DG DOCUMENTO GERAL	CLASSIFICAÇÃO DA INFORMAÇÃO E RESPONSABILIDADES

APRESENTAÇÃO

Este documento descreve as diretrizes para classificação da informação e as responsabilidades dentro da Política de Segurança da Sukyo Mahikari do Brasil.

DSI DEPARTAMENTO DE SEGURANÇA DA INFORMAÇÃO	Os comentários e sugestões referentes a este documento devem ser encaminhados ao gestor desse documento indicando o item a ser revisado, a proposta e a justificativa. Este documento normativo tem a validade de um ano a partir da sua edição, prazo máximo para a realização da próxima revisão.

GESTOR: DSI	APROVADOR
Hugo Okamoto	Hidekazu Sakamoto

CONTROLE DE REVISÕES

REV.	DESCRIÇÃO DA MUDANÇA	DATA
0	Emissão original – sem revisões	

SUMÁRIO

1. OBJETIVO

Classifica os tipos de informações e define responsabilidades dentro da Política de Segurança da Informação da Sukyo Mahikari do Brasil.

2. APLICAÇÃO

Esta Política de Segurança da Informação destina-se a todos os contratados, colaboradores, voluntários e usuários de informações da Sukyo Mahikari do Brasil, servindo de base para a definição de normas específicas, procedimentos, responsabilidades e conceitos.

3. ATRIBUIÇÕES E RESPONSABILIDADES

- Cabe ao DSI, a gestão deste documento que inclui seu desenvolvimento, implementação e manutenção.
- Cabe ao DSI manter este documento atualizado e promover as revisões necessárias.
- Cabe à Diretoria a aprovação deste documento.
- Cabem a todos os funcionários, colaboradores e voluntários a ler e seguir as diretrizes.

4. DOCUMENTOS DE REFERÊNCIA

O presente documento foi desenvolvido com base no seguinte documento externo:

- NBR ISO/IEC 27002, item 7.2

5. TERMINOLOGIA

Ativo: Qualquer coisa que tenha valor para organização.

Confidencialidade: Propriedade de que a informação não esteja disponível ou revelada a indivíduos, entidades ou processos não autorizados.

Disponibilidade: Propriedade de estar acessível e utilizável sob demanda por uma entidade autorizada.

Integridade: Propriedade de salvaguarda da exatidão e completeza de ativos.

6. DEFINIÇÕES

Toda informação é patrimônio da Sukyo Mahikari do Brasil e está associada a um único Órgão, que pode ser uma área executiva, um departamento, uma gerência, etc.

Esse Órgão é o responsável direto pela criação e classificação dessas informações.

O executivo de mais alto nível desse Órgão é denominado "Proprietário da Informação".

Dessa forma, toda informação deve possuir um único "Proprietário da Informação".

Os envolvidos com a gestão e o manuseio das informações enquadram-se nas seguintes categorias:

6.1. Proprietário da Informação

Executivo do Órgão encarregado da criação, classificação, eliminação e destruição da informação. É responsável também pela designação dos "Gestores da Informação".

6.2. Gestor da Informação

Colaborador (ou grupo de Colaboradores) designado pelo "Proprietário da Informação" para realizar a gestão da informação, sendo responsável pela validação, liberação e cancelamento dos acessos à informação. Pode assumir as funções do "Proprietário da Informação", desde que previamente autorizado pelo mesmo.

6.3. Custodiante da Informação

Colaborador ou Órgão responsável pela guarda e pelo armazenamento da informação, baseado nos critérios e controles definidos pelo "Gestor da Informação". O "Custodiante da Informação" deve ser definido pelo "Gestor da Informação". No caso das informações corporativas armazenadas e processadas no ambiente computacional da Sukyo Mahikari do Brasil, o "Custodiante da Informação" é o Departamento de Tecnologia da Informação.

6.4. Usuário da Informação

Qualquer pessoa autorizada pelo "Proprietário da Informação" ou pelo "Gestor da Informação" a acessar, ler, responder, inserir, alterar ou eliminar determinada informação.

