POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

1. Mensagem aos Stakeholders

Aos Colaboradores, Parceiros, Terceiros e Clientes,

Como fator crítico de sucesso, a ON LINE ENGENHARIA DE SISTEMAS LTDA. considera extremamente importante garantirmos a segurança das informações sob nossa responsabilidade.

Desta forma a ON LINE ENGENHARIA DE SISTEMAS LTDA. publica a sua POLÍTICA CORPORATIVA DE SEGURANÇA DA INFORMAÇÃO adequada aos nossos princípios e valores.

Este documento consiste em um conjunto de orientações que valorizam e definem o uso adequado das informações, possibilitando ambientes de TI seguros, confiáveis e íntegros.

Os pilares normativos de melhores práticas que sustentam a presente política são:

- ISO 27001:2013
- ISO 31000:2018
- Guia de CIS Controls (Center for Internet Security)
- COBIT
- AWS Well Architected Framework

O comprometimento de todos em conhecer e vivenciar esta política é de extrema importância para alcançarmos um padrão de excelência na gestão de segurança, proporcionando a evolução dos nossos negócios de forma cada vez mais transparente e segura.

2. Glossário

- **“Owner”/Dono:** Por “dono” entende-se o responsável pelo ativo e pelo risco.
- **Security Officer:** O Security Officer é o profissional responsável pela Segurança da Informação de uma instituição.
- **NDA – Non Disclosure Agreement”:** Trata-se de um acordo em que as partes que o assinam concordam em manter determinadas informações confidenciais.
- **Gestor:** Entende-se o líder de uma área em que existe o risco.
- **Risco:** É o efeito da incerteza nos objetivos. Um desvio em relação ao esperado. O risco é muitas vezes expresso em termos de uma combinação de consequências de um evento (incluindo mudanças nas circunstâncias) e a probabilidade de ocorrência associada.
- **Fonte de Risco:** Fonte de Risco é um “elemento que, individualmente ou combinado, tem o potencial intrínseco para dar origem ao risco (Nota: uma fonte de risco pode ser tangível ou intangível)”.
- **Ameaça:** Fonte tangível ou intangível de perdas.

3. Introdução

A adoção de políticas, normas e procedimentos que visem garantir a segurança da informação deve ser uma das prioridades do Compliance, reduzindo-se os riscos de falhas, os danos e/ou os prejuízos que possam comprometer a imagem e os objetivos da organização.

A informação pode existir e ser manipulada de diversas formas, ou seja, por meio de arquivos eletrônicos, mensagens eletrônicas, internet, bancos de dados, em meio impresso, verbalmente, em mídias de áudio e de vídeo, etc.

Por princípio, a segurança da informação deve abranger três aspectos básicos, destacados a seguir:

- **Confidencialidade:** somente pessoas devidamente autorizadas pela empresa devem ter acesso à informação.
- **Integridade:** somente alterações, supressões e adições autorizadas pela empresa devem ser realizadas nas informações.
- **Disponibilidade:** a informação deve estar disponível para as pessoas autorizadas sempre que necessário ou demandado.

Para assegurar esses três itens mencionados, a informação deve ser adequadamente gerenciada e protegida contra roubo, fraude, espionagem e perda não intencional, acidentes e outras ameaças.

Em geral, o sucesso da Política de Segurança da Informação adotada pela ON LINE ENGENHARIA DE SISTEMAS LTDA. depende da combinação de diversos elementos, dentre eles, a estrutura organizacional da empresa, as normas e os procedimentos

relacionados, à segurança da informação e à maneira pela qual são implantados e monitorados, os sistemas tecnológicos utilizados, os mecanismos de controle desenvolvidos, assim como o comportamento de diretores, colaboradores, associados e sócios.

4. Objetivo

Este documento tem como objetivo estabelecer a Política de Segurança da Informação da ON LINE ENGENHARIA DE SISTEMAS LTDA., definindo as diretrizes relacionadas à segurança da informação.

