



Municipalidad de Santiago de Surco

1033

RESOLUCION N° -2011-RASS
Santiago de Surco,

21 SET. 2011

EL ALCALDE DE SANTIAGO DE SURCO

VISTO:

El Proyecto de Directiva sobre "Políticas de Seguridad de la Información", presentado por la Gerencia de Sistemas y Procesos, hoy Gerencia de Tecnologías de la Información;

CONSIDERANDO:

Que, la Sociedad Auditora Chávez Escobar y Asociados S.C, mediante Carta N° 162-2011/CHEA, presenta a la Municipalidad, el Informe Largo de Auditoria Financiera Ejercicio Económico 2010, en el que plantea como observación, que falta implementar la norma técnica peruana NTP-ISO/IEC 17799:2007 v 2 Código de Buenas Prácticas para la Gestión de Seguridad de la Información;

Al respecto, la Gerencia de Sistemas y Procesos, hoy denominada Gerencia de Tecnologías de la Información, conforme a la Ordenanza N° 396-MSS, presentó mediante Memorando N° 0174-2011-GSP-MSS del 09.08.11, el proyecto de Directiva sobre "Políticas de Seguridad de la Información"; proyecto que cuenta con la opinión técnica de la Subgerencia de Planeamiento y Estadística, (hoy denominada Subgerencia de Planeamiento y Racionalización) mediante informe N° 081-2011-SGPLAE-GPP-MSS; y con la opinión favorable de la Gerencia de Planeamiento y Presupuesto, conforme se corrobora con el Memorando N° 303-2011-GPP-MSS;

Que, el proyecto presentado, tiene por objeto mejorar la seguridad de la información de la Municipalidad de Santiago de Surco, estableciendo políticas que permitan aplicar controles para evitar contingencias de negligencia o violación de confidencialidad, fallas en el uso de medidas de seguridad, mala practica contra personas particulares u organizacionales que podrían reclamar por daños o perjuicios;

Que, en consecuencia, urge su implementación a fin de establecer políticas de seguridad en la información y siendo conforme lo opinado por la Gerencia de Asesoría Jurídica, mediante Informe No. 823-2011-GAJ-MSS y con lo opinado por la Gerencia de Planeamiento y Presupuesto mediante Informe N° 090-2011-GPP-MSS; y de acuerdo a las facultades conferidas por el artículo 20°, inciso 6) de la Ley Orgánica de Municipalidades - Ley N° 27972;

RESUELVE:

003

ARTÍCULO PRIMERO.- APROBAR la Directiva N° 2011-MSS, denominada "POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN", la misma que consta de Trece (13) Numerales y que en Anexo forma parte integrante de la presente Resolución.

ARTÍCULO SEGUNDO.- La presente Directiva entrará en vigencia al partir del día siguiente de su aprobación.

ARTÍCULO TERCERO: ENCARGAR a la Secretaría General la difusión de la presente Resolución de Alcaldía y a la Gerencia de Tecnologías de la Información, la publicación de la presente Directiva y Anexo en el Portal Institucional de la Municipalidad de Santiago de Surco (www.munisurco.gob.pe).

Jr. Bolognesi N° 275, Plaza de Armas de Santiago de Surco. T. 411-5560 www.munisurco.gob.pe.





Municipalidad de Santiago de Surco

Página N° 2 de la RESOLUCION N° **1033** 2011-RASS.

ARTÍCULO CUARTO: ENCARGAR a la Gerencia Municipal, comunicar a la Sociedad Auditora Chávez Escobar y Asociados S.C, el levantamiento de la observación, señalada en el Informe Largo de Auditoria Financiera Ejercicio Económico 2010.

ARTÍCULO QUINTO: ENCARGAR a la Gerencia de Planeamiento y Presupuesto, Gerencia de Administración y Finanzas, Gerencia de Tecnologías de la Información, el cumplimiento de la presente Resolución.

Regístrese, comuníquese y cúmplase.

Municipalidad de Santiago de Surco

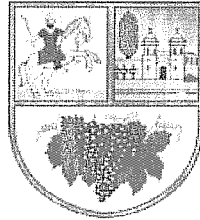

PEDRO CARLOS MONTOYA ROMERO
SECRETARIO GENERAL

Municipalidad de Santiago de Surco

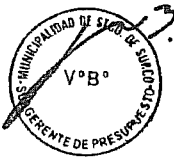
ROBERTO GOMEZ BACA
ALCALDE

RHGB/PCMR/MVM/rvc.

MUNICIPALIDAD DE
SANTIAGO DE SURCO



POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN



v1.0



SEPTIEMBRE 2011



Políticas de Seguridad de la Información

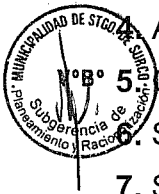
1. CONTROL DE VERSIONES

Fuente de Cambio	Fecha de Solicitud del Cambio	Version	Partes que Cambian	Descripción del Cambio	Fecha de Cambio
PSI-v0100		1.00	N/A		



INDICE GENERAL

1. CONTROL DE VERSIONES	2
2. INTRODUCCIÓN.....	4
3. POLÍTICA DE SEGURIDAD.....	5
4. ASPECTOS ORGANIZATIVOS PARA LA SEGURIDAD	5
5. CLASIFICACIÓN Y CONTROL DE ACTIVOS	8
6. SEGURIDAD LIGADA AL PERSONAL	10
7. SEGURIDAD FÍSICA Y DEL ENTORNO	13
8. GESTIÓN DE COMUNICACIONES Y OPERACIONES.....	16
9. CONTROL DE ACCESOS	22
10. DESARROLLO Y MANTENIMIENTO DE SISTEMAS.....	28
11. GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE INFORMACIÓN.....	31
12. GESTIÓN DE CONTINUIDAD DEL NEGOCIO.....	33
13. CUMPLIMIENTO	35



Políticas de Seguridad de la Información

2. INTRODUCCIÓN

Este documento es un conjunto de propuestas de políticas de seguridad de la información que sugieren como se debe manejar la seguridad de la información en la **Municipalidad de Santiago de Surco**. A partir de ellas se pueden desarrollar procedimientos detallados y guías de acción para casos de brechas y violaciones de seguridad.

Las políticas tratan los aspectos de manera general y dan base a las normas, las cuales hacen referencia específica a tecnologías, metodologías, procedimientos de implementación y otros aspectos de detalle. Asimismo las políticas se proyectan para durar varios años, a diferencia de las normas y procedimientos que pueden ir cambiando de acuerdo a las tecnologías y cambios en los procesos de negocios de la Municipalidad.

La importancia de las políticas radica en que, en primer lugar, son el punto de partida para establecer una infraestructura organizativa apropiada de seguridad, es decir, son los aspectos esenciales desde donde se derivan los otros aspectos de seguridad de la información. En segundo lugar, guían el proceso de selección e implantación de los productos de seguridad, y en tercer lugar, porque demuestran el apoyo de la Alta Dirección hacia los aspectos de seguridad de la información.

Además, las políticas pueden servir para evitar responsabilidades legales, ya que permiten aplicar controles para evitar contingencias de negligencia o violación de confidencialidad, fallas en el uso de medidas de seguridad, mala práctica, contra personas particulares u organizaciones que podrían reclamar por daños o perjuicios.

Se debe considerar la **difusión de las políticas de seguridad** de la información mediante diferentes tipos de documentos: los trabajadores podrían recibir un folleto que contiene las políticas de seguridad más importantes que ellos necesitan tener presente, el personal técnico podría recibir un documento más largo que proporcione más detalle y los contratistas pueden recibir un resumen de políticas confeccionado especialmente para ellos.

Una de las primeras acciones debería ser la conformación del Comité Gerencial de Seguridad de la Información. Este comité debería tener representantes de las distintas Unidades Orgánicas de la Municipalidad, debiendo realizar la evaluación de las políticas presentadas en el presente documento considerando su viabilidad, análisis costo/beneficio y sus implicaciones. En todo caso, se debe tener en consideración que cualquier conjunto de políticas debe empezar por los aspectos esenciales, para luego ir ampliando con políticas adicionales.

Las políticas deben **revisarse** en forma periódica, preferiblemente cada año, para asegurarse de que todavía son pertinentes y efectivas. Es importante eliminar aquellas políticas que ya no son útiles o que ya no son aplicables. Este esfuerzo también ayudará a mejorar la credibilidad de las actividades de seguridad de la información dentro de la Municipalidad.

Políticas de Seguridad de la Información

ISO 17799	Política MSS-PSI	Descripción
3. Política de Seguridad		
3.1	Política de la seguridad de la información	
3.1.1	Comité Gerencial de Seguridad de la Información	
	Política 0301-001-MSS	Conformación del Comité de Seguridad de la Información La Alta Dirección de la Municipalidad conformará el Comité Gerencial de Seguridad de la Información
3.1.2	Documento de política de la seguridad de la información	
	Política 0301-002-MSS	Establecimiento de Políticas de Seguridad de la Información La Alta Dirección de la Municipalidad se encargará de establecer, mantener y publicar las Políticas de Seguridad de la Información.
3.1.3	Revisión y evaluación	
	Política 0301-003-MSS	Revisión de las Políticas de Seguridad de la Información Las Políticas de Seguridad de la Información tendrán un propietario designado que será responsable de su mantenimiento y revisión de acuerdo a un proceso definido.

