PL 18.04

Política de Segurança da Informação da Sonda para Clientes e Parceiros

1 Objetivo

Este documento tem como objetivo apresentar a Política de Segurança da Informação da SONDA para seus clientes e parceiros, compartilhando as diretrizes relacionadas à segurança da informação, a fim de proteger as informações com base nos requisitos legais, contratuais e de negócios, utilizando as diretrizes estabelecidas na política principal de Segurança da Informação da SONDA PL 18.01 – Política de Segurança a Informação e também a PL 18.02 – Política de Gerenciamento de Riscos, provendo os mecanismos para prevenir e responder às ameaças, incluindo acessos não autorizados, uso indevido, duplicação, perda, modificação e revelação das informações de propriedade e associadas ao(s) negócio(s) da SONDA.

2 Aplicação

Este documento se aplica a todos clientes e fornecedores da SONDA, estabelecendo as regras a serem seguidas durante a execução das atividades definidas para os mesmos.

3 Escopo

Esta política abrange todos os sistemas, equipamentos e informações da SONDA, incluindo também seus profissionais que possuem relação com os clientes, fornecedores e parceiros da SONDA, em quaisquer das dependências, seja da SONDA, ou locais onde estes se façam presentes, por meio da utilização, do manuseio ou do processamento eletrônico das informações.

4 Responsabilidades

A integridade e coerência são princípios básicos das ações na SONDA, bem como a adoção de melhores práticas de segurança para garantir a confidencialidade, a integridade e a disponibilidade das informações do(s) negócio(s) da SONDA e de seus clientes. Portanto, o valor da informação para os processos de negócio da SONDA é inquestionável.

Para a SONDA, a Segurança da Informação é um dos seus principais valores, bem como faz parte dos fatores críticos de sucesso associados à credibilidade e aos processos de negócios da Empresa e em reconhecimento a estes fatos, a Área de Segurança da Informação é a responsável pelas questões de segurança, porém, é responsabilidade de todos os profissionais, assim como seus clientes e parceiros, cumprir com todas as diretrizes definidas neste documento.

5 Tratamento de Exceções

Toda e qualquer exceção a esta política deve ser apresentada à área de Segurança da Informação da SONDA, que a discutirá e avaliará, podendo, posteriormente, levá-la ao Comitê de Segurança da Informação. Todas as exceções serão discutidas com a Alta Direção da Empresa.

O registro das exceções será realizado através de carta de risco formalizada com o cliente, fornecedor ou gerente responsável pela exceção.

6 Dúvidas, Sugestões e Comunicações de Incidentes

A equipe de Segurança da Informação é responsável pelo esclarecimento de dúvidas e pela

recepção de sugestões. Também é responsável por manter e atualizar a Política Corporativa de Segurança da Informação da SONDA, juntamente com o Comitê de Segurança da Informação. As dúvidas, sugestões e comunicação de incidentes de segurança da informação deverão ser enviadas para o endereço segurancainfo.qualidade@sonda.com.

7 Apoio ao Processo

Apesar da disponibilidade de inúmeras ferramentas de proteção na área da Segurança da Informação, muitas das tarefas necessárias para a proteção da Informação não podem ser realizadas sem a participação dos profissionais das organizações.
A adesão de todos os profissionais, fornecedores e clientes da SONDA são essenciais para que o Sistema de Gestão de Segurança da Informação consiga proteger o negócio.

8 Responsabilidades com a Segurança da Informação

8.1 Security Office

A área de Qualidade | Segurança da Informação (Security Office), é gerenciada pelo *Information Security Officer* da organização. Todos os pontos relativos à Segurança da Informação são obrigatoriamente relatados para a área.
O *Infomation Security Officer* tem a função de aconselhar a Alta Direção e de orientar os níveis gerenciais envolvidos sobre as questões relativas à Segurança da Informação, sejam elas de clientes, fornecedores ou da SONDA, no intuito de minimizar os riscos existentes.
Refletindo este compromisso, esta área irá estabelecer Políticas, Padrões, Normas, Procedimentos e outros requisitos aplicáveis, provendo treinamento e conscientização de Segurança para os profissionais da SONDA, bem como para clientes e fornecedores, quando pertinente.
Periodicamente, será elaborado um relatório para a Alta Direção com o status atual da Segurança da Informação da SONDA.
O planejamento de contingência das informações é responsabilidade do custodiante, definido no item 11.3 desta política, e a área de Segurança da Informação proverá consultoria técnica para permitir a criação de procedimentos de emergência e recuperação de desastre.
A área é responsável por coordenar a resposta a incidentes e emergências de segurança, em conjunto com as áreas envolvidas, permitindo ações efetivas de combate a infecções por vírus, invasões, falhas de sistemas e outros problemas similares de segurança da informação.

8.2 Responsável Pela Informação

Os diretores, gerentes e coordenadores ligados diretamente a um diretor da SONDA são designados como responsáveis por todas as informações usadas para o desenvolvimento das atividades do grupo de profissionais que atua nos projetos ou áreas sob sua gerência.
Cada informação produzida na empresa deverá ter um responsável. Quando o responsável da informação não estiver claramente definido, o *Information Security Officer* ajudar a designá-lo. Por definição, as informações pertinentes a projetos sendo executados são de responsabilidade do gerente do projeto.
Os responsáveis pela informação tomam a decisão pela organização nos seguintes aspectos:

- Aprovar a concessão de privilégios de acesso à informação por cargo ou função;
- Aprovar as requisições de concessão e acesso que não estão no escopo dos cargos ou funções existentes;

- Definir o tempo de retenção da informação, de acordo com a conformidade legal específica do documento;
- Selecionar controles específicos necessários para proteger a informação, como um número mais frequente de realização de backups ou a necessidade de criptografia;
- Aprovar todas as novas ou diferentes formas de uso e classificação da informação;
- Aprovar todos os novos sistemas ou modificações nos sistemas existentes que utilizam à informação de sua posse antes da operacionalização do novo ambiente;
- Aderir as novas regras sistêmicas da Política de Segurança da Informação que possam estar relacionadas aos documentos sob sua responsabilidade;
- Verificar e corrigir problemas relatados com o uso corrente das informações sobre sua posse;
- Colaborar na apuração dos incidentes relacionados com os documentos sob sua sugestão, preservando as provas e relatando ao *Information Security Officer* todos os registros necessários para o enfrentamento;
- Classificar a informação de acordo com a sua criticidade, para permitir o tratamento adequado pelos usuários. Revisar esta classificação anualmente;
- Permitir a execução correta do plano de continuidade de negócios.

Os responsáveis pelas informações têm por obrigação designar um funcionário da sua área como substitutos de suas atividades, em caso de indisponibilidade. Os responsáveis não podem delegar suas responsabilidades para organizações terceiras, como outsourcing, ou para qualquer outro indivíduo que não seja funcionário da SONDA. Quando ambos, o responsável e o substituto, não estiverem presentes, a responsabilidade pela gestão será atribuída ao funcionário hierarquicamente superior.

8.3 Custodiantes

Custodiantes são as pessoas designadas pelos responsáveis pela informação que possuem as seguintes responsabilidades:

- Selecionar as tecnologias existentes para proteção da informação, de acordo com a sua criticidade, permitindo a escolha pelo responsável pela informação das opções apropriadas para a proteção da informação. Definir a arquitetura de sistemas adequada e prestar consultoria tecnológica para os responsáveis pela informação, permitindo que os sistemas da informação sejam construídos e operem da melhor forma para atingir os objetivos de negócios.
- Se requisitado, poderá prover relatórios para os responsáveis pela informação e ao *Information Security Officer* sobre os sistemas da informação e os problemas de segurança da informação identificados.
- Proteger a informação de sua posse, inclusive por meio da implementação de sistemas de controle de acesso para prevenir a divulgação não autorizada e o desenvolvimento, documentação e teste dos planos de continuidade de negócios.