5. Escopo

Esta política abrange todos os sistemas, equipamentos e informações da ON LINE ENGENHARIA DE SISTEMAS LTDA., incluindo também seus colaboradores, estagiários, terceirizados, temporários e fornecedores em quaisquer das dependências da ON LINE ENGENHARIA DE SISTEMAS LTDA., ou locais onde estes se façam presentes, por meio da utilização, do manuseio ou do processamento eletrônico das informações.

6. Papéis e Responsabilidades

6.1. Comitê de Segurança da Informação e Compliance (CSIC)

Esse comitê deverá ser constituído pelos Diretores e CSO) com a atribuição de aprovar as diretrizes da Política de Segurança da Informação, assim como alterá-las conforme as necessidades da ON LINE ENGENHARIA DE SISTEMAS LTDA.. Portanto, a revisão e a manutenção desta política são de responsabilidade do comitê. A periodicidade da revisão será anual ou realizada no momento em que for conveniente para a ON LINE ENGENHARIA DE SISTEMAS LTDA..

Suas atribuições serão:

- Propor ajustes, aprimoramentos e modificações desta Política;
- Propor melhorias e aprovar as Normas de Segurança da Informação;
- Definir a classificação das informações pertencentes e/ou custodiadas pela ON LINE ENGENHARIA DE SISTEMAS LTDA. com base na política de classificação da informação;
- Analisar os casos de violação desta Política e das Normas de Segurança da Informação, comunicar à Diretoria Executiva, quando for necessário;
- Coordenar as ações dos Comitês Interdepartamentais viabilizando possíveis ajustes no plano de ação;
- Garantir o sucesso de implantação do Modelo de Gestão de Segurança da Informação considerando os atuais e futuros desafios;
- Realizar reuniões periódicas quando solicitadas, aprovar e propor adequações relacionados à melhoria da segurança da informação da ON LINE ENGENHARIA DE SISTEMAS LTDA..
- A coordenação dos trabalhos do CSIC caberá ao responsável pela área de Segurança da Informação, cujas atribuições abrangerão a convocação das reuniões e suporte às atividades desenvolvidas.
- As reuniões do CSIC devem ser realizadas semestralmente podendo haver convocação em frequência maior ou extraordinariamente, sempre que necessário e devem ser registradas em ata. De acordo com a necessidade, outros representantes de outras áreas da ON LINE ENGENHARIA DE SISTEMAS LTDA. e convidados externos poderão participar das reuniões do CSIC.

6.2. Segurança da Informação

Essa área será responsável pela gestão de todas as frentes de Segurança da Informação da ON LINE ENGENHARIA DE SISTEMAS LTDA.. Sua missão é estabelecer e utilizar uma metodologia para avaliar, implementar e monitorar as diretrizes de proteção dos bens de informações visando garantir a continuidade dos negócios e serviços da ON LINE ENGENHARIA DE SISTEMAS LTDA..

Suas atribuições serão:

- Viabilizar, controlar a implementação e divulgar, de forma corporativa, a Política, Normas e Padrões de Segurança da Informação para todos os colaboradores, a arquitetura e os processos pertinentes à Segurança da Informação.
- Elaborar, participar e propor ao Comitê de Segurança da Informação a arquitetura e os processos pertinentes à Segurança da Informação.
- Apoiar e disseminar a cultura de Segurança da Informação.
- Apoiar os auditores internos e, eventualmente, externos.
- Elaborar e divulgar as normas e procedimentos de Segurança da Informação, assim como mantê-los sempre atualizados.
- Elaborar e implementar projetos de suporte à Segurança da Informação.
- Definir e Implantar a arquitetura de acesso lógico aos softwares de Segurança da Informação com apoio da área de Tecnologia & Operações.

