal.
   ii. No es posible eliminar el riesgo, sino sólo mitigarlo, por lo que los controles que se definen para proteger la información deben ser determinados en base a un análisis de riesgos previo, que considere el costo beneficio de aplicarlos.

d) Clasificación de la información:
   i. Los activos de información deben ser clasificados de acuerdo con el grado de importancia para la Institución, determinada según su sensibilidad y criticidad.
   ii. Toda información se considera pública, con excepción de aquella que se encuentre clasificada como secreta, confidencial o reservada, de conformidad con lo establecido en el Texto Único Ordenado de la Ley N° 27806, Ley de Transparencia y Acceso a la Información Pública, aprobado mediante Decreto Supremo 043-2003-PCM, y su Reglamento, aprobado por Decreto Supremo N' 072-2003-PCM.

e) Uso de activos de información:
   i. Los activos de información debe ser usados para los fines y objetivos de la Municipalidad, de acuerdo con las políticas, directivas y procedimientos que se definan, y considerando criterios de buen uso.
   ii. En el marco de las relaciones que la Municipalidad establezca con terceros, los convenios, contratos y órdenes, según corresponda, consignarán cláusulas o disposiciones referidas a la confidencialidad de la información que se entregue o a la que tengan acceso, así como sobre la cesión de derechos, de corresponder.
   iii. Se debe cumplir con los requisitos legales, contractuales y normativos relativos al uso de activos de información, incluyendo las políticas de seguridad que deben mantenerse alineadas con la normatividad vigente.
   iv. Se deben guardar reserva y/o proteger los elementos de control de acceso, como contraseñas y tarjetas de identificación, según corresponda.

POLÍTICAS ESPECÍFICAS DE SEGURIDAD DE LA INFORMACIÓN DE LA MUNICIPALIDAD PROVINCIAL DE HUANCAYO

CAPÍTULO 3
(POLÍTICA DE GESTIÓN DE OPERACIONES)

3.1. OBJETIVO

a) Asegurar la operación correcta y segura de los recursos de tecnología de información de la Municipalidad Provincial de Huancayo.
b) Implementar y mantener un nivel apropiado de seguridad y de entrega de servicio, en línea con los acuerdos celebrados con terceros.
c) Minimizar el riesgo de falla de los sistemas.
d) Proteger la integridad del software y de la información.
e) Proteger la información de las redes y la infraestructura que la soporta.
f) Monitorear las actividades de procesamiento de información no autorizadas.

3.2. POLÍTICA

Las actividades de gestión sobre los recursos de tecnología de información de la Municipalidad Provincial de Huancayo son esenciales para el buen funcionamiento de los servicios de la Institución. Para tales efectos, deben considerarse los siguientes lineamientos:

a) Responsabilidades de operación:
   La Sub Gerencia de Tecnologías de la Información y Comunicación, deberá asegurar la existencia de documentación formal de sus procedimientos operativos y los recursos utilizados para su ejecución eficiente.
b) Gestión de cambios:
   i. La Sub Gerencia de Tecnologías de la Información y Comunicación, deberá mantener un registro de control de cambios de los sistemas de información, aplicaciones informáticas, equipos de comunicación, bases de datos, equipos de cómputo y perfiles de acceso, a través de la implementación de acciones y procedimientos orientados a asegurar que todo cambio siga un proceso planificado que incluya responsabilidades y canales de comunicación, identificación de los recursos comprometidos, pruebas de comprobación y estrés, controles de seguridad, reversión en caso de fallas y análisis de impacto.
   ii. Todos los cambios deben ser solicitados a la Sub Gerencia de Tecnologías de la Información y Comunicación, por el propietario de la información, y se llevará un registro sobre cada solicitud de cambio. En caso existiera algún problema con el cambio realizado, se revertirá al estado anterior al cambio.
c) Segregación de tareas:
   Se deben separar las funciones críticas y áreas de responsabilidad con la finalidad de reducir el riesgo de una modificación no autorizada o accidental o el mal uso de los activos de la Municipalidad Provincial de Huancayo.

d) Separación de los recursos para desarrollo y producción:

i. Se deben separar los recursos de prueba, desarrollo y producción; implementando los controles necesarios. Asimismo, se debe definir y documentar el procedimiento para pases de desarrollo a producción.
ii. El entorno de pruebas debe ser, en lo posible, igual al ambiente de producción, en lo referido a recursos de tecnología de información.
iii. No se deben utilizar datos que contengan información personal u otra de carácter sensible en el ambiente de pruebas.

e) Gestión y niveles de servicios externos:
   i. Se debe asegurar que todos los controles de seguridad y los Acuerdos de Niveles de Servicio (SLA, por sus siglas en inglés) suscritos con terceros sean implementados y cumplidos.
   ii. Todos los servicios provistos por terceros deben ser planificados, autorizados, monitoreados y auditados regularmente, considerando los riesgos que podrían generar.

f) Planificación y aceptación de los sistemas de información y aplicaciones informáticas:
   i. La Sub Gerencia de Tecnologías de la Información y Comunicación, debe supervisar la planificación de capacidades de los sistemas en operación y proyectará las futuras demandas, a fin de garantizar un procesamiento y almacenamiento adecuado.
   ii. La Sub Gerencia de Tecnologías de la Información y Comunicación, debe establecer los criterios y las pruebas a realizar a los sistemas existentes o nuevos que permitan al área usuaria su evaluación y aceptación formal previa a su puesta en ambiente de producción.

g) Protección contra software malicioso:
   i. La Sub Gerencia de Tecnologías de la Información y Comunicación, deberá adoptar las medidas necesarias para la prevención, detección y eliminación de código malicioso (malware) a nivel de servidores de red, computadores portátiles, estaciones de trabajo, tabletas y smartphones.
   ii. La Sub Gerencia de Tecnologías de la Información y Comunicación, debe asegurar que todas las estaciones de trabajo estén protegidas con el antivirus corporativo y que éste se encuentre actualizado. Asimismo, debe garantizar que el sistema operativo y los aplicativos de oficina cuenten con las últimas actualizaciones de seguridad (parches).
   iii. Sub Gerencia de Tecnologías de la Información y Comunicación, es responsable de la renovación de licencias de software, y deberá definir su cronograma de renovación, para evitar que se produzca incumplimiento de uso legal de software.
   iv. El software utilizado por la Municipalidad Provincial de Huancayo debe ser autorizado en forma expresa por la Sub Gerencia de Tecnologías de la Información y Comunicación, de corresponder.
   v. El usuario final no debe ser facultado para deshabilitar los sistemas de control y prevención de malware.

vi. Los equipos portátiles (Laptops, Smartphone, Tabletas y/u otro dispositivo de IoT) que, por motivos laborales o en razón del servicio contratado, según corresponda, sean autorizados a ingresar en la red de la Municipalidad, deben ser revisados por el personal de soporte técnico de la Sub Gerencia de Tecnologías de la Información y Comunicación, verificando que tengan instalado software antivirus actualizado, sistema operativo actualizado y que no exista algún software instalado que implique un riesgo de seguridad.

vii. El personal de soporte técnico de la Sub Gerencia de Tecnologías de la Información y Comunicación, como medida de prevención, si detecta que algún servidor de red, estación de trabajo, computadora portátil o dispositivo de IoT, está infectada con algún tipo de malware, deberá de desinstalarla inmediatamente, desconectándola de la red de la Municipalidad.

h) Gestión interna de respaldo y recuperación:

i. Sub Gerencia de Tecnologías de la Información y Comunicación, deberá establecer procedimientos rutinarios para el respaldo de la información, de acuerdo con su criticidad, realizando copias de seguridad y pruebas de recuperación, conforme a un cronograma definido.

ii. Las copias de seguridad deben resguardarse en un ambiente distinto al de la institución (es decir, fuera de las instalaciones de la entidad), que reúna las condiciones adecuadas de acondicionamiento, temperatura y humedad. Asimismo, los equipos y los medios de respaldo deben estar a una distancia de seguridad conveniente para evitar que se dañen por un desastre en el Data Center.

iii. Los equipos y los medios de respaldo deben contar con un programa de mantenimiento preventivo y correctivo para asegurar su correcto funcionamiento.

iv. Sub Gerencia de Tecnologías de la Información y Comunicación, debe estimar anticipadamente la cantidad necesaria de medios magnéticos requeridos para realizar las copias de respaldo y en caso de no contar con ello, solicitar su oportuna adquisición.

