Política de Segurança de Informação

Histórico de Versões			
Versão:	Data:	Descrição das mudanças na versão:	Autor:
01	10/07/2013	Versão inicial	Guillermo Sepúlveda
02	02/12/2014	Revisão geral do documento	Guillermo Sepúlveda
03	18/10/2018	Revisão Geral / Adaptação	Guillermo Sepúlveda
04	07/12/2021	Revisão Geral / Adaptações	Guillermo Sepúlveda
05	13/10/2022	Revisão geral do documento	Guillermo Sepúlveda e Viviane
06	29/11/2022	Ajustes no item Gestão de Consequências	Viviane

Tabela de Conteúdo

1 Introdução

O Negócio do Grupo Synoro é empreender e apoiar empreendedores.
Nossas prioridades são o uso da tecnologia como força transformadora e a busca de soluções que incentivam o compartilhamento e a colaboração entre pessoas e empresas.

O grupo é composto por 5 iniciativas:

- TDW - Consultoria e Desenvolvimento de soluções para ambientes analíticos.
- SYNORO AAI - Escritório de Assessoria de Investimentos.
- SEU FELIX - Plataforma digital que conecta clientes com prestadores de serviços.
- TRIIBO - Plataforma de engajamento baseada no conceito de comunidades.
- AYXMA- Plataforma de controle e monitoramento de processos.

O objetivo deste documento é estabelecer as normas e diretrizes necessárias à preservação e segurança dos bens de informação utilizados no Grupo Synoro.

Definimos como bens de informação os seguintes itens: sistemas aplicativos desenvolvidos internamente e adquiridos do mercado, softwares básicos e de apoio, dados internos e de clientes, hardware, instalações físicas, equipamentos de infra-estrutura e documentos em papel.

Conforme definição da norma NBR ISO 27.002, a informação é um ativo que, como qualquer outro ativo importante para os negócios, têm um valor para a organização e, conseqüentemente, necessita ser adequadamente protegido. A segurança da informação objetiva proteger a informação de diversos tipos de ameaça, para garantir a continuidade dos negócios, minimizando os danos e maximizando o retorno dos investimentos e as oportunidades de negócio.

A segurança da informação é obtida a partir da implementação de uma série de controles, que podem ser políticas, práticas, procedimentos, instruções e funções de software. Estes controles precisam ser implementados para garantir que os objetivos de segurança específicos do Grupo Synoro sejam atendidos.

A seguir apresentamos a política de segurança da informação do Grupo Synoro, dividida em capítulos de acordo com a norma brasileira ABNT/ISO 27.002.

2 Aspectos Organizacionais e Administrativos

1.1 Comitê de Segurança

É de responsabilidade da gestão da empresa (sócios) o planejamento e a implementação da Política de Segurança da informação do Grupo Synoro.

Um Comitê de Segurança da informação será constituído com as seguintes atribuições:

- Avaliar o cumprimento da Política de Segurança da informação
- Adequação da Política de Segurança de Informação a novas normas
- Análise e tratamento de não conformidades

O comitê se reunirá trimestralmente e será composto por um dos Sócios Diretores do Grupo Synoro, um Gerente de Serviço de cada iniciativa/empresa e um Analista de segurança da informação.

1.2 Atribuições e Responsabilidades

Exclusivamente para a questão de segurança da informação, são identificadas as seguintes funções genéricas, responsáveis pelo controle de acesso aos recursos da informação (internos e externos), com as respectivas atribuições e responsabilidades:

1.2.1 Proprietário da Informação

a) Delegar responsabilidade e atribuições ao usuário com finalidade de desenvolvimento de projetos
b) Classificar os bens de informação, de acordo com sua natureza crítica e sigilosa de acordo com suas políticas de segurança;
c) Estabelecer as regras de proteção dos bens de informação quanto aos acessos, backups etc.;
d) Monitorar o cumprimento das regras estabelecidas;
e) Responder pelas violações registradas e participar da decisão a ser tomada, quando da ocorrência de não conformidade;
f) Notificar não-conformidades de segurança.