- Fornecer suporte técnico aos clientes/usuários regionais sobre aspectos de Segurança da Informação. Essas administrações regionais estão subordinadas tecnicamente a área de Segurança da Informação Corporativa.
- Assegurar em nível de software, o controle de acesso lógico aos recursos computacionais com apoio das áreas técnicas, monitorando todo o ambiente de segurança.
- Garantir que todos os procedimentos e controles de acesso lógico aos recursos de informática atendam às exigências de integridade, confiabilidade e confidencialidade dos dados e informações, assim como a continuidade das operações dos negócios.
- Assegurar a adequação, a efetividade e a eficácia das Tecnologias empregadas e as operações de segurança lógica como (hardwares, softwares, técnicas de criptografia, firewalls, autenticadores, antivírus e demais recursos pertinentes) e físicos (acesso biométrico, etc), com apoio da área de Tecnologia & Operações.
- Assegurar a definição das nomenclaturas e padrões de identificador de usuário (ID), logins e logons pela área de Tecnologia & Operações.
- Estabelecer e manter um processo de suporte aos proprietários, (owners) dos bens de informações e dos softwares aplicativos e suas plataformas quanto às revisões periódicas dos acessos concedidos pelos mesmos. As revisões são de responsabilidade dos próprios proprietários (owners) e sua periodicidade será semestral ou realizada a qualquer momento conforme solicitação/necessidade dos próprios owners.
- Analisar os riscos pertinentes à segurança da informação da ON LINE ENGENHARIA DE SISTEMAS LTDA. e apresentar relatórios sobre tais riscos ao CSIC.
- Realizar trabalhos de análise de vulnerabilidades, com intuito de assegurar o nível de segurança dos sistemas de informações e dos demais ambientes em que armazenam, processam ou transmitem as informações custodiadas da ON LINE ENGENHARIA DE SISTEMAS LTDA..
- Solicitar informações às demais áreas da ON LINE ENGENHARIA DE SISTEMAS LTDA. e realizar testes e avaliações de segurança, no intuito de verificar o cumprimento e aderência da Política de Segurança da Informação, sempre que necessário.

6.3. Proprietário da Informação

O proprietário da informação pode ser um diretor ou um gerente responsável pelo sistema ou processo da ON LINE ENGENHARIA DE SISTEMAS LTDA., os mesmos são responsáveis por estabelecer diretrizes de segurança da informação na Organização. A concessão, manutenção, revisão e cancelamento de autorizações de acesso a determinado conjunto de informações pertencentes à ON LINE ENGENHARIA DE SISTEMAS LTDA. ou sob a sua guarda envolve a área de Tecnologia & Operações e proprietário da informação.

Cabe ao proprietário da informação:

- Elaborar, para toda informação sob sua responsabilidade, matriz que relaciona cargos e funções da ON LINE ENGENHARIA DE SISTEMAS LTDA. às autorizações de acesso concedidas;
- Autorizar a liberação de acesso à informação sob sua responsabilidade, observadas a matriz de cargos e funções, a Política, Normas e Procedimentos de Segurança da Informação da ON LINE ENGENHARIA DE SISTEMAS LTDA.;
- Manter registro e controle atualizados de todas as liberações de acesso concedidas, determinando, sempre que necessário, a pronta suspensão ou alteração de tais liberações;
- Reavaliar, sempre que necessário, as liberações de acesso concedidas, cancelando aquelas que não forem mais necessárias;
- Analisar e fornecer os relatórios de controle de acesso fornecidos pela área de Tecnologia & Operações, com o objetivo de identificar desvios em relação à Política, as Normas e Procedimentos de Segurança da Informação, tomando as ações corretivas necessárias;
- Participar da investigação de incidentes de segurança relacionados à informação sob sua responsabilidade;
- Participar, sempre que convocado, das reuniões do Comitê de Segurança da Informação e Compliance (CSIC), prestando os esclarecimentos solicitados.

6.4. Recursos Humanos

Cabe ao Recursos Humanos:

- Colher a assinatura do Termo de Adoção da Política de Segurança da Informação de todos colaboradores (terceiros, estagiários, temporários, CLT's, associados, sócios e outros);
- Colher a assinatura do Termo de Sigilo e Confidencialidade (NDA) dos funcionários e estagiários, arquivando-o nos respectivos prontuários;
- Indicar, conforme o NDA, que existe a cessão de propriedade intelectual e não concorrência.
- Colher a assinatura do Termo de Sigilo e Confidencialidade específico para os colaboradores da área de Tecnologia & Operações;

- Comunicar à equipe de Tecnologia & Operações a existência de novos funcionários;
- Informar, prontamente, à equipe de TI (Controle de Acesso), todos os desligamentos, afastamentos e modificações no quadro funcional da empresa.

