DG DOCUMENTO GENERAL	CLASIFICACIÓN DE LA INFORMACIÓN Y

PRESENTACIÓN

Este documento describe las directrices para clasificación de la información y las responsabilidades dentro de la Política de Seguridad 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

Clasifica los tipos de informaciones y define responsabilidades dentro de la Política de Seguridad de la Información de Sukyo Mahikari del Perú.

2. APLICACIÓN

Esta Política de Seguridad de la Información se dirige a todos los contratados, 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 7.2

5. TERMINOLOGÍA

Activo: Cualquier cosa que tenga valor para la organización.

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

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

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

6. DEFINICIONES

Toda información es patrimonio de Sukyo Mahikari del Perú y está asociada a un único Órgano, que puede ser un área ejecutiva, un departamento, una gerencia, etc.

Ese Órgano es el responsable directo de la creación y clasificación de esas informaciones.

El ejecutivo de más alto nivel de ese Órgano es denominado "Propietario de la Información".

De esa forma, toda información debe poseer un único "Propietario de la Información".

Los relacionados con la administración y el manejo de las informaciones están dentro de las siguientes categorías:

6.1. Propietario de la Información

Ejecutivo del Órgano encargado de la creación, clasificación, eliminación y destrucción de la información. Es responsable también de la designación de los "Administradores de la Información".

6.2. Administrador de la Información

Colaborador (o grupo de Colaboradores) designado por el "Propietario de la Información" para realizar la administración de la información, siendo responsable de la validación, liberación y cancelación de los accesos a la información. Puede asumir funciones del "Propietario de la Información", a partir de que sea autorizado por él.

6.3. Custodio de la Información

Colaborador u Órgano responsable de la guardia y por el almacenamiento de la información, basado en los criterios y controles definidos por el "Administrador de la Información". El "Custodio de la Información" debe ser definido por el "Administrador de la Información". En el caso de que la información corporativa sea almacenada y procesada en el ambiente computacional de Sukyo Mahikari del Perú, el "Custodio de la Información" es el Departamento de Tecnología de la Información.

6.4. Usuario de la Información

Cualquier persona autorizada por el "Propietario de la Información" o por el "Administrador de la Información" para accesar, leer, responder, introducir, alterar o eliminar determinada información.

7. CLASIFICACIÓN DE LA INFORMACIÓN

La información es clasificada de acuerdo con su confidencialidad y su uso.

7.1. Confidencialidad

Está asociada al potencial de exposición y a los perjuicios que su divulgación no autorizada o accidental pueda causar a la continuidad de las actividades de Sukyo Mahikari del Perú, así como a sus colaboradores, socios, visitantes y simpatizantes.

7.2. Uso

Está directamente relacionada al público al cual la información se destina. Compete al "Propietario de la Información" o al "Administrador de la Información" definir o nivel de clasificación de la información bajo su responsabilidad.

Toda información que no posea una clasificación explícita en cuanto a su confidencialidad o uso debe ser considerada como "Uso Interno".

La información debe ser clasificada como "Confidencial Restringida", "Confidencial", "Uso Interno" o "Información Pública". Cada una de las nomenclaturas está detallada enseguida:

7.3. Confidencial Restringida

Es toda información asociada a los intereses estratégicos de Sukyo Mahikari del Perú, que posee la Dirección y de los Órganos relacionados. Su conocimiento debe ser limitado a un número reducido de personas autorizadas. Si es revelada o adulterado, puede traer serios perjuicios de imagen o financieros y generar impactos negativos en las actividades o en la imagen de Sukyo Mahikari del Perú, de sus colaboradores, socios, visitantes y de sus simpatizantes. Esta información requiere medidas de control y protección rigurosas contra accesos, copias o reproducciones no autorizadas.

Ejemplos de información que debe ser clasificada como "Confidencial Restringida":

- Estrategias de la actividad y principales directrices a medio y largo plazo;
- Información financiera de Sukyo Mahikari del Perú;
- Información de procesos jurídicos estratégicos;
- Información contable y resultados administrativos, que no circulan por los medios de comunicación.

La información "Confidencial Restringida" esta, en general, limitada al presidente, vicepresidentes, directores, cuerpo jurídico, auditores y colaboradores previamente designados.

En caso de indicios de extravío, tal ocurrencia debe ser informada inmediatamente al "Propietario de la Información".