4. Aspectos Organizativos para la Seguridad		
4.1	Organización para la seguridad de la información	
4.1.1	Comité Gerencial de Seguridad de la Información	
	Política 0401-001-MSS	Rol del Comité Gerencial de Seguridad de la Información El Comité Gerencial de Seguridad de la Información se encargará de promover las iniciativas de Seguridad de la Información dentro de la Municipalidad, así como obtener los recursos necesarios para dichas actividades.
4.1.2	Coordinación de Seguridad de la Información	
	Política 0401-002-MSS	Rol de la alta dirección en la seguridad de la información La Alta Dirección de la Municipalidad asignará una alta prioridad a la Seguridad de la Información en todas las actividades e iniciativas actuales y futuras.
	Política 0401-003-MSS	Actualizaciones sobre Seguridad de la Información para el Personal La Alta Dirección se compromete a brindar a todo el personal, a través de las instancias correspondientes y de manera periódica, información relevante sobre Seguridad de la Información por diversos medios.
4.1.3	Asignación de responsabilidades sobre Seguridad de la Información	

Políticas de Seguridad de la Información

ISO 17799	Política MSS-PSI	Descripción
4.1.3	Política 0401-004-MSS	<p>Designación del Oficial de Seguridad de la Información</p> <p>Se designará un Oficial de Seguridad de la Información que asuma la responsabilidad del desarrollo e implantación de la seguridad y respalde la identificación de las medidas de control. Sin embargo, la responsabilidad de proporcionar recursos e implantar las medidas de control permanecerá con los Gerentes individuales.</p>
4.1.3	Política 0401-005-MSS	<p>Administración de Sistemas</p> <p>La gestión de los sistemas de información debe estar a cargo de un profesional debidamente calificado, quien será responsable de supervisar el funcionamiento y la seguridad de los sistemas. Debe estar debidamente capacitado y tener experiencia relevante en los sistemas y plataformas utilizadas por la Municipalidad. Además, debe conocer y entender la gama de riesgos de Seguridad de la Información que requieren ser manejados.</p>
4.1.4	Proceso de autorización de recursos para el tratamiento de la información	
4.1.4	Política 0401-007-MSS	<p>Especificación de los requisitos para nuevo equipamiento</p> <p>Las requisiciones de compras significativas de nuevos equipos deben contar con un Expediente Técnico que detalle la especificación de los requerimientos del usuario, los requisitos de Seguridad de la Información, la prioridad, el cumplimiento de estándares técnicos y funcionales, y la relación con los objetivos a corto y largo plazos de la Municipalidad.</p>
4.1.4	Política 0401-008-MSS	<p>Instalación de nuevo equipamiento</p> <p>Todas las nuevas instalaciones de equipamiento, y sus respectivos requisitos de Seguridad de la Información, deben planificarse formalmente y notificarse a los interesados con la debida anticipación.</p>
4.1.4	Política 0401-009-MSS	<p>Prueba de equipamiento y sistemas</p> <p>Todo equipo debe probarse exhaustivamente y pasar por un proceso de aceptación formal de usuarios antes de ser transferido al entorno de producción.</p>
4.1.4	Política 0401-010-MSS	<p>Especificación de los requerimientos de usuario para software</p> <p>Todos las solicitudes de desarrollo de sistemas nuevos o mejoras a los mismos deben presentarse a la Gerencia de Tecnologías de la Información mediante un documento de "Especificaciones de requerimientos de usuario", donde se define detalladamente los requerimientos técnicos y funcionales.</p>
4.1.4	Política 0401-011-MSS	<p>Selección de paquetes de software comercial</p> <p>La adquisición de software comercial debe hacerse, como regla general, a proveedores cuyo software esté debidamente probado en el mercado, y que cuente con el soporte adecuado.</p>

Políticas de Seguridad de la Información

ISO 17799	Política MSS-PSI	Descripción
4.1.4	Política 0401-012-MSS	<p>Selección de paquetes de software de ofimática</p> <p>Todos los paquetes de software de oficina deben ser compatibles con el sistema operativo y plataforma de cómputo aprobados por la Municipalidad.</p>
4.1.5	Asesoramiento de especialistas en seguridad de la información	
4.1.5	Política 0401-013-MSS	<p>Asesoría especializada en Seguridad de la Información</p> <p>La Municipalidad de Santiago de Surco podrá buscar asesoría especializada sobre Seguridad de la Información de consultores internos o externos.</p>
4.1.6	Cooperación entre organizaciones	
4.1.6	Política 0401-014-MSS	<p>Identificación de organizaciones relevantes</p> <p>Se mantendrá un registro actualizado de todas las organizaciones relevantes que pudieran intervenir en casos de incidentes de seguridad, incluyendo los contactos responsables de coordinar dichos aspectos en tales organizaciones.</p>
4.1.7	Revisión independiente de la seguridad de la información	
4.1.7	Política 0401-015-MSS	<p>Revisión periódica del documento de Políticas de Seguridad de la Información</p> <p>El documento de Políticas de Seguridad de la Información será evaluado periódicamente por personas independientes o especialistas externos para garantizar que las prácticas organizacionales reflejan apropiadamente la política y que ésta es factible y eficaz.</p>
4.2	Seguridad en los accesos de terceras personas	
4.2.1	Identificación de los riesgos por acceso de terceros	
4.2.1	Política 0402-001-MSS	<p>Acceso de terceros</p> <p>Se definirá y documentará formalmente los tipos de accesos de terceros a recursos de información de la Municipalidad, así como los motivos por los cuales se les puede otorgar dicho acceso.</p>
4.2.1	Política 0402-002-MSS	<p>Permisos de acceso a terceros</p> <p>Sólo se permitirá el acceso de terceros a información de la Municipalidad cuando dicha información esté aislada y que el riesgo de posibles accesos no autorizados esté debidamente controlado.</p>

Políticas de Seguridad de la Información

ISO 17799	Política MSS-PSI	Descripción
4.2.2		Requisitos de seguridad en contratos con terceros
4.2.2	Política 0402-003-MSS	Acuerdos de acceso a la información por terceros Los acuerdos que permiten el acceso de terceros a recursos de tratamiento de información de la Municipalidad deberán estar basados en contratos formales que incluyan todos los requisitos de seguridad acordes con las políticas y normas de seguridad de la Municipalidad.
4.2.2	Política 0402-004-MSS	Difusión de las políticas a contratistas y trabajadores temporales Se entregará formalmente un resumen de las Políticas de Seguridad de la Información a todo contratista y/o trabajador temporal antes del inicio de sus servicios.
4.2.2	Política 0402-005-MSS	Conformidad de trabajos hechos por terceros Solamente las personas debidamente autorizadas expresamente pueden firmar la conformidad de trabajos hechos por terceros.
4.2.2	Política 0402-006-MSS	Compra de software desarrollado por proveedores El software desarrollado por terceros debe cumplir con las "Especificaciones de Requerimientos de Usuario" y ofrecer un soporte técnico apropiado.
4.2.2	Política 0402-007-MSS	Brechas de confidencialidad de terceros Las violaciones de confidencialidad de terceros deben ser reportadas al Oficial de Seguridad de la Información tan pronto como sea posible.
4.2.2	Política 0402-008-MSS	Servicios externos de eliminación de material y equipo Cualquier contratista usado para la eliminación externa de equipo y/o material obsoletos debe estar en capacidad de demostrar el cumplimiento de las Políticas de Seguridad de la Información de la Municipalidad.
4.2.2	Política 0402-009-MSS	Soporte de software de aplicación Todo software aplicativo debe tener un nivel apropiado de soporte técnico para garantizar que las operaciones de la Municipalidad no se vean perjudicadas, asegurándose que cualquier problema de software será manejado eficientemente en un tiempo razonable.
5. Clasificación y control de Activos		
5.1		Responsabilidad sobre los activos
5.1	Política 0501-001-MSS	Responsabilidad sobre los activos Cada activo importante de información debe tener un propietario designado que será el responsable de establecer la seguridad de dicho activo y que se mantenga la protección adecuada.

Políticas de Seguridad de la Información

ISO 17799	Política MSS-PSI	Descripción
5.1	Política 0501-002-MSS	Defensa contra delitos informáticos Los riesgos de los sistemas e información de la Municipalidad deben reducirse al mínimo fomentando la concientización y vigilancia del personal, e instalando sistemas y dispositivos de protección apropiados.
5.1.1	Inventario de activos	
5.1.1	Política 0501-003-MSS	Mantenimiento del inventario de activos de información La Municipalidad de Santiago de Surco contará con un inventario formal de todos los activos de información, el cual estará actualizado de manera permanente.
5.1.1	Política 0501-004-MSS	Gestión y uso de documentación de hardware La documentación de hardware debe estar siempre actualizada y fácilmente accesible para el personal autorizado de soporte o mantenimiento.
5.2	Clasificación de la Información	
5.2	Política 0502-001-MSS	Clasificación de Información Todo activo de información: datos y documentos, debe clasificarse según su confidencialidad, valor para el negocio y sensibilidad.
	Política 0502-002-MSS	Registro de activos de información La Municipalidad debe mantener un registro actualizado de sus activos de información.
5.2.1	Guías de clasificación	
5.2.1	Política 0502-003-MSS	Esquema de clasificación de activos de información La Municipalidad Surco contará con un esquema de clasificación de activos de información en función de su importancia, criticidad, integridad y disponibilidad para la organización. Cada propietario de activos de información será el responsable de definir y revisar periódicamente la clasificación de sus activos.
5.2.1	Política 0502-004-MSS	Datos de vecinos, administrados y terceros Se debe clasificar la información de contacto de vecinos, administrados y terceros como altamente confidencial y protegerla en consecuencia.
	Política 0502-005-MSS	Manejo de Información Financiera La información financiera debe clasificarse como altamente confidencial y se deben tomar las medidas de seguridad necesarias (técnicas y administrativas) que protejan tal información de accesos no autorizados.
5.2.2	Marcado y tratamiento de la información	

Políticas de Seguridad de la Información

ISO 17799	Política MSS-PSI	Descripción
5.2.2	Política 0502-006-MSS	Etiquetado de información Toda activo de información debe tener una etiqueta claramente visible a fin que los usuarios conozcan quien es el propietario y cuál es el nivel de clasificación designado.
5.2.2	Política 0502-007-PCM	Uso de nombres de archivos Los nombres de archivos de datos de la Municipalidad deben tener un significado reconocible por los usuarios de dichos archivos.
5.2.2	Política 0502-008-MSS	Indicación de niveles de seguridad en documentos Dentro del encabezado y pie de página de todos los documentos se deberá indicar la clasificación del nivel de seguridad y el dueño del documento.
5.2.2	Política 0502-009-MSS	Grabación periódica de datos por usuarios A fin de prevenir daños o pérdida debido a malos funcionamientos del sistema o fallas de energía, los usuarios de sistemas de información que crean o modifican archivos de datos, deben grabar su trabajo de manera periódica usando las mejores prácticas.
5.2.2	Política 0502-010-MSS	Gestión de borradores de informes Los borradores de informes se deben actualizar solamente con autorización del dueño del documento. Las sucesivas versiones de borradores de informes no deben seguir en uso después de la elaboración de una versión final, se deben eliminar o archivar. Una sola versión del archivo debe conservarse para acceso de trabajo.