O Gerente de Operação atuará como custodiante em muitos casos. Se o custodiante não estiver claramente definido, o *Information Security Officer* poderá ajudar o custodiante da informação.

8.4 Usuários da Informação

Os requisitos de segurança, definidos pelos responsáveis pela informação e implementados pelos custodiantes ou estabelecidos pela Gestão de Segurança da Informação, devem ser obrigatoriamente seguidos por todos os usuários.

Os usuários devem estar familiarizados com todos os requisitos de Segurança da Informação da SONDA, devendo participar dos treinamentos e dos processos de conscientização de Segurança da Informação.
Os usuários devem solicitar os acessos ao seu superior imediato e reportar todas as atividades suspeitas ou vulnerabilidades de segurança da informação.

9 Auditorias

O processo de auditoria de verificação de conformidade dos sistemas existentes deverá ser executado no mínimo uma vez ao ano, 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 em conformidade.
Esta atividade poderá ser realizada pelo auditor externo e pela área de Qualidade | Experiência Cliente, responsável pela equipe de auditores internos da SONDA, seguindo a programação de auditoria estabelecida pela área em conjunto com o *Information Security Officer*. Caso o processo de auditoria seja realizado pelo *Information Security Officer*, o resultado final deverá ser validado formalmente pela Gerente da área de Qualidade | Experiência Cliente.
A auditoria será comunicada para as áreas sempre que não existir requisitos de confidencialidade através de relatórios de auditorias conforme a PL 10.01 – Política de Auditorias Internas.
Em caso de dúvidas poderá ser solicitado pedido de esclarecimentos sobre os procedimentos adotados que deverão ser respondidos ao solicitante com o prazo de 5 (cinco) dias.
As auditorias realizadas são apresentadas à alta direção da SONDA, através da reunião anual de análise crítica para tomada de decisão com base nas informações fornecidas.

10 Privacidade

10.1 Gestão da Privacidade

Para gerenciar os sistemas e garantir a Segurança da Informação, a SONDA poderá auditar os registros existentes nos sistemas e na rede, inclusive os registros de acesso à Internet, e utilizar todas as informações armazenadas nos seus sistemas.
A Área de Segurança de Informação, no exercício de suas atribuições, poderá auditar todas as informações existentes na SONDA, incluindo telefones discados, sites visitados, endereços e conteúdo de e-mail recebidos e/ou enviados por meio de seu servidor e softwares instalados.
A SONDA no exercício do seu poder diretivo preceituado no artigo segundo da CLT, assegura que:

- O exercício do seu poder diretivo não deve ser apenas de ordem econômica, mas técnica, ou seja, cabe ao empregador determinar as normas de caráter técnico às quais o empregado está subordinado;
- O poder diretivo disciplinar é o direito do empregador de impor sanções disciplinares ao empregado, uma vez que o direito de propriedade assegura o poder hierárquico e disciplinar;
- O poder diretivo de controle sobre o trabalho, que dá, ao empregador, o direito de fiscalizar o trabalho do empregado, sendo estendida não só ao modo de trabalhar, mas também ao comportamento do empregado;
- Nenhum empregado ou profissional poderá presumir que todo dado, informação ou senha que possibilite acesso, edição ou compartilhamento, por meio da infraestrutura de tecnologia da informação da SONDA, seja de sua exclusiva privacidade.

As áreas de acesso restrito da SONDA têm monitoramento por circuito interno de TV e com o devido armazenamento das imagens para posterior análise em casos de incidentes.

O conteúdo de todo e qualquer diretório pode ser auditado a qualquer momento, bem como de todo documento impresso disponível em um lugar de livre acesso.
Toda e qualquer auditoria realizada será devidamente registrada e relatada ao Gerente e/ou Coordenador da área e às partes auditadas, oportunamente.

10.2 Coleta de Dados

A SONDA não coleta dados que não sejam necessárias para o desenvolvimento ou no exercício do poder diretivo do negócio. No caso de projetos, a SONDA coleta somente as informações de seus clientes com a sua devida autorização por meio de assinatura prévia de acordo NDA (Non Disclosure Agreement).

10.3 Privacidade da Informação de Terceiros

Uma grande variedade de clientes e parceiros confiam a sua informação à SONDA, para o desenvolvimento de seus respectivos negócios, e todos os profissionais da SONDA têm a responsabilidade de assegurar a preservação a privacidade e a segurança destas informações, nos termos do artigo 5, inciso X da Constituição Brasileira.
Os dados e informações de titularidade dos clientes não podem ser divulgadas ou distribuídas para terceiros, exceto por autorização por escrito do cliente. Exceções serão avaliadas pela área de comunicação da SONDA.

11 Uso de Software e Recursos de Tecnologia

11.1 Uso de Software

O uso de software é regulamentado por legislação específica ou pelos termos da respectiva licença de uso. Desta forma, alguns cuidados devem ser tomados para garantir a continuidade do negócio da SONDA.
Caso o empregado, prestador de serviço, fornecedor, profissional ou cliente, tenha necessidade de instalar algum software para uso pessoal ou corporativo, além daqueles que estão em uso para suas atividades, deverá solicitar formalmente chamado fácil (https://chamadofacil.sondait.com.br).
É vedada a instalação e/ ou remoção de softwares nos equipamentos da SONDA, salvo com o consentimento formal da equipe de Suporte Técnico da área de Tecnologia da Informação.
É vedado manter cópia não licenciada de software de terceiros, preservar mídias com músicas, imagens e vídeos protegidos por direito autoral, salvo em caso de cópia de salvaguarda mantida pelo responsável pela informação e/ou custodiante. Assim como a manutenção nas dependências da SONDA de CD's, DVD`s ou outras mídias de cópias não autorizadas de software licenciados, músicas e vídeos, mesmo que destinados para uso pessoal.

11.2 Uso de Recursos de Tecnologia

A SONDA considera como estações de trabalho quaisquer equipamentos de sua propriedade colocados à disposição de seus profissionais pela área de Tecnologia da Informação, vinculados aos domínios e grupos de trabalho disponibilizados. Assim, desktops, laptops, notebooks, PDAs (Personal Digital Assistant), VDI, dispositivos móveis de comunicação, e celulares são considerados estações de trabalho.
A SONDA considera como equipamentos de rede quaisquer equipamentos de sua propriedade necessários ao acesso, preservação e compartilhamento e segurança das informações entre as redes

internas da SONDA, Internet, ou compartilhadas com parceiros e fornecedores, tais como switches, roteadores, firewalls e equipamentos detectores de intrusos (do inglês *Intrusion Prevention System* - IPS).

Todos os servidores e estações de trabalho devem ser obrigatoriamente associadas aos domínios de controle definidos pela área de Tecnologia da Informação. É vedada a utilização de estações de trabalho que não estejam associadas a algum domínio de responsabilidade da SONDA nas redes da Empresa, salvo em condições previamente aprovadas pela equipe de Segurança da Informação.

Os profissionais e terceiros não devem utilizar computadores, dispositivos móveis e periféricos pessoais, tais como discos externos, PDAs, laptops, impressoras, bem como software pessoal nas redes da SONDA, salvo com autorização prévia da equipe de Segurança da Informação.