v. El personal de soporte técnico debe mantener el registro actualizado de las operaciones de gestión de respaldo y recuperación, así como de las fallas que pudieran presentarse y las soluciones realizadas.

vi. Se deben programar y realizar pruebas de recuperación de las copias de respaldo.

vii. Se debe revisar periódicamente la vigencia tecnológica de los equipos y software utilizados para el respaldo y recuperación de la información.

i) Diseño de la infraestructura de seguridad:

Sub Gerencia de Tecnologías de la Información y Comunicación, debe implantar los controles y medidas requeridas para proteger y conservar la seguridad de los datos en las redes y la protección de los servicios conectados contra accesos no autorizados. Estos controles deben incluir:

i. Implementación de un esquema de segmentación de redes.

ii. El desarrollo de procedimientos para la gestión remota de los recursos de tecnología de información de manera segura.
iii. Registro y monitoreo de las acciones de seguridad relevantes.
iv. Coordinación de las actividades de gestión para optimizar el servicio y para asegurar que los controles se apliquen adecuadamente a través de toda la infraestructura de procesamiento de la información.
v. Se deben establecer controles y medidas especiales para salvaguardar la confidencialidad e integridad de los datos que se transfieran a través de redes públicas, así como para proteger los sistemas conectados, tales como firewall, utm, filtro de contenidos, antispam, entre otros.

j) Buen uso de los medios de almacenamiento:
   i. Con la finalidad de prevenir daños a los recursos e interrupciones a las actividades de la Municipalidad, se deberá contar con mecanismos de seguridad que garanticen que los medios sean controlados y físicamente protegidos.
   ii. Se deben implementar controles que aseguren que todos los medios de almacenamiento que contengan información sensible sean almacenados, protegidos contra el acceso no autorizado y eliminados de manera segura y efectiva.

k) Uso adecuado de los recursos y servicios informáticos:
   i. Los recursos y servicios informáticos asignados al personal de la Municipalidad Provincial de Huancayo son de uso exclusivo para las funciones encomendadas. Está prohibido su uso para actividades que no formen parte de sus labores.

l) Seguridad del correo electrónico:
   i. La Municipalidad Provincial de Huancayo se reserva el derecho de deshabilitar una cuenta de correo electrónico por algún uso indebido que transgreda lo establecido en el presente documento.
   ii. Cada funcionario y/o servidor público es responsable por la información que se transmita desde la cuenta de correo electrónico que le haya asignado la institución.
   iii. En caso de recibir mensajes con asuntos sospechosos y/o de origen desconocido, estos deben ser eliminados sin abrir el contenido, y comunicados a la Sub gerencia de Tecnologías de Información, según corresponda, así como al Oficial de Seguridad de la Información, para los fines correspondientes.
   iv. El personal debe usar firmas estandarizadas o firmas electrónicas acorde a la Ley N°27269.
   v. El envío de mensajes masivos de correo electrónico está permitido solo para el personal o dependencias de la Municipalidad que lo requieran como parte de sus funciones. Debe ser autorizado por el superior inmediato y habilitado por la Sub Gerencia de Tecnologías de la Información y Comunicación.

vi. Solo por mandato judicial o con autorización expresa de la persona a la que se hubiera asignado una cuenta de correo institucional, La Municipalidad podrá acceder al contenido de los mensajes enviados y/o recibidos desde dicha cuenta, y por motivos debidamente justificados.

m) Registros de auditoría y monitoreo:
   i. Todos los servicios informáticos se encuentran sujetos a monitoreo por parte de la Sub Gerencia de Tecnologías de la Información y Comunicación.
   ii. Deben generarse registros de auditoría sobre el uso de los recursos de tecnología de información.
   iii. Las actividades de operadores y administradores de los sistemas deben ser monitoreadas, registradas y verificadas regularmente.
   iv. Se debe contar con registro de fallas en los sistemas, para asegurar que han sido corregidas oportunamente.
   v. Los registros de auditoría y monitoreo deben ser respaldados.

CAPÍTULO 4
(POLÍTICA DE CONTROL DE ACCESOS)

4.1. OBJETIVOS

a) Garantizar que la autorización de acceso a la información se realice de acuerdo con las atribuciones, funciones y/o tareas a desarrollar por el personal.
b) Controlar los accesos a la información.
c) Mantener el acceso autorizado del personal.
d) Prevenir accesos no autorizados a los sistemas de información y a los servicios de red.

4.2. POLÍTICA

Para el acceso a los distintos activos de información de la Municipalidad Provincial de Huancayo, se establecen los siguientes lineamientos generales:

a) Requerimientos para el control de accesos:
   Todos los accesos a los recursos de información de la Municipalidad deben basarse en la necesidad y rol del usuario, debiendo tomarse en cuenta los siguientes aspectos:
   - Los requerimientos de seguridad de cada una de las aplicaciones.
   - Identificación de toda la información relacionada a las aplicaciones y los riesgos a la que está expuesta.
   - Coherencia entre las políticas de control de accesos y las políticas de clasificación de la información.
   - Uso de perfiles de usuarios estandarizados definidos según roles.
   - Revisión periódica de los controles de acceso.
   - Revocación de los derechos de acceso.
b) Gestión de acceso del personal:

i. Con el propósito de impedir accesos no autorizados a los recursos de información, deben establecerse procedimientos formales para asignar los derechos de acceso a los sistemas.
ii. Los funcionarios son los encargados de autorizar y solicitar el acceso del personal a su cargo a los recursos de tecnología de información, conforme al procedimiento que se establezca para tal efecto. La Sub Gerencia de Gestión de Recursos Humanos, informará a la Sub Gerencia de Tecnologías de la Información y Comunicación, sobre los ceses de los trabajadores a efectos de la respectiva eliminación de accesos.
iii. La Sub Gerencia de Tecnologías de la Información y Comunicación, debe asignar un identificador (cuenta) única y exclusivo a la persona que haga uso de los recursos informáticos, ya sea de forma temporal o permanente.
iv. Deben definirse normas y procedimientos de control a nivel de sistema operativo de red, de manera que no se compartan identificadores entre diferentes usuarios ni pueda detectarse la duplicidad de sesiones de usuarios.
v. La Sub Gerencia de Tecnologías de la Información y Comunicación, debe establecer, en sus respectivos ámbitos, las normas y procedimientos para la asignación y cambio de contraseñas. Al respecto, se informará al usuario sobre lo siguiente:
    - Debe seleccionar secuencias de caracteres o palabras claras y fáciles de recordar. Se debe considerar una longitud mínima de 8 caracteres.
    - No debe considerar información relacionada directamente con el usuario (nombre, fecha de nacimiento, teléfono, etc.).
    - Cada persona es responsable de la confidencialidad de la contraseña asignada, y de las consecuencias por las acciones que, mediante su uso, terceras personas puedan realizar.
    - Las contraseñas deben ser cambiadas regularmente o cada vez que el sistema lo solicite. Está prohibido compartir las contraseñas asignadas.
    - No debe usar las contraseñas usadas en la Municipalidad para sistemas externos (por ejemplo, correo personal).
vi. Los usuarios deben bloquear su estación de trabajo si por algún motivo se retiran de su puesto de labores.
vii. Todas las estaciones de trabajo deben tener un protector de pantalla con clave y activación automática de bloqueo de usuario, cuando no se estén utilizando.
viii. El personal debe mantener sus escritorios libres de documentos y/o medios de almacenamiento removibles, cuando no los utilicen, procurando guardarlos en gabinetes con llaves cuando se retiren del centro de labores.

c) Control de acceso a las redes informáticas:
    i. El acceso a los recursos de red, internos y externos, debe ser controlado por la Sub Gerencia de Tecnologías de la Información y Comunicación, o la dependencia competente del programa, de manera que el personal no comprometa la seguridad de los activos de información.

ii. Para la seguridad en las redes informáticas, se deben tener en cuenta los siguientes aspectos:
- Lineamientos de uso de la red.
- Segmentación de redes.
- Control de conexiones a redes en base a políticas.
- Controles de enrutamiento de redes.
- Seguridad en los servicios de red.

