Sumário

A Empresa 2

Características da empresa 2

Tamanho, Colaboradores, Tipo de Negócio 2

Infraestrutura 2

Ambiente físico e layout 3

Missão, visão e valores 4

Vulnerabilidades, ameaças, riscos e impactos 4

Política de Segurança da Informação 5

1. Introdução 5

1.1 A empresa e a política de segurança 5

1.2 O não cumprimento dessa política 5

2. Classificação Da Informação 5

2.1 Informação Pública 5

2.2 Informação Interna 5

2.3 Informação Confidencial 5

2.4 Informação Restrita 6

3. Responsabilidades Específicas 6

3.1 Dos Colaboradores em Geral 6

3.2 Dos Colaboradores em Regime de Exceção (Temporários) 6

3.3 Dos Gestores de Pessoas e/ou Processos 6

3.4 Dos Custodiantes da Informação 7

3.4.1 Da Área de Tecnologia da Informação 7

3.4.2 Da Área de Segurança da Informação 8

Diamantina, maio de 2016

3.4.3 Do Comitê de Segurança da Informação 9

4. Dados Pessoais De Colaboradores 9

5. Programas Ilegais 9

6. Compartilhamento De Pastas E Dados 9

7. Backup Do Sistema Integrado E Servidores De Rede 10

8. Segurança E Integridade Do Banco De Dados 10

9. Admissão ou Demissão de Colaboradores, Temporários e/ou Estagiários 10

10. Transferência De Colaboradores 10

11. Política de Identificação e senhas 12

12. Cópias De Segurança De Arquivos 13

13. Politica de e-mails 13

14. Políticas de acesso a Internet 15

15. Política de uso de estações de trabalho e equipamentos da ELR-SI 15

16. Uso De Computadores Pessoais 16

17. Política Social 16

18. Termos e Definições 17

19. Propriedade Intelectual 17

20. Penalidades 19

A Empresa

A **ELR-SI** - Exames, Levantamentos e Revisões de Sistemas de Informação é uma empresa que trabalha com prestação de serviços de auditoria de sistemas de informação, desenvolvendo soluções criativas para garantir a segurança dos nossos clientes através da implantação de boas práticas em sistemas já existentes e criação de sistemas ground up com ferramentas inovadoras e treinamento de pessoal focado na segurança dos colaboradores.

Características da empresa

Tamanho, Colaboradores, Tipo de Negócio

A ELR-SI é uma empresa de médio porte, com renda anual maior que R$ 16 milhões e menor que R$ 90 milhões, seu corpo de colaboradores é composto por 20 pessoas trabalhando na área de Contabilidade e Auditoria.

Infraestrutura

Computadores, servidores, automóveis, link e rede dedicada de comunicação, equipamentos de teste e segurança, móveis, ferramentas de escritório.

Ambiente físico e layout

A Empresa está em uma locação segura, no centro comercial da cidade. Os cômodos estão divididos em: Sala de Servidores, Área de Atividades, Almoxarifado, Sala da Diretoria, Sala da Gerência, Recepção, Sala de Marketing, Sala de Reuniões, Cozinha, Corredor, Banheiros Internos e Banheiro para Visitantes. Há duas entradas externas, uma para o Corredor, que por medida de segurança permanece sempre fechada e outra para a Recepção.

Figura 1 - Layout da ELR-SI

Missão, visão e valores

Missão

Preservar a reputação e integridade dos nossos clientes e seus objetivos, respeitando nossos stakeholders e colaboradores com responsabilidade social, continuamente expandindo nossa estrutura de trabalho de acordo com a evolução dos nossos associados.

Visão

Continuar expandindo o portfólio de parceiros que confiam a qualidade de suas metas à nossa equipe, se tornando uma das maiores empresas de auditoria na região sudeste.

Valores

Comunicação transparente.

Reconhecer e recompensar a iniciativa e colaboração.

Adquirir e compartilhar conhecimentos.

Trabalhar com espírito de cooperação.

Vulnerabilidades, ameaças, riscos e impactos

A princípio, todos os sistemas da empresa são vulneráveis e precisam de uma avaliação cautelosa para manter a Confiabilidade, Integridade e Disponibilidade. Dentre os ativos avaliados, podemos citar: Hardware, Software, Ambiente Físico e Pessoas.

