Municipalidad de San Isidro

RESOLUCION DE ALCALDÍA N° 266

San Isidro, 05 NOV. 2010

EL ALCALDE DE SAN ISIDRO

Visto: el proyecto de "Política de Seguridad de la Información" de la Municipalidad de San Isidro; y,

CONSIDERANDO:

Que, mediante Resolución Ministerial N° 246-2007-PCM de fecha 22 de agosto de 2007, se aprobó el uso obligatorio de la Norma Técnica Peruana "NTP-ISO/IEC 17799:2007 EDI. Tecnología de la Información. Código de buenas prácticas para la gestión de la seguridad de la información. 2da. Edición" en todas las Entidades integrantes del Sistema Nacional de Informática;

Que, la referida Norma Técnica indica en su numeral 5.1 que la Política de Seguridad de la Información tiene como objetivo dirigir y dar soporte a la gestión de la seguridad de la información en concordancia con los requerimientos de la institución, las leyes y las regulaciones; en la que la Alta Dirección debería establecer en forma clara las líneas de la política de actuación y manifestar su apoyo y compromiso a la seguridad de la información, publicando y manteniendo una política de seguridad en toda la organización;

Que, la implementación de la mencionada norma requiere aprobar un documento de Política de Seguridad de la Información en la Municipalidad de San Isidro;

Que, de acuerdo al numeral 35) del artículo 17° del Reglamento de Organización y Funciones de la Municipalidad de San Isidro, aprobado con la Ordenanza N° 287-MSI, corresponde al Alcalde dentro de sus funciones aprobar los documentos técnicos de gestión institucional: Clasificador de Cargos, Manual de Organización y Funciones, Presupuesto Analítico de Personal, Cuadro Nominativo de Personal y otros;

Con las visaciones del Gerente Municipal, Gerente de Asesoría Jurídica y Gerente de Planeamiento, Presupuesto y Desarrollo Corporativo;

RESUELVE:

Artículo 1°.- Aprobar la **"Política de Seguridad de la Información"** de la Municipalidad de San Isidro, cuyo texto en Anexo forma parte integrante de la presente Resolución.

Artículo 2°.- Disponer que lo establecido en la **"Política de Seguridad de la Información"**, aprobada en el artículo precedente, es de cumplimiento obligatorio por los funcionarios y servidores de la Municipalidad de San Isidro.

Artículo 3°.- Disponer que la Gerencia de Tecnologías de Información y Comunicación publique la presente Resolución y su Anexo en la página web de la Municipalidad de San Isidro (www.msi.gob.pe), difundiendo su publicación a todas las unidades orgánicas.

Municipalidad
de
San Isidro

RESOLUCION DE ALCALDÍA N°

Artículo 4°.- Dejar sin efecto toda disposición que se oponga a lo dispuesto en la presente Resolución.

Regístrese, comuníquese y publíquese.

MUNICIPALIDAD DE SAN ISIDRO - ALCALDE -

E. ANTONIO MEIER CRESCI
ALCALDE

MUNICIPALIDAD DE SAN ISIDRO - ESTUDIOS Y PLANEAMIENTO -

MUNICIPALIDAD DE SAN ISIDRO - GERENTE MUNICIPAL -

Municipalidad de San Isidro

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

1. Definición.

La Política de Seguridad de la Información está formada por el conjunto de principios o lineamientos que la Municipalidad de San Isidro debe seguir para asegurar la confiabilidad de sus sistemas informáticos.

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.
- 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.

La Seguridad de la Información se caracteriza por la preservación de:

a) **Su confidencialidad,** asegurado que solo quienes estén autorizados pueden acceder a la información;

b) **Su integridad,** asegurando que la información y sus métodos de proceso sean exactos y completos;

c) **Su disponibilidad**, asegurando que los usuarios autorizados tengan acceso a la información y a sus activos asociados cuando lo requieran.

2. Responsabilidad.

Todo el personal de la Municipalidad de San Isidro es responsable de conocer y cumplir la Política de Seguridad de la Información, las normas relacionadas con ésta, los procedimientos y los estándares generales, y aquellos específicamente relacionados con su Gerencia, Subgerencia o área de competencia.

