Política de Segurança da Informação

Controle de Versões			
Versão	**Data**	**Autor**	**Notas da Revisão**
0.1	02/12/2016	Deborah Araujo Denis Ferreira Ezio Mendonça	-

Sumário

Dos Objetivos

O Gerenciamento da Segurança da Informação visa evitar o uso não autorizado dos ativos, viabilizar o acesso a informação da maneira correta, garantir a disponibilidade da informação e a confiabilidade das transações.

Quando um serviço é projetado, ele deve atender a vários requisitos de segurança já estabelecidos na política de organização da empresa. Este processo de gerenciamento da informação é baseado no ITIL V3 e na ISSO/IEC 27001, que estabelecem uma estrutura de etapas, para implantar um sistema de gerenciamento de segurança da informação. O principal produto deste processo é a Política de Segurança da Informação. O Gerenciamento de Segurança da Informação, nada mais é que, o alinhamento da segurança da TI com a segurança do negócio para garantir que a segurança da informação seja gerenciada de forma eficaz em todos os serviços e atividades do Gerenciamento de Serviços.

O Objetivo deste documento de Política de Segurança da Informação, é estabelecer diretrizes que permitam aos colaboradores e clientes da Gyntech Soluções seguirem padrões de comportamento relacionados à segurança da informação adequados às necessidades de negócio e de proteção legal da empresa e do indivíduo. Nortear a definição de normas e procedimentos específicos de segurança da informação, bem como a implementação de controles e processos para seu atendimento.

Preservar as informações da Gyntech Soluções quanto à:

- **Integridade:** garantia de que a informação seja mantida em seu estado original, visando protegê-la, na guarda ou transmissão, contra alterações indevidas, intencionais ou acidentais.
- **Confidencialidade:** garantia de que o acesso à informação seja obtido somente por pessoas autorizadas.
- **Disponibilidade:** garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário.

As diretrizes aqui estabelecidas deverão ser seguidas por todos os colaboradores, bem como os prestadores de serviço, e se aplicam à informação em qualquer meio físico ou suporte.

Esta política dá ciência a cada colaborador de que os ambientes, sistemas, computadores e redes da empresa poderão ser monitorados e gravados, com prévia informação, conforme previsto nas leis brasileiras. É também obrigação de cada colaborador manter-se atualizado em relação a esta política e aos procedimentos e normas relacionadas, buscando orientação do seu gestor sempre que não estiver absolutamente seguro quanto à aquisição, uso e/ou descarte de informações e equipamentos.

Das Responsabilidades Específicas

Dos Colaboradores em Geral

Compreende-se por colaborador toda e qualquer pessoa física, contratada por CLT ou prestadora de serviço, que exerça alguma função dentro ou fora da Gyntech Soluções. Será de inteira responsabilidade de cada colaborador, todo prejuízo ou dano que vier a sofrer ou causar a organização e/ou a terceiros, em decorrência da não obediência às diretrizes e normas aqui referidas.

Todo incidente que afete a segurança da informação deverá ser comunicado inicialmente à Gerência de Segurança para análise.

A Gyntech exonera-se de toda e qualquer responsabilidade decorrente do uso indevido, negligente ou imprudente dos recursos e serviços concedidos aos seus colaboradores, reservando-se o direito de analisar dados e evidências para obtenção de provas a serem utilizadas nos processos investigatórios, bem como adotar as medidas legais cabíveis.

O não cumprimento dos requisitos previstos nesta Política de Segurança da Informação acarretará violação às regras internas da organização e sujeitará o usuário às medidas administrativas e legais cabíveis.

Dos Gestores de Pessoas e Processos

Espera-se que todos os Gestores adotem postura exemplar em relação à segurança da informação, servindo como modelo de conduta para os colaboradores sob a sua gestão.

Atribuir aos colaboradores, na fase de contratação e de formalização dos contratos de trabalho e de prestação de serviços terceirizados, a responsabilidade do cumprimento da Política de Segurança da Informação da Gyntech Soluções. Exigir dos colaboradores a assinatura do Termo de Compromisso e Ciência, assumindo o dever de seguir as normas estabelecidas, bem como se comprometendo a manter sigilo e confidencialidade, mesmo quando desligado, sobre todos os ativos e informações da Gyntech Soluções.

Antes de conceder acesso às informações da instituição, exigir a assinatura do Acordo de Confidencialidade dos colaboradores e prestadores de serviços que não estejam cobertos por um contrato existente. Adaptar as normas, os processos, procedimentos e sistemas sob sua responsabilidade para atender a esta política.

Da Produção e Uso dos Ativos

Toda informação produzida ou recebida pelos colaboradores como resultado da atividade desenvolvidas pela Gyntech Soluções pertence à referida organização. As exceções devem ser explícitas e formalizadas em contrato entre as partes.