d) Control de acceso a los sistemas operativos:
i. El acceso a los sistemas operativos de las estaciones de trabajo de la Municipalidad debe ser debidamente controlado por la Sub Gerencia de Tecnologías de la Información y Comunicación, o por la dependencia competente del programa, a fin de evitar accesos no autorizados a recursos o información.
ii. Dentro de los aspectos que deben ser tomados en consideración para definir los controles, se incluyen:
- Identificación automática de estación de trabajo.
- Procedimientos de inicio de sesión seguros.
- Identificación y autenticación de usuarios.
- Sistema de gestión de contraseñas.
- Restricción del uso de herramientas utilitarias del sistema operativo con capacidades de eludir y/o sobrescribir los controles de seguridad.
- Desconexión automática de computadoras por tiempo de inactividad.
- Limitación de horarios y tiempo de conexión.

e) Control de acceso a las aplicaciones:
i. La Sub Gerencia de Tecnologías de la Información y Comunicación, debe establecer los lineamientos de control de accesos a la información y a las aplicaciones, restringiéndolas solo para el personal debidamente autorizado; asimismo, revisa periódicamente los accesos concedidos, revocando los derechos cuya vigencia de autorización; haya caducado.
ii. Se deben aislar los sistemas identificados con información sensible, asignándoles un entorno de procesamiento dedicado, creado a partir de métodos físicos o lógicos.

f) Conexiones externas:
i. Las Gerencias, Sub Gerencias y Órganos descentralizados de la Municipalidad Provincial de Huancayo deben establecer e implementar normas y procedimientos relativos a las actividades de teletrabajo o trabajo remoto, en concordancia con lo establecido en la Ley N° 30036, Ley que regula el teletrabajo, y normas complementarias, previa opinión favorable del Comité de Gobierno Digital. Las referidas normas deberán definir las horas de acceso, el tipo de información que el tele trabajador podrá utilizar, los sistemas y servicios internos a los que estará autorizado a acceder, y el periodo de autorización de los accesos, entre otros.
ii. Las actividades de teletrabajo deben ser autorizadas por la Gerencia de Administración, a través de la Sub Gerencia de Gestión de Recursos Humanos, con sujeción a la normativa aplicable.

iii. En cualquier caso, para el acceso remoto (todo acceso a la información de la Municipalidad fuera del centro de trabajo) se debe utilizar la tecnología y acceso seguro (SSL-VPN) y su uso debe ser autorizado por el Comité de Gobierno Digital.

CAPÍTULO 5
(POLÍTICA DE ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE APLICACIONES INFORMÁTICAS)

5.1. OBJETIVOS

a) Asegurar que las aplicaciones informáticas cumplan con los requisitos de seguridad de la Municipalidad Provincial de Huancayo.
b) Evitar pérdidas, modificaciones o mal uso de la información que se encuentra dentro de las aplicaciones.
c) Proteger la confidencialidad, autenticidad e integridad de las aplicaciones informáticas de la Municipalidad Provincial de Huancayo.

5.2. POLÍTICA

a) Metodología para la adquisición, desarrollo y mantenimiento de las aplicaciones informáticas:
    i. La Municipalidad Provincial de Huancayo debe aprobar una metodología sectorial estandarizada para la adquisición, desarrollo y mantenimiento de las aplicaciones informáticas.
    ii. Todo desarrollo y/o mantenimiento de aplicaciones informáticas deberá ser documentado, con la finalidad de que personas no familiarizadas con ellas en la Municipalidad, ejecuten las actividades con facilidad.
b) Requisitos de seguridad de las aplicaciones informáticas:
    i. La Sub Gerencia de Tecnologías de la Información y Comunicación, define un procedimiento que incluya controles de seguridad durante las etapas de análisis y diseño de las aplicaciones informáticas.
    ii. Toda aplicación informática desarrollada por el personal de la Sub Gerencia de Tecnologías de la Información y Comunicación, o de la que haga sus veces en los programas, o por terceros, debe satisfacer los requisitos de seguridad definidos para el desarrollo y mantenimiento de las aplicaciones informáticas. En el caso de los terceros, el desarrollo de las aplicaciones debe constar en el respectivo contrato de prestación de servicios.
    iii. El personal debe cumplir los controles, estándares y metodologías referidas al desarrollo de las aplicaciones informáticas que se hayan implementado.

iv. La Sub Gerencia de Tecnologías de la Información y Comunicación, debe verificar que los acuerdos sobre materia informática a suscribir con terceros, incluyan cláusulas relativas a la cesión de derechos y la confidencialidad de la información, para el resguardo de la propiedad intelectual de la Municipalidad.

v. Los acuerdos que involucran el acceso, procesamiento, comunicación o manejo de terceros de las instalaciones de procesamiento de información, deben cubrir los requisitos de seguridad necesarios.

vi. Toda aplicación informática desarrollada por el personal es de propiedad de la Municipalidad Provincial de Huancayo (Incluye código fuente, ejecutables, macros, gráficos, imágenes y demás que formen parte de la aplicación).

c) Procesamiento correcto de las aplicaciones:

i. Se deben implementar controles de seguridad apropiados en las aplicaciones utilizadas por la Municipalidad, para validar los datos de entrada, el procesamiento interno y los datos de salida.

ii. La validación de los datos de entrada debe tener un procedimiento que permita determinar las responsabilidades de todo el personal involucrado en el proceso de entrada de datos.

iii. Para el control del proceso interno, se deben realizar comprobaciones del correcto funcionamiento del proceso (validación de los datos generados por la aplicación, tiempos de respuesta, funciones para cambio de datos, alertas para el procesamiento).

iv. Deben identificarse los requerimientos para asegurar la autenticidad y la integridad de los mensajes en las aplicaciones, debiendo definirse e implementarse los controles apropiados.

v. La validación de datos de salida debe realizarse a fin de asegurar el correcto procesa miente de la información. Asimismo, deben definirse las responsabilidades de todos los involucrados en el proceso de salida de datos.

d) Seguridad de los archivos de las aplicaciones informáticas:
Se deben implementar controles sobre lo siguiente:

i. Control de la aplicación informática en Producción: Comprende la formulación y puesta en práctica de procedimientos orientados a controlar la instalación de la aplicación en los sistemas en producción.

ii. Protección de Datos de Prueba: Los datos de prueba de las aplicaciones informáticas deben ser cuidadosamente seleccionados, protegidos y controlados.

e) Control de acceso al Código Fuente de la aplicación informática:

i. Se debe restringir y controlar el acceso al código fuente de las aplicaciones informáticas o programas.

ii. Se debe contar con un responsable del acceso al código fuente de las aplicaciones informáticas, quien deberá implementar un registro de uso, si es que el código es requerido.

f) Uso de controles criptográficos:

Se debe implementar el uso de controles para cifrar la información y proteger la confidencialidad, autenticidad e integridad de la misma, cuando sea requerido, y de acuerdo al nivel de exposición al riesgo.

g) Seguridad en los procesos de desarrollo y pase a producción:
   i. Procedimiento para el desarrollo de las aplicaciones informáticas:
      Todo desarrollo y mantenimiento de las aplicaciones informáticas en la Municipalidad debe ser realizado conforme a los procedimientos establecidos, debiendo considerarse como mínimo las siguientes etapas:
      1. Fase de análisis.
      2. Fase de diseño.
      3. Fase de construcción.
      4. Fase de implantación y aceptación.
      5. Fase de elaboración de documentación técnico y de usuario.
   ii. Procedimiento para pase a producción:
      1. El personal encargado del desarrollo y mantenimiento de las aplicaciones informáticas, así como los terceros, no tendrán acceso a los datos de producción. Los datos sensibles con los que trabajen deben ser diferentes a los datos del ambiente de producción.
      2. Los ambientes de desarrollo y producción deben ser configurados en servidores diferentes, limitando el acceso solo al personal autorizado.
      3. El pase a producción debe ser realizado exclusivamente por la persona autorizada por la Sub Gerencia de Tecnologías de la Información y Comunicación, quien llevará un control de los pases efectuados y/o actualizaciones de las aplicaciones informáticas en un registro o bitácora.
      4. Todo desarrollo, antes de su pase a producción, debe ser revisado por la Sub Gerencia de Tecnologías de la Información y Comunicación, para asegurar que se cumplan los estándares establecidos por dicha oficina.

   iii. Análisis de requerimientos de aplicaciones:
      Se deben definir los requerimientos referidos a arquitectura, tecnología necesaria, seguridad y otros requerimientos especiales.

h) Control de cambios de las aplicaciones:
   i. El control, registro y monitoreo de los cambios de las aplicaciones informáticas de la Municipalidad debe ser supervisado y registrado por la Sub Gerencia de Tecnologías de la Información y Comunicación.
   ii. El proceso de control de cambios debe considerar:

5. Planificación del cambio.
6. Responsabilidades y canales de comunicación.
7. Identificación de los recursos comprometidos.
8. Pruebas de comprobación y estrés, controles de seguridad y reversión en ambiente de desarrollo.
9. Análisis de impacto.
10. Registro documentado de los cambios.