As vulnerabilidades físicas podem ser descritas como:

Físicas:

- Acesso de documentos impressos;
- Descarte indevido de documentos com informações sigilosas;
- Acesso a rede interna em local público;

Naturais:

- Descargas elétricas no sistema.
- Demais acidentes naturais.

Hardware e Software:

- Grampo nas linhas de comunicação;
- Fala do circuito de proteção;
- Roubo, Cópia ou Acesso indevido aos arquivos;
- Falha de controle de acesso

Humanas:

- Vazamento de informações confidenciais;
- Uso de computadores para fins pessoais;
- Acesso a conteúdo suspeito nas máquinas da empresa.

Política de Segurança da Informação

1. Introdução

1.1 A empresa e a política de segurança

Todas as normas aqui estabelecidas serão seguidas rigorosamente por todos os colaboradores (funcionários, parceiros, prestadores de serviços) sendo seu dever tomar conhecimento da PSI (Politica de segurança da Informação) e aplicá-la em toda sua participação dentro da empresa e em determinador casos, fora da ELR-SI de acordo com as normas estabelecidas pela PSI. Todo trafego de internet e atividade de e-mail(s) bem como sistemas diversos poderão ser monitorados para garantir o cumprimento da PSI. Auditorias internas serão efetivadas sempre que necessário realizar atualizações à PSI.

1.2 O não cumprimento dessa política

O não comprimento dessas políticas acarretará em sanções administrativas de acordo com a Cláusula 20.

2. Classificação Da Informação

É de responsabilidade do Gerente/Supervisor de cada área estabelecer critérios relativos ao nível de confidencialidade da informação gerada por sua área. Toda informação gerada deve ser classificada de acordo com um dos quatro critérios abaixo.

2.1 Informação Pública

É toda informação que pode ser acessada por usuários da organização, clientes , fornecedores, prestadores de serviços e público em geral.

2.2 Informação Interna

É toda informação que só pode ser acessada por colaboradores da organização. São informações que possuem um grau de confidencialidade que pode comprometer a imagem da organização.

2.3 Informação Confidencial

É toda informação que pode ser acessada por usuários da organização e por parceiros da organização. A divulgação não autorizada dessa informação pode causar impacto (financeiro, de imagem ou operacional) ao negócio da organização ou ao negócio do parceiro.

2.4 Informação Restrita

É toda informação que pode ser acessada somente por usuários da organização explicitamente indicado pelo nome ou por área a que pertence. A divulgação não autorizada dessa informação pode causar sérios danos ao negócio e/ou comprometer a estratégia de negócio da organização.

3. Responsabilidades Específicas

3.1 Dos Colaboradores em Geral

Entende-se por colaborador toda e qualquer pessoa física, contratada CLT ou prestadora de serviço por intermédio de pessoa jurídica ou não, que exerça alguma atividade dentro ou fora da instituição.

Será de inteira responsabilidade de cada colaborador, todo prejuízo ou dano que vier a sofrer ou causar à ELR-SI e/ou a terceiros, em decorrência da não obediência às diretrizes e normas aqui referidas.

3.2 Dos Colaboradores em Regime de Exceção (Temporários)

Devem entender os riscos associados à sua condição especial e cumprir rigorosamente o que está previsto no aceite concedido pelo Comitê de Segurança da Informação.

A concessão poderá ser revogada a qualquer tempo se for verificado que a justificativa de motivo de negócio não mais compensa o risco relacionado ao regime de exceção ou se o colaborador que o recebeu não estiver cumprindo as condições definidas no aceite.

Não poderão ter acesso a dados Confidenciais e/ou Restritos ou a máquinas que contenham tais dados.

3.3 Dos Gestores de Pessoas e/ou Processos

Ter postura exemplar em relação à segurança da informação, servindo como modelo de conduta para os colaboradores sob a sua gestão.

Atribuir aos colaboradores, na fase de contratação e de formalização dos contratos individuais de trabalho, de prestação de serviços ou de parceria, a responsabilidade do cumprimento da PSI da ELR-SI.

Exigir dos colaboradores a assinatura do Termo de Compromisso e Ciência, assumindo o dever de seguir as normas estabelecidas, bem como se comprometendo a manter sigilo e confidencialidade, mesmo quando desligado, sobre todos os ativos de informações da ELR-SI.