7. CLASSIFICAÇÃO DA INFORMAÇÃO

A informação é classificada de acordo com sua confidencialidade e sua utilização.

7.1. Confidencialidade

Está associada ao potencial de exposição e aos prejuízos que sua divulgação não autorizada ou acidental possa causar à continuidade das atividades da Sukyo Mahikari do Brasil, bem como a seus colaboradores, parceiros, visitantes e simpatizantes.

7.2. Utilização

Está diretamente relacionada ao público ao qual a informação se destina. Compete ao "Proprietário da Informação" ou ao "Gestor da Informação" definir o nível de classificação da informação sob sua responsabilidade.

Toda informação que não possuir uma classificação explícita quanto a sua confidencialidade ou utilização deve ser considerada como "Uso Interno".

As informações devem ser classificadas como "Confidencial Restrita", "Confidencial", "Uso Interno" ou "Informação Pública". Cada uma das nomenclaturas está detalhada a seguir:

7.3. Confidencial Restrita

É toda informação associada aos interesses estratégicos da Sukyo Mahikari do Brasil, de posse da diretoria e dos Órgãos afins. Seu conhecimento deve ser limitado a um número reduzido de pessoas autorizadas. Se revelada ou adulterada, pode trazer sérios prejuízos de imagem ou financeiros e gerar impactos negativos nas atividades ou na imagem da Sukyo Mahikari do Brasil, de seus colaboradores, parceiros, visitantes e de seus simpatizantes. Essas informações requerem medidas de controle e proteção rigorosos contra acessos, cópias ou reproduções não autorizadas.

Exemplos de informações que devem ser classificadas como "Confidencial Restrita":

- Estratégias da atividade e principais direções de médio e longo prazo;
- Informações financeiras da Sukyo Mahikari do Brasil;
- Informações de processos jurídicos estratégicos;
- Informações contábeis e resultados gerenciais, não veiculados pela mídia.

As informações "Confidenciais Restritas" são, em geral, limitadas ao presidente, vice-presidentes, diretores, corpo jurídico, auditores e colaboradores previamente designados.

Em caso de indícios de extravio, tal ocorrência deve ser informada imediatamente ao "Proprietário da Informação".

7.3.1. Em relação à sua criação, deve-se observar que:

- Na classificação de uma informação como "Confidencial Restrita", deve ser explicitado para qual grupo ou propósito a informação é reservada;
- No caso de papel, a expressão "Confidencial Restrita" deve ser explicitada por meio do uso de carimbo, de etiqueta ou de impressão no material;
- No caso de arquivo eletrônico, a expressão "Confidencial Restrita" deve estar visível e ser de fácil identificação para o "Usuário da Informação".

7.3.2. Em relação à sua divulgação, deve-se observar que:

- A divulgação interna de uma informação "Confidencial Restrita" para Colaboradores que não pertençam ao Órgão ou à equipe de trabalho originalmente autorizada requer um controle rigoroso e deve ser previamente aprovada pelo "Proprietário da Informação" ou pelo "Gestor da Informação";
- Para seu transporte interno ou externo, medidas de segurança física devem ser adotadas para garantir o seu sigilo e o controle de acesso restrito aos autorizados.
- Se necessário o seu envio externo, o procedimento deve ser formal e previamente autorizado pelo "Gestor da Informação";
- A reprodução de documentos classificados como "Confidenciais Restritos" deve ser previamente aprovada pelo "Proprietário da Informação" ou pelo "Gestor da Informação" e deve possuir uma identificação única, bem como o registro de "cópia autorizada" em cada uma das cópias;
- Na transmissão eletrônica de informações "Confidenciais Restritas", é obrigatório o uso de criptografia. Se necessário o seu envio externo, o procedimento deve ser formal e previamente autorizado pelo "Gestor da Informação";
- A divulgação não autorizada de informações "Confidenciais Restritas" resultará na aplicação das sanções previstas na instrução normativa SGSI-007 (Medidas Disciplinares), em tratados de sigilo e na legislação em vigor.