Em algumas situações, principalmente no caso da TDW, os proprietários da informação são os clientes do grupo. Nestes casos, as empresas do grupo Synoro têm acesso a sistemas totalmente gerenciados pelos clientes, que passam a ser responsáveis pela segurança da informação disponível nestes sistemas.

1.2.2 Usuário da Informação

Cada usuário da informação terá a responsabilidade de:

a) Zelar por todo acesso a ambientes de informação de cada um dos projetos que participar com a sua identificação de acesso;
b) Respeitar e preservar o grau de confidencialidade da informação, divulgando-a exclusivamente para as pessoas autorizadas a terem esse conhecimento;
c) Utilizar os recursos tecnológicos (equipamentos, programas e sistemas) e as informações somente para desempenho das suas atividades profissionais, sendo assim vedado o seu uso para fins pessoais;
d) Assinar o Termo de Responsabilidade da Synoro e do cliente (quando houver) onde são estabelecidas as regras sobre o uso das informações;
e) Notificar não conformidades de segurança.

1.3 Termo de Responsabilidade

Todos os colaboradores e prestadores de serviço da Synoro deverão assinar um termo de responsabilidade, documento oficial da empresa que atesta o conhecimento e comprometimento com a política de segurança do Grupo Synoro. Anexo 1

2 Gestão de Ativos

Os ativos do Grupo Synoro são basicamente os seguintes:

- Ativos de informação – são divididos em quatro categorias:
    - Dados de projetos de desenvolvimento: são dados que possam vir a ser manipulados/tratados no desenvolvimento de projetos de sistemas de informação – estes dados são acessados exclusivamente para os projetos e os mesmos não são mantidos no Grupo Synoro.
    - Dados de processamento para terceiros - estes dados são de propriedade dos clientes mas ficam residentes em infra-estrutura administrada pelo Grupo Synoro.
    - Dados de processamento internos - são os dados utilizados pelos sistemas internos do Grupo Synoro (Contas a Pagar/Receber, Folha de Pagamento, Gestão de Caixa, Controle de Propostas/Pedidos, Documentos de Projetos, etc.).
    - Dados de processamento externos - são dados que residem nas aplicações oferecidas pelo grupo Synoro ao mercado e que pertencem aos usuários destas aplicações.

- Ativos físicos: equipamentos computacionais (Servidores, Notebooks, Impressoras, etc); equipamentos de comunicação (roteadores, modems, switches, telefones, etc.); equipamentos de infra estrutura (no-breaks, racks, filtros de linha, etc.) e equipamentos de escritório (mesas, cadeiras, etc.)

Os dados de processamento para terceiros, externos e internos residirão em sistemas com acesso controlado, seguindo as políticas de termos de uso e confidencialidade de cada serviço.

Os dados de projetos de desenvolvimento serão de responsabilidade do Gerente/Líder de cada projeto, que deverá seguir os critérios relativos ao nível de confidencialidade da informação (documentos em papel e/ou em formato digital) gerado/manipulado por sua equipe de acordo com a orientação do cliente.

A título de exemplo, utilizamos a tabela abaixo como referência de tipos de informação que o cliente deverá classificar:

1 – Pública
2 – Interna
3 – Confidencial
4 – Restrita

Conceitos:

- Informação Pública: É toda informação que pode ser acessada por usuários da empresa, clientes, fornecedores, prestadores de serviços e público em geral.
- Informação Interna: É toda informação que só pode ser acessada por funcionários da organização. São informações que possuem um grau de confidencialidade que pode comprometer a imagem da organização.
- Informação Confidencial: É toda informação que pode ser acessada por usuários da organização e por parceiros da organização. A divulgação não autorizada dessa informação pode causar impacto (financeiro, de imagem ou operacional) ao negócio da organização ou ao negócio do parceiro.
- Informação Restrita: É toda informação que pode ser acessada somente por usuários da organização explicitamente indicados pelo nome ou por área a que pertence. A divulgação não autorizada dessa informação pode causar sérios danos ao negócio e/ou comprometer a estratégia de negócio da organização.

Todo Gerente/Líder deve orientar sua equipe a não circularem informações e/ou mídias consideradas confidenciais e/ou restritas, como também não deixar relatórios nas impressoras, e mídias em locais de fácil acesso, tendo sempre em mente o conceito "mesa limpa", ou seja, ao terminar o trabalho não deixar nenhum documento (escrito ou digital) seja ele confidencial e/ou restrito sobre suas mesas.