Todos os servidores, estações de trabalho e equipamentos de rede da SONDA devem obrigatoriamente apresentar aviso de advertência no processo de logon (banner) onde deverá constar de forma detalhada as condições de uso da infraestrutura de tecnologia da informação da SONDA.

Os servidores e equipamentos de rede críticos da Empresa têm que estar em local fisicamente protegido, que possua condições de temperatura e umidade adequadas ao bom funcionamento destes. É responsabilidade da área de Tecnologia da Informação garantir estas condições. Para sites remotos, onde não exista infraestrutura física adequada, é necessário considerar o uso de cofres e racks com controle de acesso.

As manutenções e intervenções realizadas por terceiros nos equipamentos de rede e servidores requer acompanhamento obrigatório por pessoal especializado da SONDA. Todas as intervenções devem ser registradas por meio de procedimento de gestão de mudança e devem ser solicitadas / agendadas pelo processo de requisição de serviço, via one touch.

O transporte de equipamentos que em sua característica não possuem mobilidade natural, tais como servidores, desktops, switches e roteadores só poderá ser realizado após liberação formal da área de Tecnologia da Informação e sob acondicionamento adequado.

11.3 Armazenamento de Informações

Proteger a informação também implica armazená-la de forma adequada de modo a coibir acessos não autorizados. Assim, alguns cuidados no armazenamento, para que as informações não sejam perdidas ou expostas, devem ser considerados:

- Nenhuma informação vital ao negócio deve ser armazenada localmente nos computadores ou dispositivos móveis. A SONDA disponibiliza mecanismos de armazenamento das informações em diretórios de rede, sendo que estes mecanismos devem apresentar opções de redundância, controle e registro de acesso definidos pela área de TI, bem como cópias de segurança, salvo os casos excepcionalmente analisados e aprovados pela área de Tecnologia da Informação.
- Os arquivos não relacionados ao trabalho, tais como fotos, vídeos, músicas e software não licenciados não podem ser armazenados em servidores, diretórios de rede e estações de trabalho.
- Softwares de instalação, mesmo com as devidas licenças, não devem ser armazenados nos diretórios de rede e sim em mídias adequadas como CD's, DVD`s ou fitas de backup. Apenas os softwares de titularidade da SONDA podem ser armazenados pelo pessoal responsável da área de Tecnologia da Informação.
- Nenhuma informação estratégica poderá ser armazenada em mídias removíveis e repassadas a entidades externas, tais como fornecedores, parceiros e prestadores de serviço, sem a prévia autorização da área de Segurança da Informação, com o aval da Diretoria da SONDA e da área responsável pela comunicação. Este processo deve ser realizado com o suporte da

área de Tecnologia da Informação, sendo pré-requisito para início do processo de aprovação a assinatura de Acordo de Confidencialidade (NDA) pelas partes envolvidas.

- Não é permitido o armazenamento de software ou arquivos com conteúdo pornográfico, pedófilo, racista, preconceituoso ou outros conteúdos ilícitos em qualquer tipo de mídia, mesmo que para uso pessoal, dentro da infraestrutura de tecnologia da informação da SONDA.

11.4 Acesso Remoto às Informações

Os requisitos atuais de mobilidade e flexibilidade para o trabalho exigem alto nível de acessibilidade e produtividade, logo, é cada vez mais comum a necessidade de acessos entre diversas redes, de empresas diferentes ou não. Desta forma, alguns cuidados se fazem necessários:

- O acesso remoto à(s) rede(s) da SONDA, ou seja, o acesso a partir de outra empresa ou de algum ponto da Internet deve ser realizado somente por meio de projeto previamente elaborado e implementado pela área de Tecnologia da Informação ou dos meios de VPN já implantados e disponíveis aos profissionais da empresa.
- O acesso remoto para terceiros, fornecedores e clientes só pode ser feito por intermédio de projeto específico da equipe de Segurança da Informação, considerando que terão acesso controlado apenas ao que for necessário e não a todo o ambiente.
- Sempre que o empregado, fornecedor, cliente ou prestador de serviços estiverem trabalhando remotamente, deverão observar todos os demais cuidados descritos nesta política.
- Atenção redobrada às informações disponíveis na tela tem que ser observada quando o associado estiver em ambientes públicos, tais como aeroportos, hotéis e redes sem fio de outras empresas.
- Os equipamentos conectados à rede corporativa da SONDA não podem ser diretamente conectados à outras redes ou diretamente à Internet. Estas conexões devem ser feitas somente através de firewall, desde que aprovadas e configuradas pela equipe de Segurança da Informação.
- Nenhuma estação de trabalho, estando conectada a(s) rede(s) da SONDA, deve ao mesmo tempo fazer uso de modems conectados a linhas dedicadas ou discadas que forneçam acesso a outras redes ou à Internet, salvo os casos analisados e aprovados pela equipe de Segurança da Informação. Estes acessos criam um caminho alternativo entre estas redes, permitindo que ataques ocorram por estes caminhos.

12 E-Mail Corporativo e Internet

12.1 Internet

A Internet é uma opção de comunicação na qual não existem barreiras nem limites. E, na maioria das vezes, não existem regras efetivas contra o seu uso indiscriminado. Por ser uma rede distribuída com abrangência mundial, permite a conexão de entidades com todos os tipos de propósitos e, em virtude disso, vários cuidados devem ser considerados.

A SONDA se reserva o direito de bloquear acesso a sites de conteúdo ilícito, sexo, atividades hacker, vídeos, áudios dentre outros, sem aviso prévio e de forma automática. Os registros de acesso serão avaliados pela área de Gestão de Segurança da Informação.

É proibido navegação na internet para quaisquer fins pessoais em servidores hospedados na infraestrutura tecnológica da SONDA.

O acesso à internet para fins pessoais, exceto (Facebook, Youtube, Vimeo, E-mail pessoal, Downloads, etc) é permitido através da estação de trabalho do funcionário, desde que não afete o desempenho dos negócios da SONDA.
Caso seja necessário o acesso via estação de trabalho a algum site cujo conteúdo esteja bloqueado, o colaborador deve solicitar através de requisição de serviço a liberação do site ao grupo IT SECURITY para análise da demanda. Nesta solicitação deve ser informada a justificativa e anexada a aprovação do gestor imediato do colaborador.
O acesso a sites de internet banking e lojas virtuais é permitido, porém a SONDA não se responsabiliza por perdas ou danos relativos ao uso em suas dependências, devendo o associado se responsabilizar integralmente pela segurança desta transação.
A SONDA armazena os registros de navegação na Internet e poderá monitorá-los para exercício do seu poder diretivo.

12.2 E-Mail

Os titulares da conta de correio eletrônico corporativo serão os únicos responsáveis pelo conteúdo nela armazenado, devendo fazer uso deste recurso em caráter pessoal e intransferível.

Não é permitido a utilização de e-mail pessoal dentro da infraestrutura de tecnologia da informação da SONDA.

12.3 Microsoft Teams

A SONDA utiliza o Microsoft Teams como ferramenta de comunicação de trabalho para troca de informações que poderão ser objeto de monitoramento. O uso pessoal é tolerado desde que não interfira nas atividades profissionais e na entrega dos serviços da SONDA para seus clientes.
É vedada a transferência de informações classificadas como para uso interno e confidencial nestes canais, assim como a transferência de arquivos.
A permissão de acesso aos serviços será controlada e poderá ser removida caso solicitado por um Gerente/Coordenador ou Diretor da SONDA.