6.5. Processo de Divulgação da PSI

A Política de Segurança da Informação deve ser de conhecimento de todos os funcionários, estagiários, colaboradores, associados e sócios da organização, portanto deve ser amplamente divulgada, inclusive e principalmente para novos colaboradores. Os métodos de divulgação, serão:

- Campanhas internas de conscientização;
- Palestras de conscientização;
- Site público da ON LINE ENGENHARIA DE SISTEMAS LTDA.;
- Ou outra mídia definida pelo Comitê de Segurança da informação conforme necessidade da ON LINE ENGENHARIA DE SISTEMAS LTDA..

Uma vez que a Política de Segurança da Informação da ON LINE ENGENHARIA DE SISTEMAS LTDA. seja de conhecimento de todos, não poderá ser admissível que os colaboradores aleguem o desconhecimento das regras nelas estabelecidas.

7. Diretrizes

A seguir, são apresentadas as diretrizes da Política de Segurança da Informação da ON LINE ENGENHARIA DE SISTEMAS LTDA.. Tais diretrizes constituem os principais pilares da Gestão de Segurança da Informação da ON LINE ENGENHARIA DE SISTEMAS LTDA., norteando a elaboração das Normas e dos procedimentos.

7.1. Leis e Regulamentações

Cabe à Diretoria de Segurança da Informação e Compliance:

Manter as áreas da ON LINE ENGENHARIA DE SISTEMAS LTDA. informadas sobre eventuais alterações legais e/ou regulatórias que impliquem responsabilidade e/ou ações envolvendo a gestão de segurança da informação;

Incluir, na análise e na elaboração de contratos, sempre que necessárias cláusulas específicas relacionadas à segurança da informação, com o objetivo de proteger os interesses da ON LINE ENGENHARIA DE SISTEMAS LTDA.;

Avaliar, quando solicitada, as Normas e os Procedimentos de Segurança da Informação elaborados pelas diversas áreas da ON LINE ENGENHARIA DE SISTEMAS LTDA..

7.2. Classificação da Informação

O Comitê, representado por seus membros, é designado proprietário das informações custodiadas pela ON LINE ENGENHARIA DE SISTEMAS LTDA., com a responsabilidade da gestão da sua segurança durante todo o ciclo de vida da informação.

O Comitê deve classificar as Informações custodiadas pela ON LINE ENGENHARIA DE SISTEMAS LTDA. utilizando um dos seguintes níveis de Classificações de Informação:

- **Confidencial:** Informação que, se revelada a pessoas não autorizadas, pode ter um impacto significativo nas obrigações legais ou regulatórias, na condição financeira ou reputação, da ON LINE ENGENHARIA DE SISTEMAS LTDA. ou de seus clientes. Dados de autenticação como: senhas, PINs, chaves privadas de criptografia, informações sobre ou pertencente a clientes e funcionários, Informação que o Comitê de Segurança da Informação determina ter o potencial de fornecer uma vantagem competitiva ou ter um impacto significativo sobre a ON LINE ENGENHARIA DE SISTEMAS LTDA. se revelada a pessoas não autorizadas. A essas informações será utilizado o princípio do “Need to Know”, em que só serão fornecidas pelo proprietário da informação aos colaboradores que devem ter acesso a elas para a execução da sua atividade.
- **Interna:** Informação que é normalmente compartilhada dentro da ON LINE ENGENHARIA DE SISTEMAS LTDA., não é destinada a distribuição fora da ON LINE ENGENHARIA DE SISTEMAS LTDA. e não é classificada como RESTRITA ou CONFIDENCIAL.
- **Pública:** Informação que é livremente disponível fora da ON LINE ENGENHARIA DE SISTEMAS LTDA. ou é destinada a uso público pelo Comitê Corporativo. Cada gestor para o gerenciamento de risco dos processos sob sua responsabilidade deve seguir esta política através de práticas e procedimentos estabelecidos na ON LINE ENGENHARIA DE SISTEMAS LTDA. e em sua área.

Com base no processo de gerenciamento de risco, na classificação da informação, e na classificação da infraestrutura que a suporta, cada gestor deve especificar os requisitos para proteção da informação e deve implementar os controles suficientes para assegurar a proteção especificada.