7.3.3. Em relação à sua guarda, deve-se observar que:

- As informações classificadas como "Confidenciais Restritas" precisam ser armazenadas ou guardadas em local com acesso controlado e restrito;
- As informações classificadas como "Confidenciais Restritas" não devem ser armazenadas localmente nas estações de trabalho;
- No armazenamento eletrônico de informações "Confidenciais Restritas", é obrigatório o uso de criptografia.

7.3.4. Em relação ao seu descarte, deve-se observar que:

Seja efetivado de forma a impossibilitar sua recuperação, de acordo com cada ambiente e meio utilizado:

- No caso de papel, a destruição desses documentos deve ser feita em máquina fragmentadora;
- As mídias eletrônicas utilizadas para armazenamento temporário de informações "Confidenciais Restritas", tais como disquete e unidade de disco

rígido, devem ser apagadas por meio de procedimento que impossibilite a recuperação das informações nelas contidas;

- As mídias eletrônicas utilizadas para armazenamento permanente, tais como CDROM, devem ser destruídas.

7.4. Confidencial

É toda informação cujo conhecimento está limitado a colaboradores que, pela natureza da função que desempenham, dela necessitam para o exercício profissional. Sua divulgação ou adulteração pode trazer impactos negativos nos negócios e na gestão de processos, ou prejuízos à imagem da Sukyo Mahikari do Brasil, seus colaboradores, seus parceiros, seus visitantes ou seus simpatizantes. Essas informações requerem controle e proteção contra acessos não autorizados.

Exemplos de informações que devem ser classificadas como "Confidencial":

- Dados cadastrais dos visitantes;
- Pagamento de pessoal;
- Procedimentos internos críticos;
- Estudos e projetos;
- Programas de computador que manipulam dados confidenciais, componentes do Sistema Operacional ou softwares de segurança;
- Documentação do ambiente computacional;
- Arquivos relativos a senhas, criptografia e dados de clientes.

Em caso de indícios de extravio, tal ocorrência deve ser informada imediatamente ao "Gestor da Informação".

7.4.1. Em relação à sua criação, deve-se observar que:

- Na classificação de uma informação como "Confidencial", deve ser explicitado para qual grupo ou propósito a informação é reservada;
- No caso de papel, a expressão "Confidencial" deve ser explicitada por meio do uso de carimbo, de etiqueta ou de impressão no material;
- No caso de arquivo eletrônico, a expressão "Confidencial" deve estar visível e ser de fácil identificação para o "Usuário da Informação".

7.4.2. Em relação à sua divulgação, deve-se observar que:

- A informação classificada como "Confidencial" requer controle rigoroso para sua divulgação, sendo necessária a autorização do "Gestor da Informação" ou do "Proprietário da Informação";
- A reprodução de documentos classificados como "Confidenciais" deve ser previamente aprovada pelo "Proprietário da Informação" ou pelo "Gestor da

Informação" e deve possuir uma identificação única, bem como o registro de cópia autorizada em cada uma das cópias;

- Para seu transporte interno ou externo, medidas de segurança física devem ser adotadas para garantir o sigilo e o controle de acesso restrito aos autorizados. Se necessário o seu envio externo, o procedimento deve ser previamente autorizado pelo respectivo "Gestor da Informação";
- Na transmissão eletrônica interna de informações classificadas como "Confidenciais", a utilização de controles adicionais de segurança deve ser especificada pelo "Gestor da Informação". Na transmissão externa, é obrigatório o uso de criptografia;
- A divulgação não autorizada de informações classificadas como "Confidenciais" por terceiros, parceiros, prestadores de serviços, resultará na aplicação das sanções previstas na instrução normativa SGSI-009 (Termo de Sigilo), em tratados de sigilo e na legislação em vigor.
- A divulgação não autorizada de informações "Confidenciais" resultará na aplicação das sanções previstas na instrução normativa SGSI-007 (Medidas Disciplinares), em tratados de sigilo na legislação em vigor.