3 Recursos Humanos

Serão adotados os seguintes procedimentos para funcionários, estagiários, temporários e prestadores de serviço:

a) Obter referências pessoais e profissionais;
b) Verificar a exatidão e inteireza do curriculum vitae, profissional e acadêmico;
c) Verificar idoneidade de crédito, nos órgãos competentes, como SERASA, SPC etc.;
d) Providenciar a assinatura do Termo de Responsabilidade, quando aplicável;
e) Providenciar o ajuste do perfil de acesso aos sistemas internos com os devidos login e senhas;
f) Providenciar a eliminação do acesso aos sistemas internos e de clientes, quando houver saída de pessoal, quer seja por demissão ou por suspensão de contrato;
g) Na demissão do funcionário ou no encerramento de contrato, emitir um termo, isentando o usuário de responsabilidade sobre a utilização do login que está sendo eliminado, após seu desligamento.

O Grupo Synoro se compromete em não acumular ou manter intencionalmente Dados Pessoais de Funcionários além daqueles relevantes na condução do seu negócio. Todos os Dados Pessoais de Funcionários serão considerados dados confidenciais. Dados Pessoais de Funcionários sob a responsabilidade do Grupo Synoro não serão usados para fins diferentes daqueles para os quais foram coletados. Dados Pessoais de Funcionários não serão transferidos para terceiros, exceto quando exigido pelo nosso negócio, e desde que tais terceiros mantenham a confidencialidade dos referidos dados, incluindo-se, neste caso a lista de endereços eletrônicos (e-mails) usados pelos funcionários do Grupo Synoro.

4 Segurança Física e do Ambiente

4.1 Área de Segurança

O Grupo Synoro tem seu perímetro de segurança estabelecido e possui as normas adequadas para proteção física do ambiente com adoção de proteções físicas e lógicas adequadas ao recinto de trabalho estabelecido. A área que armazena os equipamentos de rede e comunicação encontra-se isolada e seu acesso é controlado. O Grupo Synoro possui os equipamentos adequados a possíveis ameaças externas e a possível queda de energia por período determinado pelos equipamentos de proteção.

Todos os servidores das empresas do Grupo Synoro devem residir em provedores de infraestrutura de grande porte e com reputação reconhecida pelo mercado e devem estar protegidos por recursos de segurança compatíveis com a sensibilidade das informações que são armazenadas e processadas.

4.2 Controle e Entrada de Saída de Pessoas

O Grupo Synoro tem controle de entrada e saída de pessoas através de reconhecimento (biometria para os colaboradores) e posterior identificação dos mesmos (portaria eletrônica). O acesso ao ambiente de trabalho, fora dos horários de trabalho, é realizado através de autorização e com utilização de senha de acesso ao ambiente. Todos os ambientes de trabalho do Grupo Synoro encontram-se adequados aos trabalhos realizados, tendo sido vistoriados e recebido o certificado PPRA de acordo com a norma vigente. Da mesma maneira, o Grupo Synoro possui as certificações necessárias para funcionamento tais como dos Bombeiros entre outras.

Política de "Mesa Limpa"

Deverá ser implantada a política de mesa e tela limpas, procurando evitar que documentos contendo informações confidenciais ou restritas fiquem expostos para pessoas não autorizadas, nas mesas ou nas telas das estações de trabalho.

5 Gerenciamento das operações e comunicações

5.1 Documentação dos Procedimentos de Operação

A documentação de operação do Grupo Synoro possui dois focos distintos:

- Operação de projetos de clientes: estes projetos são desenvolvidos para os clientes e neste caso, o Grupo Synoro possui uma metodologia de trabalho, documentada e disponível para todos os seus consultores. Para cada projeto pode ser utilizada a metodologia específica de cada cliente e sempre utilizamos a política de segurança dos ambientes dos mesmos.
- Operação interna: todos os sistemas utilizados pelo Grupo Synoro tem sua documentação atualizada e disponível para os respectivos usuários. Os sistemas são utilizados na modalidade SaaS (Software as a Service) e possuem as respectivas políticas de segurança e confidencialidade da informação previstas em contrato.