7.3. Identificação e Autenticação

Todas as plataformas de Tecnologia & Operações da ON LINE ENGENHARIA DE SISTEMAS LTDA. devem autenticar a identidade de usuários (incluindo outros sistemas que acessam estas plataformas) antes de iniciar uma sessão ou transação, a menos que o usuário tenha direitos de acesso limitados a leitura de dados com classificação INTERNA ou PÚBLICA.

Todo usuário deve possuir uma identidade e ser identificado para cada plataforma de Tecnologia & Operações por:

- Um ID (Iogin) de usuário não compartilhado.
- Um método de autenticação que possibilite a identificação do usuário, por exemplo: senha única (estática) ou dinâmica, chave privada, dados biométricos ou outro mecanismo de autenticação homologado pelo Comitê Corporativo.
- Todo usuário é responsável por toda atividade associada com o login de usuário associados à sua identidade ou sob sua custódia.

Os usuários devem seguir as seguintes práticas para proteção de senhas estáticas:

- Nunca podem ser compartilhadas ou apresentadas a terceiros.
- Nunca podem ser apresentadas/escritas em claro (com exceção de senha pré-expirada, utilizada no processo de senha inicial).

Um processo documentado deve ser implementado para garantir que todas as senhas estáticas sejam mudadas periodicamente e que os IDs (Iogin) de usuário sejam desabilitados depois de um período definido de inatividade, compatível com o nível de risco, com a classificação da informação e com a classificação da infraestrutura correspondente. Com a aprovação do Comitê Corporativo, este requisito pode ser substituído por um processo de esclarecimento periódico dos usuários quanto à necessidade de troca de senhas para a garantia da eficácia deste método de autenticação.

7.4. Confidencialidade e Integridade

Os gestores devem informar a todos da ON LINE ENGENHARIA DE SISTEMAS LTDA., os clientes e os fornecedores, usuários em geral dos sistemas de informação e dos processos que todas as informações armazenadas, transmitidas ou manuseadas por estes processos e sistemas são de propriedade da ON LINE ENGENHARIA DE SISTEMAS LTDA. de seus clientes ou licenciadas por terceiros. Sempre que permitido pela legislação, a ON LINE ENGENHARIA DE SISTEMAS LTDA. reserva o direito de revisar e monitorar estas informações para fins administrativos, de segurança ou legais.

Informações confidenciais da ON LINE ENGENHARIA DE SISTEMAS LTDA., independentemente da mídia ou ambiente onde estejam sendo mantidas, devem ser protegidas contra acessos não autorizados e com as devidas aprovações. Este padrão se aplica, mas não está limitado, aos seguintes tipos de mídia ou ambiente, nos quais as informações estão contidas, registradas ou armazenadas: cartões, CD, DVD, cópia impressa, disco magnético, fita magnética, pen drive, microfilme, disco ótico, documentos em geral, equipamentos de processamento, de rede, Internet, etc.

Para a proteção adequada das informações custodiadas pela ON LINE ENGENHARIA DE SISTEMAS LTDA., que estão sendo manuseadas nas estações de trabalho, sempre que o colaborador se ausentar do ambiente, em particular fora do horário de trabalho, é sua responsabilidade bloquear a estação de trabalho, solicitar e utilizar os recursos disponibilizados pela ON LINE ENGENHARIA DE SISTEMAS LTDA. para proteger as informações de acessos não autorizados. Para a proteção adequada das informações custodiadas pela ON LINE ENGENHARIA DE SISTEMAS LTDA., que estão sendo manuseadas em equipamentos portáteis (notebook), todos os usuários devem cumprir os requerimentos definidos pela norma específica.

As informações classificadas como RESTRITA ou CONFIDENCIAL, no momento em que não forem mais úteis a ON LINE ENGENHARIA DE SISTEMAS LTDA. ou seus clientes, considerados os períodos de retenção estabelecidos por lei, regulamento ou contrato, devem ser destruídas segundo os procedimentos definidos. Cada gestor deve assegurar que Terceiros (clientes ou fornecedores) protejam adequadamente as informações custodiadas pela ON LINE ENGENHARIA DE SISTEMAS LTDA. às quais eles têm acesso.

