DG DOCUMENTO GENERAL	SEGURIDAD EM COMPUTADORAS PERSONALES Y PORTÁTILES

PRESENTACIÓN

Este documento establece normas para el uso de los recursos de computación personal y portátil en el ambiente de Sukyo Mahikari del Perú.

DSI DEPARTAMENTO DE SEGURIDAD DE LA INFORMACIÓN	Los comentarios de opiniones referentes a este documento deben ser dirigidos al administrador de este documento indicando el artículo a ser revisado, la propuesta y la justificación. Este documento normativo tiene la validad de un año a partir de su edición, plazo máximo para la realización de la próxima revisión.

ADMINISTRADOR: DSI	APROBADOR
Hugo Okamoto	Hidekazu Sakamoto

CONTROL DE REVISIONES

REV.	DESCRIPCIÓN DEL CAMBIO	FECHA
0	Emisión original – sin revisiones	05/06/09
1	Traducción al español (Perú) de la emisión original.	05/02/16

RESUMEN

1. OBJETIVO **4**

2. APLICACIÓN **4**

3. ATRIBUCIONES Y RESPONSABILIDADES **4**

4. DOCUMENTOS DE REFERENCIA **4**

5. TERMINOLOGÍA **4**

6. CONCEPTO **5**

7. CONTROL DE ACCESO A LA ESTACIÓN DE TRABAJO **5**

7.1. PROTECCIÓN DE PANTALLA CON CONTRASEÑA 5

8. SEGURIDAD DE LA ESTACIÓN DE TRABAJO **6**

8.1. USO SEGURO DEL EQUIPO 6

8.2. SEGURIDAD FÍSICA 7

8.3. SEGURIDAD CONTRA MALWARE 7

1. OBJETIVO

Este documento establece normas para el uso de los recursos de computación personal y portátil en el ambiente de Sukyo Mahikari del Perú. Recomienda controles de protección al activo físico, uso adecuado, responsabilidad del usuario y prevención de daños. Este trabajo fue desarrollado para auxiliar en el planeamiento y la implementación de mecanismos que garantizan integridad y disponibilidad de las estaciones de trabajo.

2. APLICACIÓN

Esta Política de Seguridad de la Información se destina a todos los funcionarios, colaboradores, voluntarios y usuarios de informaciones de Sukyo Mahikari del Perú, sirviendo de base para la definición de normas específicas, procedimientos, responsabilidades y conceptos.

3. ATRIBUCIONES Y RESPONSABILIDADES

- Cabe al DSI, la administración de este documento que incluye su desarrollo, implementación y mantenimiento.
- Cabe al DSI mantener este documento actualizado y promover las revisiones necesarias.
- Cabe a la Dirección la aprobación de este documento.
- Cabe a todos los funcionarios, colaboradores y voluntarios leer y seguir las directrices.

4. DOCUMENTOS DE REFERENCIA

El presente documento fue desarrollado con base al siguiente documento externo:

- NBR ISO/IEC 27002, artículos 10.4.1, 10.4.2

5. TERMINOLOGÍA

Malware: El término malware es proveniente del inglés malicious software; es un software destinado a infiltrarse en un sistema de computadora ajeno de forma ilícita, con el fin de causar algún daño o robo de informaciones (confidenciales o no). Virus de computadora, worms, trojan horses (caballos de troya) y spywares son considerados malware.

6. CONCEPTO

Este documento se refiere los siguientes términos:

a) **Computadoras Personales**
Son las estaciones de trabajo, de propiedad de Sukyo Mahikari del Perú, disponibles para las actividades de la organización.

b) **Computadores Portátiles**
Son las estaciones de trabajo portátiles, de propiedad de Sukyo Mahikari del Perú o de voluntarios, usadas para las actividades profesionales de la Institución. Se enmarcan en esa categoría:

- Notebook;
- Asistentes digitales personales (PDA): palmtop, iPaq, pocket PC, aparatos de teléfono celular, smartphones, etc;
- Medios de lectura y/o de grabación, como disquetes, CDs, DVDs, memoria flash, discos externos, etc.

c) **Acceso a los Recursos**
Se trata de la conexión física o lógica de cualquier equipo a las redes de Sukyo Mahikari del Perú, efectuada local o lejanamente.

d) **Usuario (persona física)**
Persona, funcionario o no, al cual es dada, explícitamente, la autorización para el uso de un recurso computacional a fin de ejecutar las actividades relacionadas exclusivamente a las actividades de Sukyo Mahikari del Perú.