6. Seguridad ligada al Personal

6.1	Seguridad en la definición del trabajo y los recursos	
6.1.1	Inclusión de la seguridad en las responsabilidades laborales	
6.1.1	Política 0601-001-MSS	Inclusión de cláusulas en el contrato de trabajo El contrato de trabajo debe incluir cláusulas de cumplimiento de la Seguridad de la Información.
6.1.1	Política 0601-002-MSS	Responsabilidad de los empleados sobre datos confidenciales Todos los trabajadores que tengan acceso a información clasificada como confidencial deben firmar cláusulas de protección de la confidencialidad de dicha información, durante y después de la relación contractual con la Municipalidad.
6.1.2	Selección y política de personal	





Políticas de Seguridad de la Información

ISO 17799	Política MSS-PSI	Descripción
6.1.2	Política 0601-003-MSS	Contratación de nuevo personal Debe existir un mecanismo de verificación de identificación, referencias de nuevos trabajadores, el cual corresponderá al nivel de las responsabilidades que se le asignarán. En los casos de responsabilidades financieras, se hará una verificación del crédito.
6.1.3	Compromiso de Confidencialidad	
6.1.3	Política 0601-004-MSS	Acuerdos de confidencialidad En los casos donde la información esté clasificada como confidencial, se deben generar y suscribir "Acuerdos de confidencialidad" por los trabajadores o terceros que tengan acceso a dicha información.
6.1.3	Política 0601-005-MSS	Confidencialidad de las contraseñas y números PIN Las contraseñas otorgadas a los trabajadores son privadas y altamente confidenciales. La violación a dicha confidencialidad puede dar lugar a una acción disciplinaria.
6.1.3	Política 0601-006-MSS	Respuesta a requerimientos telefónicos Las solicitudes telefónicas de información confidencial se deben canalizar a la plana ejecutiva para su atención. Sólo personas autorizadas pueden divulgar información reservada, previa verificación de la identidad de la persona que recibirá dicha información.
6.1.3	Política 0601-007-MSS	Compartir información confidencial con otros Toda información que no sea de dominio público, sobre asuntos de la Municipalidad y a sus trabajadores, no debe divulgarse, así sea a miembros de la familia o personas cercanas.
6.1.3	Política 0601-008-MSS	Declaraciones a medios de comunicación Sólo personas expresamente autorizadas pueden dirigirse a medios de difusión sobre temas referidos a la Municipalidad.
6.1.4	Términos y condiciones de la relación laboral	
6.1.4	Política 0601-009-MSS	Conocimiento de obligaciones legales Las responsabilidades legales de los trabajadores en el uso de sistemas de información y datos computarizados de la Municipalidad deben ser incluidas dentro de la documentación clave de personal tales como cláusulas del Contrato de Trabajo y Reglamento Interno de Trabajo. La Subgerencia de Recursos Humanos debe garantizar que todos los empleados estén completamente enterados de dichas responsabilidades.
6.1.4	Política 0601-010-MSS	Respeto de la privacidad en el trabajo La Municipalidad respeta la privacidad del trabajador en su lugar de trabajo; sin embargo, esto no limitará el derecho la Municipalidad a tener acceso a la información creada y almacenada en equipos de la Municipalidad.
6.2	Capacitación de Usuarios	

Políticas de Seguridad de la Información

ISO 17799	Política MSS-PSI	Descripción
6.2.1	Capacitación en seguridad de la información	
6.2.1	Política 0602-001-MSS	Capacitación en Seguridad de la Información a trabajadores La capacitación en Seguridad de la Información se impartirá de manera individual, obligatoria y actualizada a todos los trabajadores.
6.2.1	Política 0602-002-MSS	Capacitación en Seguridad de la Información al personal técnico La capacitación del personal técnico en Seguridad de la Información deberá estar actualizada y acorde con la responsabilidad de configurar y mantener las protecciones requeridas por la Municipalidad. Se debe priorizar la capacitación al Oficial de Seguridad de la Información
6.2.1	Política 0602-003-MSS	Capacitación en Seguridad de la Información a personal nuevo El personal nuevo debe recibir capacitación básica en Seguridad de la Información como parte del proceso de inducción.
6.2.1	Política 0602-004-MSS	Programas de concientización para el personal permanente. Se debe concientizar en temas de seguridad de la información al personal permanente de la Municipalidad mediante información actualizada sobre amenazas existentes y las medidas de seguridad apropiadas.
6.3	Respuesta ante incidentes y malos funcionamientos de la seguridad	
6.3	Política 0603-001-MSS	Investigación de causas e impacto de incidentes Los incidentes de Seguridad de la Información deben ser investigados apropiadamente por personal debidamente capacitado.
6.3.1	Reporte de incidentes de seguridad	
6.3.1	Política 0603-002-MSS	Reporte de incidentes de Seguridad de la Información Los incidentes, sospechas de incidentes y brechas de seguridad de la información deben reportarse al Oficial de Seguridad de la Información lo más rápidamente posible para agilizar las actividades de identificación de daños, reparación y recuperación, así como facilitar la recolección de evidencias.
6.3.1	Política 0603-003-MSS	Reporte de incidentes de Seguridad de la Información a autoridades externas Sólo se deben comunicar los incidentes de Seguridad de la Información a autoridades externas siempre que sea necesario debido a requisitos legales o regulatorios.
6.3.2	Reporte de debilidades de seguridad	
6.3.2	Política 0603-004-MSS	Notificación de debilidades de Seguridad de la Información Las debilidades o sospechas de debilidades de Seguridad de la Información deben notificarse al Oficial de Seguridad de la Información lo más rápidamente posible.
6.3.3	Reporte de fallas de software	

Políticas de Seguridad de la Información

ISO 17799	Política MSS-PSI	Descripción
	Política 0603-005-MSS	Reporte de fallas de software Las fallas de software deben ser reportadas mediante un procedimiento existente para tal fin.
6.3.4	Aprendiendo de los incidentes	
6.3.4	Política 0603-006-MSS	Revisión del registro de incidentes de Seguridad de la Información Se debe crear y mantener un registro de incidentes, sospechas de incidentes, brechas y amenazas a la seguridad de la información y las acciones correctivas identificadas. El registro debe estudiarse regularmente para tomar medidas de reducción del riesgo y frecuencia de los incidentes de la seguridad de la información en la Municipalidad.
6.3.5	Proceso disciplinario	
	Política 0603-007-MSS	Cumplimiento de las Políticas de Seguridad de la Información Cualquier incidente de seguridad originado por un incumplimiento de dichas políticas, podrá dar lugar a una acción o sanción disciplinaria.
7. Seguridad Física y del Entorno		
7.1	Áreas Seguras	
7.1.1	Perímetro de Seguridad Física	
7.1.1	Política 0701-001-MSS	Seguridad de ambientes de cómputo Los ambientes que contengan computadoras deben protegerse contra cualquier intrusión física.
	Política 0701-002-MSS	Gestión de repositorios de datos Los locales donde se almacenan datos o información deben tener controles de acceso para reducir el riesgo de pérdida o daño a un nivel aceptable.
7.1.2	Controles físicos de ingreso	
7.1.2	Política 0701-003-MSS	Protección de acceso físico Se debe controlar el acceso físico a ambientes de alta seguridad mediante técnicas de identificación y autenticación. Se debe tener un sistema de control que monitoree todos los intentos de acceso. Se debe informar al personal con autorización de ingreso a tales áreas sobre los riesgos de seguridad inherentes.
		
7.1.3	Seguridad de oficinas, despachos y recursos	
7.1.3	Política 0701-004-MSS	Configuración de oficinas Las oficinas deben estar configuradas para minimizar los daños por incendio, inundación, explosión, disturbio y otras formas de desastres naturales o provocados, así como amenazas que procedan de lugares vecinos.
		

Políticas de Seguridad de la Información

ISO 17799	Política MSS-PSI	Descripción
7.1.3	Política 0701-005-MSS	<p>Seguridad de oficinas</p> <p>Se deben instalar sistemas de detección de intrusos y probarse regularmente para cubrir todas las puertas externas y las ventanas accesibles. Las ventanas y puertas deben permanecer cerradas cuando la oficina esté vacía, y las alarmas deben estar activadas.</p>
7.1.3	Política 0701-006-MSS	<p>Almacenamiento seguro</p> <p>El material y equipo con información sensible o valiosa deben almacenarse con seguridad y según el nivel de clasificación de la información almacenada.</p>
7.1.3	Política 0701-007-MSS	<p>Desconfiar de extraños en los locales de la Municipalidad.</p> <p>Todos los trabajadores deben conocer la necesidad de desconfiar de extraños en los ambientes de la Municipalidad.</p>
7.1.4	El trabajo en las Áreas Seguras	
7.1.4	Política 0701-008-MSS	<p>Acceso de terceros a las áreas seguras</p> <p>El personal de terceros sólo podrá acceder a áreas seguras cuando sea aprobado expresamente y su acceso se supervisará. No se permitirá la presencia de equipos de fotografía, video, audio u otras formas de registro salvo autorización especial.</p>
7.1.5	Áreas de acceso público, entrega y recepción	
7.1.5	Política 0701-009-MSS	<p>Controles en áreas de acceso público</p> <p>Las áreas de acceso público, entrega y recepción deben tener controles apropiados y, de ser posible, aislarse de los recursos de tratamiento de información para evitar accesos no autorizados.</p>
7.2	Seguridad de los Equipos	
7.2.1	Instalación y protección de equipos	
7.2.1	Política 0702-001 - MSS	<p>Preparación de ambientes para cómputo</p> <p>Los lugares elegidos para instalar computadoras y almacenar datos deben protegerse convenientemente contra intrusión física, hurto, incendio, inundación, temperatura y humedad excesivas, y otros peligros.</p>
7.2.2	Suministro eléctrico	
7.2.2	Política 0702-002-MSS	<p>Suministro continuo de energía eléctrica a equipos críticos</p> <p>Se debe instalar fuentes de alimentación continua (UPS) donde sea necesario para asegurar la continuidad del servicio durante interrupciones del suministro eléctrico.</p>
7.2.2	Política 0702-003-MSS	<p>Gestión y mantenimiento de generadores de reserva</p> <p>Se deben usar generadores de reserva cuando sea necesario para asegurar la continuidad del servicio durante interrupciones del suministro eléctrico.</p>
7.2.3	Seguridad del cableado	