7.4.3. Em relação à sua guarda, deve-se observar que:

- As informações classificadas como "Confidenciais" devem ser armazenadas ou guardadas em local com acesso controlado e restrito aos Colaboradores autorizados.

7.4.4. Em relação ao seu descarte, deve-se observar que:

Seja efetivado de forma que não seja possível sua recuperação, de acordo com cada ambiente e meio utilizado:

- No caso de papel, a destruição desses documentos deve ser feita de forma a impossibilitar a sua recuperação;
- As mídias eletrônicas utilizadas para armazenamento temporário de informações classificadas como "Confidenciais", tais como disquete e unidade de disco rígido, devem ser apagadas por meio de procedimento que impossibilite a recuperação das informações nela contida;
- As mídias eletrônicas utilizadas para armazenamento permanente, tais como CDROM, devem ser destruídas.

7.5. Uso Interno

É toda informação cujo conhecimento e uso estão restritos exclusivamente ao ambiente interno e aos propósitos da Sukyo Mahikari do Brasil, estando disponível aos

Colaboradores e podendo ser revelada ao público externo apenas mediante autorização do "Gestor da Informação".

Exemplos de informações que devem ser classificadas como "Uso Interno":

- Instrução normativa;
- Programas internos e de treinamento;
- Normas internas;
- Manuais de procedimentos e instruções de uso geral, bem como de inter-relacionamento entre os Órgãos;
- Resultados de metas;
- Programas de computador.

Em caso de indícios de extravio, tal ocorrência deve ser informada imediatamente ao "Gestor da Informação".

7.5.1. Em relação à sua criação, deve-se observar que:

- No caso de papel, recomenda-se que a expressão "Uso Interno" seja explicitada por meio do uso de carimbo, de etiqueta ou de impressão no material;
- No caso de arquivo eletrônico, recomenda-se que a expressão "Uso Interno" esteja visível e de fácil identificação para o "Usuário da Informação".

7.5.2. Em relação à sua divulgação, deve-se observar que:

- Para seu transporte externo, medidas de segurança física devem ser adotadas para garantir o sigilo das informações. O procedimento deve ser previamente autorizado pelo respectivo "Gestor da Informação";
- A divulgação não autorizada de informações classificadas como "Uso Interno" por terceiros, parceiros, prestadores de serviços, resultará na aplicação das sanções previstas na SGSI-009 (Termo de Sigilo), em tratados de sigilo e na legislação em vigor.
- A divulgação não autorizada de informações "Uso Interno" resultará na aplicação das sanções previstas na instrução normativa SGSI-007 (Medidas Disciplinares), em tratados de sigilo e na legislação em vigor.

7.5.3. Em relação à sua guarda, deve-se observar que:

- As informações classificadas como de "Uso Interno" devem ser armazenadas ou guardadas de forma organizada.

7.5.4. Em relação ao seu descarte, deve-se observar que:

- No caso de papel, a destruição desses documentos deve ser feita de forma a impossibilitar a sua recuperação;

- As mídias eletrônicas utilizadas para armazenamento temporário de informações de "Uso Interno", tais como disquete e unidade de disco rígido, devem ser apagadas por meio de procedimento que impossibilite a recuperação das informações nela contida;
- As mídias eletrônicas utilizadas para armazenamento permanente, tais como CDROM, devem ser destruídas.

7.6. Informação Pública

É toda informação que pode ou deve ser divulgada para o público externo à Sukyo Mahikari do Brasil, sem implicações de proteção e controle de acesso.

Exemplos de informações que devem ser classificadas como "Informação Pública":

1. Folders com informações das atividades abertas ao público e inauguração de regionais;
2. Materiais promocionais de divulgação;
3. Informativos;
4. Código de Ética.

7.7. Reclassificação da Informação

A reclassificação de uma informação deve obedecer aos mesmos princípios adotados na sua classificação. Portanto, compete apenas ao "Proprietário da Informação" ou ao "Gestor da Informação". A nova classificação deve ser formalizada para o "Custodiante da Informação".