12.4 Redes Sociais

O acesso a redes sociais é liberado apenas para os profissionais/terceiros da área comercial e planejamento estratégico e inteligência de mercado para fins de pesquisa e interação com o cliente.

13 Acesso Físico e Lógico

13.1 Controle de Acesso às Informações

O acesso às informações e aos sistemas da SONDA deve ser autorizado de acordo com as atividades atribuídas ao cargo ou função exercida pelo profissional/terceiro. Os privilégios de acesso atribuídos aos profissionais/terceiros devem ser revistos periodicamente pelas coordenações responsáveis pelos mesmos.
Todo associado/terceiro deve possuir uma única identificação de usuário (User IDs, ou logon) e senha(s) (password) relacionada às suas atribuições ou funções em exercício no contrato de trabalho ou de prestação de serviço. Os privilégios e direitos de acesso devem ser atribuídos de acordo com

as atribuições ou funções em exercício no contrato de trabalho ou de prestação de serviço. Cada associado/terceiro é responsável pelo uso e pela segurança de sua senha.
É proibido o empréstimo e compartilhamento de identificação de usuários e senhas associadas a qualquer tipo de acesso às informações, aos sistemas e aos equipamentos da SONDA.
Nenhum equipamento ou sistema contendo senhas de fábrica (default) deve ser colocado em regime de operação sem que antes estas senhas sejam alteradas de acordo com os procedimentos definidos pelas áreas responsáveis pelos mesmos.
Usuários administrativos de sistemas operacionais, bancos de dados e equipamentos de rede não devem ser genéricos para garantir a possibilidade de auditorias, controles de mudança, configurações e segurança das informações.
A construção de qualquer senha deve considerar o uso e a composição entre caracteres alfabéticos, maiúsculos, minúsculos, números e alfanuméricos. Toda senha deve ter no mínimo 8 (oito) caracteres, por exemplo Abe$10sa2. Entretanto, para o caso de senha para celular corporativo esta consideração é indicada, mas não é obrigatória.
O profissional/terceiro não poderá repetir nenhuma das últimas 13 (treze) senhas já previamente utilizadas.
É responsabilidade da equipe de Segurança da Informação garantir configurações no domínio(s) de controle para assegurar a construção de senhas fortes, aplicação de histórico e expiração automática das senhas.
Os profissionais/terceiros devem escolher senhas fáceis de serem memorizadas, porém ao mesmo tempo difíceis de serem descobertas ou quebradas. Técnicas para esta escolha incluem:

- Combinar palavras de fácil memorização através de caracteres alfanuméricos, por exemplo: Mar04@aberto, Verde06claro#;
- Combinar as primeiras letras das palavras que compõe o trecho de uma música ou frase;
- Combinar sinais de pontuação e números com uma palavra conhecida, por exemplo: Carro1020v.

No processo de elaboração de uma senha os profissionais não devem utilizar padrões repetidos, com sequência básica de caracteres, por exemplo: aaaaa10, 101010. Senhas idênticas e similares não devem ser utilizadas, por exemplo: mes01a, mes02a e mes03b.
As senhas devem obrigatoriamente ser alteradas a cada 60 (sessenta) dias. É responsabilidade da Área de Tecnologia da Informação garantir as configurações necessárias nos sistemas para que as senhas expirem automaticamente. Informações de expiração da senha devem ser apresentadas no mínimo 7 (sete) dias antes da expiração no processo de identificação (logon) do usuário.
Quando o associado/terceiro suspeitar de utilização indevida de sua(s) senha(s) deverá alterá-la(s) imediatamente e tratar a situação como um incidente de segurança (vide seção 22 – Gerenciamento de Incidentes).
As senhas não devem ser armazenadas em forma compreensível (leitura) em código fonte, scripts, macros e papel para evitar a divulgação inadvertida e uso indevido destas.
Todas as estações de trabalho da SONDA devem utilizar proteção de tela (screen saver) previamente homologada pela área de Tecnologia da Informação e com ação automática de execução a partir de 10 (dez) minutos de inatividade da estação de trabalho. É responsabilidade da equipe de Tecnologia da Informação configurar políticas nos diversos domínios para assegurar a utilização de proteção de tela. É vedada ao profissional/terceiro a remoção das configurações de proteção de tela da estação de trabalho.

13.2 Engenharia Social

Embora pareça inofensiva, a engenharia social é uma das mais eficientes técnicas de ataque. Neste caso, o agressor (cracker) faz uso de técnicas sociais com objetivo de conseguir informações, senhas ou até mesmo a realização de uma invasão. Alguns exemplos incluem:

- Um agressor, dizendo-se ser um analista do suporte da empresa, liga para um usuário questionando se seu sistema está mais lento do que o normal. Provavelmente, o usuário responderá que sim e, neste caso, o agressor dirá que existe um problema no sistema Windows e que eles estão instalando uma correção e pode até solicitar a senha do associado. Educadamente, ainda questiona se o usuário pode executar o procedimento de atualização naquele momento ou se prefere deixar para o período da tarde. O usuário aceita executar o procedimento e, inadvertidamente, acessa um endereço web, de acordo com as orientações do agressor e acaba instalando um backdoor em seu computador;
- O associado recebe um e-mail indicando que acaba de ser sorteado com um prêmio de alguns milhares de reais para utilizar em compras em uma loja. O site indica que o mesmo deve acessar um endereço e preencher um pequeno cadastro, por meio do qual algumas informações serão coletadas e utilizadas indevidamente alguns dias depois;
- Em um almoço com um fornecedor, este cita exemplos de outras empresas e disfarçadamente questiona sobre dados, processos e resultados de sua empresa, obtendo informações privilegiadas.

Portanto, é muito importante que o associado esteja sempre atento e alerta, desconfiando de tudo o que possa parecer um golpe. Sempre que houver dúvidas, a equipe de segurança da informação da SONDA deverá ser contatada para verificar a veracidade da informação por meio dos e-mails ou do telefone referenciado na seção 3 (Dúvidas e Sugestões).

É responsabilidade dos profissionais/terceiros cuidar para que informações sensíveis impressas não estejam ao alcance de pessoas indevidas, ou seja, não devem permanecer sobre mesas e na própria impressora. Toda vez que se ausentar de sua estação de trabalho, o associado/terceiro deverá efetuar o processo de bloqueio da estação de trabalho (lock) bem como o armazenamento de informações sensíveis impressas em gavetas que possuam trancas.

14 Malware

Malware (código maléfico), junção das palavras “malicious” e “software” é um software projetado para infiltrar e danificar um sistema de computador sem o consentimento do proprietário do sistema. A expressão constitui um termo geral utilizado pelos profissionais da área de Tecnologia da Informação para designar uma série de ameaças hostis, intrusivas e perigosas inseridas em algum código de computador. O termo “vírus de computador” é o mais abrangente e utilizado para incluir todos os tipos de malware. Porém, existem também os chamados vermes, cavalos de tróia, spyware, keystroke loggers, e etc.

Vírus é um programa ou parte de um programa de computador, normalmente malicioso, que se propaga infectando, isto é, inserindo cópias de si mesmo e se tornando parte de outros programas e arquivos de um computador. O vírus depende da execução de programa ou arquivo hospedeiro para que possa se tornar ativo e continuar o processo de contaminação a outros computadores e arquivos. São capazes de destruir e danificar informações, causando grandes transtornos e prejuízos para as empresas. Alguns sintomas de equipamento contaminado são:

- Tempo de carga de programas muito demorado, fora do usual;
- Redução abrupta de memória e espaço em disco repentinamente;
- Mensagens de erros não usuais;

- Atividades de tela anormais, por exemplo: letras caindo, “bolinhas” saltando, e etc.;
- Queda ou interrupções frequentes do sistema;
- Situações estranhas estão acontecendo com os arquivos, isto é, desaparecem, não carregam, não executam ou aumentam de tamanho exageradamente, etc.