Dentro de este contexto, podemos diferenciar los siguientes niveles de responsabilidad:

- **Empleados.**

  Todos los Empleados del Municipalidad de San Isidro deberán garantizar activamente la protección de la información. Esto implica:

  - ✓ La utilización de la información y de los sistemas de información, sólo para fines laborales.
  - ✓ El cuidadoso manejo de dicha información y de los sistemas informáticos, poniendo especial énfasis si se trata de información pública, privada o confidencial, asegurando la no divulgación de estas últimas.
  - ✓ La observación de las reglamentaciones y el fiel cumplimiento de los procedimientos y estándares en cuanto a la seguridad en materia de información.
  - ✓ El informe de las deficiencias e incidentes en materia de seguridad de la información o administración de activos a sus superiores inmediatos.
  - ✓ Participar en las pruebas e implementación de los Planes de Contingencia ante eventuales caídas de los sistemas de información.

- **Funcionarios.**

  Los Funcionarios de la Municipalidad de San Isidro deberán garantizar e implementar la seguridad de la información y los sistemas de información dentro de su Gerencia, Subgerencia o área de responsabilidad. Ellos deberán:

  - ✓ Supervisar periódicamente su ámbito de acción a fin de detectar posibles deficiencias en materia de seguridad de la información.
  - ✓ Iniciar rápidamente medidas correctivas e informar al Comité de Seguridad de Información de las deficiencias y demás incidentes de carácter relevante.
  - ✓ Informar regularmente a los empleados de la Municipalidad de San Isidro acerca de los objetivos, medidas y reglamentaciones en materia de seguridad informática que se encuentren en vigencia.
  - ✓ Asegurar los niveles de confidencialidad de la información bajo su ámbito, verificando que las reglamentaciones operativas sean debidamente cumplidas.
  - ✓ Definir las autorizaciones para obtener el acceso a la información y a los sistemas de información del personal de su dependencia.
  - ✓ Participar activamente en el establecimiento de políticas y directivas de seguridad, proponiendo al Comité de Seguridad de Información aquellas recomendaciones que considere importante implementar.
  - ✓ Designar a los líderes usuarios que participen activamente en la definición, creación, pruebas e implementación de los sistemas de información.
  - ✓ Coordinar la activación de los Planes de Contingencia ante eventuales caídas de los sistemas de información, asegurando la continuidad de los servicios y actividades de la Municipalidad de San Isidro.

3. Alcance.

La presente Política tiene alcance en todo a la Municipalidad de San Isidro, e involucrara a todos los funcionarios, empleados y terceros que tengan acceso o que estén desarrollando, adquiriendo o usando sistemas de información y/o datos del mismo.

Este documento y las siguientes disposiciones en materia de seguridad de la información se aplicarán en toda clase de cooperación de terceras partes, al igual que en el supuesto de información creada externamente bajo contrato, o de información propia de la Municipalidad de San Isidro que haya sido revelada a terceras personas como parte constituyente de un contrato.

Asimismo, se aplica a toda la información producida, manejada, transmitida y almacenada en la Municipalidad de San Isidro; y a todos los sistemas y datos asociados con el almacenamiento, procesamiento y transmisión de la información por y a favor de la Municipalidad de San Isidro.

4. Política de Seguridad de la Información.

Para dirigir y dar soporte a la gestión de la seguridad de la información, la Gerencia de Tecnologías de Información y Comunicación de la Municipalidad de San Isidro ha propuesto la Política de Seguridad de la Información que rige en la institución, la cual establece:

4.1 La información es un activo institucional

La MSI reconoce que la información que genera es un activo que, como otros activos importantes, tiene especial valor y requiere en consecuencia una protección adecuada.

La información en sus diversas formas, puede estar impresa o escrita en papel, almacenada en medios electrónicos, transmitida por correo, grabada en video, en medio sonoro o cualquier otro medio de almacenamiento. Por esto, se debe proteger adecuadamente sin importar la forma que tome, o los medios por los que se comparta o almacene.

4.2 La información requiere clasificación

En base al dominio de "Clasificación y Control de Activos" de la NTP-ISO/IEC 17799:2004, la información y los activos de tratamiento de la información necesitan ser clasificados de acuerdo a los niveles de protección requeridos en base a su sensibilidad e importancia, y protegidos contra acceso no autorizado.

La confidencialidad e integridad de la información es asegurada y su disponibilidad establecida mediante acuerdos de nivel de servicio.

4.3 La información requiere de seguridad

Se establecen, prueban y mantienen los requerimientos de Seguridad ligados al Personal, Seguridad Fisica y Lógica del entorno, los Planes de Contingencia y los Planes de Continuidad de las labores Institucionales.