5.2 Proteção contra códigos maliciosos e códigos móveis

É terminantemente proibido o uso de programas ilegais (“piratas”) no Grupo Synoro. Os usuários não podem, em hipótese alguma, instalar esse tipo de "software" (programa) nos equipamentos utilizados como ferramenta de trabalho (sejam eles próprios e/ou do Grupo Synoro).

Todas as estações de trabalho (PCs e /ou notebooks) dos colaboradores da empresa devem ter um antivírus instalado.

Todo arquivo em mídia proveniente de entidade externa o Grupo Synoro deve ser verificado por programa antivírus.

Todo arquivo recebido / obtido através do ambiente Internet deve ser verificado por programa antivírus.

O usuário não pode, em hipótese alguma, desabilitar o programa antivírus instalado nas estações de trabalho.

5.3 Cópias de Segurança

É responsabilidade dos próprios usuários a elaboração de cópias de segurança ("backups") de textos, planilhas, mensagens eletrônicas, e outros arquivos ou documentos, desenvolvidos pelos colaboradores, em suas estações de trabalho, e que não sejam considerados de fundamental importância para a continuidade dos negócios do o Grupo Synoro.

No caso das informações consideradas de fundamental importância para a continuidade dos negócios do Grupo Synoro é disponibilizado um espaço nos servidores da empresa onde cada usuário deverá manter estas informações.

Cópias de segurança dos sistemas utilizados pelo Grupo Synoro e dos respectivos servidores de rede são de responsabilidade da área de Infraestrutura e deverão ser feitas regularmente.

Ao final de cada mês também deverá ser feita uma cópia de segurança com os dados relativos ao fechamento do mês.

Gerenciamento de Segurança em Redes

A conexão do ambiente do Grupo Synoro com seus clientes é realizada através de VPN fornecida pelos próprios clientes, seguindo as especificações e segurança dos mesmos.

Nossa topologia de rede interna utiliza roteadores CISCO e TPLINK e, para alguns dos clientes, temos roteadores ou links dedicados.

5.4 Troca de Informações

Os usuários devem rever periodicamente todos os compartilhamentos existentes em suas estações de trabalho e garantir que dados considerados confidenciais e/ou restritos não estejam disponíveis a acessos indevidos. É de responsabilidade de cada colaborador manter e seguir as políticas de confidencialidade que o Grupo Synoro possui com os seus clientes no que se refere à troca de informações.

5.5 Monitoramento

Os softwares de segurança deverão manter registros sobre os acessos dos usuários, indicando, sempre que possível, o arquivo, o software, a data e a hora que foram acessados.

Os SGBDs – sistemas gerenciadores de bancos de dados deverão manter logs próprios que permitam a recuperação de informações, em qualquer situação.

6 Controle de Acesso

O controle de acesso aos sistemas que processam informações internas ou de terceiros da empresa será de responsabilidade da área de infraestrutura, que seguirá as diretrizes estabelecidas no procedimento de controle e solicitação de acesso do Grupo Synoro.

No caso de projetos de desenvolvimento o controle de acessos será de responsabilidade do cliente.

Devem existir mecanismos que permitam registros de acessos aos ambientes, indicando sempre que possível os recursos acessados, identificação de quem efetuou o acesso, data e hora do acesso, tentativas de acesso com senhas erradas, tentativas de acesso de estações de trabalho não permitidas, tentativas de acesso em horários não permitidos etc.

Devem ser criadas consultas e relatórios que permitam o monitoramento e gerenciamento dos acessos, pelo Grupo Synoro e quando necessário por auditores.

7 Aquisição, desenvolvimento e manutenção de sistemas de informação.

A diretoria da empresa é responsável pela definição de compra, substituição e/ou desenvolvimento de novos aplicativos de utilização interna e /ou externa. É também responsável pela aquisição e/ou substituição de equipamentos de informática e outros.

Qualquer necessidade de novos programas ("softwares") ou de novos equipamentos de informática (hardware) deverá ser discutida no mínimo por dois sócios da empresa.

Não é permitida a compra ou o desenvolvimento de "softwares" ou "hardwares" diretamente pelos colaboradores, sem prévia autorização dos sócios.