Vermes são parecidos com os vírus, porém a grande diferença é que não necessitam da interação humana para se propagarem e contaminar os sistemas. Descobrem as falhas de segurança dos sistemas (vulnerabilidades) e se instalam automaticamente por meio delas. Geralmente difundem-se por e-mail (correio eletrônico), descobrindo a caixa postal do usuário e disparando cópias para outros usuários automaticamente.

“Cavalos de Tróia” (Trojan Horses) são programas não autorizados escondidos dentro de outros programas, isto é, por trás da finalidade aparentemente inocente de um programa, existe um código maléfico a ser executado, que poderá causar perda, desvio e destruição de informações.

Por definição, o cavalo de tróia distingue-se de um vírus ou de um verme por não infectar outros arquivos, nem propagar cópias de si mesmo automaticamente. Normalmente um cavalo de tróia consiste em um único arquivo que necessita ser explicitamente executado. Um exemplo comum: o associado baixa (download) um novo jogo da Internet e este jogo esconde um código para roubar informações do computador e enviar para um agressor.

As recomendações seguintes se fazem mandatórias para que os riscos de contaminação por malware e consequentes prejuízos ao negócio, produtividade e instabilidade dos sistemas sejam minimizados.

14.1 Servidores e Estações de Trabalho

Todas as estações de trabalho e todos os servidores sob responsabilidade da SONDA TÊM que possuir software antivírus instalado. O processo de remoção de vírus e atualização da base de dados de vírus deverá ser automático e transparente. A geração de registros de ocorrência, comumente conhecidos como “log”, é imprescindível para monitoramento e evolução das políticas vírus. É vedada ao associado/terceiro remover ou desabilitar o software antivírus.

A instalação e configuração do software antivírus será realizada pela área operacional da Segurança da Informação (IT SECURITY), utilizando-se sempre de software previamente testado e homologado pela SONDA.

14.2 Suspeita de Contaminação

Se existir a suspeita de contaminação por Malware, o associado/terceiro deverá interromper a utilização da estação de trabalho imediatamente. O associado/terceiro deverá avisar imediatamente a equipe de Segurança da Informação.

O processo de erradicação deverá ser realizado o mais rápido possível pela área de Tecnologia da Informação com apoio do suporte do fornecedor do produto antivírus.

14.3 Software de Fonte Duvidosa

Os sistemas e as redes de computadores das empresas podem ser atacados por vírus, vermes, cavalos de tróia e/ou outros Malwares. Para prevenir problemas resultantes da ação destes, é proibida a execução de softwares cuja fonte seja duvidosa. Fontes aparentemente NÃO duvidosas seriam:

- Fornecedores de software e hardware estabelecidos no mercado;
- Entidades de segurança bem conhecidas no mercado;
- Empresas de negócio conhecidas.

Software extraído (download) da Internet, sites de shareware, software de domínio público (freeware) não deve ser utilizado sem que processos de teste e homologação sejam previamente realizados pela equipe de Segurança da Informação.

15 Backup

Todas as informações críticas de negócio da SONDA e de seus clientes têm que possuir cópia de segurança (backup) realizada de acordo com os seus requisitos. É responsabilidade da área de Tecnologia da Informação providenciar os recursos físicos e lógicos para armazenamento e restauração das cópias de segurança.
As cópias de segurança devem ser verificadas sistemicamente para assegurar o processo de restauração. É responsabilidade da área de Tecnologia da Informação prover os recursos necessários e realizar a restauração das cópias de segurança regularmente.
O processo de restauração das informações críticas armazenadas em cópias de segurança é responsabilidade exclusiva da área de Tecnologia da Informação. A restauração da informação deverá ser solicitada formalmente a este departamento pelo dono da informação e registrada por meio de gestão de mudança.
Informações críticas armazenadas em cópias de segurança não devem ser utilizadas com o propósito de restauração, a não ser que as mesmas informações existam em cópias adicionais e mídias distintas. Se não existe cópia adicional, uma cópia deve obrigatoriamente ser realizada em equipamento diferente do destino final da informação.
Informações críticas ao negócio da SONDA presentes em equipamentos móveis, tais como laptops, VDI, celulares e PDAs (Personal Digital Assistant) também devem estar presentes em diretórios de rede para que o processo de cópia de segurança seja assegurado. É responsabilidade dos profissionais garantir a cópia das informações nos diretórios de rede.
Todas as alterações de configuração na rede e sistemas críticos da SONDA obrigatoriamente requerem a realização de cópia de segurança das configurações, antes e após a realização das mudanças. A equipe responsável pelas alterações também é responsável pela realização, classificação e armazenamento das cópias de segurança.

16 Criptografia

Criptografia é a ciência e arte de escrever mensagens em forma cifrada ou em código. É usada, dentre outras finalidades para: autenticar a identidade de usuários; autenticar transações bancárias; proteger a integridade de transferências eletrônicas de fundos; proteger o sigilo de comunicações pessoais e comerciais.
Sempre que informações confidenciais ou secretas forem enviadas para fora da rede corporativa da SONDA, métodos autorizados de criptografia são recomendados para proteger a informação.
Caso sejam utilizados mecanismos de criptografia, somente será permitido o uso de algoritmos e padrões normatizados pelos órgãos governamentais.
Sempre que esta informação ficar armazenada em um computador, o local de armazenamento terá uma proteção similar.
As comunicações e transferências de informações entre a SONDA, instituições financeiras, parceiros e fornecedores estratégicos devem ser realizadas preferencialmente através de redes privadas (VPNs) utilizando-se de esquemas criptográficos previamente avaliados e aprovados pela equipe de Segurança da Informação.

A Segurança da Informação deve utilizar da criptografia para proteger informações vitais para a SONDA, é indicado que seja criptografado o disco rígido das estações de trabalho de profissionais de áreas críticas para o negócio tais como Vendas, Segurança da Informação.

17 Aquisição e Desenvolvimento de Sistemas

O processo de desenvolvimento e aquisição de novos sistemas deve considerar as melhores práticas de segurança da informação. Estas práticas devem ser atualizadas, discutidas e disseminadas dentro da SONDA pela equipe de Segurança da Informação.
Todo o software desenvolvido pelos profissionais da SONDA, com o intuito de processar informação crítica, valiosa e sensível deve possuir uma especificação formal escrita. Esta especificação deve ser parte de um acordo entre o(s) proprietário(s) envolvido(s) com informação e o(s) desenvolvedor(es) do sistema. Esta declaração deve ser elaborada e aprovada antes do momento em que se iniciam os esforços de programação.
Todas as aquisições de novos sistemas devem considerar a verificação de requisitos mínimos de segurança da informação. A definição destes requisitos é responsabilidade da equipe de Segurança da Informação.
A Política de Corporativa Segurança da Informação deve obrigatoriamente fazer parte como anexo de qualquer contrato envolvendo a aquisição de novos sistemas. O fornecedor proponente deverá atender as condições estabelecidas neste documento para garantir a integridade, disponibilidade e confidencialidade das informações.