Monitorando os Terceiros que armazenam, processam, gerenciam ou acessam as informações da ON LINE ENGENHARIA DE SISTEMAS LTDA. (exceto as informações classificadas como INTERNA ou PÚBLICA) ou têm conexão com os recursos de rede da ON LINE ENGENHARIA DE SISTEMAS LTDA., para que cumpram os padrões aqui definidos.

Realizando avaliações de segurança da informação nos Terceiros de acordo com os procedimentos aprovados pelo Comitê Corporativo.

Formalizando acordos de confidencialidade NDA – "Non Disclosure Agreement" ou disposições equivalentes, aprovados pela área jurídica da ON LINE ENGENHARIA DE SISTEMAS LTDA., com os Terceiros que armazenem, processem, gerenciem ou acessem informações custodiadas pela ON LINE ENGENHARIA DE SISTEMAS LTDA. (exceto informações classificadas corno PÚBLICA).

7.5. Adoção de Comportamento Seguro

Independentemente do meio ou da forma em que exista, a informação está presente no trabalho de todos os profissionais. Portanto, é fundamental para a proteção e salvaguarda das informações que os profissionais adotem comportamento seguro e consistente com o objetivo de proteção das informações da ON LINE ENGENHARIA DE SISTEMAS LTDA., com destaque para os seguintes itens:

- Sócios, colaboradores e prestadores de serviços devem assumir atitude proativa e engajada no que diz respeito à proteção das informações da ON LINE ENGENHARIA DE SISTEMAS LTDA..
- Todos na ON LINE ENGENHARIA DE SISTEMAS LTDA. devem compreender as ameaças externas que podem afetar a segurança das informações da empresa, tais como vírus de computador, interceptação de mensagens eletrônicas, grampos telefônicos etc., bem como fraudes destinadas a roubar senhas de acesso aos sistemas de informação.
- Todo tipo de acesso à informação da ON LINE ENGENHARIA DE SISTEMAS LTDA. que não for explicitamente autorizado é proibido.
- Assuntos confidenciais de trabalho não devem ser discutidos em ambientes públicos ou em áreas expostas (aviões, restaurantes, encontros sociais, elevadores, táxis, espaços de coworking, etc.).
- As senhas de usuário são pessoais e intransferíveis, não podendo ser compartilhadas, divulgadas a terceiros (inclusive colaboradores da própria empresa), anotadas em papel ou em sistema visível ou de acesso não-protegido.
- Somente softwares homologados pela equipe de TI da ON LINE ENGENHARIA DE SISTEMAS LTDA. podem ser instalados nas estações de trabalho, o que deve ser feito, com exclusividade, pela equipe de Tecnologia & Operações da ON LINE ENGENHARIA DE SISTEMAS LTDA., respeitando as questões legais de licenciamento;
- A política para uso de internet e correio eletrônico deve ser rigorosamente seguida;
- Arquivos de origem desconhecida nunca devem ser abertos e/ou executados;
- Documentos impressos e arquivos contendo informações confidenciais devem ser adequadamente armazenados e protegidos.
- Qualquer tipo de dúvida sobre a Política de Segurança da Informação e suas Normas deve ser imediatamente esclarecido com a área de Segurança Corporativa;
- Todas as normas de segurança da informação devem ser rigorosamente seguidas. Casos não previstos devem ser imediatamente submetidos para análise e a validação à área de Segurança Corporativa.

7.6. Avaliação dos Riscos de Segurança da Informação

A área de Segurança da Informação Corporativa deve realizar, de forma sistemática, a avaliação dos riscos relacionados à segurança da informação da ON LINE ENGENHARIA DE SISTEMAS LTDA..