Os equipamentos de informática e comunicação, sistemas e informações são utilizados pelos colaboradores para a realização das atividades profissionais. O uso pessoal dos recursos é permitido desde que não prejudique o desempenho dos sistemas e serviços.

A Gyntech Soluções poderá registrar todo o uso dos sistemas e serviços, visando garantir a disponibilidade e a segurança das informações utilizadas.

Deve-se ter um plano de contingência e a continuidade dos principais sistemas e serviços, e estes deverão ser implantados e testados semestralmente, visando reduzir riscos de perda de confidencialidade, integridade e disponibilidade dos ativos de informação.

Do Monitoramento e Da Auditoria Do Ambiente.

Para garantir o cumprimento das regras e diretrizes aqui mencionadas, a Gyntech reserva-se ao direito de:

- Implantar sistemas de monitoramento nas estações de trabalho, servidores, conexões com a internet, dispositivos móveis e periféricos e outros componentes da rede – Toda

informação gerada por esses sistemas poderá ser usada para identificar usuários e respectivos acessos efetuados, bem como o que foi acessado;

- Tornar conhecidas as informações obtidas pelos sistemas de monitoramento, no caso de solicitação do gerente ou por determinação do Gerencia de Segurança da Informação;
- Realizar, sem aviso prévio, inspeção física nas máquinas de sua propriedade;
- Instalar sistemas de proteção para garantir a segurança das informações.

Internet

Qualquer informação que é acessada ou produzida na internet está sujeita a divulgação e auditoria. Portanto, a Gyntech, reserva-se ao direito de monitorar e registrar todos os acessos à internet.

As estações de trabalho e outros equipamentos fornecidos para o acesso à internet são de propriedade da Gyntech Soluções, e se necessário poderá pode analisar e bloquear qualquer arquivo, site, e-mail, domínio, palavra ou aplicação armazenados na internet, visando garantir o cumprimento de sua Política de Segurança da Informação.

A internet disponibilizada pela organização, pode ser utilizada para fins pessoais, desde que não prejudique a banda da rede e o andamento dos trabalhos desenvolvidos na empresa.

É proibida a divulgação ou compartilhamento indevido de informações da área administrativa em sites, redes sociais, ou qualquer outra tecnologia semelhante que venha surgir na internet.

Os colaboradores com acesso à internet poderão fazer o download somente de programas ligados diretamente às suas atividades e deverão providenciar o que for necessário para regularizar a licença e o registro desses programas. Qualquer software não autorizado baixado será excluído pela Gerência de Sistemas.

Os colaboradores não poderão em hipótese alguma utilizar os recursos da Gyntech para fazer o download ou distribuição de software pirateados, está atividade é considerada criminosa de acordo com a legislação brasileira.

Não é permitido em nenhuma circunstância o download, armazenamento, e/ou acesso a materiais de cunho sexual.

Não é permitido acesso a sites de proxy, e qualquer tentativa identificada de burlar o sistema deverá ser comunicada a gestão que deve avaliar e aplicar as devidas punições.

Identificação

Os dispositivos de identificação e senhas protegem a identidade do usuário, evitando que uma pessoa se faça passar por outra perante os sistemas de segurança da Gyntech e de Terceiros. O uso dos dispositivos e/ou senhas de identificação de outra pessoa é considerado crime tipificado no Código Penal Brasileiro.

Todos os dispositivos de identificação utilizados, sejam eles o número de registro do colaborador, o crachá, as identificações de acesso aos sistemas, os certificados e assinaturas digitais e os dados biométricos têm de estar associados a uma pessoa física. O usuário, vinculado a tais dispositivos identificadores, será responsável pelo seu uso.

Não é permitido, em hipótese alguma, que dispositivos de identificação sejam emprestados e compartilhados com outras pessoas, a responsabilidade do uso indevido é do usuário a que pertence a identificação. É proibido o compartilhamento de login para funções de administração de sistemas.

Todos os colaboradores devem ser identificados por meio de crachá, que deverá conter nome e cargo exercido por ele.

É de responsabilidade de cada usuário a memorização de sua própria senha, bem como a proteção e a guarda dos dispositivos de identificação que lhe forem atribuídos. As senhas não devem ser armazenadas em arquivos eletrônicos (Word, Excel, Notepad++ etc.). Os usuários que suspeitem que terceiros obtiveram acesso indevido ao seu login/senha, podem e devem fazer a alteração da própria senha.

Os sistemas administrativos devem forçar a troca das senhas dentro do prazo de 30 dias. A nova senha deve ser diferente da utilizada nos últimos 3 meses.

Todos os acessos devem ser bloqueados quando deixarem de ser necessários a função atual do usuário ou em caso de desligamento do mesmo.

Caso o colaborador esqueça sua senha, ele deverá requisitar formalmente a troca ou comparecer pessoalmente à área técnica responsável para cadastrar uma nova.