Qualquer nova aquisição, substituição e/ou desenvolvimento deverá atender a esta Política de Segurança da informação.

8 Senhas

Operação interna:

A senha é a forma de identificação e acesso do usuário, é um recurso pessoal e intransferível que protege a identidade do colaborador, evitando que uma pessoa se faça passar por outra.

O uso de dispositivos e/ou senhas de identificação de outra pessoa constitui crime tipificado no Código Penal Brasileiro (art. 307 – falsa identidade). Assim, com o objetivo de orientar a criação de senhas seguras, estabelecem-se as seguintes regras:

1) A senha é de total responsabilidade do colaborador, sendo expressamente proibida sua divulgação ou empréstimo, devendo a mesma ser imediatamente alterada no caso de suspeita de sua divulgação;

2) A senha inicial só será fornecida ao próprio colaborador, através de um e-mail fornecido de uso pessoal do colaborador e obrigatoriamente deve ser trocada no primeiro acesso. Não poderão ser fornecidas por telefone, comunicador instantâneo ou qualquer outra forma que não assegure a identidade do colaborador;

3) É proibido o compartilhamento de login para funções de administração de sistemas;

4) As senhas não devem ser anotadas e deixadas próximo ao computador (debaixo do teclado, colada no monitor, etc.);

5) As senhas deverão seguir os seguintes pré-requisitos definidos pelo time de Infra-estrutura

6) O acesso do usuário deverá ser imediatamente cancelado nas seguintes situações:
   a. - Desligamento do colaborador;
   b. - Mudança de função do colaborador;

c. - Quando, por qualquer razão, cessar a necessidade de acesso do usuário ao sistema ou informação.

7) Para os cancelamentos acima mencionados, o Depto Pessoal ficará responsável por informar prontamente o time de Infra-estrutura acerca dos desligamentos e mudança de função dos colaboradores.

Operação de projetos de Clientes:

Serão adotadas as políticas e procedimentos estabelecidos pelo Cliente.

9 E-mail e Telefonia

Em relação ao uso do e-mail e comunicação por voz, todos devem observar as seguintes regras abaixo transcritas:

1. O uso para fim pessoal deve ser de caráter resumido e objetivo. Todavia, é proibido o uso para ganho pessoal, malas diretas, "correntes", ameaças, assédio, entretenimento, dentre outros considerados impróprios, ilegais ou desnecessários para as atividades diárias;

2. E-mails de remetentes ou assuntos desconhecidos não devem ser abertos em nenhuma hipótese, sendo imediatamente reportados à infra estrutura

10 Uso da Internet

O uso da Internet pelos colaboradores é permitido e encorajado desde que seu uso seja aderente aos objetivos e atividades fins do negócio. Entretanto, Grupo Synoro tem uma política para o uso da Internet desde que os funcionários/colaboradores assegurem que cada um deles:

1. Uso razoável da Internet, sempre prezando pelo bom senso quanto aos sites acessados e tempo de utilização;

2. Usar o computador para executar quaisquer tipos ou formas de fraudes, ou software/música pirata;

3. Usar a Internet para enviar material ofensivo ou de assédio para outros usuários;

4. Baixar (download) software comercial ou qualquer outro material cujo direito pertença a terceiros (copyright), sem ter um contrato de licenciamento ou outros tipos de licenciamento;

5. Atacar e/ou pesquisar em áreas não autorizadas (Hacking);

6. Criar ou transmitir material difamatório;

7. Introduzir de qualquer forma um vírus de computador dentro da rede corporativa.

11 Monitoramento

Grupo Synoro reafirma que o uso da Internet é uma ferramenta valiosa para seus negócios. Entretanto, o mau uso dessa facilidade pode ter impacto negativo sobre a produtividade dos funcionários e a própria reputação do negócio.

Assim, todo e qualquer pode ser monitorado pelo Time de Infraestrutura , não havendo qualquer privacidade em relação ao tráfego de dados utilizados nas estações de trabalho dos colaboradores, tudo de modo a facilitar a transparência e o controle das atividades.