11. Acta de conformidad de puesta en producción.
    i. Todo acceso a la librería de los programas fuente será controlado por la Sub Gerencia de Tecnologías de la Información y Comunicación, para evitar accesos y/o cambios no autorizados.
    ii. Todo cambio efectuado en las aplicaciones informáticas de la Municipalidad deberá ser documentado, contar con un registro de los cambios efectuados, y ser archivado por la Sub Gerencia de Tecnologías de la Información y Comunicación.
    iii. La Sub Gerencia de Tecnologías de la Información y Comunicación, debe efectuar revisiones periódicas de las aplicaciones informáticas en el ambiente de producción, a fin de asegurar que sólo se hayan efectuado los cambios autorizados.

i) Gestión de vulnerabilidades técnicas:
    i. La Sub Gerencia de Tecnologías de la Información y Comunicación, debe programar la realización de pruebas de comprobación técnica a cargo de especialistas externos para verificar que se han implementado correctamente los controles de seguridad definidos para el hardware y software.
    ii. Identificadas las vulnerabilidades técnicas, se deben determinar los riesgos asociados e implementar los controles necesarios para mitigarlos. Las aplicaciones informáticas críticas y en alto riesgo deben ser tratadas primero.
    iii. Para la aplicación de una actualización de seguridad (parches) se debe probar y evaluar su efectividad en un ambiente de pruebas: asimismo, se deben considerar los riesgos asociados a su aplicación y, en todos los casos, se deben cumplir los controles establecidos para la gestión de cambios.

CAPÍTULO 6
(POLÍTICA DE GESTIÓN DE INCIDENTES)

6.1.OBJETIVO

Asegurar que los eventos y debilidades en la seguridad de la información de la Municipalidad, asociados con los sistemas de información y aplicaciones informáticas, sean comunicados oportunamente a las instancias correspondientes, con la finalidad de adoptar acciones correctivas a tiempo. Se aplica a todos los funcionarios y servidores públicos de la organización.

6.2.POLÍTICA

a) Reporte de eventos y debilidades de la Seguridad de la Información:
    i. Los incidentes relativos a la seguridad de la información deben comunicarse a la Sub Gerencia de Tecnologías de la Información y Comunicación, y al Oficial de Seguridad de la Información, conforme al procedimiento que se establezca para tal efecto.

ii. El personal de la Municipalidad debe conocer el procedimiento de comunicación de incidentes de seguridad, e informar de su ocurrencia tan pronto tome conocimiento de ellos.

iii. Son considerados incidentes de seguridad para la Municipalidad:

1) Pérdida de servicio, equipos o instalaciones (disponibilidad del servicio de TI).
2) Sobrecargas en los sistemas (software y hardware).
3) Errores humanos en uso de los sistemas y aplicaciones informáticas.
4) Incumplimientos de políticas, normas y/o procedimientos sobre seguridad de la información.
5) Cambios no controlados en los sistemas (software y hardware) y servicios.
6) Fallas en software y/o hardware.
7) Violaciones de acceso a los sistemas y aplicaciones informáticas.
8) Ataques por software de tipo malicioso (malware).
9) Correos fraudulentos (phishing) solicitando información del usuario.
10) Pérdida o fuga de Información.
11) Uso indebido del correo electrónico.
12) Detección de vulnerabilidades de la seguridad.
13) Ataques de secuestro de información (ransomware).

b) Gestión de las mejoras e incidentes en la seguridad de información:

i. El personal de la Municipalidad debe conocer su responsabilidad respecto a la comunicación de los incidentes de seguridad que tome conocimiento, debiendo ser notificados de los resultados una vez que el incidente haya sido resuelto.

ii. Reportados los incidentes de seguridad a la Sub Gerencia de Tecnologías de la Información y Comunicación, y al Oficial de Seguridad de la Información, se debe proceder a su exhaustivo análisis por parte del personal que designe la referida oficina o dependencia del programa, a efectos de adoptar las acciones que correspondan.

iii. Los incidentes de seguridad serán evaluados por el Comité de Gobierno Digital, a efectos de proponer las acciones preventivas que correspondan, para lo sucesivo.

iv. El personal comprendido en el incidente de seguridad podrá ser sancionado, conforme a la normatividad vigente.

v. Periódicamente, la Sub Gerencia de Tecnologías de la Información y Comunicación, o la dependencia competente del programa, deberá analizar las actividades realizadas y estudiar posibles mejoras o cambios que puedan proponerse al Comité de Gobierno Digital para prevenir la ocurrencia de futuros incidentes.

CAPÍTULO 7
(POLÍTICA DE ESCRITORIO LIMPIO)

7.1. OBJETIVO

Establecer los requisitos mínimos para mantener un "escritorio limpio". Se aplica a todos los funcionarios y servidores públicos de la organización.

7.2. POLÍTICA

a) Los empleados deben asegurarse de que toda la información sensible / confidencial en forma impresa o electrónica esté segura en su área de trabajo al final del día y cuando se espera que se vayan por un período prolongado.
b) Las estaciones de trabajo de los equipos deben estar bloqueadas cuando no estén en uso. Si utiliza el sistema operativo Windows puede bloquear la estación con la combinación simultanea de las teclas Windows + L.
c) Las estaciones de trabajo de la computadora deben estar completamente apagadas al final de la jornada laboral.
d) Las estaciones de trabajo de la computadora que se dejen de usar por periodos mayores a 1 hora deben pasar al modo "Suspender".
e) Cualquier información restringida o sensible debe retirarse del escritorio y encerrarse en un cajón cuando el escritorio esté desocupado y al final de la jornada laboral.
f) Los archivadores que contienen información restringida o confidencial deben mantenerse cerrados y bloqueados cuando no estén en uso o cuando no estén atendidos.
g) Las claves utilizadas para acceder a información restringida o confidencial no deben dejarse en un mostrador desatendido.
h) Las computadoras portátiles deben estar bloqueadas con un cable de bloqueo o encerradas en un cajón.
i) Las contraseñas no se pueden dejar en notas adhesivas publicadas en o debajo de una computadora, ni pueden dejarse escritas en un lugar accesible.
j) Las impresiones que contengan información restringida o confidencial deben eliminarse inmediatamente de la impresora.
k) Una vez eliminados, los documentos restringidos y/o sensibles deben romperse y colocarse en los contenedores de eliminación confidenciales de la cerradura.
l) Las pizarras que contengan información restringida y/o confidencial deben borrarse.
m) Bloquee los dispositivos informáticos portátiles, como computadoras portátiles y tabletas.
n) Trate los dispositivos de almacenamiento masivo como CDROM, DVD o unidades USB como sensibles y asegúrelos en un cajón cerrado.
o) Todas las impresoras deben limpiarse de papel tan pronto como se impriman; esto ayuda a garantizar que los documentos confidenciales no se dejen en bandejas de impresora para que la persona equivocada los recoja.

CAPÍTULO 8
(POLÍTICA DE USO DEL CORREO ELECTRÓNICO)

8.1. OBJETIVO

Garantizar el uso adecuado del sistema de correo electrónico y hacer que los usuarios sean conscientes de lo que se considera como uso aceptable e inaceptable de su sistema de correo electrónico. Esta política describe los requisitos mínimos para el uso del correo electrónico dentro de la Red de la organización.

Esta política cubre el uso apropiado de cualquier correo electrónico enviado desde una dirección de correo electrónico de <muni.gob.pe> y se aplica a todos los funcionarios y servidores públicos de la organización que operan en nombre de dominio <muni.gob.pe>.