18 Gerenciamento de Fornecedores de Serviço e Terceiros

Todo negócio celebrado entre a SONDA e seus parceiros comerciais, contratados e provedores de serviços serão tratados considerando os seguintes aspectos de segurança da informação:

- Controles essenciais para a organização do ponto de vista legal, de acordo com a legislação aplicável:
  - Proteção de dados e privacidade de informações pessoais;
  - Proteção de registros organizacionais;
  - Direitos de propriedade intelectual.
- II - As características sociais, culturais e ambientes de onde estão inseridos.
- III - Provisão de recursos financeiros para o cumprimento dos requisitos de segurança da informação.
- IV - Os controles de segurança que serão considerados na especificação dos requisitos e nos estágios dos negócios.
- IV - Gestão da continuidade do negócio.

19 Gerenciamento de Incidentes de Segurança da Informação

Incidente de segurança é qualquer fato que possa comprometer o bom andamento dos sistemas da SONDA e dos seus clientes. Exemplos incluem o uso não autorizado de senhas, a adulteração de informações em um banco de dados, o envio ou recepção de mensagens ameaçadoras, roubo de informação, ocorrência de vírus, ou qualquer outro fato que contrarie as disposições dessa política.
Qualquer incidente de segurança deve ser informado ao superior imediato, bem como envio de mensagem eletrônica para segurancainfo.qualidade@sonda.com e para o e-mail e endereços referenciados na seção Dúvidas, Sugestões e Comunicação de Incidentes.
Os incidentes recebidos por este canal serão analisados pela equipe de Segurança da Informação da SONDA, de acordo com as diretrizes organizacionais e melhores práticas de internacionais.

É responsabilidade de todos os profissionais da SONDA informar sobre incidentes dos quais tenham ciência ou nos quais estejam envolvidos. Casos de omissão poderão ser considerados como negligência ou cumplicidade.
É responsabilidade da equipe de Segurança da Informação da SONDA proceder à coleta e exame de dados, bem como definir as ações a serem tomadas para enfrentamento de incidentes, com a validação da Diretoria.

20 Classificação da Informação

A informação é o ativo mais importante para o negócio da SONDA. Portanto, os responsáveis pelas informações são os coordenadores/gerentes dos departamentos, membros da alta gestão ou aqueles que receberam delegação da SONDA para aquisição, desenvolvimento e manutenção das aplicações em regime de produção que processam as informações da empresa. Todos os sistemas de informação da empresa possuem um responsável designado. Para cada tipo de informação, o respectivo responsável deve designar a classificação desta, o nível de risco, definir quais profissionais terão acesso e o nível deste acesso, bem como aprovar requisições para os vários modos de utilização destas informações.

Os membros dos departamentos administradores de sistemas e profissionais que utilizam e transportam informações em dispositivos pessoais também são custodiantes. Os custodiantes são responsáveis pela salvaguarda das informações, incluindo a implementação de controles de acesso para prevenir acesso e divulgação inadvertida; responsáveis pelas cópias de segurança (backup) para garantir que informações críticas não serão perdidas. Esses também são responsáveis pela implementação, operação e manutenção das medidas de segurança requisitadas pelos responsáveis da informação.

20.1 Diretrizes de Classificação

A informação deve ser classificada e receber um nível de proteção adequado, de acordo com o seu valor, requisitos legais, grau de sigilo, sensibilidade e criticidade para o negócio.

A informação deve ser classificada pelo proprietário da informação, considerando os seguintes critérios:

a) **[CONFIDENCIAL]** Informação de alta sensibilidade que necessita de um controle e nível de proteção mais elevado. Deve ser protegida por sua relevância sobre questões estratégicas, detalhamento técnico de produtos e serviços, oportunidades de negócio, informações jurídicas, impacto financeiro, entre outros. O vazamento ou perda desse tipo de informação pode resultar em prejuízos financeiros para a SONDA, tais como, aplicação de multas e quebra contratual, perda de imagem, bem como, favorecimento indevido da concorrência.

Exemplos de Informações que devem ser classificadas como [CONFIDENCIAL] são:

- Informações de planejamento estratégico (projetos de investimentos, reposicionamento da marca, novos produtos/serviços, fusões/aquisições);
- Informações de atividades jurídicas e/ou processuais;
- Informações de contratos comerciais, comissionamento e cobrança de fornecedores;
- Pesquisas de mercado e informações de inteligência comercial (propostas, contratos e

similares);
- Resultados financeiros e contábeis, previamente a data de publicação;
- Dados de riscos corporativos e financeiros;
- Informações salariais;
- Dados pessoais diretos e sensíveis dos colaboradores, clientes, fornecedores, ativos e inativos.

b) **[RESERVADA]** Informação restrita, interna para áreas ou projetos aos quais deve ter acesso controlado um grupo restrito/ de pessoas. Deve ser protegida por seu impacto nos interesses da SONDA, de seus clientes ou parceiros e colaboradores. O vazamento, divulgação ou adulteração desse tipo de informação pode resultar em impactos negativos para as operações ou gestão dos negócios.

Exemplos de Informações que devem ser classificadas como [RESERVADA] são:

- Planejamento organizacional;
- Planos de marketing e estratégias de negócio;
- Dados cadastrais de clientes;
- Dados de atendimento de clientes;
- Informações sobre segurança da informação e patrimonial;
- Informações de auditoria;
- Documentação de arquitetura de sistemas e de topologia de redes;
- Informações de planejamento e implementação de tecnologias.
- Dados pessoais indiretos dos colaboradores ativos e inativos.

c) **[CORPORATIVA/INTERNA]** Informação sem restrição, que deve ser mantida no âmbito interno da SONDA e, que pode ser acessada por todos os colaboradores mediante a necessidade de desempenho de suas funções. A restrição ocorre quanto ao uso e/ou divulgação fora do âmbito corporativo.

Exemplos de Informações que devem ser classificadas como [CORPORATIVA/INTERNA] são:

- Políticas, diretrizes, processos e procedimentos corporativos;
- Material de treinamento e/ou capacitação interna;
- Informações sobre desempenho operacional;
- Orçamento corporativo.

d) **[PÚBLICA]** Informação cuja divulgação pública não gera impactos negativos financeiros e/ou de imagem aos negócios da SONDA e/ou de parceiros, podendo ser divulgada a funcionários, clientes, fornecedores e público em geral.

Exemplos de Informações que devem ser classificadas como [PÚBLICA] são:

- Material de marketing sobre produtos e serviços lançados;

- Relatórios e indicadores financeiros, contábeis e de balanço publicados para o mercado.

Nota: Para informações com dados pessoais de pessoas físicas ou jurídicas. Essas informações devem ser protegidas por sua relevância para fins de atendimento à PL 158.02.00 - Política de Privacidade de Dados, podendo ser cliente, visitante, colaborador ativo e inativo, fornecedores, terceiros ou prestadores de serviços.

20.2 Rotulagem

O proprietário da informação, após realizar a classificação da informação de acordo com o seu nível de confidencialidade, deve rotular a mesma através de uma indicação inteligível e, assegurar a aplicação e cumprimento dos controles de segurança adequados;

É obrigatório que a classificação atribuída a informação [CONFIDENCIAL] ou [RESERVADA] seja rotulada no início/cabeçalho ou término/rodapé dos documentos, mesmo que em formato eletrônico (apresentações, relatórios, planilhas, procedimentos, extrações de informações realizada em sistemas, etc.), bem como, através de rótulos externos (etiquetas) aplicáveis em mídias removíveis (CD, DVD, fita de backup, pen drive, entre outros). A rotulagem da informação com níveis de classificação [CORPORATIVA] e [PÚBLICA] é facultativa ao proprietário da informação;

Os rótulos de classificação da informação devem seguir os padrões listados abaixo, destacados em negrito:

[NC-40] Confidencial - A informação deve ser classificada como confidencial quando sua exposição fora do ambiente da organização possa acarretar em perdas financeiras, de imagem, de competitividade. Somente poderá ser divulgada para as entidades (usuários, clientes, fornecedores e outros) definidas como autorizados a receberem a informação, por exemplo: informações relacionadas a novos planos de negócio e estratégias de crescimento da empresa.