7.3.1. En relación a su creación, se debe observar que:

- En la clasificación de la información como "Confidencial Restringida", se debe indicar para qué grupo o propósito la información es reservada;
- En el caso de papel, la expresión "Confidencial Restringida" debe ser explícita por medio del uso de sello, etiqueta o de impresión en el material;
- En el caso de archivo electrónico, la expresión "Confidencial Restringida" debe estar visible y ser de fácil identificación para el "Usuario de la Información".

7.3.2. En relación a su divulgación, se debe observar que:

- La divulgación interna de la información "Confidencial Restringida" para colaboradores que no pertenecen al Órgano o al equipo de trabajo originalmente autorizado requiere un control riguroso y debe ser previamente aprobada por el "Propietario de la Información" o por el "Administrador de la Información";
- Para su transporte interno o externo, se deben tomar medidas de seguridad física para garantizar su secreto y el control de acceso restringido a los autorizados.
- Si es necesario el envío externo, el procedimiento debe ser formal y previamente autorizado por el "Administrador de la Información";
- La reproducción de documentos clasificados como "Confidenciales Restringidos" debe ser previamente aprobada por el "Propietario de la Información" o por el "Administrador de la Información" y debe poseer una identificación única, así como el registro de "copia autorizada" en cada una de las copias;
- En la transmisión electrónica de información "Confidencial Restringida", es obligatorio el uso de criptografía. Si es necesario su envío externo, el procedimiento debe ser formal y previamente autorizado por el "Administrador de la Información";
- La divulgación no autorizada de información "Confidencial Restringida" dará como resultado la aplicación de las sanciones previstas en la instrucción normativa SGSI-007 (Medidas Disciplinarias), en tratados secretos y en la legislación en vigor.

7.3.3. En relación a su guardia, se debe observar que:

- La información clasificada como "Confidencial Restringida" debe ser almacenadas o guardadas en lugares con acceso controlado y restringido;
- Las información clasificadas como "Confidencial Restringida" no debe ser almacenadas localmente en las estaciones de trabajo;

- No almacenamiento electrónico de información "Confidencial Restringida", es obligatorio el uso de criptografía.

7.3.4. En relación a su eliminación, se debe observar que:

Es efectuado de forma que sea imposible su recuperación, de acuerdo a cada ambiente y medio usado:

- En el caso de papel, la destrucción de esos documentos debe ser hecha en máquina trituradora;
- Los medios de comunicación electrónicos usados para el almacenamiento temporal de informaciones "Confidenciales Restringidas", tales como disco y unidad de disco duro, debe ser eliminadas por medio de procedimientos que imposibiliten la recuperación de las informaciones en ellas contenidas;
- Los medios de comunicación electrónicos usados para el almacenamiento permanente, tales como CDROM, deben ser destruidos.

7.4. Confidencial

Es toda información cuyo conocimiento está limitado a colaboradores que, por la naturaleza de la función que desempeñan, la necesitan para el ejercicio profesional. Su divulgación o manipulación puede traer impactos negativos en los negocios y en la administración de procesos, o perjuicios a la imagen de Sukyo Mahikari del Perú, sus colaboradores, sus socios, visitantes o sus simpatizantes. Esta información requiere control y protección contra accesos no autorizados.

Ejemplos de información que debe ser clasificadas como "Confidencial":

- Datos registrados de los visitantes;
- Pago a personal;
- Procedimientos internos críticos;
- Estudios y proyectos;
- Programas de computadora que manipulan datos confidenciales, componentes de Sistema Operacional o software de seguridad;
- Documentación de ambiente computacional;
- Archivos relativos a contraseñas, criptografía y datos de personas.

En caso de indicios de extravío, tal ocurrencia debe ser informada inmediatamente al "Administrador de la Información".

7.4.1. En relación a su creación, se debe observar que:

- En la clasificación de la información como "Confidencial", debe ser explicitado para qué grupo o propósito la información es reservada;

- En caso de papel, la expresión "Confidencial" debe ser explicitada por medio de uso de sello, etiqueta o de impresión en el material;
- En el caso de archivo electrónico, la expresión "Confidencial" debe estar visible y ser de fácil identificación para el "Usuario de la Información".