A reclassificação pode ser permanente ou temporária. No caso de uma reclassificação temporária deve-se também formalizar a sua data-limite.

7.7.1. Considerações sobre a Classificação da Informação

O detalhamento dos procedimentos adotados na classificação das informações será objeto de normas específicas. O departamento de Administração da Segurança da Informação deve ser consultado em casos de dúvida.

As informações em desuso, mas que precisam ser preservadas, devem ser guardadas em local externo ao seu ambiente normal de uso, com nível de segurança compatível com a sua classificação original.

Na classificação de um conjunto de informações que apresentam diversos níveis de confidencialidade, deve-se adotar a classificação de maior nível presente no conjunto.

8. RESPONSABILIDADES

Neste tópico estão relacionadas às principais responsabilidades dos Colaboradores e Órgãos da Sukyo Mahikari do Brasil, no que se refere à Política de Segurança da Informação.

É importante ressaltar que um mesmo Colaborador pode exercer simultaneamente mais de uma função. Nesse caso, deve-se considerar o conjunto das responsabilidades de cada uma dessas funções.

8.1. Comitê de Segurança da Informação

É composto por representantes dos Órgãos de Recursos Humanos, do Jurídico, de Tecnologia da Informação e do Conselho Administrativo da Sukyo Mahikari do Brasil.

Compete a ele:

- Coordenar ações de divulgação da Política de Segurança da Informação;
- Planejar e coordenar a implementação das normas de segurança contidas na Política de Segurança da Informação;
- Promover a divulgação dessas normas para os Órgãos da Sukyo Mahikari do Brasil e dirimir dúvidas quanto à sua aplicação;
- Coordenar, com os demais Órgãos da Sukyo Mahikari do Brasil, a avaliação das normas vigentes quanto à necessidade de adequação em função desta Política;
- Deliberar sobre eventuais alterações da Política de Segurança da Informação da Sukyo Mahikari do Brasil e definir as ações necessárias para a divulgação dessas alterações;
- Reportar-se à alta administração da Sukyo Mahikari do Brasil;
- Analisar e revisar os incidentes relacionados com a segurança de informações.

8.2. Órgão de Administração da Segurança da Informação

Compete esse Órgão:

- Executar o acompanhamento permanente, verificando o cumprimento e a evolução das medidas de Segurança da Informação aplicáveis;
- Realizar a revisão periódica desse documento ou quando houver ocorrência de fatos que recomendem essa ação; e submetê-lo ao Comitê de Segurança da Informação para aprovação e divulgação;
- Realizar a gestão da Política de Segurança da Informação, centralizando as sugestões de alteração provenientes dos diversos Órgãos e submetendo-as ao Comitê de Segurança da Informação, sempre que necessário;
- Garantir o cumprimento desta Política e das demais normas de segurança por todos os Colaboradores sob sua responsabilidade;

- Manter as normas e os procedimentos internos do Órgão alinhados com esta Política;
- Atuar como "Proprietário da Informação", das informações do seu Órgão, indicando gestores para essas informações ou assumindo a responsabilidade de "Gestor da Informação";
- Divulgar a importância de sigilo de senhas, bem como o cuidado com seu uso, evitando a utilização de uma mesma senha por um grupo de diversos usuários;
- Garantir que os contratos celebrados com outras entidades e pessoas externas à Sukyo Mahikari do Brasil (parceiros, terceiros, prestadores de serviços, fornecedores, temporários, contratados, voluntários e visitantes) contenham uma cláusula que preserve a Segurança da Informação da Sukyo Mahikari do Brasil, de seus clientes, parceiros e Colaboradores;
- Garantir que nos contratos de serviços em que os Colaboradores vinculados à empresa contratada venham desempenhar atividades que impliquem no acesso ou no manuseio de informações da Sukyo Mahikari do Brasil, cada um desses Colaboradores tenha firmado o Termo de Sigilo (SGSI-009);
- Orientar os Colaboradores que, por dever do ofício, manuseiam ou tomam conhecimento de documentos com informações classificadas como "Confidenciais" ou "Confidenciais Restritas" quanto ao zelo que devem ter com tais informações;
- Reportar à Infra-estrutura de Tecnologia da Informação as falhas e os riscos que podem levar à exposição indevida de informações classificadas como "Confidenciais Restritas", "Confidenciais" ou de "Uso Interno".
- Prover recursos de criptografia para a transmissão eletrônica de informações classificadas como "Confidenciais Restritas" ou "Confidenciais" através de meios de comunicação internos e externos;
- Prover ferramentas para controle de acesso com registros de auditoria e procedimentos de segurança para garantia da integridade da informação classificada como "Confidencial Restrita" ou "Confidencial";
- Prover ferramentas para formatação das mídias eletrônicas de armazenamento temporário e para a eliminação de arquivos, de forma a garantir a confidencialidade da informação classificada como "Confidencial Restrita", "Confidencial" ou de "Uso Interno".