Antes de conceder acesso às informações da instituição, exigir a assinatura do Acordo de Confidencialidade dos colaboradores casuais e prestadores de serviços que não estejam cobertos por um contrato existente, por exemplo, durante a fase de levantamento para apresentação de propostas comerciais.

Adaptar as normas, os processos, procedimentos e sistemas sob sua responsabilidade para atender a esta PSI, bem como aos termos da Norma Educacional.

3.4 Dos Custodiantes da Informação

3.4.1 Da Área de Tecnologia da Informação

Testar a eficácia dos controles utilizados e informar aos gestores os riscos residuais.

Acordar com os gestores o nível de serviço que será prestado e os procedimentos de resposta aos incidentes.

Configurar os equipamentos, ferramentas e sistemas concedidos aos colaboradores com todos os controles necessários para cumprir os requerimentos de segurança estabelecidos por esta PSI, e em sua versão educacional, pelas Normas de Segurança da Informação complementares.

Os administradores e operadores dos sistemas computacionais podem, pela característica de seus privilégios como usuários, acessar os arquivos e dados de outros usuários. No entanto, isso só será permitido quando for necessário para a execução de atividades operacionais sob sua responsabilidade como, por exemplo, a manutenção de computadores, a realização de cópias de segurança, auditorias ou testes no ambiente, mantidos os devidos registros de acesso.

Segregar as funções administrativas, operacionais e educacionais a fim de restringir ao mínimo necessário os poderes de cada indivíduo e eliminar, ou ao menos reduzir, a existência de pessoas que possam excluir os logs e trilhas de auditoria das suas próprias ações.

Garantir segurança especial para sistemas com acesso público, incluindo o ambiente educacional, fazendo guarda de evidências que permitam a rastreabilidade para fins de auditoria ou investigação.

Gerar e manter as trilhas para auditoria com nível de detalhe suficiente para rastrear possíveis falhas e fraudes. Para as trilhas geradas e/ou mantidas em meio eletrônico, implantar controles de integridade para torná-las juridicamente válidas como evidências.

Administrar, proteger e testar as cópias de segurança dos programas e dados relacionados aos processos críticos e relevantes para a ELR-SI.

Implantar controles que gerem registros auditáveis para retirada e transporte de mídias das informações custodiadas pela TI, nos ambientes totalmente controlados por ela.

O gestor da informação deve ser previamente informado sobre o fim do prazo de retenção, para que tenha a alternativa de alterá-lo antes que a informação seja definitivamente descartada pelo custodiante.

Quando ocorrer movimentação interna dos ativos de TI, garantir que as informações de um usuário não serão removidas de forma irrecuperável antes de disponibilizar o ativo para outro usuário.

Planejar, implantar, fornecer e monitorar a capacidade de armazenagem, processamento e transmissão necessários para garantir a segurança requerida pelas áreas de negócio.

Atribuir cada conta ou dispositivo de acesso a computadores, sistemas, bases de dados e qualquer outro ativo de informação a um responsável identificável como pessoa física, sendo que:

- os usuários (logins) individuais de funcionários serão de responsabilidade do próprio funcionário.
- os usuários (logins) de terceiros serão de responsabilidade do gestor da área contratante.

Proteger continuamente todos os ativos de informação da empresa contra código malicioso, e garantir que todos os novos ativos só entrem para o ambiente de produção após

estarem livres de código malicioso e/ou indesejado.

Garantir que não sejam introduzidas vulnerabilidades ou fragilidades no ambiente de produção da empresa em processos de mudança, sendo ideal a auditoria de código e a proteção contratual para controle e responsabilização no caso de uso de terceiros.

Definir as regras formais para instalação de software e hardware em ambiente de produção corporativo, bem como em ambiente exclusivamente educacional, exigindo o seu cumprimento dentro da empresa.

Realizar auditorias periódicas de configurações técnicas e análise de riscos.

Responsabilizar-se pelo uso, manuseio, guarda de assinatura e certificados digitais.

Garantir, da forma mais rápida possível, com solicitação formal, o bloqueio de acesso de usuários por motivo de desligamento da empresa, incidente, investigação ou outra situação que exija medida restritiva para fins de salvaguardar os ativos da empresa.

Garantir que todos os servidores, estações e demais dispositivos com acesso à rede da empresa operem com o relógio sincronizado com os servidores de tempo oficiais do governo brasileiro.