7.4.2. En relación a su divulgación, se debe observar que::

- La información clasificada como "Confidencial" requiere control riguroso para su divulgación, siendo necesaria la autorización del "Administrador de la Información" o del "Propietario de la Información";
- La reproducción de documentos clasificados como "Confidenciales" debe ser previamente aprobada por el "Propietario de la Información" o por el "Administrador de la Información" y debe poseer una identificación única, así como el registro de copia autorizada en cada una de las copias;
- Para su transporte interno o externo, medidas de seguridad física debe ser adoptadas para garantizar la confidencialidad y el control de acceso restringido a los autorizados. Si es necesario su envío externo, el procedimiento debe ser previamente autorizado por el respectivo "Administrador de la Información";
- En la transmisión electrónica interna de informaciones clasificadas como "Confidenciales", el uso de controles adicionales de seguridad debe ser especificada por el "Administrador de la Información". En la transmisión externa, es obligatorio el uso de criptografía;
- La divulgación no autorizada de información clasificada como "Confidencial" por terceros, socios, proveedores de servicios, tendrá como resultado la aplicación de las sanciones previstas en la instrucción normativa SGSI-009 (Termo de Confidencialidad), en tratados de confidencialidad y en la legislación en vigor.
- La divulgación no autorizada de información "Confidencial" tendrá como resultado la aplicación de las sanciones previstas en la instrucción normativa SGSI-007 (Medidas Disciplinarias), en tratados de confidencialidad en la legislación en vigor.

7.4.3. En relación a su guardiã, se debe observar que:

- La información clasificada como "Confidencial" debe ser almacenada o guardada en lugares con acceso controlado y restringido a los colaboradores autorizados.

7.4.4. En relación a su eliminación, se debe observar que:

Debe efectuarse de forma que no sea posible su recuperación, de acuerdo con cada ambiente y medio utilizado:

- En el caso de papel, la destrucción de estos documentos debe hacerse de forma que se imposibilite su recuperación;

- Los medios electrónicos utilizados para almacenamiento temporal de información clasificada como "Confidencial", tal como disco y unidad de disco duro, deben ser eliminadas por medio de un procedimiento que imposibilite la recuperación de la información contenida;
- Los medios electrónicos utilizados para el almacenamiento permanente, tales como CDROM, deben ser destruidas.

7.5. Uso Interno

Es toda información cuyo conocimiento y uso están restringidos exclusivamente al ambiente interno y a los propósitos de Sukyo Mahikari del Perú, estando disponible a los colaboradores y pudiendo revelarse al público externo sólo con autorización del "Administrador de la Información".

Ejemplos de información que debe ser clasificada como "Uso Interno":

- Instrucción normativa;
- Programas internos y de entrenamiento;
- Normas internas;
- Manuales de procedimientos e instrucciones de uso general, así como de interrelacionamiento entre los Órganos;
- Resultados de metas;
- Programas de computadora.

En caso de indicios de extravío, tal ocurrencia debe ser informada inmediatamente al "Administrador de la Información".

7.5.1. En relación a su creación, se debe observar que:

- En el caso de papel, se recomienda que la expresión "Uso Interno" sea explicitada por medio del uso de sello, etiqueta o de impresión en el material;
- En el caso de archivo electrónico, se recomienda que la expresión "Uso Interno" esté visible y de fácil identificación para el "Usuario de la Información".

7.5.2. En relación su divulgación, se debe observar que:

- Para su transporte externo, medidas de seguridad física deben ser adoptadas para garantizar la confidencialidad de las informaciones. El procedimiento debe ser previamente autorizado por el respectivo "Administrador de la Información"; La divulgación no autorizada de informaciones clasificadas como "Uso Interno" por terceros, socios, proveedores de servicios, tendrá como resultado la aplicación de las sanciones previstas en la SGSI-009 (Término de Confidencialidad), en tratados de confidencialidad en la legislación en vigor.

- La divulgación no autorizada de informaciones "Uso Interno" resultará en la aplicación de las sanciones previstas en la instrucción normativa SGSI-007 (Medidas Disciplinarias), en tratados de confidencialidad y en la legislación en vigor.

7.5.3. En relación a su guardia, se debe observar que:

- Las informaciones clasificadas como de "Uso Interno" deben ser almacenadas o guardadas de forma organizada.