8.2. POLÍTICA

a) Todo uso del correo electrónico debe ser consistente con las políticas y procedimientos de conducta ética, seguridad, cumplimiento de las leyes aplicables y prácticas comerciales adecuadas.
b) No comparta la contraseña de su cuenta de correo electrónico con nadie.
c) Utilice la delegación, cuando corresponda, si otro usuario necesita acceso a su correo electrónico.
d) No utilice el correo electrónico para acosar a otros.
e) No falsifique cuentas de correo electrónico para enviar correos electrónicos como otra persona.
f) No inunde / envíe spam a las personas con correo electrónico en un intento de interrumpir su servicio.
g) No acepte números de tarjetas de crédito enviados por correo electrónico para fines de pago.
h) No cree reglas que permitan el reenvío automatizado a cuentas de correo electrónico que no sean de la institución.
i) No envíe datos confidenciales a ninguna parte por correo electrónico sin usar cifrado.
j) No utilices direcciones de correo electrónico personales, como Gmail o Yahoo!, para comunicaciones relacionadas con el trabajo.
k) La cuenta de correo electrónico debe usarse principalmente para fines institucionales; la comunicación personal está permitida de forma limitada, pero no para usos institucionales relacionados, en este caso están prohibidos.
l) Todos los datos contenidos en un mensaje de correo electrónico o un archivo adjunto deben protegerse de acuerdo con el Estándar de Protección de Datos.
m) El correo electrónico debe conservarse solo si califica como un registro comercial.
n) El correo electrónico que se identifica como un registro comercial, se conservará de acuerdo con la Programación de retención de registros.
o) El sistema de correo electrónico no se utilizará para la creación o distribución de mensajes perturbadores u ofensivos, incluidos comentarios ofensivos sobre raza, género, color de cabello, discapacidades, edad, orientación sexual, pornografía, creencias y prácticas religiosas, creencias políticas u origen nacional. Los empleados que reciban correos electrónicos con este contenido de cualquier empleado de deberá informar el asunto a su supervisor de inmediato.

p) Los usuarios tienen prohibido reenviar automáticamente un correo electrónico a un sistema de correo electrónico de terceros. Los mensajes individuales que son reenviados por el usuario no deben contener información confidencial o superior.
q) Los usuarios tienen prohibido utilizar sistemas de correo electrónico y servidores de almacenamiento de terceros como Google, Yahoo y MSN Hotmail, etc. para llevar a cabo un negocio, para crear o conmemorar cualquier transacción vinculante, o para almacenar o retener correo electrónico en nombre de la organización. Dichas comunicaciones y transacciones deben llevarse a cabo a través de los canales adecuados utilizando documentación aprobada.
r) El uso de una cantidad razonable de recursos para correos electrónicos personales es aceptable, pero el correo electrónico no relacionado con el trabajo se guardará en una carpeta separada del correo electrónico relacionado con el trabajo. Está prohibido enviar cartas en cadena o correos electrónicos de broma desde una cuenta de correo electrónico de la organización.
s) El tamaño de todos los mensajes de correo electrónico salientes y entrantes, incluidos los archivos adjuntos, a 20 megabytes (MB).
t) Cualquier dato considerado como de naturaleza confidencial que deba transmitirse por correo electrónico utilizará cifrado cuando se envíe a través de una red insegura y solo se enviará a destinatarios que tengan una necesidad legítima de la información.
u) El correo electrónico enviado dentro de la red interna se considera contenido dentro de un entorno seguro de confianza.
v) Aviso de confidencialidad que deberá ir al final de todo correo: "Aviso de confidencialidad: Esta transmisión de correo electrónico, y cualquier documento, archivo o mensaje de correo electrónico anterior adjunto a ella, pueden contener información confidencial y / o privilegiada y pueden estar legalmente protegidos contra la divulgación. Cualquier revisión, uso, divulgación o distribución no autorizada está estrictamente prohibida. Si usted no es el destinatario previsto, o una persona responsable de entregarlo al destinatario previsto, comuníquese con el remitente por correo electrónico de respuesta y destruya todas las copias del mensaje original, incluidos los archivos adjuntos."
w) La delegación se produce cuando el propietario de una cuenta de correo electrónico (el "delegado") concede permisos a otro usuario ("el delegado") para acceder al correo electrónico, el calendario y/o los contactos del propietario. La delegación no está permitida compartiendo contraseñas o iniciando sesión en la cuenta para que la use el delegado: el delegado debe usar su propia cuenta.

CAPÍTULO 9
(POLÍTICA DE EQUIPOS DE COMUNICACIONES)

9.1. OBJETIVO

Es establecer los requisitos mínimos para las configuraciones de seguridad de "equipos de comunicaciones". Se aplica a todos los funcionarios y servidores públicos de la organización.

9.2. POLÍTICA

a) Las características de seguridad necesarias para minimizar los riesgos para los equipos de comunicación deben configurarse en el equipo antes de su puesta en servicio.
b) Debe haber dos roles posibles para el personal que administra el equipo de comunicación: supervisor y administrador.
c) El rol de supervisor debe tener privilegios de solo lectura.
d) El rol de administrador debe poder cambiar los parámetros de configuración.
e) Se debe registrar todos los comandos emitidos por los usuarios en un log, así como cualquier otro evento de seguridad que pueda representar una amenaza para el equipo.
f) Los usuarios locales no están permitidos en los equipos de comunicación.
g) Todos deben autenticarse a través del repositorio central de usuarios (Directorio Activo) utilizando un protocolo que reduce el riesgo de robo de identidad.
h) Toda la información transmitida desde el dispositivo debe estar cifrada por un algoritmo de cifrado fuerte para minimizar los riesgos de espiar las comunicaciones y los ataques man-in-the-middle.
i) Los eventos registrados por el equipo de comunicación deben mantenerse en medios de almacenamiento que estén sujetos a un proceso de copia de seguridad regular, es conveniente que estos eventos o logs se envíen a un centralizador de logs.
j) El proceso de mantenimiento de las copias de seguridad debe garantizar que la información no se modifique.
k) Si, por cualquier motivo, es necesario hacer uso de los más altos privilegios administrativos dentro del dispositivo, entonces el personal debe presentar una solicitud a la división de seguridad interna para la contraseña adjuntando la justificación de su uso y completando los formularios requeridos.
l) La contraseña debe ser restablecida por el administrador más alto para mantener la seguridad.

CAPÍTULO 10
(POLÍTICA DE MEDIOS EXTRAÍBLES)

10.1. OBJETIVO

Minimizar el riesgo de pérdida o exposición de información confidencial mantenida en "medios extraíbles". Se aplica a todos los funcionarios y servidores públicos de la organización.

10.2. POLÍTICA

a) Si es posible se debe restringir el uso de medios extraíbles.
b) Solo si es absolutamente necesario de debe utilizar dispositivos de medios extraíbles.
c) Se debe utilizar los medios extraíbles de forma segura y protegida (información confidencial).
d) Se debe utilizar los dispositivos de medios extraíbles solo con fines laborales.
e) Se debe asegurar que la estación de trabajo no tenga habilitada la función de ejecución automática.

f) Se debe limitar la copia de archivos mediante medios extraíbles, a menos que sea necesario o haya sido autorizado, se recomienda tener un sistema DLP (prevención de pérdida de datos).
g) Se debe escanear los medios extraíbles en busca de malware antes de transferir información.
h) Se debe aplicar protección con contraseña al medio extraíble de almacenamiento.
i) Se debe cifrar cualquier información contenida en un dispositivo de almacenamiento extraíble.
j) Los empleados deben informar al Oficial de Seguridad de la Información o a la Sub Gerencia de Tecnologías de la Información y Comunicación sobre los dispositivos de medios extraíbles perdidos.

CAPÍTULO 11
(POLÍTICA DE SEGURIDAD DE LA RED)

11.1. OBJETIVO

Es establecer los requisitos mínimos para mantener la "seguridad de la red". Se aplica a todos los funcionarios y servidores públicos de la organización.