Monitorar o ambiente de TI, gerando indicadores e históricos de:

- uso da capacidade instalada da rede e dos equipamentos;
- tempo de resposta no acesso à internet e aos sistemas críticos da ELR-SI;
- períodos de indisponibilidade no acesso à internet e aos sistemas críticos da ELR-SI;
- incidentes de segurança (vírus, trojans, furtos, acessos indevidos, e assim por diante);
- atividade de todos os colaboradores durante os acessos às redes externas, inclusive internet (por exemplo: sites visitados, e-mails recebidos/enviados, upload/download de arquivos, entre outros);

3.4.2 Da Área de Segurança da Informação

Propor as metodologias e os processos específicos para a segurança da informação, como avaliação de risco e sistema de classificação da informação.

Propor e apoiar iniciativas que visem à segurança dos ativos de informação da ELR-SI.

Publicar e promover as versões da PSI e as Normas de Segurança da Informação aprovadas pelo Comitê de Segurança da Informação.

Promover a conscientização dos colaboradores em relação à relevância da segurança da informação para o negócio da ELR-SI, mediante campanhas, palestras, treinamentos e outros meios de Endomarketing.

Apoiar a avaliação e a adequação de controles específicos de segurança da informação para novos sistemas ou serviços.

Analisar criticamente incidentes em conjunto com o Comitê de Segurança da Informação.

Apresentar as atas e os resumos das reuniões do Comitê de Segurança da Informação, destacando os assuntos que exijam intervenção do próprio comitê ou de outros membros da diretoria.

Manter comunicação efetiva com o Comitê de Segurança da Informação sobre assuntos relacionados ao tema que afetem ou tenham potencial para afetar a ELR-SI.

Buscar alinhamento com as diretrizes corporativas da instituição.

3.4.3 Do Comitê de Segurança da Informação

Deve ser formalmente constituído por colaboradores com nível hierárquico mínimo gerencial, nomeados para participar do grupo pelo período de um ano.

A composição mínima deve incluir um colaborador de cada uma das gerências da ELR-SI.

Deverá o CSI reunir-se formalmente pelo menos uma vez a cada seis meses. Reuniões adicionais devem ser realizadas sempre que for necessário deliberar sobre algum incidente grave ou definição relevante para a ELR-SI.

O CSI poderá utilizar especialistas, internos ou externos, para apoiarem nos assuntos que exijam conhecimento técnico específico.

Cabe ao CSI:

- propor investimentos relacionados à segurança da informação com o objetivo de reduzir mais os riscos;
- propor alterações nas versões da PSI e a inclusão, a eliminação ou a mudança de normas complementares;
- avaliar os incidentes de segurança e propor ações corretivas;
- definir as medidas cabíveis nos casos de descumprimento da PSI e/ou das Normas de Segurança da Informação complementares.

4. Dados Pessoais De Colaboradores

A ELR-SI se compromete em não acumular ou manter intencionalmente Dados Pessoais de Colaboradores além daqueles relevantes na condução de auditoria de sistemas de informação. Todos os Dados Pessoais de Colaboradores serão considerados dados confidenciais (ver item 2.3). Dados Pessoais de Colaborador sob a responsabilidade da ELR-SI não serão usados para fins diferentes daqueles para os quais foram coletados. Dados Pessoais de Colaboradores não serão transferidos para terceiros, exceto quando exigido por parceiro da empresa de acordo com suas necessidades auditoriais, e desde que tais terceiros mantenham a confidencialidade dos referidos dados, incluindo-se, neste caso a lista de endereços eletrônicos (e-mails) usados pelos colaboradores da ELR-SI.

5. Programas Ilegais

E vedado o uso de todo e qualquer software que não seja devidamente licenciado para a ELR-SI. O mesmo se aplica para softwares em versões conhecidas como “crack(s)” patches e demais praticas de pirataria.

6. Compartilhamento De Pastas E Dados

É de obrigação dos colaboradores rever periodicamente todos os compartilhamentos existentes em suas estações de trabalho e garantir que dados considerados confidenciais e/ou restritos não estejam disponíveis a acessos indevidos, inclusive acessos por outros colaboradores a material sensível que não faz parte das suas necessidades de trabalho.