A análise dos riscos deve atuar como ferramenta de orientação ao Comitê Corporativo de Segurança da Informação, principalmente, no que diz respeito à:

- Identificação dos principais riscos aos quais as informações da ON LINE ENGENHARIA DE SISTEMAS LTDA. estão expostas;
- Priorização das ações voltadas à mitigação dos riscos apontados, tais como implantação de novos controles, criação de novas regras e procedimentos, reformulação de sistemas etc. O escopo da análise/avaliação de riscos de segurança da informação pode ser toda a organização, partes da organização, um sistema de informação específico, componentes de um sistema específico etc.
- Planejamento trimestral de identificação e análise dos riscos, podendo ser alterado o ciclo de análise conforme definido pelo Comitê de Segurança da Informação.
- Implantação de ferramentas para identificação de riscos e compliance.

7.7. Gestão de Acesso a Sistemas de Informação e a Outros Ambientes

Todo acesso às informações e aos ambientes lógicos e físicos da ON LINE ENGENHARIA DE SISTEMAS LTDA. deve ser controlado, de forma a garantir acesso apenas às pessoas autorizadas pelo respectivo proprietário da informação. A política de controle de acesso deve ser documentada e formalizada por meio de Normas e Procedimentos que contemplem, pelo menos, os seguintes itens:

- Procedimento formal de concessão e cancelamento de autorização de acesso do usuário aos sistemas de informação;
- Comprovação da autorização do proprietário da informação;
- Utilização de identificadores de usuário (ID de usuário) individualizados, de forma a assegurar a responsabilidade de cada usuário por suas ações;
- Verificação se o nível de acesso concedido é apropriado ao propósito do negócio e se é consistente com a Política de Segurança da Informação, as Normas e Procedimentos;
- Remoção imediata de autorizações dadas a usuários afastados ou desligados da empresa, ou que tenham mudado de função;
- Processo de revisão periódica das autorizações concedidas;

- Política de atribuição, manutenção e uso de senhas.

7.8. Monitoração e Controle
Os equipamentos, os sistemas, as informações e os serviços utilizados pelos usuários são de exclusiva propriedade da ON LINE ENGENHARIA DE SISTEMAS LTDA., não podendo ser interpretados como de uso pessoal.

Todos os profissionais da ON LINE ENGENHARIA DE SISTEMAS LTDA. devem ter ciência de que o uso das informações e dos sistemas de informação da ON LINE ENGENHARIA DE SISTEMAS LTDA. pode ser monitorado, e que os registros assim obtidos poderão ser utilizados para detecção de violações da Política, as Normas e Procedimentos de Segurança da Informação e, conforme o caso, servir como evidência em processos administrativos e/ou legais.

7.9. Grupo de Resposta a Incidentes de Segurança (GRIS)
A área de Segurança da Informação, em conjunto as áreas de Tecnologia & Operações e Segurança da Informação, são responsáveis por manter procedimentos para os processos de Gerenciamento de Incidente e de Resposta a Incidente de Segurança (GRIS).

Os gestores devem assegurar que todos os sistemas de informação que armazenam informações custodiadas (confidenciais) pela ON LINE ENGENHARIA DE SISTEMAS LTDA. usam trilhas de auditoria para registrar e reportar:

- Todas as tentativas de violação da segurança do sistema.
- Todos os eventos significativos relacionados à administração do sistema bem como a segurança das transações e informações custodiadas (confidenciais) pela ON LINE ENGENHARIA DE SISTEMAS LTDA..
- O nível de detalhe das trilhas de auditoria deve ser compatível com o nível de risco do processo associado.
- Os gestores devem assegurar que as trilhas de auditoria sejam revisadas periodicamente de forma compatível com o nível de risco do processo associado. O processo de revisão deve ser segregado para assegurar que os revisores não revisem sua própria atividade.
- Qualquer atividade suspeita deve ser imediatamente verificada e tomadas as ações corretivas necessárias.

7.10. Treinamento e Conscientização de Segurança da Informação
Cada gestor deve garantir que todos da ON LINE ENGENHARIA DE SISTEMAS LTDA. e os fornecedores, ao iniciar a relação com a ON LINE ENGENHARIA DE SISTEMAS LTDA. ou quando tiverem alteração significativa na responsabilidade do trabalho, recebam treinamento sobre aspectos de segurança da informação relacionados a sua função dentro de 30 dias do início do trabalho.

Os gestores devem assegurar que todos os colaboradores da ON LINE ENGENHARIA DE SISTEMAS LTDA. e de fornecedores recebam anualmente material de conscientização aprovado pelo Comitê Corporativo sobre Segurança da Informação.