7.5.4. En relación a su eliminación, se debe observar que:

- En el caso de papel, la destrucción de esos documentos debe hacerse de forma que imposibilite su recuperación;
- Los medios electrónicos utilizados para almacenamiento temporal de informaciones de "Uso Interno", tales como disco y unidad de disco duro, debe ser eliminadas por medio de un procedimiento que imposibilite la recuperación de la información contenida;
- Los medios electrónicos utilizados para almacenamiento permanente, tales como CDROM, deben ser destruidas.

7.6. Información Pública

Es toda información que puede o debe ser divulgada para o público externo a Sukyo Mahikari del Perú, sin implicaciones de protección y control de acceso.

Ejemplos de informaciones que deben ser clasificadas como "Información Pública":

1. Folders con informaciones de las actividades abiertas al público e inauguración de regionales;
2. Materiales promocionales de divulgación;
3. Informativos;
4. Código de Ética;

7.7. Reclasificación de la Información

La reclasificación de la información debe obedecer a los mismos principios adoptados en su clasificación. Por lo tanto, compete sólo al "Propietario de la Información" o al "Administrador de la Información". La nueva clasificación debe ser formalizada para el "Custodio de la Información".

La reclasificación puede ser permanente o temporal. En el caso de una reclasificación temporal se debe también formalizar a su fecha límite.

7.7.1. Consideraciones sobre la Clasificación de la Información

El detalle de los procedimientos adoptados en la clasificación de la información será objeto de normas específicas. El departamento de Administración de la Seguridad de la Información debe ser consultado en casos de duda.

La información en desuso, pero que necesita ser preservada, debe ser guardada en un lugar externo a su ambiente normal de uso, con nivel de seguridad compatible con su clasificación original.

En la clasificación de un conjunto de informaciones que presentan diversos niveles de confidencialidad, se debe adoptar la clasificación de mayor nivel presente en el conjunto.

8. RESPONSABILIDADES

En este tema están relacionadas las principales responsabilidades de los colaboradores y Órganos de Sukyo Mahikari del Perú, no que se refiere a la Política de Seguridad de la Información.

Es importante resaltar que un mismo colaborador puede ejercer simultáneamente más de una función. En ese caso, se debe considerar o conjunto de las responsabilidades de cada una de esas funciones.

8.1. Comité de Seguridad de la Información

Está compuesto por representantes de los Órganos de Recursos Humanos, Jurídico, de Tecnología de la Información y del Consejo Administrativo de Sukyo Mahikari del Perú.

Compete a este:

- Coordinar acciones de divulgación de la Política de Seguridad de la Información;
- Planear y coordinar la implementación de las normas de seguridad contenidas en la Política de Seguridad de la Información;
- Promover la divulgación de esas normas para los Órganos de Sukyo Mahikari del Perú y resolver dudas en cuanto a su aplicación;
- Coordinar, con los demás Órganos de Sukyo Mahikari del Perú, la evaluación de las normas vigentes en cuanto haya necesidad de adecuar en función de esta Política;
- Deliberar sobre alteraciones eventuales de la Política de Seguridad de la Información de Sukyo Mahikari del Perú y definir las acciones necesarias para la divulgación de esas alteraciones;
- Reportarse a la alta administración de Sukyo Mahikari del Perú;
- Analizar y revisar los incidentes relacionados con la seguridad de informaciones.

8.2. Órgano de Administración de la Seguridad de la Información

Compete a ese Órgano:

- Ejecutar el seguimiento permanente, verificando el cumplimiento y la evolución de las medidas de Seguridad de la Información aplicables;
- Realizar la revisión periódica de ese documento o cuando ocurriesen actos que recomiende esa acción; y presentarlo al Comité de Seguridad de la Información para aprobación y divulgación;
- Realizar la administración de la Política de Seguridad de la Información, centralizando las sugerencias de alteraciones provenientes de los diversos Órganos y presentarlo al Comité de Seguridad de la Información, siempre que sea necesario;
- Garantizar el cumplimiento de esta Política y de las demás normas de seguridad por todos los colaboradores bajo su responsabilidad;
- Mantener las normas y los procedimientos internos del Órgano alineados con esta Política;
- Actuar como "Propietario de la Información", de la información de su Órgano, indicando administradores o asumiendo la responsabilidad de "Administrador de la Información";
- Divulgar la importancia de la confidencialidad de contraseñas, así como el cuidado con su uso, evitando el uso de una misma contraseña por un grupo de diversos usuarios;
- Garantizar que los contratos celebrados con otras entidades y personas externas a Sukyo Mahikari del Perú (socios, terceros, proveedores de servicios, proveedores temporales, contratados, voluntarios y visitantes) contengan una cláusula que preserve la Seguridad de la Información de Sukyo Mahikari del Perú, de sus clientes, socios y colaboradores;
- Garantizar que en los contratos de servicios en que los colaboradores vinculados a empresas contratadas desempeñen actividades que impliquen el acceso o manejo de información de Sukyo Mahikari del Perú, ya que cada da uno de los colaboradores haya firmado el Término de Confidencialidad (SGSI-009);