12 Gestão de Consequências

As violações da Política, Normas e Procedimentos de Segurança de Informação de segurança devem ser informadas imediatamente ao Comitê de Segurança, através do e-mail comitedeseguranca@synoro.com.br , sua identidade será mantida em sigilo.

Toda violação ou desvio será investigado para a determinação das medidas necessárias, visando à correção da falha ou reestruturação de processos. Exemplos que podem ocasionar sanções:

- uso ilegal de software; – introdução (intencional ou não) de vírus de informática;
- tentativas de acesso não autorizado a dados e sistemas;
- compartilhamento de informações sensíveis do negócio;
- divulgação de informações de Funcionários e das operações contratadas;

A não-conformidade com as diretrizes desta política e a violação de normas derivadas da mesma estão sujeitas às penas de responsabilidade civil e criminal. Dependendo do desvio ocorrido medidas disciplinares podem ser empregadas obedecendo a seguinte sequência:

- Advertências verbais com aconselhamento;
- Advertências escritas;
- Rescisão do contrato de trabalho ou prestação de Serviço;
- Rescisão do contrato de trabalho por justa causa.

A utilização adequada dessa política é de extrema importância para alertar e conscientizar o colaborador sobre as suas ações e as possíveis consequências.

A apuração dos fatos será conduzida pelo time do Comitê de Segurança e o Setor Administrativo, as evidências apuradas serão apresentadas ao corpo diretor do Grupo para se determinar as medidas disciplinares cabíveis.

13 Treinamento

Para efeito de treinamento e conscientização da Política de Segurança serão realizadas as seguintes ações:

a) Apresentação da Política de Segurança sempre que houver nova contratação na equipe, seja funcionário, terceiro, temporário, estagiário;
b) Treinamento semestral da Política de Segurança da Informação, podendo a mesma ser realizada através de meios digitais;
c) Reforço da política de segurança de informação nos encontros com colaboradores realizados do Grupo Synoro;
d) Comunicação formal por meio digital, sempre que houver mudança Significativa nesta Política.

13.1 Controles

A conscientização sobre segurança se refere à transmissão de conceitos de segurança, de diferentes maneiras, com o objetivo de fazer com que os usuários dos sistemas de informação do Grupo Synoro estejam mais cientes sobre o assunto e possam proteger de maneira adequada os ativos de informações e sistemas de informação da empresa. Serão adotados o programa de Treinamento dos processos.
Registros de participação de treinamentos serão feitos no aplicativo da Triibo dentro da comunidade Synoro.

13.2 Conteúdo do Treinamento de conscientização sobre SI

O Comitê de Segurança da Informação fornecerá o treinamento adequado de conscientização de segurança a todos os usuários dos sistemas de informação do Grupo Synoro.

Este treinamento pode abranger tópicos gerais, para todos os usuários, e conteúdo específico de conscientização de segurança para determinadas funções além de treinamentos voltados para desenvolvimento seguro para os desenvolvedores (OWASP TOP).

O treinamento deve abordar tópicos sobre a proteção adequada dos ativos e sistemas de informação.

O conteúdo específico deve ser definido com base nas necessidades e considerar os requisitos jurídicos, regulatórios e/ou contratuais.

Todo o programa de conscientização sobre segurança deve ser avaliado e aprovado pelo Comitê ou pessoa indicada.

13.3 Periodicidade

O treinamento de conscientização sobre segurança é obrigatório para todos os usuários que precisam de acesso aos ativos e sistemas de informação do Grupo Synoro.

O treinamento de conscientização sobre segurança deve ser concluído dentro de 30 (trinta) dias após o usuário receber o acesso inicial ao sistema ou rede de informações da instituição e uma reciclagem que ocorre nos meses de Janeiro.

13.4 Execução do Treinamento de conscientização sobre SI

O treinamento de conscientização sobre segurança deve ser oferecido de forma eficiente. O uso de treinamentos via Web pode ser considerado.

O Grupo Synoro deverá oferecer treinamentos de conscientização sobre segurança específicos para funções que exijam um treinamento adicional por conta do acesso necessário para a responsabilidade da função.

O Comitê de segurança da informação, o departamento de recursos humanos e a Direção Geral do Grupo devem garantir que a documentação mantida evidencie a conformidade com esta política.