4.4 La información de la Gerencia de Tecnologías de Información y Comunicación, está sujeta a usos, procesos y procedimientos estandarizados

La MSI a través de la Gerencia de Tecnologías de Información y Comunicación elabora y aprueba estándares, prácticas, procedimientos y normas internas para sostener la Política de Seguridad de la Información. Éstas medidas incluirán como mínimo la protección contra virus informáticos y otros software maliciosos, la gestión de contraseñas, el correcto uso de los recursos informáticos, la administración eficiente del software, los procedimientos de respaldo y recuperación de la información, los acuerdos de confidencialidad, los acuerdos de intercambio de información y los planes de capacitación en seguridad de la información para todo el personal de la institución y terceros que utilicen la información de la misma.

4.5 Compromiso en el desarrollo y mantenimiento de Sistemas de Información

El desarrollo y mantenimiento de los sistemas son ejecutados usando una metodologia que incluye requerimientos de seguridad en su ciclo de vida.

4.6 Responsabilidad compartida en la Seguridad de la Información

Los roles son compartidos en la seguridad de la información y son definidos según el siguiente orden de responsabilidad:

a. El Comité de Seguridad de Información.

b. Los responsables de seguridad de la información.

c. Los responsables de la información.

d. Los responsables de los procesos.

4.7 Respeto por la Seguridad de los Sistemas de Información

Todas las brechas de seguridad de los sistemas de información, reales o bajo sospecha, son reportadas mediante los procedimientos establecidos, investigados y resueltos por la instancia pertinente.

Las violaciones a la Política de Seguridad de la Información son revisadas. En caso de ser probada la falta, esta deriva en sanciones o penalidades de conformidad con la normatividad vigente.

4.8 Cumplimiento y manejo de violaciones a la Política

El cumplimiento de la política junto con el modelo de seguridad de la información que la despliega, es de ejecución obligatoria. Cada usuario debe entender su rol y asumir su responsabilidad respecto a los riesgos en el uso de la información y la protección de los recursos de información. No existen excepciones al cumplimiento de la política de seguridad de la información, por lo tanto cualquier inobservancia que comprometa la integridad, confidencialidad o disponibilidad de la información, resultará en una acción de acuerdo a las normas vigentes.

4.9 De la protección de la información

La información de la Municipalidad y de los clientes es un activo vital de la MSI, por lo tanto su protección debe ser permanente.

Los propietarios y custodios en coordinación con los responsables de la gestión de informática, deben asegurar que los activos de información que se encuentran bajo su responsabilidad cuenten con la protección apropiada que permita preservar su integridad, confiabilidad y disponibilidad. La organización debe proveer los medios necesarios para que los usuarios preserven y protejan los activos de información de una manera consistente y confiable.

4.10 De la protección de la propiedad intelectual

La propiedad intelectual sobre patentes, derechos de autor, licencias de uso debe prevalecer al interior de la Municipalidad; por lo tanto todo software debe ser autorizado, por la Gerencia de Tecnologías de Información y Comunicación.

Todo activo de información que es desarrollado en la MSI, ya sea por un trabajador o un tercero, se considera como propiedad intelectual de la entidad y es de su uso exclusivo; por lo tanto debe ser marcado como propiedad de la MSI para protegerlo contra un uso que menoscabe la imagen y competitividad de la MSI.

Cualquier software instalado en los sistemas de cómputo debe tener una aprobación previa de la MSI y estar dentro de los estándares aceptados previamente por la Gerencia de Tecnologías de Información y Comunicación para que pueda ser utilizado.

El software licenciado no debe ser copiado o duplicado, excepto si los términos o condiciones de la licencia explícitamente lo permiten. Ningún programa proveniente de fuentes externas, incluyendo Internet, licenciado o no, debe ser personalmente traído e instalado.

4.11 Del cumplimiento de responsabilidades en seguridad de información

La MSI debe proveer los mecanismos necesarios que le permitan a los usuarios y clientes cumplir con sus responsabilidades en seguridad de la información, desde su vinculo inicial hasta que cesen sus compromisos con la organización.

Los nuevos trabajadores que ingresen a la MSI, los que cambien de posición o requieran una re inducción; deben pasar por un proceso que permita mitigar los riesgos futuros en el uso de la información de la MSI. El grado de investigación dependerá del nivel de sensibilidad que tiene la posición del trabajador dentro de la MSI y el contacto que éstos tendrán con la información. Los criterios para definir el nivel de investigación deben ser propuestos por la Gerencia de Tecnologías de Información y Comunicación en coordinación con la Gerencia de Recursos Humanos.