  Orientar a los colaboradores que, por obligación del trabajo manipulan o tienen conocimiento de documentos con información clasificada como "Confidencial" o "Confidencial Restringida", en cuanto al cuidado que deben tener con tal información;
- Reportar a la Infra-estructura de Tecnología de la Información las fallas y los riesgos que puede llevar a la exposición indebida de información clasificada como "Confidencial Restringid", "Confidencial" o de "Uso Interno".

- Proveer recursos de criptografía para la transmisión electrónica de información clasificada como "Confidencial Restringida" o "Confidencial" a través de medios de comunicación internos y externos;
- Proveer herramientas para el control de acceso con registros de auditoría y procedimientos de seguridad para garantizar la integridad de la información clasificada como "Confidencial Restringida" o "Confidencial";
- Proveer herramientas para formatear los medios electrónicos de almacenamiento temporal y para la eliminación de archivos, de forma que garantice la confidencialidad de la información clasificada como "Confidencial Restringida", "Confidencial" o de "Uso Interno".

8.3. Propietario de la Información

Compete a este:

- Designar uno o más administradores para las informaciones de su propiedad o asumir el papel de "Administrador de la Información" en ausencia (o inexistencia) de los administradores designados;
- Clasificar la información bajo su responsabilidad;
- Revisar periódicamente la relación de "Administrador de la Información" designados, haciendo las alteraciones necesarias.

8.4. Administrador de la Información

Compete a este:

- Clasificar la información bajo su responsabilidad, desde que sea previamente autorizado por el "Propietario de la Información";
- Comunicar la clasificación al "Custodio de la Información" y a los "Usuarios de la Información" directamente afectados;
- Conceder cuidadosamente y controlar las autorizaciones de acceso a las informaciones bajo su administración;
- Asumir las funciones de "Propietario de la Información" desde que sea previsto y formalmente autorizado por éste;

  Establecer controles específicos y diferenciados para informaciones clasificadas como "Confidenciales Restringidas" y "Confidenciales";
- Elaborar y mantener el plan de continuidad de negocio de los procesos y el flujo de informaciones bajo su responsabilidad;
- Especificar para el "Custodio de la Información" los criterios para la disponibilidad de la información, tales como tiempo de retención y número de copias, pudiendo sugerir el tipo de medio para el almacenamiento.

8.5. Custodio de la Información

Compete a este:

- Solamente conceder acceso a la información que tiene bajo su custodia con la previa autorización del "Administrador de la Información";
- Mantener la integridad de la información bajo su custodia;
- Controlar el acceso la información "Confidencial Restringida" y "Confidencial" que le fueran confiadas, manteniendo registros históricos sobre esos accesos, conforme determinado por el "Administrador de la Información";
- Implantar los controles establecidos por el "Administrador de la Información" y adoptar los procedimientos de seguridad necesarios para preservar a clasificación de las informaciones que le fueren confiadas;
- Elaborar y mantener el plano de contingencia de procesamiento de la información bajo su custodia;
- Comunicar a los "Administradores de la Información" los casos de indicio de problemas que puedan generar pérdida de confidencialidad, integridad o disponibilidad de la información bajo su custodia.
- En el caso específico de información corporativa almacenada y procesada en el ambiente computacional, compete al Órgano de Administración de la Seguridad de la Información (que es el "Custodio de las Informaciones" de ese ambiente) proveer herramientas (hardware, software y red) adecuado, de forma que preserve los aspectos de confidencialidad, integridad e disponibilidad de la información bajo su custodia.