8.3. Proprietário da Informação

Compete a ele:

- Designar um ou mais gestores para as informações de sua propriedade ou assumir o papel de "Gestor da Informação" na ausência (ou inexistência) dos gestores designados;
- Classificar as informações sob sua responsabilidade;
- Rever periodicamente a relação de "Gestores da Informação" designados, fazendo as alterações necessárias.

8.4. Gestor da Informação

Compete a ele:

- Classificar as informações sob sua responsabilidade, desde que previamente autorizado pelo "Proprietário da Informação";
- Comunicar a classificação ao "Custodiante da Informação" e aos "Usuários da Informação" diretamente afetados;
- Conceder criteriosamente e controlar as autorizações de acesso às informações sob sua gestão;
- Assumir as funções do "Proprietário da Informação" desde que prévia e formalmente autorizado por ele;
- Estabelecer controles específicos e diferenciados para informações classificadas como "Confidencias Restritas" e "Confidenciais";
- Elaborar e manter o plano de continuidade de negócio dos processos e o fluxo de informações sob sua responsabilidade;
- Especificar para o "Custodiante da Informação" os critérios para a disponibilidade da informação, tais como tempo de retenção e número de cópias, podendo sugerir o tipo de mídia para armazenamento.

8.5. Custodiante da Informação

Compete a ele:

- Somente conceder acesso às informações sob sua custódia com a prévia autorização do "Gestor da Informação";
- Manter a integridade das informações sob sua custódia;
- Controlar o acesso às informações "Confidenciais Restritas" e "Confidenciais" que lhe foram confiadas, mantendo registros históricos sobre esses acessos, conforme determinado pelo "Gestor da Informação";
- Implantar os controles estabelecidos pelo "Gestor da Informação" e adotar os procedimentos de segurança necessários para preservar a classificação das informações que lhe forem confiadas;
- Elaborar e manter plano de contingência de processamento das informações sob sua custódia;

- Comunicar aos "Gestores da Informação" os casos de indício de problemas que possam gerar perda de confidencialidade, integridade ou disponibilidade das informações sob sua custódia.
- No caso específico de informações corporativas armazenadas e processadas no ambiente computacional, compete ao Órgão de Administração da Segurança da Informação (que é a "Custodiante das Informações" desse ambiente) prover ferramental (hardware, software e rede) adequado, de forma a preservar os aspectos de confidencialidade, integridade e disponibilidade das informações sob sua custódia.

8.6. Responsabilidades Gerais

Compete a todos os Colaboradores:

- Evitar a discussão de assuntos confidenciais em elevadores, transportes públicos, restaurantes ou outros locais onde pessoas estranhas ou Colaboradores não autorizados possam obter informações sigilosas que possam prejudicar a Sukyo Mahikari do Brasil, seus visitantes e voluntários;
- Restringir-se às informações e os recursos de informação a que está autorizado;
- Observar todas as recomendações e normas de segurança e privacidade;
- Manter as mesas de trabalho limpas e os arquivos trancados;
- Reportar ao superior imediato qualquer exposição indevida e riscos às informações classificadas como "Confidenciais Restritas", "Confidenciais" ou de "Uso Interno";
- Conhecer e cumprir os controles de segurança estabelecidos.