Los contratos con clientes, trabajadores o terceros, deben incluir cláusulas que especifiquen las responsabilidades que éstos deben tener con el manejo de la información de la MSI y las consecuencias que se generan por su mal uso.

4.12 De los Usuarios que acceden a recursos de información de la MSI local o remotamente

Los usuarios que utilizan local o remotamente recursos de información de la MSI deben cumplir con la política de seguridad de la información.

Los usuarios que hacen uso de los recursos de información de la MSI deben formalizar esta acción mediante acuerdos que hagan obligatorio el cumplimiento de la presente política. Estos acuerdos deben incluir cláusulas de confidencialidad y buen uso de la información.

Cuando se delegue a terceros servicios de la MSI, se deben incluir además, acuerdos de niveles de servicios de seguridad de la información donde se consideren las sanciones que conlleva el incumplimiento de la presente política.

Toda relación con un tercero debe contar con la participación del propietario de la información o un representante que éste designe, a fin de velar por el correcto uso y la protección de los recursos de información, siendo el responsable por la actividad de dichos trabajadores (tercero) durante la vigencia del contrato.

4.13 De la identificación y autenticación individual

Todo usuario que accede a información de la MSI que no es pública debe disponer de un medio de identificación, y su acceso debe ser controlado a través de una autenticación personal.

La identidad debe ser establecida y autenticada de manera única, no pudiendo ser compartirla bajo ninguna circunstancia. El usuario es responsable de las acciones que se realicen en los recursos de información y sobre la información declarada no publica de la MSI una vez autenticado.

Dependiendo del valor y de la privacidad de la información, al igual que el nivel de riesgo, La MSI definirá medios de identificación y autenticación apropiados que no podrán ser compartidos y deberán estar habilitados solamente para las jornadas de trabajo y recursos de información acordados con los clientes y los establecidos por La MSI. Dichos medios de autenticación contienen información que no debe ser revelada o almacenada en lugares que puedan ser accedidos de manera no autorizada.

Las funciones de la MSI se apoyan en los medios electrónicos; por lo tanto para cualquier negocio o transacción .que se haga por estos medios, La MSI debe asegurar la autenticidad de cada parte que interviene y evitar que alguna de ellas niegue su participación (no repudio).

4.14 Del control y administración del acceso a la información

El uso de la información de la MSI debe ser dado, mantenido y controlado con base en una necesidad de la entidad demostrada y no deben comprometer la segregación de tareas y responsabilidades. El acceso a los recursos de información de la MSI debe ser restringido en todos los casos sin excepción.

Se deben establecer mecanismos de control de acceso físico y lógico para asegurar que la información de la MSI se mantenga protegida de una manera consistente con su valor para la entidad y con los riesgos de pérdida de integridad, confidencialidad y disponibilidad.

4.15 De la protección a la privacidad de la información.

La información será utilizada únicamente para los fines que fue obtenida. La MSI maneja información externa proveniente de sus trabajadores, usuarios o terceros; su mal uso expone a la MSI a demandas de violación a la privacidad, así como a pérdida de imagen. Por lo tanto, su uso solo debe corresponder al objeto por el cual fue requerida y por las personas que están autorizadas para tal fin.

La información de usuarios debe tener un custodio al interior de la MSI responsable de resguardarla y su uso debe estar claramente establecido en acuerdos que deben ser desplegados, cumplidos y verificados en La MSI. El custodio de la información es responsable de verificar el cumplimiento de los acuerdos y uso de la información de los usuarios.

La política de uso de cada servicio que presta La MSI debe incluir las responsabilidades de los usuarios de respetar la integridad, confidencialidad y disponibilidad de la información de la MSI.

4.16 De la seguridad física

Todas las áreas físicas de la MSI deben tener un nivel de seguridad acorde con el valor y la sensibilidad, de la información que se procesa y administra en ellas. Los controles para la seguridad física son consistentes con el valor y sensibilidad de la información que contienen y los derechos mínimos de acceso deben ser otorgados teniendo en cuenta si los sitios de trabajo son permanentes o no.

Los recursos de información de la MSI y los equipos de procesamiento donde residan, deben estar físicamente protegidos contra amenazas de acceso no autorizado y amenazas ambientales para prevenir exposición, daño o pérdida intencional o no intencional e interrupción de las actividades de negocio.