8.6. Responsabilidades Generales

Compete a todos los Colaboradores:

- Evitar la discusión de asuntos confidenciales en elevadores, transportes públicos, restaurantes u otros lugares donde personas extrañas o colaboradores no autorizados puedan obtener información confidencial que pueda perjudicar a Sukyo Mahikari del Perú, sus visitantes y voluntarios;

  Restringir la información y los recursos de información a quien está autorizado;
- Observar todas las recomendaciones y normas de seguridad y privacidad;
- Mantener las mesas de trabajo limpias y los archivos cerrados;
- Reportar al superior inmediato cualquier exposición indebida y riesgos en la información clasificada como "Confidencial Restringida", "Confidencial" o de "Uso Interno";
- Conocer y cumplir los controles de seguridad establecidos.

Con relación al trato de documentos y correspondencias, se recomienda:

- Establecer la rutina de realizar a destrucción de documentos y relatos que no serán utilizados, de forma que imposibilite su recuperación;
- No abrir sobres o carpetas que contengan documentos con informaciones clasificadas como "Confidencial Restringida" o "Confidencial" fuera de su ambiente de trabajo (restaurantes, elevadores, corredores, etc.);
- No dejar documentos y correspondencias expuestos en salas de reuniones, sobre mesas o e otros ambientes inadecuados, de forma que puedan ser vistos por personas no autorizadas;
- Esclarecer al destinatario el carácter de confidencialidad de la información "Confidencial Restringida" y "Confidencial" a este enviadas;
- Seguir y cumplir todas las orientaciones expresas en la correspondencia, en cuanto a su destrucción, regreso a ser guardado en archivo de seguridad;
- Identificar, por el uso de etiquetas, sellos, impresión en el material o procesos especiales, los documentos que contengan información clasificada como "Confidencial Restringida" o "Confidencial";
- No permitir la reproducción de documentos que contengan información clasificada como "Confidencial Restringida" y "Confidencial". Mantener control de circulación, de forma que sólo personas autorizadas tengan acceso a la información.

9. PRINCIPIOS DE SEGURIDAD

9.1. Ambiente

Los Recursos de Información solamente estarán disponibles en el ambiente computacional de producción después de realizar pruebas en ambientes segregados. Estos recursos deben ser identificados de forma individual, inventariados, protegidos de accesos indebidos, tener documentación actualizada y planes de mantenimiento.

Los recursos de información deben ser utilizados en conformidad con las cláusulas contractuales firmadas con proveedores, socios y clientes.

El uso de recursos de información debe respetar la legislación vigente y las normas internas de Sukyo Mahikari del Perú.

Las actividades críticas deben tener su contingencia asegurada a través de planes para su continuidad, definidos por el "Administrador de la Información", y planes de contingencia de recursos, definidos por el "Custodio de la Información".

Los procesos de trabajo de Sukyo Mahikari del Perú necesitan ser resguardados a través de la segregación de funciones, de forma que las actividades no sean ejecutadas y

controladas por el mismo colaborador o por el mismo equipo de colaboradores. Debe haber procesos de autorización formalizados para el uso de recursos de información.

Compete a los administradores responsables por los Órganos, monitorear los recursos de información utilizados por su Órgano, identificar los riesgos involucrados y asegurar que los colaboradores estén conscientes de los deberes en cuanto a su uso adecuado, a fin de preservar su integridad física y buen funcionamiento.

La entrada y la salida de recursos de información de las dependencias de Sukyo Mahikari del Perú deben ser realizadas mediante autorización formal.

9.2. Control de Acceso

Los usuarios deben tener identificación única, personal e intransferible, calificándolos como responsables por las acciones realizadas por medio de esta.

La concesión de accesos a los colaboradores debe obedecer al criterio de menor privilegio, en el cual los usuarios tienen acceso solamente a los recursos de información imprescindible para el pleno desempeño de sus actividades.

10. PATRONES DE SEGURIDAD

Los patrones de seguridad deben ser establecidos y comunicados. A cada patrón corresponde un análisis de nivel de confidencialidad de la información de cada Órgano, así como los respectivos controles que el Órgano debe ejercer sobre su información.

Compete a la Administración de Seguridad de la Información, con base en el patrón de seguridad explícito, determinar el grado de conformidad existente.

La Presidencia y la Dirección deben acompañar los mecanismos de monitoreo establecidos por los "Administradores de la Información", discutiendo los casos relevantes en el Comité de Seguridad de la Información.