7. Backup Do Sistema Integrado E Servidores De Rede

Cópias de segurança do sistema integrado e servidores de rede são de responsabilidade da equipe de segurança e deverão ser atualizadas semanalmente. Ao final de cada mês também deverá ser feita uma cópia de segurança com os dados de fechamento do mês

e do sistema integrado de banco de dados. Esta cópia será feita imediatamente após a comunicação formal da Contabilidade, por meio de memorando eletrônico, que o referido mês foi encerrado. Trimestralmente, a equipe de segurança enviará uma cópia extra do backup de fechamento dos referidos meses, para ser arquivada na Contabilidade.

8. Segurança E Integridade Do Banco De Dados

O gerenciamento dos bancos de dados é responsabilidade exclusiva da equipe de segurança de informação, assim como a manutenção, alteração e atualização de equipamentos e programas nas estações de trabalho disponíveis aos colaboradores.

9. Admissão ou Demissão de Colaboradores, Temporários e/ou Estagiários

A equipe de Recursos Humanos da ELR-SI deverá informar a equipe de segurança da informação, toda e qualquer movimentação de temporários e/ou estagiários, e admissão/demissão de colaboradores, para que os mesmos possam ser efetivamente cadastrados ou excluídos no sistema da ELR-SI. Isto inclui o fornecimento de suas senhas e registro do seu nome como usuário no sistema pela equipe de segurança da informação.

Cabe ao setor solicitante da contratação a comunicação a equipe de segurança da informação sobre as rotinas a que o novo contratado terá direito de acesso. No caso de temporários e/ou estagiários deverá também ser informado o tempo em que o mesmo prestará serviço á ELR-SI, para que na data de seu desligamento possam também ser encerradas as atividades relacionadas ao direito de seu acesso ao sistema. No caso de demissão, a equipe de Recursos Humanos deverá comunicar o fato o mais rapidamente possível à equipe de segurança da informação, para que o colaborador demitido seja excluído do sistema. Cabe ao setor de Recursos Humanos dar conhecimento e obter as devidas assinaturas de concordância dos novos contratados em relação à Política de Segurança da Informação da ELR-SI. Nenhum colaborador, estagiário ou temporário, poderá ser contratado, sem ter expressamente concordado com esta política.

Cabe ao setor de segurança da informação recolher os equipamentos, mídias digitais, e quaisquer dispositivos tecnológicos que contenham informações *Internas, Confidenciais ou Restritas* que estiverem em posse de um colaborador a ser demitido.

10. Transferência De Colaboradores

Quando um colaborador for promovido ou transferido de seção ou gerência, a equipe de recursos humanos deverá comunicar o fato à equipe de segurança de informação, para que sejam feitas as adequações necessárias para o acesso do referido colaborador ao sistema da ELR-SI.

11. Política de Identificação e senhas

Os dispositivos de identificação e senhas protegem a identidade do colaborador usuário, evitando e prevenindo que uma pessoa se faça passar por outra perante a ELR-SI e/ou terceiros.

O uso dos dispositivos e/ou senhas de identificação de outra pessoa constitui crime tipificado no Código Penal Brasileiro (art. 307 – falsa identidade).

Tal norma visa estabelecer critérios de responsabilidade sobre o uso dos dispositivos de dentificação e deverá ser aplicada a todos os colaboradores.

Todos os dispositivos de identificação utilizados na ELR-SI, como o número de registro do colaborador, o crachá, as identificações de acesso aos sistemas, os certificados e assinaturas digitais e os dados biométricos têm de estar associados a uma pessoa física e atrelados inequivocamente aos seus documentos oficiais reconhecidos pela legislação brasileira.

O usuário, vinculado a tais dispositivos identificadores, será responsável pelo seu uso correto perante a instituição e a legislação (cível e criminal).

Todo e qualquer dispositivo de identificação pessoal, portanto, não poderá ser compartilhado com outras pessoas em nenhuma hipótese.

Se existir login de uso compartilhado por mais de um colaborador, a responsabilidade perante a ELR-SI e a legislação (cível e criminal) será dos usuários que dele se utilizarem. Somente se for identificado conhecimento ou solicitação do gestor de uso compartilhado ele deverá ser responsabilizado.

É proibido o compartilhamento de login para funções de administração de sistemas.

O Departamento de Recursos Humanos da ELR-SI é o responsável pela emissão e pelo controle dos documentos físicos de identidade dos colaboradores.

A Equipe de Segurança da Informação responde pela criação da identidade lógica dos colaboradores na instituição, nos termos do Procedimento para Gerenciamento de Contas de Grupos e Usuários.