7.10. Auditoria
O processo de auditoria de verificação de conformidade dos sistemas existentes será executado semestralmente, ou a qualquer momento de acordo com a necessidade do negócio, para garantir que todas as partes estão executando corretamente as suas atividades e garantir que todos os outros requisitos de Segurança da Informação estão sendo constantemente observados. A auditoria poderá ser realizada por auditor externo ou equipe interna, seguindo a programação de auditoria estabelecida pelo Security Officer.

Obs: Neste processo será observada a independência do auditor com os processos a serem auditados.

O Security Officer deverá planejar a correção dos itens de não conformidade identificados nas auditorias com envolvimento das equipes responsáveis pelas não conformidades.

7.12. Grupo de Resposta a Incidentes de Segurança (GRIS)
Todas as áreas devem garantir que todos os produtos, serviços ou aplicativos sob gestão da ON LINE ENGENHARIA DE SISTEMAS LTDA., que usam a Internet para conexão ou comunicações, seguem o processo de avaliação de vulnerabilidade de aplicativos aprovado pelo Comitê Corporativo.

Problemas classificados como de alto risco, identificados em teste de vulnerabilidade, devem ser resolvidos antes que o produto, serviço ou aplicativo entre em produção ou que as atualizações sejam implantadas no ambiente de produção. O gestor responsável pelo produto, serviço ou aplicativo deve manter registro de todas as ações tomadas para resolver os problemas de alto risco identificados.

Os gestores da área de Tecnologia & Operações devem assegurar que, a cada mudança significativa e no mínimo anualmente, sejam realizados testes de vulnerabilidade dos componentes sob sua responsabilidade.

7.13. Produtos e Serviços de Gerenciamento da Segurança

Sistemas de detecção de invasão e demais produtos e serviços de segurança da informação só podem ser contratados se aprovados pelo Comitê Corporativo de Segurança da Informação.

Todos os alarmes de sistema associados a Segurança da Informação e eventos de segurança gerados sejam registrados e arquivados diariamente.

Quando ocorrer um Evento de Segurança, o Grupo de Resposta a Incidente de Segurança (GRIS) deve ser acionado através do processo e procedimento definidos pela área de Segurança da Informação.

Os controles da área TI devem assegurar que todas as conexões IP a Terceiros são protegidas por firewalls gerenciados pela Tecnologia & Operações ou ao menos submetidos a Diretoria de Segurança e Compliance.

8. Violações da Política e Sanções

Nos casos em que houver violação desta Política, as Normas e Procedimentos de Segurança da Informação, sanções administrativas e/ou legais poderão ser adotadas, podendo culminar o desligamento do profissional e ou eventuais processos criminais, se aplicáveis.

Qualquer caso de não cumprimento da política de segurança da informação da ON LINE ENGENHARIA DE SISTEMAS LTDA., por uma área, cliente ou fornecedor, deve ser documentado seguindo o processo correspondente definido pela área de Segurança da Informação. Deve e é necessário indicar a razão do não cumprimento/violação, os controles compensatórios dos riscos residuais relacionados, e deve ser aprovado tanto pelo membro do Comitê Executivo responsável pela área quanto pelo Diretor Executivo da ON LINE ENGENHARIA DE SISTEMAS LTDA..

No caso de um cliente optar por não cumprir algum padrão estabelecido pela ON LINE ENGENHARIA DE SISTEMAS LTDA., deve formalizar esta decisão através de um Termo de Sigilo e Confidencialidade onde estejam claras as responsabilidades e ônus da decisão.

9. Gestão de Continuidade de Negócios

O processo de gestão de continuidade de negócios da ON LINE ENGENHARIA DE SISTEMAS LTDA. é estabelecido por um conjunto de políticas, normas e práticas operacionais que seguem os princípios da NBR ISO 22301, o objetivo do processo de gestão de continuidade de negócios é garantir que os processos críticos tenham continuidade, atendendo aos requisitos mínimos operacionais e evitando impactos nos negócios da ON LINE ENGENHARIA DE SISTEMAS LTDA. e seus clientes.