Com relação ao trato de documentos e correspondências, recomenda-se:

- Estabelecer a rotina de realizar a destruição de documentos e relatórios que não serão mais utilizados, de forma que impossibilite a sua recuperação;
- Não abrir envelopes ou pastas contendo documentos com informações classificadas como "Confidenciais Restritas" ou "Confidenciais" fora de seu ambiente de trabalho (restaurantes, elevadores, corredores, etc.);
- Não deixar documentos e correspondências expostos em salas de reuniões, sobre mesas ou em outros ambientes inadequados, de forma que possam ser vistos por pessoas não autorizadas;
- Esclarecer ao destinatário o caráter de confidencialidade das informações "Confidenciais Restritas" e "Confidenciais" a ele enviadas;
- Seguir e cumprir todas as orientações expressas na correspondência, quanto à sua destruição, retorno ou guarda em arquivo de segurança;

- Identificar, pelo uso de etiquetas, carimbos, impressão no material ou processos especiais, os documentos que contenham informações classificadas como "Confidenciais Restritas" ou "Confidenciais";
- Não permitir a reprodução de documentos que contenham informações classificadas como "Confidenciais Restritas" e "Confidenciais". Manter controle de circulação, de forma que apenas pessoas autorizadas tenham acesso às informações.

9. PRINCÍPIOS DE SEGURANÇA

9.1. Ambiente

Os Recursos de Informação somente estarão disponíveis em ambiente computacional de produção após a realização de testes em ambientes segregados. Esses recursos devem ser identificados de forma individual, inventariados, protegidos de acessos indevidos, ter documentação atualizada e planos de manutenção.

Os recursos de informação devem ser utilizados em conformidade com as cláusulas contratuais firmadas com fornecedores, parceiros e clientes.

A utilização de recursos de informação deve respeitar a legislação vigente e as normas internas da Sukyo Mahikari do Brasil.

As atividades críticas devem ter sua contingência assegurada através de planos para sua continuidade, definidos pelo "Gestor da Informação", e planos de contingência de recursos, definidos pelo "Custodiante da Informação".

Os processos de trabalho da Sukyo Mahikari do Brasil precisam ser resguardados através da segregação de funções, de forma que as atividades não sejam executadas e controladas pelo mesmo Colaborador ou pela mesma equipe de Colaboradores. Deve haver processos de autorização formalizados para o uso de recursos de informação.

Compete aos administradores responsáveis pelos Órgãos monitorar os recursos de informação utilizados pelo seu Órgão, identificar os riscos envolvidos e assegurar que os Colaboradores estejam cientes dos deveres quanto ao seu uso adequado, a fim de preservar sua integridade física e bom funcionamento.

A entrada e a saída de recursos de informação das dependências da Sukyo Mahikari do Brasil devem ser realizadas mediante autorização formal.

9.2. Controle de Acesso

Os usuários devem ter identificação única, pessoal e intransferível, qualificando-os como responsáveis pelas ações realizadas por intermédio dela.

A concessão de acessos aos Colaboradores deve obedecer ao critério de menor privilégio, no qual os usuários têm acesso somente aos recursos de informação imprescindíveis para o pleno desempenho de suas atividades.

10. PADRÕES DE SEGURANÇA

Os padrões de segurança devem ser estabelecidos e comunicados. A cada padrão corresponde uma análise do nível de confidencialidade das informações de cada Órgão, bem como os respectivos controles que o Órgão deve exercer sobre suas informações.

Compete à Administração da Segurança da Informação, com base no padrão de segurança explicitado, determinar o grau de conformidade existente.

A Presidência e a Diretoria devem acompanhar os mecanismos de monitoração estabelecidos pelos "Gestores da Informação", discutindo os casos relevantes no Comitê de Segurança da Informação.