7. CONTROL DE ACCESO A LA ESTACIÓN DE TRABAJO

Para el acceso a las estaciones de trabajo y a las computadoras portátiles, es necesaria la identificación del usuario antes de tener su acceso liberado. Su objetivo es restringir el acceso no autorizado a la información y a los sistemas delicados por medio del uso de controles de seguridad en lo que se refiere al sistema operacional.

7.1. Protección de pantalla con contraseña

Todas las estaciones de trabajo deben estar configuradas para activar la protección de pantalla con contraseña. Esa protección debe ser activada después de cierto tempo de inactividad de la estación de trabajo.

8. SEGURIDAD DE LA ESTACIÓN DE TRABAJO

8.1. Uso seguro del equipo

La integridad y la confidencialidad de las informaciones almacenadas en estaciones de trabajo son de responsabilidad del usuario. Las normas descritas a seguir se destinan a todas las estaciones de trabajo que utilizan los recursos de la red interna de Sukyo Mahikari del Perú.

- Su uso se restringe exclusivamente a los asuntos de las actividades de Sukyo Mahikari del Perú.
- Se debe aplicar la configuración de la protección de pantalla en todas las estaciones de trabajo, con activación después de cierto tempo de inactividad de la estación de trabajo.
- Siempre que el funcionario se ausenta del ambiente de trabajo, el acceso a su computadora debe ser bloqueado, o el equipo deberá ser desconectado para evitar que sean usados sus recursos de forma ilícita.
- No debe ser grabada información confidencial o relacionada al trabajo en el drive local de la máquina. Ese drive no está contemplado dentro del proceso de backup diario y los datos allí grabados quedan disponibles a cualquiera que tenga acceso físico a la estación de trabajo.
- La información delicada debe siempre ser salvada en los servidores de archivo de la red interna.
- Las salas deben ser cerradas al término de la jornada y durante los fines de semana.
- Se deben usar softwares de antivirus y protección contra malwares en todas las computadoras personales y en los servidores de Sukyo Mahikari del Perú. Su versión se debe siempre mantener actualizada.
- El acceso a una computadora portátil en el ambiente computacional de Sukyo Mahikari del Perú sólo podrá ser concedido mediante la solicitud de un dirigente responsable.
- Antes de permitir el acceso al ambiente computacional de Sukyo Mahikari del Perú, las computadoras portátiles que sean propiedad de los voluntarios deben:
    - Utilizar la red Wi-Fi de Sukyo Mahikari del Perú que es aislada y destinada para ese fin o;
    - Pasar por una evaluación de seguridad teniendo como mínimo:

- Verificación de las actualizaciones de seguridad del sistema operacional,
- Protección (antivirus) contra malware instalado y actualizado,
- Realizar una exploración (scanner) en la computadora portátil.

- Los Notebooks deberán siempre ser guardados en lugares seguros.
- Solamente deben ser instalados en las computadoras personales los softwares proporcionados por el área de tecnología de la información de Sukyo Mahikari del Perú, y que tenga su uso autorizado. Aquí se incluyen también los programas y los patrones aplicativos de la Institución.
- No debe ser copiado o instalado ningún software sin el consentimiento del Área de Informática.

8.2. Seguridad Física

Los equipos deben ser instalados y protegidos contra amenazas ambientales, peligros y oportunidades de accesos no autorizados.

Los equipos deben ser protegidos contra fallas de energía y otras anomalías en la alimentación eléctrica. El abasto de energía eléctrica debe estar en conformidad con las especificaciones del equipo.

Los cables eléctricos, de telecomunicaciones y de datos deben ser protegidos contra intercepción o daño.

El uso de cualquier equipo para el proceso de la información localizado afuera de los límites físicos de la organización debe siempre ser autorizado por la administración. La seguridad a ser implementada debe ser igual a la de los equipos similares instalados dentro de la organización, teniendo en consideración los riesgos del ambiente en el cual está inserido.

8.3. Seguridad contra malware

Todos los sistemas computacionales de la red interna deben estar equipados de softwares de verificación contra malware y deben estar regularmente actualizados.

Para garantizar la integridad y protección de la información, deben tomarse en cuenta las siguientes normas:

- Todas las estaciones de trabajo deben tener un software de antivirus (protección contra malware) homologado y actualizado por la Institución;
- Está prohibida la instalación de cualquier software sin la debida autorización;

- En caso que sea detectado algún malware o se sospeche de la existencia de alguno, el usuario debe ser instruido para contactar al Área de Seguridad de la Información. Bajo ninguna circunstancia deberá intentar eliminar el malware por cuenta propia.