Políticas de Seguridad de la Información

ISO 17799	Política MSS-PSI	Descripción
7.2.3	Política 0702-004-MSS	Instalación y mantenimiento de cableado de red El cableado de red debe ser instalado y mantenido por profesionales calificados. Cualquier punto de red que no esté en uso debe ser sellado y su estado registrado.
7.2.3	Política 0702-005-MSS	Seguridad del cableado La seguridad del cableado de red debe ser revisada cada vez que se hagan mejoras, cambios de equipo o de ambientes.
7.2.4	Mantenimiento de equipos	
7.2.4	Política 0702-006-MSS	Mantenimiento de equipos Todo equipo de la Municipalidad debe tener mantenimiento apropiado a cargo de profesionales calificados, lo cual debe reflejarse en un documento formal.
7.2.4	Política 0702-007-MSS	Limpeza de equipos Deben implementarse procedimientos de limpieza de equipos que no comprometan la seguridad de la información, ni la integridad de los equipos. Los materiales y personal de limpieza deben estar aprobados para dicha función.
7.2.4	Política 0702-008-MSS	Seguros de equipos Todo equipo de tratamiento de la información de propiedad de la Municipalidad debe tener cobertura de seguro contra robo, daño o pérdida. Los equipos portátiles deben tener un seguro que cubra viajes nacionales y al exterior.
7.2.5	Seguridad de equipos fuera de los locales de la Municipalidad	
7.2.5	Política 0702-009-MSS	Traslado de equipos Todo movimiento de equipos entre locales de la Municipalidad debe ser estrictamente controlado por el personal responsable de dichos activos.
7.2.6	Seguridad en el reuso o eliminación de equipos	
7.2.6	Política 0702-010-MSS	Desecho de equipo obsoleto Solo personal autorizado puede disponer de equipos de propiedad de la Municipalidad para su desecho, siempre y cuando se hayan controlado los riesgos de seguridad asociados a la información contenida en dicho equipo.
7.3	Controles Generales	
7.3.1	Política de puesto de trabajo despejado y bloqueo de pantalla	
7.3.1	Política 0703-001-MSS	Política de escritorios limpios Los trabajadores que manejan información deben mantener sus áreas de trabajo despejadas para reducir el riesgo de accesos no autorizados

Políticas de Seguridad de la Información

ISO 17799	Política MSS-PSI	Descripción
7.3.1	Política 0703-002-MSS	Impresión de documentos confidenciales Se debe asegurar que una persona autorizada reciba la impresión de documentos confidenciales que se envían a una impresora de red, a fin de proteger la confidencialidad durante y después de la impresión.
7.3.2	Retiro de propiedad	
7.3.2	Política 0703-003-MSS	Retiro de equipos Solo se permite a personal autorizado retirar equipos de la Municipalidad, siendo dicho personal responsable de su seguridad.

8. Gestión de Comunicaciones y Operaciones		
8.1	Procedimientos y responsabilidades de operación	
8.1.1	Documentación de procedimientos operativos	
8.1.1	Política 0801-001-MSS	Documentación de procedimientos operativos Los procedimientos operativos deben especificar las instrucciones detalladas para la ejecución de cada tarea, incluyendo las actividades de administración de sistemas. Dichos procedimientos deben estar documentados formalmente (MAPRO).
8.1.1	Política 0801-002-MSS	Cronograma de operaciones Los cronogramas de operaciones deben planearse y pasar por un proceso formal de autorización.
8.1.2	Control de cambios operacionales	
8.1.2	Política 0801-003-MSS	Control de cambios operacionales Los cambios operacionales deben probarse exhaustivamente y ser aprobados formalmente antes de ser puestos en producción.
8.1.3	Procedimientos de gestión de incidentes	
8.1.3	Política 0801-004-MSS	Respuestas ante incidentes de Seguridad de la Información El Oficial de Seguridad de la Información debe responder rápidamente a cualquier incidente de Seguridad de la Información, coordinando la recolección de información y sugiriendo medidas a tomar donde sea necesario.
8.1.3	Política 0801-005-MSS	Protección contra ataques de negación de servicio (DoS) Se deben tener listos planes de acción contra ataques de negación del servicio (DoS) los cuales deben ser mantenidos y probados periódicamente para asegurarse de su eficacia.




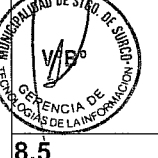
Políticas de Seguridad de la Información

ISO 17799	Política MSS-PSI	Descripción
8.1.3	Política 0801-006-MSS	<p>Análisis de incidentes de Seguridad de la Información ocasionados por fallas de sistemas</p> <p>Los incidentes de seguridad de la información originados por fallas de hardware o software deben investigarse de manera apropiada por especialistas.</p>
8.1.3	Política 0801-007-MSS	<p>Confidencialidad de los incidentes de Seguridad de la Información</p> <p>La información relacionada a incidentes de seguridad de la información sólo puede ser divulgada por personas autorizadas.</p>
8.1.4	Segregación de funciones	
8.1.4	Política 0801-008-MSS	<p>Necesidad de control dual / segregación de funciones</p> <p>Dondequiera que un incidente de seguridad de la información pueda ocasionar daño material o financiero a la Municipalidad, debe emplearse técnicas de control dual y segregación de funciones para mejorar el control de procedimientos de seguridad.</p>
8.1.5	Separación de los recursos de desarrollo y de producción	
8.1.5	Política 0801-009-MSS	<p>Separación de funciones en desarrollo y producción</p> <p>La Gerencia de Tecnologías de la Información debe asegurarse que una segregación de funciones apropiada se aplique a todas las áreas que se tienen que ver con el desarrollo, operaciones y administración de sistemas.</p>
8.1.6	Gestión de servicios externos	
8.1.6	Política 0801-010-MSS	<p>Tercerización de operaciones</p> <p>En el caso de tercerización de operaciones, se deben identificar los riesgos por anticipado e incorporar al contrato las medidas de seguridad apropiadas.</p>
8.2	Planificación y Aceptación del Sistema	
8.2.1	Planificación de la capacidad	
8.2.1	Política 0802-001-MSS	<p>Planeamiento de capacidad y prueba de nuevos sistemas</p> <p>Para las pruebas de nuevos sistemas se deben aplicar criterios de capacidad, carga máxima y prueba de stress. Debe demostrarse que sus niveles de rendimiento y resistencia cumplen o exceden las necesidades o requisitos técnicos de la Municipalidad.</p>
8.2.2	Aceptación del sistema	
8.2.2	Política 0802-002-MSS	<p>Paralelo de sistemas</p> <p>Los procedimientos de prueba de sistemas deben considerar un período de funcionamiento paralelo antes que el sistema nuevo o mejorado sea aceptado para su uso en producción. Los resultados del paralelo no deben revelar problemas o dificultades diferentes a los ya vistos durante la prueba de aceptación de usuario.</p>

Políticas de Seguridad de la Información

ISO 17799	Política MSS-PSI	Descripción
8.2.2	Política 0802-003-MSS	<p>Elaboración de bases de datos</p> <p>Antes de poner una base de datos en producción, se deben realizar pruebas exhaustivas de su funcionamiento, tanto a nivel lógico de su estructura, como de su eficiencia en un ambiente de producción.</p>
8.3	Protección contra software malicioso	
8.3.1	Medidas y controles contra software malicioso	
8.3.1	Política 0803-001-MSS	<p>Defensa de la red contra ataques maliciosos</p> <p>Todos los recursos activos de tratamiento de información: infraestructura de red, software base y de aplicación, deben configurarse y protegerse adecuadamente contra ataques físicos e intrusión.</p>
8.3.1	Política 0803-002-MSS	<p>Defensa contra virus informáticos</p> <p>Todas las PCs y servidores de la Municipalidad deben tener instalado un software antivirus. Igualmente, se deben mantener actualizado el archivo de firmas y escanear regularmente todos los equipos.</p>
8.3.1	Política 0803-003-MSS	<p>Software antivirus</p> <p>El software antivirus debe adquirirse de un proveedor reconocido, que tenga soporte técnico adecuado.</p>
8.3.1	Política 0803-004-MSS	<p>Respuesta a incidentes de virus</p> <p>Se debe desarrollar una estrategia integral y procedimientos de actuación para hacer frente a los virus informáticos, lo cual incluirá procedimientos y responsabilidades de administración, capacitación en el uso de software antivirus y recuperación después de los ataques de virus.</p>
8.3.1	Política 0803-005-MSS	<p>Descargar archivos e Información de Internet</p> <p>Se debe tener mucho cuidado al descargar información y archivos de Internet a fin de evitar el ingreso de código malicioso así como la descarga de material no apropiado.</p>
8.3.1	Política 0803-005-MSS	<p>Certeza de orígenes de archivos</p> <p>Los archivos electrónicos recibidos de remitentes desconocidos deben ser eliminados sin ser abiertos.</p>
8.3.1	Política 0803-006-MSS	<p>Instalación usuaria de software adicional</p> <p>Está prohibido instalar software no autorizado en las computadoras de la Municipalidad, tales como protectores de pantalla, software demostrativo, manejadores de música, video, mensajería instantánea, etc., salvo autorización expresa de la Gerencia de Tecnologías de la Información.</p>
8.3.1	Política 0803-007-MSS	<p>Manejo de rumores de virus</p> <p>Debe existir un procedimiento formal de tratamiento de los rumores de virus y otros ataques.</p>
8.4	Gestión interna de respaldo y recuperación	

Políticas de Seguridad de la Información

ISO 17799	Política MSS-PSI	Descripción
8.4.1		Respaldo y recuperación de la información
8.4.1	Política 0804-001-MSS	Gestión de procedimientos de respaldo y recuperación Se dará alta prioridad al respaldo de archivos de datos (backup) de la Municipalidad y la capacidad de restaurarlos. La Gerencia de Tecnologías de la Información será responsable de que la frecuencia de tales operaciones y que los procedimientos aplicados se adecuan a las necesidades de la Municipalidad.
8.4.1	Política 0804-002-MSS	Respaldo y recuperación de sistemas Los dueños de sistemas de información deben asegurarse que los procedimientos de respaldo y recuperación de sistemas sean los adecuados y estén implementados y funcionando.
8.4.1	 Política 0804-003-MSS	Duración de los medios Los medios usados para almacenar información deben corresponder a las necesidades de duración. El formato en el que se almacenan los datos debe ser evaluado cuidadosamente, especialmente donde hayan formatos propietarios.
8.4.1	Política 0804-004-MSS	Caducidad de archivos electrónicos El almacenamiento de datos electrónicos debe reflejar las necesidades de la Municipalidad y los dispositivos legales y regulatorios.
8.4.2		Diarios de operación
8.4.2	 Política 0804-005-MSS	Monitoreo de los logs de operaciones Los registros de log operacional deben ser revisados periódicamente por personal calificado y las discrepancias con los procedimientos operacionales deben ser comunicadas al dueño (propietario) del sistema de información.
8.4.3		Registro de fallas
8.4.3	 Política 0804-006-MSS	Registro y reporte de fallas de equipos Toda falla de equipos (incluyendo daño) debe anotarse en un registro especialmente designado para tal fin por el personal encargado de su mantenimiento.
8.4.3	 Política 0804-007-MSS	Registro y reporte de fallas de software Se debe registrar y reportar formalmente toda falla de software a los responsables de soporte de software (Gerencia de Tecnologías de la Información).
8.5		Gestión de Redes
8.5.1		Controles de red