Equipamentos, Servidores e Estações de Trabalho

Os equipamentos disponíveis aos colaboradores são de propriedade da Gyntech Soluções, cabendo a cada um utilizá-los corretamente. É proibido todo procedimento de manutenção física ou lógica, instalação, desinstalação, configuração ou modificação, sem o conhecimento prévio e o acompanhamento de um técnico.

Todas as atualizações e correções de segurança do sistema operacional ou aplicações somente poderão ser feitas após a validação no ambiente de homologação, e depois de sua disponibilização pelo fabricante ou fornecedor.

Os sistemas e computadores devem ter versões do software antivírus instaladas, ativadas e atualizadas permanentemente. O usuário, em caso de suspeita de vírus ou problemas na funcionalidade, deverá acionar o departamento técnico responsável.

Arquivos pessoais ou não pertinentes ao negócio (fotos, músicas, vídeos, etc.) não deverão ser copiados/movidos para os drives de rede, pois podem sobrecarregar o armazenamento nos servidores. Caso seja identificado esse tipo de arquivo, a sua exclusão deve ser imediata não necessitando de aviso ao usuário proprietário.

Todos os arquivos indispensáveis para as atividades dos colaboradores na organização devem ser armazenados em drives de rede, para que possam ser recuperados caso ocorra uma falha no computador, sendo de responsabilidade do usuário. Os arquivos salvos em drives de rede serão backupeados para um servidor de backup em nuvem.

Para garantir a segurança durante o uso dos computadores, equipamentos e servidores, algumas regras devem ser atendidas.

- Todos os computadores de uso individual deverão ter senha de Bios para restringir o acesso de colaboradores não autorizados. Tais senhas serão definidas pela Gerência de Sistemas, que terá acesso a elas para manutenção dos equipamentos.
- Os colaboradores devem informar ao departamento técnico qualquer identificação de dispositivo estranho conectado ao seu computador.
- Deverão ser bloqueados com senhas, todos os computadores e impressoras quando não estiverem sendo utilizados.
- Todos os recursos tecnológicos adquiridos pela Gyntech Soluções devem ter imediatamente suas senhas padrões alteradas.

- Os equipamentos deverão manter preservados, de modo seguro, os registros de eventos, constando identificação dos colaboradores, datas e horários de acesso.

É proibido:

- Tentar ou obter acesso não autorizado a outro computador, servidores ou rede.
- Burlar quaisquer sistemas de segurança.
- Acessar informações confidenciais sem explícita autorização do proprietário.
- Abrir computadores ou outros equipamentos de informática para qualquer tipo de reparo que não seja realizado por um técnico.
- Consumir alimentos e bebidas nas estações de trabalho e próximo aos equipamentos.

Dispositivos Móveis

Por dispositivo móvel entende-se, qualquer equipamento eletrônico com atribuições de mobilidade de propriedade da instituição, ou aprovado e permitido por sua Gerência, como: notebooks, smartphones e pendrives.

Todo colaborador deverá realizar periodicamente cópia de segurança (backup) dos dados de dispositivo móvel utilizado para fins organizacionais. Deverá, também, manter estes backups separados de seu dispositivo móvel, seja em nuvem ou outro dispositivo de backup.

Todo colaborador deverá utilizar senhas de bloqueio automático para seu dispositivo móvel.

Não será permitida, em nenhuma hipótese, a alteração da configuração dos sistemas operacionais dos equipamentos sem a devida comunicação e a autorização da área responsável e sem a condução, auxílio ou presença de um técnico especializado.

É responsabilidade do colaborador, no caso de furto ou roubo de um dispositivo móvel fornecido pela Gyntech, notificar imediatamente seu gestor. Também deverá procurar a ajuda das autoridades policiais registrando, assim que possível, um boletim de ocorrência.

O colaborador que deseje utilizar equipamentos moveis particulares e conecta-los à rede da Gyntech deverá submeter previamente tais equipamentos ao processo de autorização da Gerência de Segurança da Informação.

Backup

Todos os backups devem ser automatizados por sistemas de agendamento para que sejam preferencialmente executados fora do horário comercial, períodos em que não há nenhum ou pouco acesso de usuários ou processos automatizados aos sistemas de informática.

As mídias de backup devem ser guardadas em local seco, climatizado e seguro, de preferência em cofres corta-fogo seguindo as normas da ABNT, e distantes o máximo possível do servidor de origem.

Os backups devem ser feitos seguindo política de backup da organização, e armazenados em no mínimo três mídias distintas, sendo uma delas a nuvem.

Testes de restauração de backup devem ser executados por seus responsáveis, nos termos dos procedimentos específicos, aproximadamente a cada 15 ou 30 dias, de acordo com a criticidade do backup. Os testes devem ser executados em um servidor de teste em local diferente do original, para que assim não sobreponha os arquivos válidos.

Para formalizar o controle de execução de backups e restores, deverá haver um formulário de controle das execução dessas rotinas, o qual deverá ser preenchido pelos responsáveis, nos termos da Política de Controle de Backup e Restore.