

DG
DOCUMENTO
GENERAL

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

PRESENTACIÓN

Este documento describe las directrices de los objetivos de la Política de Seguridad de la Información, así como los conceptos de sus definiciones.

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 validez de un año a partir de su edición, plazo máximo para la realización de la próxima revisión.

ADMINISTRADOR: DSI

Hugo Okamoto

APROBADOR

Hidekazu Sakamoto

LA IMPRESIÓN O REPRODUCCIÓN DE ESTE DOCUMENTO SE VUELVE UNA COPIA NO CONTROLADA

CONTROL DE REVISIONES

RESUMEN

1. OBJETIVO	4
2. APLICACIÓN	4
3. ATRIBUCIONES Y RESPONSABILIDADES	4
4. DOCUMENTOS DE REFERENCIA	4
5. TERMINOLOGÍA	4
6. CONCEPTO	5
7. OBJETIVO	5
8. DIRECTRICES	6
8.1. SEGURIDAD	6
8.2. PRIVACIDAD	6

1. OBJETIVO

Define la Política de Seguridad de la Información de Sukyo Mahikari del Perú, presenta las directrices de los objetivos de la Política de Seguridad de la Información, así como sus conceptos y sus definiciones.

2. APLICACIÓN

Esta Política de Seguridad de la Información se dirige a todos los 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 a leer y seguir las directrices.

4. DOCUMENTOS DE REFERENCIA

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

- NBR ISO/IEC 27002, artículo 5.1.1

5. TERMINOLOGÍA

Activo: Cualquier cosa que tenga valor para organización.

Confidencialidad: Propiedad de que la información no esté disponible o revelada a individuos, entidades o procesos no autorizados.

Disponibilidad: Propiedad de estar accesible e utilizable bajo demanda de una entidad autorizada.

Integridad: Propiedad de salvaguarda de la exactitud y totalidad de los activos.

6. CONCEPTO

La información es uno de los activos más importantes para cualquier organización. Con el objetivo de evitar perjuicios de imagen, asegurar la continuidad de las actividades, viabilizar nuevas oportunidades y minimizar pérdidas; la Seguridad de la Información protege la información contra pérdida de confidencialidad, integridad y disponibilidad.

La Seguridad de la Información es el conjunto de normas, procedimientos, controles, prácticas y estructuras organizacionales que tienen como objetivo proteger y preservar este importante activo de Sukyo Mahikari del Perú, denominado "Información".

La Seguridad de la Información protege la información almacenada electrónicamente, transmitida verbalmente, escrita en papel, transmitida por cualquier medio (electrónico o mecánico), disponible en programas de computador, sistemas aplicativos y medios audiovisuales.

7. OBJETIVO

Los objetivos de esta Política de Seguridad de la Información son:

1. Documentar la visión estratégica de la seguridad de la información;
2. Busca la conformidad con a NBR ISO/IEC 27001 y ISO/IEC 27002;
3. Estructurar el Departamento de la Seguridad de la Información y áreas de apoyo;
4. Asegurar el manejo, almacenamiento, transporte y eliminación adecuado de la información.
5. Asegurar la continuidad de las actividades;
6. Asegurar la conformidad con la legislación;
7. Definir las normas y procedimientos de seguridad para orientar la conducta adecuada en la clasificación, control y protección de la información, con el fin de minimizar los riesgos y disminuir el grado de exposición de Sukyo Mahikari del Perú sin comprometer el buen funcionamiento de las actividades;
8. Ampliar la conciencia sobre seguridad y privacidad de la información;
9. Definir responsabilidades.

8. DIRECTRICES

La información es considerada un valioso patrimonio de Sukyo Mahikari del Perú y debe ser utilizada en conformidad con esta Política de Seguridad de la Información delante de sus miembros, proveedores, socios y visitantes. Debe ser utilizada sólo para atender los intereses inherentes a las actividades de Sukyo Mahikari del Perú.

La Seguridad de la Información comprende los aspectos de confidencialidad, integridad y disponibilidad. Esos tres aspectos pueden ser esenciales para el desarrollo de las actividades, el flujo de fondos, la rentabilidad, el cuidado con la legislación y la imagen de Sukyo Mahikari del Perú. Por lo tanto, se necesita analizar los costos y los beneficios que surgen de su implementación, asumiendo formalmente los riesgos de no adoptar las protecciones necesarias.

En esa perspectiva, es fundamental caracterizar los conceptos de Seguridad y de Privacidad.

8.1. Seguridad

Es la cualidad de aquello en que se puede confiar. Es el resultado del empleo de tecnologías, procedimientos y acciones que confirmen la certeza de que determinado bien no está bajo amenaza. Considerándolo todo, no basta adquirir equipos y productos actualizados y disciplinar el manejo de las informaciones a través de normas e instrucciones normativas, sin concientizar a los colaboradores relacionados en los procesos. Existe, por lo tanto, la cuestión humana, sus valores y su ética.

8.2. Privacidad

Es agregar seguridad y ética con la finalidad de proteger y garantizar la confidencialidad de las informaciones de Sukyo Mahikari del Perú, de sus colaboradores, socios, voluntarios, donadores y visitantes.

De esa forma, se pueden definir las directrices de seguridad de Sukyo Mahikari del Perú siendo estas como:

1. La Sensibilización sobre la importancia de la ética y de la confidencialidad en el trato de información de voluntarios, socios, proveedores, colaboradores y de carácter confidencial y restringido, de Sukyo Mahikari del Perú;
2. Capacitación técnica y concientización constante de las personas en el trato de la información;
3. Mejora continua de los procesos y procedimientos;
4. Inversión continua en tecnología.