Políticas de Seguridad de la Información

ISO 17799	Política MSS-PSI	Descripción
8.5.1	Política 0805-001-MSS	<p>Gestión de redes</p> <p>Los administradores de redes deberán implantar los controles y medidas requeridas para conseguir y conservar la seguridad de los datos en las redes de computadoras, así como la integridad de la red y protección de los servicios conectados contra accesos no autorizados.</p>
8.6	Utilización y seguridad de medios	
8.6.1	Gestión de medios removibles	
8.6.1	Política 0806-001-MSS	<p>Uso de medios removibles de almacenamiento</p> <p>Solamente el personal autorizado a instalar o a modificar el software podrá utilizar medios removibles para transferir datos de la Municipalidad. Cualquier otra persona requerirá autorización expresa.</p>
8.6.2	Eliminación de medios	
8.6.2	Política 0806-002-MSS	<p>Eliminación segura de documentos</p> <p>Todos los documentos de naturaleza confidencial deben ser destruidos cuando ya no se requieren. El dueño del documento debe autorizar o realizar esta destrucción en coordinación con la Subgerencia de Tramite Documentario y Archivo.</p>
8.6.2	Política 0806-003-MSS	<p>Eliminación de Software</p> <p>Sólo se debe eliminar un programa de software cuando se haya decidido que dicho programa ya no es necesario y que no se necesita tener acceso a sus archivos de datos mediante dicho programa.</p>
8.6.3	Procedimientos de manejo de la información	
8.6.3	Política 0806-004-MSS	<p>Uso de buenas prácticas de gestión de información</p> <p>Todos los usuarios deben proteger la confidencialidad, integridad y disponibilidad de los archivos durante la creación, almacenamiento, modificación, copiado y borrado/eliminación de archivos de datos.</p>
8.6.3	Política 0806-005-MSS	<p>Comprobación de exactitud y validez de documentos</p> <p>Se debe confirmar la validez e integridad de documentos, especialmente aquellos que comprometen u obligan a la Municipalidad.</p>
8.6.3	Política 0806-006-MSS	<p>Dependencias entre documentos y archivos</p> <p>Los documentos altamente sensibles o críticos no deben depender de la disponibilidad o integridad de archivos de datos sobre los que el autor no tenga control. Los documentos e informes importantes deben ser autónomos y contener toda la información necesaria.</p>
8.6.3	Política 0806-007-MSS	<p>Fotocopiado de información confidencial</p> <p>Los trabajadores deben conocer los riesgos de brechas de confidencialidad durante el fotocopiado/duplicación de documentos. Sólo se debe duplicar documentos confidenciales con la debida autorización del dueño del documento.</p>

Políticas de Seguridad de la Información

ISO 17799	Política MSS-PSI	Descripción
8.6.3	Política 0806-008-MSS	Eliminación de archivos temporales (tmp) Los archivos temporales en las computadoras de usuarios deben ser eliminados con regularidad para prevenir su posible mal uso por usuarios no autorizados.
8.6.4	Seguridad de la documentación de sistemas	
8.6.4	Política 0806-009-MSS	Gestión de documentación de sistemas La documentación de sistemas es un requisito obligatorio para todo sistema de información de la Municipalidad. Dicha documentación debe mantenerse actualizada y disponible.
8.7	Intercambio de Información y software	
8.7.1	Acuerdos para intercambio de información y software	
8.7.1	Política 0807-001-MSS	Envío de información a terceros Antes de enviar información a terceros, se debe verificar que el receptor está autorizado a recibir dicha información y que las medidas adoptadas por los receptores aseguran la confidencialidad e integridad de la información que se envía.
8.7.2	Seguridad física de medios en tránsito	
8.7.2	Política 0807-002-MSS	Transporte de documentos confidenciales Las medidas de protección de la confidencialidad, integridad y disponibilidad en el transporte o transmisión de documentos confidenciales serán establecidas por los dueños de dichos documentos, quienes deberán asegurarse que tales medidas son las apropiadas.
8.7.3	Seguridad en Comercio Electrónico	
8.7.3	Política 0807-003-MSS	Desarrollo y mantenimiento de sitios Web Solamente personal debidamente calificado y autorizado participará en el desarrollo y mantenimiento de sitios Web de la Municipalidad.
8.7.4	Seguridad del correo electrónico	
8.7.4	Política 0807-004-MSS	Envío de correo electrónico Se debe utilizar el correo electrónico solamente para fines relacionados con la Municipalidad. Antes de adjuntar archivos a un mensaje de e-mail se debe verificar que la clasificación de información de dicho archivo permite su envío al destinatario previsto y también, previamente se debe escanear y verificar que no exista virus u otro código malicioso.
8.7.4	Política 0807-005-MSS	Recepción de correo erróneo Los mensajes de correo electrónico no solicitado deben ser tratados con precaución y no ser respondidos.
8.7.4	Política 0807-006-MSS	Recepción de correo no solicitado Se debe verificar la identidad y la autenticidad del remitente de cualquier mensaje de correo electrónico no solicitado antes de abrirlo.

Políticas de Seguridad de la Información

ISO 17799	Política MSS-PSI	Descripción
8.7.5	Seguridad de los sistemas ofimáticos	
8.7.5	Política 0807-007-MSS	<p>Uso de equipos de fax</p> <p>Sólo se puede enviar información confidencial por fax cuando no estén disponibles métodos más seguros de transmisión. El dueño de la información y el recipiente previsto deben autorizar las transmisiones por anticipado.</p>
8.7.5	Política 0807-008-MSS	<p>Gestión de máquinas contestadoras y correo de voz</p> <p>No se debe grabar información confidencial en contestadoras automáticas o sistemas de correo de voz.</p>
8.7.5	Política 0807-009-MSS	<p>Información por teléfono</p> <p>Se debe tener mucha precaución cuando se comunica información confidencial vía telefónica, verificando además la identidad de los destinatarios.</p>
8.7.5	Política 0807-010-MSS	<p>Envío erróneo de información a terceros</p> <p>Se debe comprobar cuidadosamente las direcciones de email y números de fax antes de enviar información, especialmente en los casos de información confidencial. La misma precaución debe aplicarse cuando existe la posibilidad que se divulguen las direcciones de E-mail u otra información de contacto.</p>
8.7.6	Sistemas públicamente disponibles	
8.7.6	Política 0807-011-MSS	<p>Seguridad de sistemas públicamente disponibles</p> <p>Se deben establecer controles en los sistemas públicamente disponibles de captura de información con la finalidad que la información confidencial se proteja durante su recojo y almacenamiento, y que el acceso a dicho sistema no permita accesos no autorizados a otras redes a las que está conectado el sistema.</p>
8.7.7	Otras formas de intercambio de información	
8.7.7	Política 0807-012-MSS	<p>Transmisión e intercambio de datos</p> <p>Solamente se puede transmitir datos o información confidenciales cuando la seguridad de los datos puede garantizarse razonablemente usando técnicas de encriptación.</p>
9. Control de Accesos		
9.1	Requisitos de negocio para el Control de Accesos	
9.1	Política 0901-001-MSS	<p>Control de distribución de información</p> <p>Los datos e información deben protegerse mediante controles técnicos y administrativos a fin de asegurarse que están disponibles solo para personas autorizadas.</p>
9.1.1	Política de control de accesos	

Políticas de Seguridad de la Información

ISO 17799	Política MSS-PSI	Descripción
9.1.1	Política 0901-002-MSS	<p>Gestión de estándares de control de accesos</p> <p>Los estándares de control de acceso de los sistemas de información deben establecerse de tal manera que prevengan accesos no autorizados y a la vez proporcionen acceso inmediato según los requerimientos de la Municipalidad.</p>
9.1.1	Política 0901-003-MSS	<p>Establecimiento de una estructura de carpetas y datos para usuarios</p> <p>Las estructuras de carpetas de datos de usuarios deben ser definidas por la Gerencia de Tecnologías de la Información y los usuarios deben seguir dicha estructura. Las restricciones de acceso a tales carpetas se deben aplicar como convenga para restringir el acceso no autorizado.</p>
9.1.1	Política 0901-004-MSS	<p>Protección de documentos con contraseñas</p> <p>Se debe proteger la información confidencial usando, preferentemente, el control de acceso de la carpeta donde está situado el archivo correspondiente. No se recomienda el uso solamente de contraseñas para proteger documentos ya que es poco eficaz.</p>
9.1.1	Política 0901-005-MSS	<p>Defensa contra ataques internos intencionales</p> <p>Los estándares de control de acceso y de clasificación de datos deben ser revisados y actualizados periódicamente para reducir la incidencia y la posibilidad de ataques internos.</p>
9.1.1	Política 0901-006-MSS	<p>Configuración de acceso a la Intranet/Extranet</p> <p>Los responsables de configurar el acceso de la Intranet/Extranet deben asegurarse que la configuración del acceso replique, como mínimo, las restricciones de los sistemas convencionales de la Municipalidad.</p>
9.1.1	Política 0901-007-MSS	<p>Configuración de acceso a Internet</p> <p>El personal encargado de configurar el acceso a Internet debe asegurarse que la red de la Municipalidad tenga la debida protección. Como mínimo se debe instalar un firewall debidamente configurado.</p>
9.1.1	Política 0901-008-MSS	<p>Acceso a información sobre proyectos de la Municipalidad</p> <p>Solamente personas autorizadas pueden tener acceso a datos confidenciales sobre proyectos de propiedad de la Municipalidad o gerenciados por sus trabajadores.</p>
9.2	Gestión de Acceso de Usuarios	
9.2	Política 0902-001-MSS	<p>Gestión de Acceso de Usuarios</p> <p>El acceso a los sistemas de información debe autorizarse por su dueño y tal acceso debe registrarse en una Lista de Control de Accesos. Estos registros deben considerarse como altamente confidenciales y ser debidamente protegidos.</p>