[NC-30] Reservada - A informação deve ser classificada como restrita quando acessos não autorizados a ela, mesmo que por membros da própria organização, sejam capazes de trazer sérios danos ao negócio.

[NC-20] Corporativa/Interna - A informação deve ser classificada como interna quando não for desejável que ela se torne conhecida por pessoas de fora da organização, e/ou requerendo um contrato firmado entre as partes para divulgação de dados relacionados a operação da Empresa, por exemplo book de clientes contendo métricas.

[NC-10] Pública - A informação deve ser classificada como pública quando ela puder ser divulgada a todos, isto é, funcionários, terceirizados, clientes, fornecedores e público em geral, sem que isso provoque impactos no negócio.

No caso de classificação de um conjunto de informações que apresentam diversos níveis de confidencialidade, deve ser atribuída a classificação de maior nível presente no conjunto.

Qualquer informação sem classificação explícita deve ser tratada no mínimo como de [RESERVADA],

rótulo: [NC-30].

A informação recebida de entidade externa deve ser classificada conforme definido pela mesma. Caso nenhum critério esteja especificado, então, deve ser atribuída a classificação [RESERVADA], de rótulo [NC-30].

20.3 Reclassificação

Caso a informação previamente classificada tenha o seu nível de confidencialidade alterado, é necessário que a mesma seja reclassificada pelo proprietário da informação, atribuindo-se o nível de sigilo adequado, bem como, assegurando a aplicação e cumprimento dos controles de segurança exigidos.

20.4 Ciclo de vida da informação

20.4.1 Criação

Toda informação é criada com a classificação mínima [CORPORATIVA], rótulo [NC-20], até que seja avaliada pelo proprietário da informação.

20.4.2 Armazenamento

A informação classificada como [CONFIDENCIAL] ou [RESERVADA] deve ser armazenada de forma controlada, evitando o acesso indevido;

O proprietário da informação deve observar a aplicação dos controles de segurança lógica e/ou física existentes e disponibilizados pela SONDA para assegurar a proteção adequada. Exemplo de controles: pastas de rede com controle de acesso lógico, armários e gavetas com chaves ou cadeados e cofres.

Toda documentação referente aos processos das áreas e/ou normativa, deve ser rotulada segundo as diretrizes dessa política, elaborada e armazenada no Sistema de Gestão de Documentos - SONDA GRC, conforme definido na PL 10.03 - Gestão de Documentos.

20.4.3 Divulgação

Deve haver especial atenção a divulgação de dados pessoais ou arquivos que possam conter dados pessoais, sendo que se o dado pessoal manipulado for de controle da SONDA, ela deverá proceder com a definição da finalidade de uso do dado, recolhimento do termo de concessão de uso do dado, garantia do direito de alteração ou revogação da concessão de uso, garantia dos processos de exclusão dos dados após a tempo de retenção estabelecido e rastreabilidade da divulgação internas destes dados.

Para a manipulação de dados ou arquivos que possam conter dados pessoais em que o controlador dos dados é um parceiro, cliente ou fornecedor, a SONDA deverá conter os acordos comerciais e cláusulas contratuais de segurança da informação e de proteção de dados conforme a PL 158.02.00

- Política de Privacidade de Dados_SONDA.

20.4.4 Utilização e Distribuição

A informação classificada como [CONFIDENCIAL] ou [RESERVADA] deve ser acessada por um grupo restrito de pessoas envolvidas na questão, e/ou entre áreas estratégicas;

A informação classificada como [CORPORATIVA] pode ser acessada por todos os colaboradores, sendo restrito apenas o seu uso fora do âmbito corporativo;

A informação classificada como [PÚBLICA] não possui restrição de acesso.

20.4.5 Destruição e Descarte

A informação classificada como [CONFIDENCIAL] ou [RESERVADA] deve ser destruída e descartada de forma segura, seja qual for a mídia de armazenamento, impossibilitando a reconstrução da informação. Para esta etapa aplicam-se as diretrizes estabelecidas na PL 18.25 - Política de Uso Aceitável do Ativo e PT 10.62.02 - Descarte de Ativos TI Brasil.

21 Relações Trabalhistas

Todos os associados da SONDA em processo de contratação devem receber esta política, ler e assinar o Termo de Aceite caracterizando a concordância com as diretrizes definidas neste documento. É responsabilidade da Gerência de Gente a garantia deste processo.
Todos os associados em processo de terminação do contrato de trabalho devem ter os acessos revogados imediatamente. É responsabilidade da área de Gerência de Gente iniciar o processo de revogação e garantir o término com sucesso deste processo.
É responsabilidade da área de Gerência de Gente e da equipe de Segurança da Informação prover meios de divulgação desta política e de aculturação relacionada à Segurança da Informação para profissionais já contratados e/ou em fase de contratação.

22 Direitos Autorais e Propriedade Intelectual

A SONDA é titular de todos os direitos sobre patentes, direitos autorais, invenções ou outras propriedades intelectuais originadas e desenvolvidas por seus profissionais individualmente ou em grupo constituído por outros profissionais ou fornecedores de serviço externos, durante a vigência dos respectivos contratos de trabalho e prestação de serviço.
Todos os programas e documentos criados ou providos pelos profissionais em benefício da SONDA são considerados de titularidade da SONDA, salvo menção expressa em contrário, nos termos do artigo 4º. da Lei 9609/98.
A SONDA é titular exclusiva dos dados e informações contidas em sistemas de informação sob seu controle e/ou administração. A SONDA se reserva o direito de acesso, uso e poder de decisão sob estas informações.
É vedado aos profissionais, visitantes, parceiros, terceiros e fornecedores o uso de câmera de vídeo, fotográfica ou celulares que possuam esta função no interior das dependências da SONDA, salvo com o consentimento formal da área de Segurança da Informação. Esta política se faz necessária para evitar o vazamento de informação e segredos de negócio de forma inadvertida ou proposital.

Informações importantes, tais como projetos, listas de clientes e outras, disponíveis em papel e mídias de fácil transporte, tais como CDs, DVDs e pen drives devem se acondicionadas em gavetas e armários com chaves.

23 Gestão de Continuidade de Negócios

O processo de gestão de continuidade de negócios da SONDA 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 SONDA e seus clientes.