11.2. POLÍTICA

a) Se deben administrar y controlar las redes para proteger la información en los sistemas y aplicaciones.
b) Los usuarios privilegiados autorizados deben utilizar dispositivos dedicados que estén técnicamente segregados y asegurados al mismo nivel que las redes y los sistemas que se mantienen.
c) Los mecanismos de seguridad, los niveles de servicio y los requisitos de gestión de todos los servicios de red, se deben identificar e incluir en los acuerdos de servicios de red, ya sea que estos servicios se proporcionen internamente o se subcontraten.
d) Todos los dispositivos de red, excepto los cortafuegos, deben ser accesibles desde dentro de la red privada.
e) Todas las conexiones de red deben pasar a través de un cortafuegos.
f) Se debe llevar a cabo una evaluación de riesgos antes de que se permitan enlaces y, cuando corresponda, se debe implementar medidas de seguridad adicionales.
g) La conectividad entrante a la red se debe permitir desde una VPN.
h) La conectividad entrante desde Internet se debe permitir a dispositivos designados en la DMZ usando Servicios TCP / IP.
i) Los cambios en el firewall deben pasar por solicitud y autorización.
j) Cada enrutador debe cumplir con la configuración estándar.
k) Cada enrutador y conmutador debe utilizar el proceso de autenticación y administración estándar.
l) Todas las contraseñas de enrutador / conmutador deben estar cifradas.
m) Los protocolos de enrutamiento dinámico deben utilizar la autenticación en las actualizaciones de enrutamiento.
n) El hash de contraseña para la cadena de autenticación debe estar habilitado cuando sea compatible.
o) El administrador de red debe verificar el cumplimiento de la política.

p) Los dispositivos inalámbricos deben cumplir las condiciones de esta política y ser aprobados para la conectividad a la red.
q) Los dispositivos deben ser instalados, respaldados y mantenidos por un equipo de soporte aprobado.
r) Los dispositivos deben usar protocolos de cifrado.
s) Se debe deshabilitar cualquier dispositivo que presente un riesgo para la red.
t) Se debe supervisar el tráfico entrante y saliente, y los flujos de datos de todos los puntos finales dentro de la red.
u) Se debe revisar la red continuamente de acuerdo con las mejores prácticas y utilización del proveedor.
v) Se debe realizar un control de cambios formal e incluir la actualización de la documentación y los diagramas de red que se almacenan de forma segura.
w) Se debe utilizar VLAN para proporcionar segmentación de la red cuando no se pueden aplicar políticas de seguridad corporativas.

CAPÍTULO 12
(POLÍTICA DE AUDITORÍA DE SISTEMAS)

12.1. OBJETIVO

Es obtener evidencias de cómo los sistemas de información cumplen con los requisitos de seguridad deseados. Se aplica a todos los funcionarios y servidores públicos de la organización.

12.2. POLÍTICA

a) Se debe tener identificado los activos más relevantes que deben ser auditados, estos activos pueden ser desde archivos, bases de datos, páginas web, equipos o programas hasta servicios completos.
b) Se debe enfocar el proceso de auditoría desde un punto de vista de mejora continua o de consecución de niveles de madurez.
c) Se debe realizar auditorías específicas para verificar el cumplimiento de los requerimientos legales.
d) Se debe realizar auditorías forenses para determinar lo ocurrido tras un incidente de seguridad.
e) Se debe definir y/o revisar los procedimientos detallados para auditar la seguridad de cada activo clave de los sistemas de información.
f) Se debe seleccionar el tipo de auditoría más conveniente, como, por ejemplo: test de penetración, auditoría de red, auditoría de seguridad perimetral, auditoría web, auditoría forense, auditoría legal, etc.
g) Se debe definir con detalle los procedimientos y logs necesarios para realizar cada tipo de auditoría.
h) Se debe concretar cómo registrar los resultados de las revisiones.
i) Se debe realizar auditorías de los sistemas de información al menos dos veces por año.
j) Se debe evaluar si se repite las auditorías tras la implantación de algún cambio significativo en los sistemas.
k) Se debe analizar los resultados de la auditoría en busca de debilidades a corregir.

CAPÍTULO 13
(POLÍTICA DE INSTALACIÓN DE SOFTWARE)

13.1. OBJETIVO

Es describir los requisitos en torno al software de instalación en dispositivos informáticos.

13.2. POLÍTICA

a) Todo el software instalado en los sistemas, debe cumplir con las pautas de licencia de software aplicables.
b) La especificación de software de prueba también debe ser registrada previamente como tal.
c) La especificación de software de prueba también debe seguir procedimientos y controles respectivos.
d) Todas las licencias deben actualizarse anualmente.
e) Los empleados no deben instalar software en los dispositivos.
f) El software debe seleccionarse de una lista de software aprobada.
g) El personal de tecnología debe obtener información, rastrear las licencias y probar el nuevo software.
h) El personal debe reportar si se detecta conflictos y/o compatibilidad después de instalado el software.
i) El software instalado no debe entrar en conflicto con las aplicaciones y los controladores de dispositivos existentes.
j) Todos los hosts basados en PC deben ser protegidos por antivirus aprobado, antes de la conexión de red.

CAPÍTULO 14
(POLÍTICA DE ACTUALIZACIÓN DE SOFTWARE)

14.1. OBJETIVO

Revisar la existencia de actualizaciones y parches de seguridad para el software instalado. Y elaborar procedimientos que permitan que tales actualizaciones y parches sean instalados en los equipos de forma segura y controlada.

14.2. POLÍTICA

a) Se debe realizar un inventario del software y firmware instalado, ya que pueden descubrirse errores o mejoras de funcionalidad.
b) Se debe realizar un listado del software actualmente existente en la organización, para incluirlo en el plan de actualizaciones.
c) Se debe determinar el momento específico para ejecutar las actualizaciones, de este modo no interferir con las operaciones de la organización.
d) Se debe usar los canales de alerta y los procedimientos oportunos para detectar e instalar las actualizaciones correspondientes.
e) Antes de la actualización se debe considerar la utilidad de las nuevas mejoras y la gravedad los errores que subsanan, así como los requisitos hardware/software necesarios.
f) Se debe instalar actualizaciones provenientes de fuentes confiables.
g) Se debe revisar las características y los requisitos de las actualizaciones y parches antes de instalarlos.

h) Se debe analizar y contrastar en un entorno de pruebas las actualizaciones que se desea instalar.
i) Se debe contar con los mecanismos y procedimientos adecuados para deshacer los cambios sufridos tras ejecutar una actualización en caso de no resultar conveniente.
j) Se debe utilizar herramientas de autodiagnóstico para detectar software no actualizado en los equipos.
k) Se debe tener configurado un sistema de alertas para recibir avisos y notificaciones sobre vulnerabilidades, actualizaciones y parches de seguridad.
l) Se debe registrar cada una de las actualizaciones y parches que se instala.

CAPÍTULO 15
(POLÍTICA DE CONCIENTIZACIÓN Y FORMACIÓN)

15.1. OBJETIVO

Es asegurar que, en todo momento, los empleados conocen, entienden y cumplan las normas y las medidas de protección en materia de ciberseguridad y seguridad de la información adoptadas, advirtiéndoles de los riesgos que puede suponer un mal uso de los dispositivos y soluciones tecnológicas a su alcance.

15.2. POLÍTICA

a) Se debe documentar y difundir las normas de ciberseguridad y seguridad de la información de la organización para que estén siempre accesibles.
b) Las normas de ciberseguridad y seguridad de la información de la organización deben estar correctamente documentadas y al alcance de todo el personal en todo momento.
c) Se debe elaborar o revisar el plan de formación para elevar el nivel de seguridad digital.
d) Se debe desarrollar programas de formación y concientización especializados para ciertos perfiles de empleados en ciberseguridad y seguridad de la información.
e) Se debe elaborar una actividad formativa introductoria para los nuevos empleados.
f) Se debe desarrollar y aplicar programas de formación en ciberseguridad y seguridad de información adecuados a los distintos puestos de trabajo.
g) Los empleados deben realizar cursos o charlas de concientización, al menos dos veces al año.
h) Se debe comprobar la asimilación del conocimiento adquirido por los empleados.
i) Se debe evaluar el aprendizaje obtenido por los empleados, para determinar el grado de concientización y formación alcanzado.
j) Se debe promover una cultura de seguridad de la información.
k) Se debe coordinar el uso de la plataforma del Centro de Conocimiento Digital en todas las entidades.

CAPÍTULO 16
(POLÍTICA DE USO DE INTERNET)

16.1. OBJETIVO

Es definir lo que está permitido o no, a fin de que la organización pueda atender las necesidades esenciales para que los colaboradores puedan desempeñar sus funciones en un ambiente de calidad.