Políticas de Seguridad de la Información

ISO 17799	Política MSS-PSI	Descripción
9.2	Política 0902-002-MSS	Inicio y fin de sesión Los sistemas deben considerar el manejo de sesiones con los usuarios, las cuales se cerrarán después de un tiempo de no uso (time-out).
9.2.1	Registro de usuarios	
9.2.1	Política 0902-003-MSS	Registro e identificador de usuarios Se debe formalizar un procedimiento de registro de altas y bajas de usuarios para garantizar el acceso a los sistemas y servicios de información de la Municipalidad.
9.2.2	Gestión de privilegios	
9.2.2	Política 0902-004-MSS	Asignación de privilegios La asignación de privilegios de acceso en los sistemas de la Municipalidad debe controlarse mediante un proceso formal de autorización, en el cual debe participar el dueño del sistema en cuestión.
9.2.3	Gestión de contraseñas de usuario	
9.2.3	Política 0902-005-MSS	Gestión de contraseñas La selección, uso y gestión de contraseñas como medio principal para el control de acceso a los sistemas de la Municipalidad debe adecuarse a las mejores prácticas existentes. En particular, las contraseñas no deben ser compartidas con otra persona bajo ninguna circunstancia.
9.2.4	Revisión de los derechos de acceso de los usuarios	
9.2.4	Política 0902-006-MSS	Manejo de renuncias de personal En el caso de renuncias o ceses de personal, la Subgerencia de Recursos Humanos debe considerar, conjuntamente con el Oficial de Seguridad de la Información, si los derechos de acceso del personal saliente constituyen un riesgo inaceptable para la Municipalidad y, si es así, deben revocarse todos los derechos de acceso.
9.2.4	Política 0902-007-MSS	Personal que trabajará en otras Entidades. Se debe anular los derechos de acceso a la información de la Municipalidad de manera inmediata a los trabajadores que se van a trabajar a otra Entidad.
9.3	Responsabilidades de los Usuarios	
9.3.1	Uso de contraseñas	
9.3.1	Política 0902-008-MSS	Responsabilidad de usuarios en el uso de contraseñas Los usuarios deberán proteger sus contraseñas usando las mejores prácticas existentes, como por ejemplo: no se deben usar contraseñas fáciles de adivinar, como nombres, números de la placas de vehículos, fechas del nacimiento, o similares; la contraseña no debe almacenarse en teclas de función programables, debe ser cambiada si llega a ser conocida por personas no autorizadas, entre otras.
9.3.2	Equipo informático de usuario desatendido	

Políticas de Seguridad de la Información

ISO 17799	Política MSS-PSI	Descripción
9.3.2	Política 0903-009-MSS	<p>Protección de computadoras desatendidas</p> <p>Todos los usuarios de computadoras personales y laptops deben asegurarse que sus pantallas queden protegidas y no muestren información cuando estén desatendidas.</p>
9.4	Control de Acceso a la Red	
9.4	Política 0904-001-MSS	<p>Gestión de controles de acceso a la red</p> <p>El acceso a los recursos de red debe controlarse estrictamente para evitar accesos no autorizados. El acceso a sistemas de cómputo y periféricos debe estar restringido por defecto y autorizarse expresamente.</p>
9.4	Política 0904-002-MSS	<p>Configuración de redes</p> <p>Las redes deben estar diseñadas y configuradas de tal manera que se restrinjan los accesos de acuerdo a reglas claramente definidas sin afectar la confiabilidad y el rendimiento.</p>
9.4	Política 0904-003-MSS	<p>Gestión de seguridad de redes</p> <p>El acceso a los recursos de la red de la Municipalidad debe controlarse estrictamente de acuerdo con la Lista de Control de Accesos aprobada, la cual debe estar actualizada permanentemente.</p>
9.4.1	Política de uso de los servicios de la red	
9.4.2	Ruta forzosa	
9.4.2	Política 0904-004-MSS	<p>Establecimiento de rutas forzosas</p> <p>La red debe estar configurada y equipada de tal manera que se puedan establecer rutas forzosas desde las estaciones de trabajo hacia los servidores de la Municipalidad.</p>
9.4.3	Autenticación de usuarios para conexiones externas	
9.4.3	Política 0904-005-MSS	<p>Acceso remoto a la red</p> <p>El acceso remoto a la red de la Municipalidad será permitido solamente cuando el usuario se identifique de manera segura, los datos que viajan por la red estén encriptados y los privilegios restringidos a la ocasión.</p>
9.4.4	Autenticación de nodos de la red	
9.4.4	Política 0904-006-MSS	<p>Autenticación de dispositivos remotos</p> <p>Las conexiones remotas a sistemas informáticos se deberán autenticar con la finalidad de reducir la amenaza de accesos no autorizados a las aplicaciones.</p>
9.4.5	Protección a puertos de diagnóstico remoto	

Políticas de Seguridad de la Información

ISO 17799	Política MSS-PSI	Descripción
9.4.5	Política 0904-007-MSS	Protección acceso a puertos de diagnóstico Se deberá proteger, con un mecanismo de seguridad probado, el acceso a puertos de diagnóstico remoto para asegurar que sólo son accesibles tras un acuerdo formal de la Gerencia de Tecnologías de la Información con el personal de mantenimiento del hardware o software que solicita el acceso.
9.5	Control de acceso al sistema operativo	
9.5	Política 0905-001-MSS	Control de acceso al Sistema Operativo El acceso a comandos del sistema operativo debe restringirse para que solamente las personas autorizadas puedan ejecutar dichos comandos. Las funciones de administración de dichos sistemas deben requerir aprobación específica.
9.5.1	Identificación automática de terminales	
9.5.1	Política 0905-002-MSS	Identificación automática de terminales Se debe usar la identificación automática de terminales para autenticar las conexiones a ubicaciones específicas y a equipos portátiles.
9.5.2	Procedimientos de conexión de terminales	
9.5.2	Política 0905-003-MSS	Conexión al sistema informático El procedimiento de conexión a los sistemas informáticos debe minimizar la posibilidad de accesos no autorizados.
9.5.3	Identificación y autenticación del usuario	
9.5.3	Política 0905-004-MSS	Identificación del usuario Todos los usuarios deberán disponer de un identificador único para su uso personal y exclusivo, a fin de vincular a los usuarios con la responsabilidad de sus acciones.
9.6	Control de Acceso a las aplicaciones	
9.6.1	Restricción de acceso a la información	
9.6.1	Política 0906-001-MSS	Restricción de acceso Los controles de acceso deben ser fijados de tal manera que se reduzcan al mínimo los riesgos de la seguridad de la información pero que a la vez no impidan la operatividad de la Municipalidad.
9.6.2	Aislamiento de sistemas sensibles	
9.6.2	Política 0906-002-MSS	Administración de acceso a sistemas altamente confidenciales Los controles de acceso para sistemas de información altamente confidenciales deben ser fijados en concordancia con la clasificación de los activos de información a ser protegidos.
9.7	Seguimiento de accesos y usos del sistema	
9.7.1	Registro de incidentes	

Políticas de Seguridad de la Información

ISO 17799	Política MSS-PSI	Descripción
9.7.1	Política 0907-001-MSS	Registro de evidencias de incidentes Se debe advertir a todos los empleados que en caso de incidentes de seguridad, es necesario registrar y conservar evidencias o pistas para uso del Oficial de Seguridad de la Información
9.7.2	Seguimiento del uso de los sistemas	
9.7.2	Política 0907-002-MSS	Monitoreo de accesos y uso del sistema Se debe registrar y supervisar el acceso a los sistemas para identificar su posible mala utilización.
9.7.2	Política 0907-003-MSS	Integridad de las investigaciones de incidentes de Seguridad de la Información Se debe monitorear regularmente el uso de los sistemas de información, registrando e investigando todos los eventos inesperados. Tales registros también deben auditarse periódicamente de tal manera que sus resultados, sumados al historial de errores fortalezcan la investigación.
9.7.3	Sincronización de relojes	
9.7.3	Política 0907-004 - MSS	Sincronización de relojes del sistema Los relojes del sistema se deben sincronizar regularmente, especialmente cuando hay diferentes plataformas de procesamiento.
9.8	Informática móvil y teletrabajo	
9.8.1	Informática móvil	
9.8.1	Política 0908-001-MSS	Uso de equipos portátiles de cómputo Las personas que usan computadoras portátiles fuera de la Municipalidad deben conocer los riesgos de Seguridad de Información referidos a equipos portátiles e implementar las protecciones apropiadas para reducir al mínimo dichos riesgos.
9.8.1	Política 0908-002-MSS	Uso de facilidades de centros empresariales El personal que usa centros empresariales para trabajar asuntos de la Municipalidad es responsable de la seguridad y subsecuente remoción de toda información registrada por él en los sistemas de dicho centro.
9.8.1	Política 0908-003-MSS	Respaldo de datos (backup) de equipos portátiles de cómputo La información y datos almacenados en computadoras portátiles se deben respaldar regularmente (backup). Es responsabilidad del usuario asegurarse de que esto se realice de manera periódica.
9.8.1	Política 0908-004-MSS	Viajes de trabajo Los empleados que viajan por asuntos de la Municipalidad son responsables de la seguridad de la información en su poder.

Políticas de Seguridad de la Información

ISO 17799	Política MSS-PSI	Descripción
10. Desarrollo y mantenimiento de Sistemas		
10.1	Requisitos de seguridad de los sistemas	
10.1	Política 1001-001-MSS	Implementación de software nuevo o mejorado Toda implementación de software debe considerar una planificación adecuada para reducir los riesgos de seguridad de la información mediante la aplicación de los controles apropiados.
10.1	Política 1001-002-MSS	Documentación de sistemas Todos los sistemas deben tener documentación completa y actualizada. Ningún sistema debe pasar a producción si no tiene la documentación de soporte disponible.
10.1.1	Análisis y especificación de los requisitos de seguridad	
10.1.1	Política 1001-003-MSS	Justificación de desarrollo de nuevos sistemas Todo desarrollo de software, dentro o fuera de la Municipalidad debe contar con un sustento técnico-económico, un presupuesto adecuado y el compromiso de disponer de los recursos necesarios para solventar el proyecto de inicio a fin. El proceso de aprobación debe ser formal e incluir a la Alta Dirección si fuera necesario.
10.1.1	Política 1001-004-MSS	Desarrollo y mantenimiento de software Las especificaciones técnicas y funcionales para el desarrollo y mantenimiento de un software deben contemplar formalmente los requerimientos de seguridad, incluyendo los controles técnicos de acceso, la asignación restringida de privilegios y otros requisitos que resulten convenientes para dicha aplicación.
10.1.1	Política 1001-005-MSS	Interfases de software aplicativo El desarrollo de interfases de sistemas es una tarea altamente especializada y por lo tanto sólo debe ser realizada por profesionales con la debida calificación y experiencia comprobada en el tema. Debe considerar sobremanera los aspectos de seguridad de los sistemas que son conectados y de las plataformas que intervienen.
10.2	Seguridad de las aplicaciones del sistema	
10.2.1	Validación de los datos de entrada	
	Política 1002-001-MSS	Control de datos de entrada Como parte del proceso de diseño, desarrollo y/o implementación de todo software en la Municipalidad de Santiago de Surco debe realizarse, de manera obligatoria, el control de datos de entrada, considerando, como mínimo, los procedimientos de consistencia de datos, correspondencia a las autorizaciones y privilegios de usuario, y procedimientos de manejo de errores.