24 Redes Wireless

A(s) rede(s) local(is) sem fios (WIRELESS), instalada(s) na SONDA tem o objetivo de melhorar a produtividade e flexibilizar o acesso de seus profissionais, terceiros e visitantes. No entanto, alguns cuidados se fazem necessários:
Apenas os equipamentos provedores de acesso (Access Points) e interfaces homologados pela área de Tecnologia da Informação podem ser utilizados nesta rede.
As configurações de segurança, autenticação e criptografia da rede devem seguir as melhores práticas de segurança do mercado. É responsabilidade da área de Segurança da Informação definir e divulgar estas práticas por meio de procedimentos.
Os recursos de segurança disponíveis e configurados nos equipamentos não podem ser desabilitados pelos usuários.
O serviço de acesso à rede wireless (WLAN) de convidados da SONDA fornece acesso público não criptografado para a internet. Este serviço é fornecido apenas aos usuários autorizados. A concessão de acesso para visitantes está condicionada ao cadastro prévio das informações de contato: nome completo, Registro Geral (RG), empresa, data e hora inicial e final do uso da rede, contato na SONDA e assinatura do termo de Uso de Redes Wireless. O termo assinado deverá ser armazenado em local fisicamente seguro por pelo menos 1 (um) ano. Este armazenamento é responsabilidade da equipe de Operações (Field e Pré-site).
Todas as considerações que compõe a Política de Segurança Corporativa da SONDA devem ser observadas quando se fizer uso da(s) rede(s) local(is) sem fios.
Nenhum dispositivo que forneça algum tipo de acesso sem fios (Wireless) pode ser instalado no ambiente corporativo da SONDA, salvo quando especificado por projeto elaborado e implantado pela equipe Tecnologia da Informação. Dispositivos móveis só poderão acessar a rede wireless da SONDA mediante a aprovação de um gerente.

25 Monitoração, Sanções e Penalidades

A SONDA se reserva o direito de monitorar e manter registros de todos os tipos de acesso aos seus sistemas, redes e informações, incluindo e-mails pessoais, quando recursos de Tecnologia da Informação da empresa forem utilizados. Estes registros são utilizados para análises estatísticas e para verificação em casos relacionados com incidentes de segurança.
No caso de descumprimento de quaisquer das considerações desta política e também nos casos de não conformidade de auditorias internas, medidas disciplinares serão tomadas junto à Gerência de Gente. Cada caso será avaliado face aos impactos e contexto aplicáveis. Como medidas disciplinares poderão ser consideradas desde a simples advertência ao término do contrato de trabalho por justa causa.

26 Papéis e Responsabilidades

Nesta seção é apresentado o conjunto de papéis e responsabilidades do processo de Gerenciamento de Segurança da Informação da SONDA. Os papéis representam os diferentes atores do processo, e estão descritos da seguinte forma:

- Nome: nome do papel.
- Descrição: descrição geral do papel, incluindo seus objetivos e responsabilidades.
- Responsabilidades: responsabilidades atribuídas.

26.1 Proprietário do Processo de Gerenciamento Financeiro de Serviços de TI

É o responsável final pelo processo e seus resultados. Suas atividades garantem um melhor equilíbrio entre os componentes- chaves do ambiente de gerenciamento de serviços. Suas principais responsabilidades são:

- Dar assistência e ser o responsável final pelo desenho do processo.
- Garantir que o processo de Segurança da Informação atenda aos propósitos estabelecidos.
- Integrar o processo de Segurança da Informação nas áreas da organização.
- Tratar as questões relacionadas à integração entre os vários processos.
- Participar de reuniões com a Direção para avaliar o impacto das decisões organizacionais no ambiente de Segurança da Informação.
- Possui autoridade para aprovar mudanças propostas no processo, organizar treinamento e nomear funcionários para treinamentos.
- A autoridade máxima em relação ao processo garantindo sua especificação e execução.
- Revisar periodicamente os perímetros definidos.
- Definir Indicadores-chave de desempenho e desenhar as especificações de relatórios.
- Aprovar e iniciar treinamento quando necessário.
- Revisar e comunicar as propostas de mudanças no processo.
- Acompanhamento da divulgação da Segurança da Informação.

26.2 Information Security Officer

Tem o objetivo de organizar e coordenar as atividades referentes a segurança da Informação dentro da organização, estabelecendo padrões, regras e avaliando a eficiência do sistema de segurança da informação dentro do Sistema de Gestão Integrado da SONDA. Suas principais responsabilidades são:

- Elaborar as políticas e controles de segurança;
- Definir a metodologia de risco que será utilizada;
- Coordenar a implantação de políticas, controles e da metodologia;
- Monitorar o desempenho do sistema de segurança da informação;
- Acompanhar os planos de ação e seus resultados;
- Garantir que as evidências do processo serão registradas e mantidas;
- Auditar o gerenciamento de ameaças e vulnerabilidades encontradas;
- Programar auditorias periódicas.
- Propor melhorias e correções que melhorem a segurança da informação.
- Definir políticas, controles e metodologia;

- Cobrar atuação das áreas envolvidas nos planos de ação;
- Responder pela área de Qualidade | Segurança da informação.

26.3 Analista das Áreas de Negócio

Dá o apoio aos Analistas de Segurança da informação fornecendo a visão de negócio para as ameaças / vulnerabilidades encontradas, auxiliando na elaboração das políticas e na avaliação dos resultados dos planos de ação. Os Analistas das áreas de negócio auxiliam no alinhamento entre segurança da informação e o negócio. Suas principais responsabilidades são:

- Analisar riscos do ponto de vista do negócio;
- Acompanhar os planos de ação;
- Interagir com o gerente de segurança buscando a eficácia do sistema de segurança da informação;
- Conscientizar seus colaboradores sobre segurança da informação.
- Garantir a execução dos itens de segurança na sua área;
- Interferir / cancelar / reagendar ações de segurança relativas à sua área de negócio.

26.4 Colaboradores

São afetados diretamente pelas políticas e regras de segurança da informação. Os colaboradores devem seguir estas determinações e estarem sempre informados das mudanças ocorridas. Suas principais responsabilidades são:

- Seguir as políticas, controles e metodologias de segurança implementadas;
- Participar das divulgações agendadas pela área de segurança.
- Proprietário da informação
- Restrita a seguir políticas, controles e metodologia de segurança da informação

26.5 Alta Direção

A alta direção deve estar envolvida no processo de Gerenciamento de Segurança da informação visando reforçar a importância deste assunto e garantir o alinhamento com as políticas organizacionais. O comprometimento da alta direção é um fator crítico de sucesso para o bom desempenho deste processo. Suas principais responsabilidades são:

- Aprovar novas políticas e controles;
- Patrocinar sistema de segurança da informação, ressaltando sua importância;
- Tomar conhecimento dos planos de ação e iniciativas de segurança;
- Checar se políticas de segurança estão alinhadas às políticas organizacionais.
- Aprovar políticas e controles;
- Patrocinar o processo.

26.6 Operação

Esta área é responsável pela operacionalização das regras definidas, monitoração e coleta dos dados. As políticas e metodologias implementadas necessitarão de ferramentas e do auxílio das áreas técnicas de TI para que sejam operacionalmente viáveis e tragam os resultados desejados. Suas principais responsabilidades são:

- Instalar ferramentas utilizadas para segurança da informação;
- Realizar as atividades propostas nos planos de ação;
- Monitorar os itens de segurança;
- Coletar dados para auditorias e avaliações do sistema de segurança.
- Administração dos recursos e componentes envolvidos.

26.7 Relações Trabalhistas

Tem o objetivo de comunicar, divulgar e apoiar o processo, principalmente quando os colaboradores estão envolvidos. RT tem papel importante na divulgação das regras de segurança da informação (principalmente para novos contratados) e na aceitação das mesmas (assinatura do código de ética, por exemplo). Suas principais responsabilidades são:

- Divulgar normas de segurança para novos colaboradores;
- Garantir que o código de ética contenha itens de segurança;
- Criar medidas / penalidades para infratores das normas de segurança.
- Gestão das pessoas;
- Definição da política de restrições e penalidades.

SONDA®
make it easy