16.2. POLÍTICA

a) El acceso a internet debe ser solo de interés laboral y no personal.
b) Todos los usuarios deben seguir los principios corporativos con respecto al uso de los recursos y ejercer un buen juicio en el uso de Internet.
c) El uso aceptable de internet debe incluir la comunicación entre empleados y no empleados con fines comerciales.
d) El uso aceptable de internet debe incluir el soporte técnico de TI para descargar actualizaciones y parches de software.
e) El uso aceptable de internet debe incluir la revisión de posibles sitios web de proveedores para obtener información sobre productos.
f) El uso aceptable de internet debe incluir información reglamentaria o técnica de referencia.
g) El uso aceptable de internet debe incluir temas de investigación.
h) No se debe ingresar a páginas con temas de violencia, pornografías u otros contenidos inapropiados.
i) Se debe mantener en todo momento la confidencialidad de sus datos de acceso a internet, siendo el único responsable del buen o mal uso de sus datos de acceso.
j) Se debe notificar de manera inmediata al área de Soporte Técnico cualquier uso no autorizado de su cuenta o cualquier otra observación de seguridad.
k) Se debe usar herramientas de software instaladas que habiliten servicios potencialmente riesgosos para la organización.
l) Solo se debe manejar correos electrónicos institucionales.
m) El uso de los datos confidenciales de la organización debe ser de acceso restringido.
n) Se debe usar sitios web oficialmente permitidos (https).

CAPÍTULO 17
(POLÍTICA DE CLASIFICACIÓN DE LA INFORMACIÓN)

17.1. OBJETIVO

Es clasificar los activos de información para garantizar una eficaz gestión de su seguridad con criterios de confidencialidad, disponibilidad e integridad.

17.2. POLÍTICA

a) Se debe elaborar un inventario detallado de los activos de información de la organización.
b) Se debe considerar registrar aspectos tales como su tamaño, ubicación, servicios o departamentos a los que pertenecen, quienes son sus responsables, etc.
c) Se debe etiquetar los activos de información según los criterios de seguridad establecidos.

d) Se debe establecer una lista con todos los tratamientos de seguridad de la información.
e) Se debe considerar dentro de la lista de tratamientos de seguridad de la información las herramientas de cifrado, sistemas de copias de seguridad, sistemas de control de acceso, entre otros.
f) Se debe asignar los tratamientos de seguridad oportunos para cada tipo de información.
g) Se debe aplicar los tratamientos de seguridad oportunos para cada tipo de información.
h) Se debe realizar auditorías de comprobación al menos dos veces al año.
i) Se debe incluir las políticas de almacenamiento en la nube.

CAPÍTULO 18
(POLÍTICA DE ALMACENAMIENTO EN LA NUBE)

18.1. OBJETIVO

Es establecer en qué casos se permite utilizar el almacenamiento en la nube y mantener de modo seguro la información almacenada en la nube, especificando reglas, criterios y procedimientos que deben seguir todos los empleados que usen estos servicios.

18.2. POLÍTICA

a) Se debe informar a los empleados sobre si se permite o se prohíbe el uso de servicios de almacenamiento en nube pública.
b) Se debe elaborar una lista donde los empleados pueden consultar qué servicios de almacenamiento en la nube están permitidos y cuáles no.
c) Se debe evitare el uso de servicios de almacenamiento que no consideremos seguros.
d) Se debe informar al personal sobre el procedimiento de borrado adecuado para los repositorios de información en la nube.
e) Se debe informar a los empleados del tipo de información que pueden almacenar en la nube.
f) Se debe informar a los empleados si la información almacenada en la nube necesita ser cifrada.
g) Se deberá incluir la información almacenada en la nube cifrada en la política de clasificación de la información.
h) Se debe valorar las ventajas e inconvenientes antes de almacenar las copias de seguridad en la nube.
i) Se debe contratar un servicio de almacenamiento en la nube que cumpla con los criterios organizativos y obligaciones legales.
j) Se debe considerar como criterios de seguridad específicos la garantía de confidencialidad, disponibilidad de la información, copias de seguridad, entre otros.
k) Se debe conocer la política de seguridad del proveedor de servicios de almacenamiento en la nube.
l) Se debe conocer las seguridades técnicas que ofrece la nube y éstas deberán ser evaluadas por el área responsable de TI en la organización.

CAPÍTULO 19
(POLÍTICA DE TRANSFERENCIA DE INFORMACIÓN Y DATOS)

19.1. OBJETIVO

Es establecer mantener la seguridad de la información y los datos transferidos, dentro de la organización y con cualquier entidad externa.

19.2. POLÍTICA

a) Se debe autenticar la identidad y autorización del destinatario para una transferencia de información de forma segura.
b) Se debe utilizar un proceso de transferencia seguro aprobado.
c) Se debe proteger los datos confidenciales.
d) Se debe cifrar los datos.
e) Debe existir un acuerdo de procesamiento de datos entre las organizaciones para el propósito especificado.
f) Los usuarios pueden intercambiar información confidencial de forma segura, pero debe ser dentro de la organización o con otros usuarios que se encuentren dentro del límite de correo electrónico seguro.
g) Si los usuarios necesitan intercambiar información de forma segura fuera del límite de correo electrónico seguro, deben utilizar el cifrado.
h) Debe usarse el cifrado para intercambiar datos confidenciales como parte de un flujo de trabajo acordado.
i) Los usuarios deben seguir las políticas locales de gobernanza de la información que se establezcan localmente para el envío de datos confidenciales.
j) Las soluciones de correo electrónico deben utilizar las comprobaciones pertinentes.
k) Los acuerdos de confidencialidad o no divulgación que reflejen las necesidades de la organización para la protección de la información deben ser identificadas, revisadas y documentadas periódicamente.
l) Se debe contar con los medios físicos o técnicos adecuados para la protección de datos.
m) Se debe monitorear los flujos de información y datos en toda transferencia.
n) Se debe identificar los enlaces de red asociados y se cuenta con la protección adecuada.
o) Los acuerdos deben abordar la transferencia segura de información comercial entre la organización y partes externas.
p) La información relacionada con la mensajería electrónica debe estar debidamente protegida.

CAPÍTULO 20
(POLÍTICA DE USO DE TÉCNICAS CRIPTOGRÁFICAS)

20.1. OBJETIVO

Es asegurar el uso efectivo de la criptografía para proteger la confidencialidad, autenticidad y/o integridad de la información.

20.2. POLÍTICA

a) Se deben tomar las medidas técnicas y organizativas adecuadas contra procesamiento no autorizado o ilegal de datos personales y contra pérdida accidental o destrucción o daño de datos personales.
b) Los datos deben estar protegidos física o técnicamente cuando los datos se mantienen dentro de un centro de datos, se recomiendan que estén cifrados.
c) Cuando los datos se guardan en la estación de trabajo o servidor fuera de una computadora deben estar físicamente asegurada el área y los datos o el disco deberá estar cifrado.
d) Cuando los datos están en posesión de un proveedor, deben estar cifrados.
e) Mientras se transfieren datos de un dispositivo a otro, a través de una red, ya sea a través de Internet o mediante una conexión inalámbrica, los datos deben estar cifrados.
f) Se debe utilizar al menos WPA3 con protocolo de seguridad para conexiones inalámbricas.
g) Se deben utilizar el protocolo https para todas las páginas internas y externas de la organización.
h) Cuando los datos se transfieren en medios extraíbles, los medios deben estar cifrados. La clave de descifrado debe pasarse al destinatario por separado.
i) Cuando las aplicaciones o bases de datos se alojan fuera del centro de datos deben estar cifradas.
j) Para el descifrado se debe tener una contraseña compleja de al menos 20 caracteres.
k) Todas las computadoras portátiles y tabletas deben estar cifradas.
l) Los dispositivos con Windows 10 o 11 deben estar cifrados.
m) Se debería crear una autoridad de certificación (CA) interna que solo permita dispositivos conocidos para acceder a los sistemas.
n) Los servicios de acceso a Internet deben admitir conexiones cifradas al tener un certificado firmado Secure Socket Layer (SSL) aprobado.
o) Cuando se accede a los servicios a través de un túnel VPN, el túnel debe estar cifrado.
p) La generación de claves no debe ser predecible y generada al azar.
q) El acceso a los códigos clave debe estar restringido a las personas clave.
r) Solo se deben usar algoritmos criptográficos confiables y verificados.
s) Asegúrese de que la longitud de las claves sea proporcional a la información que se protege

CAPÍTULO 21
(POLÍTICA DE GESTIÓN DE LOGS)

21.1. OBJETIVO

Es determinar los eventos más significativos dentro de nuestros sistemas de información que han de ser registrados, y en qué modo ha de efectuarse dicho registro. Establecer mecanismos de monitorización que permitan la detección de intrusiones, errores y situaciones anómalas o potencialmente peligrosas.