Políticas de Seguridad de la Información

ISO 17799	Política MSS-PSI	Descripción
10.2.2	Control del proceso interno	
	Política 1002-002-MSS	Control de datos en proceso Todo sistema en producción debe contemplar el control de los datos en proceso. Dichos controles deberán ser diseñados conjuntamente con el dueño del sistema. Como mínimo se debe considerar controles externos de integridad de datos así como momentos de ejecución de programas.
10.2.3	Autenticación de mensajes	
	Política 1002-003-MSS	Autenticación de mensajes en intercambio de datos Todo intercambio electrónico de información confidencial deberá tener implementado un procedimiento probado de autenticación de mensajes.
10.2.4	Validación de los datos de salida	
	Política 1002-004-MSS	Control de datos de salida Como parte del proceso de diseño, desarrollo y/o implementación de todo software en la Municipalidad debe existir, de manera obligatoria, un procedimiento para controlar los datos de salida, considerando, como mínimo, procedimientos de consistencia de datos de salida, correspondencia a las autorizaciones y privilegios de usuario, y procedimientos de manejo de errores.
10.3	Controles Criptográficos	
10.3.1	Política de uso de los controles criptográficos	
	Política 1003-001-MSS	Uso de medidas criptográficas La Municipalidad debe evaluar constantemente, mediante un análisis de riesgos, qué información requiere ser protegida con medidas criptográficas.
10.3.2	Cifrado	
	Política 1003-002-MSS	Uso de técnicas de encriptación Las técnicas de encriptación a ser usadas en la Municipalidad deben considerar las regulaciones y restricciones nacionales e internacionales. Antes de la transmisión, se deben coordinar los procedimientos que utilizarán el emisor y el receptor.
10.3.3	Firmas digitales	
	Política 1003-003-MSS	Uso de firmas digitales en la Municipalidad La conveniencia y viabilidad, así como los casos en los que se puede usar firmas digitales debe analizarse conjuntamente entre la parte técnica y legal de la Municipalidad, teniendo en cuenta toda la legislación relativa que describe las condiciones en las que una firma digital tiene validez legal.

Políticas de Seguridad de la Información

ISO 17799	Política MSS-PSI	Descripción
10.4	Seguridad de los archivos del sistema	
10.4.1	Control del software en producción	
10.4.1	Política 1004-001-MSS	Gestión de operaciones y administración de sistemas La operación y administración de sistemas de la Municipalidad debe llevarse a cabo siguiendo procedimientos diseñados y documentados detalladamente según las mejores prácticas y debidamente aprobadas por los dueños de los sistemas.
10.4.1	Política 1004-002-MSS	Gestión de bibliotecas de programas en producción Las bibliotecas de programas que están en producción deben tener controles que impidan el acceso de personas no autorizadas, el cual se debe otorgar estrictamente por necesidad de uso. Los procedimientos de modificación deben estar formalmente autorizados por el dueño del sistema y prever el control dual.
10.4.2	Protección de los datos de prueba del sistema	
10.4.2	Política 1004-003-MSS	Uso de datos para pruebas Todo sistema de información debe tener un juego de datos de prueba que sea consistente y no contenga datos reales o confidenciales. Si no se puede evitar el uso de datos reales confidenciales, éstos deben ser despersonalizados antes de ser usados.
10.4.3	Control de acceso a la biblioteca de programas fuente	
10.4.3	Política 1004-004-MSS	Gestión de bibliotecas de programas fuente Las bibliotecas de programas fuente deben tener controles que impidan el acceso de personas no autorizadas y manejarse con un adecuado control de versiones. Los procedimientos de uso de los programas fuente deben estar definidos formalmente de acuerdo a la metodología de desarrollo de sistemas de la Municipalidad.
10.5	Seguridad en los procesos de desarrollo y soporte	
10.5.1	Procedimientos de control de cambios	
10.5.1	Política 1005-001-MSS	Gestión de procedimientos de control de cambios Todo cambio a sistemas de información debe realizarse mediante procedimientos formales de control de cambios, y debe autorizarse y probarse exhaustivamente en un ambiente de la prueba antes de pasarlo al ambiente de producción.
10.5.1	Política 1005-002-MSS	Control de versiones Se deben aplicar procedimientos del control de versiones a todos los programas de software y procedimientos pertenecientes a la Municipalidad.

Políticas de Seguridad de la Información

ISO 17799	Política MSS-PSI	Descripción
10.5.1	Política 1005-003-MSS	<p>Actualizaciones de software recomendadas por el proveedor</p> <p>Solo de se debe actualizar el software a una nueva versión si se han evaluado adecuadamente las ventajas previstas, la necesidad de dicha actualización y las implicancias de dicha actualización así como sus riesgos.</p>
10.5.1	Política 1005-004-MSS	<p>Reparaciones de emergencia al software</p> <p>En el caso que se requiera realizar reparaciones de emergencia al software aplicativo, será la gerencia quien tome la decisión al respecto, después de evaluar la necesidad e implicancias de dicha operación. En cualquier caso, la reparación deberá hacerse estrictamente de acuerdo a procedimientos acordados de control de cambios.</p>
10.5.2	Revisión técnica de los cambios en el sistema operativo	
10.5.2	Política 1005-005-MSS	<p>Mejoras (upgrades) de software al sistema operativo</p> <p>Toda decisión de instalar mejoras a sistemas operativos debe considerar los riesgos asociados y tener la adecuada planificación mediante el establecimiento de un proyecto formal que también considere el manejo de contingencias.</p>
10.5.3	Restricciones en los cambios a los paquetes de software	
	Política 1005-006-MSS	<p>Cambios a paquetes de software</p> <p>No se deben realizar modificaciones a los paquetes de software a menos que sea estrictamente necesario, en cuyo caso se deberá guardar el software original (sin cambios) y probar y documentar los cambios realizados.</p>
10.5.5	Desarrollo externo del software	
	Política 1005-007-MSS	<p>Calidad de desarrollo externo</p> <p>Todo desarrollo externo de software debe hacerse por empresas debidamente certificadas en dicha actividad y determinar los derechos de propiedad intelectual. Se debe tener acuerdos para manejar los posibles fallos del contratista.</p>

11. Gestión de Incidentes en la Seguridad de Información		
11.1	Reporte de eventos y debilidades de la Seguridad de la Información	
11.1.1	Reporte de Eventos	
11.1.1	Política -1105-001-MSS	<p>Procedimiento formal</p> <p>Un procedimiento formal de reporte de eventos en la seguridad de la información debe ser establecido conjuntamente con una respuesta de incidencias y procedimientos de escalada, estableciendo las acciones que serán tomadas al recibir dicho reporte. Se debe establecer dentro de este reporte un punto de contacto que siempre este disponible y que sea capaz de proveer respuestas adecuadas a tiempo.</p>

Políticas de Seguridad de la Información

ISO 17799	Política MSS-PSI	Descripción
	Política -1105-002-MSS	Procedimiento del reporte Los procedimientos de reporte del cual deben tener conocimiento los empleados, contratistas y terceros, deben incluir: procesos de retroalimentación que aseguren que los eventos sean notificados; formulario de reporte, el cual apoya la acción del reporte y ayuda al encargado del reporte a recordar las acciones necesarias cuando se produce un evento.
11.1.1	Política -1105-003-MSS	Recolectando evidencias Para ser capaz de tratar propiamente eventos e incidentes de la seguridad de información puede ser necesario recolectar evidencias lo mas pronto posible después de la ocurrencia
11.1.1	Política -1105-004-MSS	Respuesta del sistema El mal funcionamiento u otro comportamiento anormal en el sistema puede ser un indicador de un ataque de seguridad o de una abertura en la seguridad, debiendo ser reportado como un evento de la seguridad de información.
11.1.2		Reporte de Debilidades
11.1.2	Política -1105-005-MSS	Mecanismo de reporte El mecanismo del reporte debe ser fácil, accesible y disponible como sea posible. Deben ser informados que por ninguna circunstancia deben tratar de probar una debilidad sospechosa.
11.1.2	Política -1105-006-MSS	Probar debilidades Probar las debilidades puede ser interpretado como un potencial mal uso del sistema y puede ocasionar un daño al sistema o servicio de información y resultar en responsabilidad legal para el individuo que realiza la prueba.
11.2		Gestión de las mejoras e incidentes de la Seguridad de Información
	Política -1105-007-MSS	Responsabilidades y procedimiento de las mejoras e incidentes de la seguridad de información. Las responsabilidades y procedimientos deben establecerse para maniobrar los eventos y debilidades en la seguridad de información de una manera efectiva una vez que hayan sido reportados.
11.2.1		Responsabilidades y procedimientos
11.2.1	Política -1105-008-MSS	Monitoreo del sistema, alerta y vulnerabilidad El monitoreo de los sistemas, alertas y vulnerabilidades deben ser utilizados para detectar los incidentes en la seguridad de información.

Políticas de Seguridad de la Información

ISO 17799	Política MSS-PSI	Descripción
11.2.1	Política -1105-009-MSS	<p>Pautas para procedimientos de la gestión de incidentes en la seguridad de información</p> <p>Los procedimientos deben ser establecidos para maniobrar diferentes tipos de incidentes en la seguridad de información como, las fallas y pérdidas de servicio en el sistema, código malicioso, negación de servicios, apertura de confidencialidad e integridad y el mal uso de los sistemas de información.</p>
11.2.2	Recolección de evidencia	
11.2.2	Política -1105-010-MSS	<p>Acciones para recolectar evidencias</p> <p>Cuando una acción o seguimiento contra una persona u Municipalidad, después de un incidente en la seguridad de información, implique acción legal, la evidencia debe ser recolectada, retenida y presentada para estar conforme con las reglas para la colocación de evidencia en la jurisdicción relevante.</p>
11.2.2	Política -1105-011-MSS	<p>Acciones para los Procesos internos</p> <p>Los procesos internos deben ser desarrollados y seguidos cuando se recolecte y presente evidencia para propósitos disciplinarios maniobrados dentro de la Municipalidad.</p>
11.2.2	Política -1105-012-MSS	<p>Admisibilidad de la evidencia</p> <p>Para lograr admisibilidad de la evidencia, la Municipalidad debe asegurar que sus sistemas de información cumplen con cualquier estándar o código publicado de práctica para la producción de evidencia admisible.</p>
11.2.2	Política -1105-013-MSS	<p>Integridad de material de evidencia</p> <p>La integridad de todo material de evidencia debe ser protegida. Las copias deben ser supervisadas por personal confiable y se debe registrar la información de cuando y donde fue ejecutado el proceso de copia, quien realizo dicha actividad, y que herramientas y programas se utilizaron.</p>

12. Gestión de Continuidad del Negocio

12.1	Aspectos de la Gestión de Continuidad del Negocio	
12.1.1	Proceso de gestión de la continuidad del negocio	
12.1.1	Política 1201-001-MSS	<p>Gestión de continuidad del negocio</p> <p>La gestión de la continuidad del negocio debe incorporarse en los procesos y estructura de la Municipalidad, asignando la responsabilidad de coordinación de este proceso al comité de seguridad de la información.</p>