La información confidencial y reservada será asegurada bajo llave cuando se deje desatendida y no se dejará desplegada en las estaciones de trabajo. Asimismo, se debe habilitar protectores de pantalla autorizados con palabras clave en cada estación de trabajo.

Cuando termina el vínculo laboral de un trabajador en la MSI, todos los elementos y facilidades de acceso a ambientes físicos deben ser reasumidos por La MSI.

4.17 Del uso de la información en redes de comunicación no confiables

La información debe preservar los controles establecidos por La MSI cuando pasa a través de redes de comunicación no confiables con el fin de mantener su integridad, confidencialidad y disponibilidad. El flujo de información debe realizarse desde los puntos autorizados por La MSI y los controles establecidos deben corresponder a un manejo de riesgo en relación a la criticidad de la información.

Los usuarios que se conecten a la red privada de la MSI desde redes no confiables, deben cumplir con la presente política antes que se realice la conexión. Esto aplica igualmente a cualquier conexión actual o futura en la red de la MSI que utilice medios públicos para integrar lugares que estén geográficamente dispersos. Es necesaria la aprobación del propietario de la información para acceder remotamente a la información de la MSI, y dichos accesos deben cumplir con las políticas de identificación y autenticación individual, así como también las de control y administración del acceso a la información.

4.18 Del uso de los recursos de información

Los recursos de información son provistos a los usuarios para uso exclusivo de los propósitos de la MSI y deben ser tratados como activos dedicados que proveen las herramientas para realizar el trabajo requerido.

Se debe conservar la privacidad de la información de los usuarios, así como crear registros sobre el uso de los recursos de información que puedan ser revisados con el objetivo de detectar abusos y amenazas.

La MSI se reserva el derecho de restringir el acceso a cualquier información en el momento que lo considere conveniente, por lo que solo personal autorizado podrá utilizar elementos y tecnologías de uso restringido como la de monitoreo de red y datos operacionales. Ningún

hardware o software no autorizado debe ser cargado, instalado o activado en los recursos de información de la MSI sin previa autorización de la Gerencia de Tecnologías de Información y Comunicación.

4.19 Del proceso de administración de la plataforma informática de la información

Todos los procesos en la administración de la plataforma informática de la MSI deben estar alineados a la política de seguridad de la información.

La Gerencia de Tecnologías de Información y Comunicación mantendrá una metodología que controle el ciclo completo de desarrollo y mantenimiento de sistemas.

Los requerimientos de seguridad de la información deben ser identificados antes del diseño de los sistemas de información y durante su desarrollo deben ser incluidos. Si una modificación es requerida debe cumplir estrictamente con los requerimientos previamente establecidos. El nivel de seguridad de la información de un sistema no puede verse reducido, por lo que la información y los sistemas en producción no serán utilizados para desarrollo, prueba o mantenimiento de aplicaciones.

Todos los problemas de seguridad de la información relacionados a la plataforma informática de la MSI, deben ser administrados mediante el registro, asignación, seguimiento y resolución de situaciones que comprometen la presente política y la disponibilidad de servicios que provee esta plataforma.

5. Revisión y Actualización.

Anualmente o cuando la magnitud de los cambios lo justifiquen, la Gerencia de Tecnologías de la Información y Comunicación propondrá una nueva versión como parte del proceso de mejora continua a fin de asegurar su uso continuo, adecuación y efectividad.

6. Publicación y Distribución.

La Política de Seguridad de la Información debe ser comunicada a todos los usuarios de la Municipalidad de San Isidro, siendo de conocimiento y aplicación obligatorio para todo el personal de la entidad.

La Gerencia de Tecnologías de Información y Comunicación deberá publicar y distribuir de forma adecuada la presente Política hacia todos los niveles de la organización.

7. Capacitación.

La Gerencia de Tecnologías de Información y Comunicación deberá buscar de forma adecuada la formación y sensibilización del personal, contratistas y terceros involucrados, respecto a la seguridad de la información para garantizar el cumplimiento de las normativas legales aplicables.

8. Incumplimiento y Violaciones a la Política.

Las violaciones a la Política de Seguridad de la Información y a cualquier procedimiento derivado de ésta, que ocasionen cualquier riesgo o pérdida para la organización, será sancionado conforme a la normativa que corresponda.

La Gerencia de Tecnologías de Información y Comunicación informará a la Alta Dirección de las consecuencias derivadas por el incumplimiento y violación de las políticas establecidas.