21.2. POLÍTICA

a) Todos los sistemas de producción dentro de la organización deben registrar y retener información de registro de auditoría que incluya la siguiente información:
   - Actividades realizadas en el sistema.
   - El usuario o entidad (es decir, la cuenta del sistema) que realizó la actividad, incluido el sistema desde el que se realizó la actividad.
   - El archivo, la aplicación u otro objeto en el que se realizó la actividad.
   - La hora en que ocurrió la actividad.
   - La herramienta con la que se realizó la actividad.
   - El resultado (por ejemplo, éxito o fracaso) de la actividad.
   - Las actividades específicas que se registrarán deben incluir, como mínimo:
   - La información (incluida la información de autenticación, como nombres de usuario o contraseñas) se crea, lee, actualiza o elimina.
   - Conexiones de red aceptadas o iniciadas.
   - Autenticación y autorización de usuarios a sistemas y redes.
   - Concesión, modificación o revocación de derechos de acceso, incluida la adición de un nuevo usuario o grupo; cambiar privilegios de usuario, permisos de archivos, permisos de objetos de base de datos, reglas de firewall y contraseñas.
   - Cambios en la configuración del sistema, la red o los servicios, incluida la instalación de software, parches, actualizaciones u otros cambios de software instalados.
   - Inicio, apagado o reinicio de una aplicación.
   - El proceso de la aplicación aborta, falla o finaliza anormalmente, especialmente debido al agotamiento de los recursos o al alcanzar un límite o umbral de recursos (como CPU, memoria, conexiones de red, ancho de banda de red, espacio en disco u otros recursos), la falla de servicios de red como DHCP o DNS, o falla de hardware.
   - Detección de actividad sospechosa y / o maliciosa de un sistema de seguridad, como un sistema de detección o prevención de intrusiones (IDS / IPS), un sistema antivirus o un sistema anti-spyware.

b) A menos que sea técnicamente impráctico o inviable, todos los registros deben agregarse en un sistema central para que las actividades en diferentes sistemas puedan correlacionarse, analizarse y rastrearse en busca de similitudes, tendencias y efectos en cascada. Los sistemas de agregación de registros deben

tener ingesta de registros automáticos y oportunos, etiquetado y alerta de eventos y anomalías, y capacidad de revisión manual.

c) Los registros deben revisarse manualmente de forma regular:
   - Las actividades de los usuarios, administradores y operadores del sistema deben ser revisadas al menos una vez al mes.
   - Los registros relacionados con la PII deben revisarse al menos una vez al mes para identificar comportamientos inusuales.

d) Cuando se utiliza un entorno de nube subcontratado, los registros deben mantenerse en el acceso y uso del entorno de nube, asignación y utilización de recursos y cambios en la PII. Se deben mantener registros para todos los administradores y operadores que realizan actividades en entornos de nube.

e) Todos los sistemas de información dentro de la organización deben sincronizar sus relojes implementando Network Protocolo de tiempo (NTP) o una capacidad similar. Todos los sistemas de información deben sincronizarse con el mismo sistema primario fuente de tiempo.

CAPÍTULO 22
(POLÍTICA DE BUENAS PRÁCTICAS EN PORTAL WEB Y REDES SOCIALES)

22.1. OBJETIVO

Es explicar cómo se deben usar la página web, redes sociales y establecer las normas de comportamiento que se esperan de los usuarios.

22.2. POLÍTICA

a) Como administrador de la página web y redes sociales, se debe utilizar una contraseña fuerte y habilitar siempre que sea posible el doble factor de autenticación en todos los perfiles de la organización.

b) Se debe establecer la configuración de la privacidad de manera que permita utilizar las distintas redes sociales de forma efectiva.

c) Se debe permitir interactuar con el público sin descuidar la seguridad y privacidad del perfil de la organización.

d) Se debe designar un responsable de la actualización y publicación de la información (Ordenanzas, Decretos, Resoluciones. etc.), que no deberán exceder en su difusión un plazo de 24 horas de emitido el documento.

f) Se debe definir normas de publicación.

g) Se debe elegir la imagen que desea reflejar, qué pública y qué no, el tono o lenguaje, cómo se responde a las consultas y quejas de los usuarios.

h) Antes de conceder acceso u otro permiso a ciertas aplicaciones (de gestión, estadísticas, publicitarias, etc.), se debe analizar detalladamente los riesgos que pueden suponer para el perfil de la organización (acceso a información confidencial, publicaciones sin supervisión, etc.)

i) Se debe estar informado de las distintas campañas utilizadas por los ciberdelincuentes para conseguir acceso a los perfiles de las organizaciones en las distintas redes sociales.

j) Se debe formar a los empleados en ciberseguridad y seguridad de la información para minimizar los riesgos relativos al uso de las tecnologías, en particular las redes sociales.
k) Se debe tratar los enlaces de las redes sociales y los documentos adjuntos con las mismas precauciones que el correo electrónico.
l) En caso de que un enlace lo dirija a cualquier web que solicite cualquier tipo de información confidencial o bancaria, se debe comprobar el certificado de seguridad y que corresponda con el sitio al que se está accediendo.
m) Se debe usar el sentido común al momento de publicar, ya que puede afectar la imagen de la organización.
n) Se debe evitar acciones como dar información confidencial, participar en discusiones, propagar noticias falsas, entre otros.
o) No se debe publicar mensajes, actualizaciones de estado o enlaces a material o contenido que sea inapropiado: pornografía, insultos raciales o religiosos, comentarios específicos de género, información que fomente las habilidades delictivas o terrorismo, o materiales relacionados con cultos, juegos de azar o drogas ilegales.
p) Solo se debe publicar actualizaciones, mensajes o utilizarlos de otro modo como: responder a las consultas, solicitudes, compartir publicaciones de blog, artículos y otros contenidos creados relevante para la entidad.
q) Se debe usar un lenguaje de una manera respetuosa, buena ortografía y gramática a la hora de crear contenidos en las redes sociales.

CAPÍTULO 23
(POLÍTICA DE COPIAS DE SEGURIDAD)

23.1. OBJETIVO

Es restaurar un sistema a un estado actual (a partir de la fecha de la copia de seguridad más reciente) en caso de falla del sistema.

23.2. POLÍTICA

a) La organización debe contar con copias instantáneas a los sistemas operativos, para poder regresar el sistema operativo a una fecha anterior a la de un incidente.
b) La copia de seguridad se debe realizar durante la noche y deberá ser comprobada.
c) Las copias de seguridad tendrán una retención en función a los dispositivos legales vigentes.
d) La responsabilidad de las copias de seguridad de los computadores personales recaerá en el usuario final.
e) Se debe mantener un inventario de activos de información (software, datos, soportes, responsables, ubicación).
f) Se debe clasificar los activos de información e identificar los necesarios (críticos).
g) Se debe controlar el acceso a las copias de seguridad (personal autorizado).
h) Se debe hacer copias de seguridad de la información crítica de la organización.
i) Se debe realizar copias de seguridad al menos 1 vez al día, según sea el caso.

j) Se debe hacer copias de seguridad completa, incremental o diferencial (según se dé el caso).
k) Se debe guardar al menos una copia completa fuera de la organización.
l) Se debe guardar las copias de seguridad en una caja ignífuga y bajo llave.
m) Se debe realizar copias de seguridad en la nube.
n) Se debe elaborar y aplicar los procedimientos de copia y restauración.
o) Se debe comprobar que las copias estén bien realizadas y que pueden restaurarse, esto se debe evidenciar con pruebas de restauración de backups que deberán estar documentadas.
p) Antes de hacer la copia se debe revisar que el soporte sea el adecuado (tasa de transferencia, capacidad, etc.) y que se encuentre en buen estado.
q) Se debe etiquetar los soportes para realizar las copias de seguridad.
r) Se debe llevar un registro de los soportes sobre los que se haya realizado alguna copia de seguridad.
s) Cuando se desechan los soportes utilizados para las copias de seguridad, se debe destruir de forma segura.
t) Se debe cifrar las copias de seguridad que contenga información confidencial y las que se suba a la nube.
u) Se debe cifrar de manera obligatoria toda copia de seguridad que salga del local principal.