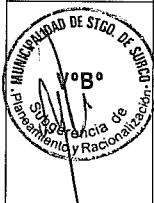



Políticas de Seguridad de la Información

ISO 17799	Política MSS-PSI	Descripción
	Política 1201-002-MSS	Proceso de continuidad del negocio El proceso de continuidad del negocio debe incluir la identificación y priorización de los procesos críticos y el impacto de las interrupciones. Los planes y procesos de continuidad así definidos deben probarse y actualizarse periódicamente.
12.1.1	Política 1201-003-MSS	Iniciativa para el Plan de Continuidad del Negocio La gerencia debe tener la iniciativa en la realización del Plan de Continuidad del Negocio.
12.1.1	Política 1201-004-MSS	Plan de recuperación de desastres Los dueños de sistemas de información deben asegurarse que sus sistemas cuentan con planes de recuperación de desastres probados y en funcionamiento.
12.1.2	Continuidad del negocio y análisis de impactos	
12.1.2	Política 1201-005-MSS	Análisis de impactos Los dueños de los sistemas de información, conjuntamente con los responsables técnicos de su manejo y respaldados por la Alta Dirección, identificarán los eventos potencialmente causantes de interrupciones a procesos y/o servicios.
12.1.2	Política 1201-006-MSS	Minimización de impacto de ataques informáticos Se deben elaborar planes para minimizar los daños por posibles ataques informáticos, los que deberán ser mantenidos y probados periódicamente para asegurar su eficacia y que los tiempos de recuperación sean razonables.
12.1.4	Marco de planificación para la continuidad del negocio	
	Política 1201-007-MSS	Responsabilidades de los Planes de Continuidad La Alta Dirección será responsable de la existencia de un esquema único de planes de continuidad del negocio que garantice que los diferentes planes son consistentes entre sí y que cada plan tiene un dueño designado. Asimismo que los procedimientos de emergencia y los planes de respaldo manual y de reanudación estén bajo la responsabilidad de los dueños de los correspondientes recursos o procesos del negocio involucrados.
	Política 1201-008-MSS	Activación de los Planes de Continuidad Cada plan de continuidad del negocio debería especificar claramente las condiciones para su activación, los procedimientos de emergencia a llevar a cabo, los procedimientos de respaldo que permitirán operar, los procedimientos de reanudación en condiciones de normalidad así como las personas responsables de ejecutar cada etapa del plan.

Políticas de Seguridad de la Información

ISO 17799	Política MSS-PSI	Descripción
	Política 1201-009-MSS	Mantenimiento y concientización Todo plan de continuidad debe tener un calendario de mantenimiento de pruebas del plan, así como prever actividades de concientización y capacitación diseñadas para asegurar que los procesos sean eficaces
12.1.5		Prueba, mantenimiento y reevaluación de los Planes de Continuidad
12.1.5	Política 1201-010-MSS	Prueba del Plan de Continuidad del Negocio El Plan de Continuidad del Negocio debe ser probado periódicamente para asegurarse que cada uno de los responsables de las diferentes acciones entiendan correctamente la ejecución del Plan.
12.1.5	Política 1201-011-MSS	Mantenimiento y reevaluación del Plan de Continuidad del Negocio El Plan de Continuidad del Negocio debe ser continuamente actualizado para reflejar los cambios en los recursos, procesos y servicios de la Municipalidad.

13. Cumplimiento

13.1		Cumplimiento con requisitos legales
13.1.1		Identificación de legislación aplicable
		Política 1301-001-MSS Documentación de requisitos Cada dueño de sistema de información será responsable de documentar de forma explícita todos los requisitos legales, regulatorios y contractuales que sean importantes para su sistema. Esta documentación estará disponible para uso legal y técnico del sistema.
13.1.1		Política 1301-002-MSS Cuidados contra denuncias de difamación y calumnias A fin de evitar denuncias por difamación y/o calumnia, se prohíbe que los trabajadores realicen observaciones despectivas sobre otras personas u organizaciones usando el nombre y/o recursos de la Municipalidad.
13.1.2		Derechos de propiedad intelectual
		Política 1301-003-MSS Responsabilidad de la Alta Dirección La Alta Dirección es responsable de implantar los procedimientos apropiados de cumplimiento de las restricciones legales sobre uso de material protegido por derechos de propiedad intelectual.
13.1.2		Política 1301-004-MSS Responsabilidad de la Subgerencia de Recursos Humanos La Subgerencia de Recursos Humanos ejecutará las acciones necesarias para que todos los trabajadores conozcan los principales aspectos de propiedad intelectual y licenciamiento de software que guarden relación con sus funciones.
13.1.2		Política 1301-005-MSS Renovación de nombres de dominio de sitios Web Se deben proteger y asegurar los nombres de dominio de Internet de forma similar a cualquier otro activo valioso de la Municipalidad.

Políticas de Seguridad de la Información

ISO 17799	Política MSS-PSI	Descripción
13.1.2	Política 1301-006-MSS	Propiedad intelectual de trabajos dentro de la Municipalidad Los derechos de propiedad intelectual de trabajos llevados a cabo dentro de un contrato con la Municipalidad se protegerán mediante acuerdos formales.
13.1.2.	Política 1301-007-MSS	Uso de software licenciado Todo software que se utilice en la Municipalidad debe estar amparado en una Licencia de Usuario, cuyos términos se deben respetar estrictamente con la finalidad de cumplir con las leyes y asegurar el soporte continuo por parte de los proveedores.
13.1.2	Política 1301-008-MSS	Uso de información protegida por derechos de autor (con copyright) de la Internet Para utilizar información obtenida de la Internet o de otras fuentes electrónicas, se debe obtener la autorización del propietario de los derechos de autor.
13.1.2	Política 1301-009-MSS	Envío electrónico de información protegida por derechos de autor (con copyright) Para retransmitir información por Internet u otras fuentes electrónicas, se deben obtener la autorización del propietario de los derechos de autor.
13.1.3	Protección de los registros de la Municipalidad	
13.1.3	Política 1301-010-MSS	Archivamiento de documentos Se deben aplicar controles técnicos y administrativos para garantizar el cumplimiento de las consideraciones legales y regulatorias en el archivamiento de los registros de la Municipalidad.
13.1.3	Política 1301-011-MSS	Conservación de información Los registros e información creados y almacenados por sistemas de información de la Municipalidad deben conservarse por el tiempo que sea necesario para cumplir con los requisitos legales, sectoriales y los propios de la actividad de la Municipalidad.
13.1.3	Política 1301-012-MSS	Conservación o borrado de correo electrónico Los mensajes de correo electrónico almacenados en sistemas de organización deben conservarse por el tiempo que sea necesario para cumplir con los requisitos legales, sectoriales y los propios de la actividad de la Municipalidad.
13.1.4	Protección de los datos y de la privacidad de la información personal	
13.1.4	Política 1301-013-MSS	Confidencialidad de información de vecinos y contribuyentes Se debe proteger la información de contacto de vecinos, contribuyentes y terceros de cualquier acceso no autorizado.

Políticas de Seguridad de la Información

ISO 17799	Política MSS-PSI	Descripción
13.1.4	Política 1301-014-MSS	Información confidencial de trabajadores Sólo personas expresamente autorizadas podrán tener acceso a información personal sobre los trabajadores de la Municipalidad, al ser dicha información estrictamente confidencial.
13.1.4	Política 1301-015-MSS	Gestión de datos de tarjetas de crédito de contribuyentes La información obtenida a partir del acceso a tarjetas de crédito de vecinos o contribuyentes debe procesarse de tal manera que dicha información esté protegida contra todas las formas conocidas de acceso no autorizado, para lo cual deben usarse controles técnicos y administrativos.
13.1.5	Prevención del mal uso de los recursos de tratamiento de la información	
13.1.5	Política 1301-016-MSS	Uso de fotocopiadoras con fines personales Las fotocopiadoras o duplicadoras no deben usarse para uso personal. De manera excepcional, el supervisor inmediato puede dar permiso específico al empleado para su uso.
13.1.5	Política 1301-017-MSS	Uso del correo para fines personales El uso personal del correo electrónico (email) debe reducirse al mínimo. El correo postal sólo se debe utilizar para propósitos de la Municipalidad.
13.1.5	Política 1301-018-MSS	Uso del teléfono para fines personales Las llamadas telefónicas personales a través de sistemas telefónicos, incluidos los móviles, de la Municipalidad deben ser reducidas al mínimo.
13.1.5	Política 1301-019-PCM	Juegos en computadores El uso de computadoras de la Municipalidad para juegos está estrictamente prohibido.
13.1.7	Recopilación de pruebas	
13.1.7	Política 1301-020-MSS	Recolección de pruebas de delitos informáticos La Municipalidad denunciará, con toda el peso de la ley, a autores de delitos informáticos. Se deben desarrollar procedimientos apropiados para asegurar la recolección y protección adecuada de evidencias.
13.1.7	Política 1301-021-MSS	Recopilación de evidencias de brechas de Seguridad de la Información Toda evidencia referente a brechas de seguridad de la información debe ser recopilada y remitida al Oficial de Seguridad de la Información.
13.2	Revisiones de la Política de Seguridad y de la conformidad técnica	
13.2.1	Conformidad con la política de seguridad	

Políticas de Seguridad de la Información

ISO 17799	Política MSS-PSI	Descripción
13.2.1	Política 1302-001-MSS	<p>Cumplimiento de las Políticas de Seguridad de la Información</p> <p>El cabal cumplimiento de las Políticas de Seguridad de la Información de la Municipalidad por parte de los trabajadores es obligatorio. La supervisión de tal cumplimiento es responsabilidad de la Alta Dirección.</p>
13.2.2	Comprobación de la conformidad técnica	
	Política 1302-002-MSS	<p>Examen y pruebas de conformidad</p> <p>Se debe comprobar regularmente la conformidad técnica de las medidas de seguridad mediante el examen de los sistemas y pruebas de intrusión a diversos sistemas, realizables por profesionales independientes especialistas en el tema.</p>
13.3	Consideraciones sobre la auditoria de sistemas	
13.3.1	Controles de auditoria de sistemas	
	Política 1302-003-MSS	<p>Planificación de las actividades de auditoría</p> <p>Para minimizar el riesgo de interrupción de los procesos de negocio, las actividades de auditoría se deberán planificar cuidadosamente, registrándose y supervisándose todos los accesos. Asimismo, todos los procedimientos, requisitos y responsabilidades deberán estar documentados.</p>