Devem ser distintamente identificados os visitantes, estagiários, empregados temporários, empregados regulares e prestadores de serviços, sejam eles pessoas físicas e/ou jurídicas. Ao realizar o primeiro acesso ao ambiente de rede local, o usuário deverá trocar imediatamente a sua senha conforme as orientações apresentadas.

Os usuários que não possuem perfil de administrador deverão ter senha de tamanho variável, possuindo no mínimo 8 (oito) caracteres alfanuméricos, utilizando caracteres especiais (@ # $ %) e variação entre caixa-alta e caixa-baixa (maiúsculo e minúsculo) sempre que possível.

Já os usuários que possuem perfil de administrador ou acesso privilegiado deverão utilizar uma senha de no mínimo 10 (dez) caracteres, alfanumérica, utilizando caracteres especiais (@ # $ %) e variação de caixa-alta e caixa-baixa (maiúsculo e minúsculo) obrigatoriamente.

É de responsabilidade de cada usuário a memorização de sua própria senha, bem como a proteção e a guarda dos dispositivos de identificação que lhe forem designados.

As senhas não devem ser anotadas ou armazenadas em arquivos eletrônicos (Word, Excel, etc.), compreensíveis por linguagem humana (não criptografados); não devem ser baseadas em informações pessoais, como próprio nome, nome de familiares, data de nascimento, endereço, placa de veículo, nome da empresa, nome do departamento; e não devem ser constituídas de combinações óbvias de teclado, como “abcdefgh”, “87654321”, entre outras.

Após 3 (três) tentativas de acesso, a conta do usuário será bloqueada. Para o desbloqueio é necessário que o usuário entre em contato com a Equipe de Segurança da ELR-SI.

Deverá ser estabelecido um processo para a renovação de senha (confirmar a identidade).

Os usuários podem alterar a própria senha, e devem ser orientados a fazê-lo, caso suspeitem que terceiros obtiveram acesso indevido ao seu login/senha.

A periodicidade máxima para troca das senhas é 45 (quarenta e cinco) dias, não podendo ser repetidas as 3 (três) últimas senhas. Os sistemas críticos e sensíveis para a instituição e os logins com privilégios administrativos devem exigir a troca de senhas a cada 30 dias. Os sistemas devem forçar a troca das senhas dentro desse prazo máximo.

Todos os acessos devem ser imediatamente bloqueados quando se tornarem desnecessários.

Portanto, assim que algum usuário for demitido ou solicitar demissão, o Departamento de Recursos Humanos deverá imediatamente comunicar tal fato à Equipe de Segurança, a fim de que essa providência seja tomada. A mesma conduta se aplica aos usuários cujo contrato ou prestação de serviços tenha se encerrado, bem como aos usuários de testes e outras situações similares.

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

As senhas dos colaboradores não devem ser reveladas a ninguém, inclusive à própria equipe de segurança, nem serem utilizadas em ambientes descriptografados e que possam ser lidos facilmente.

Todos os programas que forem executados com a senha de um colaborador serão de responsabilidade do mesmo, válido também para qualquer emissão de relatório, acesso aos servidores, mudanças feitas aos bancos de dados e envio de e-mails.

12. Cópias De Segurança De Arquivos

É vedada toda e qualquer copia de arquivos que não seja expressamente autorizada pela diretoria. Cabendo somente a equipe de segurança da informação realizá-la.

13. Politica de e-mails

- Não abra anexos com as extensões .bat, .exe, .src, .lnk e .com caso estes anexos não tenham sido solicitados.
- E-mails com assuntos não relacionados ao trabalho e de remetentes desconhecidos não devem ser acessados. Os colaboradores devem submeter qualquer dúvida em relação a e-mails ao seus supervisores.
- Não reenvie e-mails do tipo corrente, aviso de vírus, avisos da Microsoft/AOL/Symantec, Bancos, apelos sociais e similares.
- Não utilize o e-mail da empresa para assuntos pessoais.
- Não enviar e-mails para mais de 10 destinatários de uma única vez (to, cc, bcc).
- Evite anexos maiores que 2GB.
- Não compartilhe senhas por e-mail.
- Utilize sempre a assinatura digital providenciada.

14. Políticas de acesso a Internet

A internet deve ser utilizada para fins corporativos, enriquecimento intelectual ou como ferramenta de busca de informações, tudo que possa vir a contribuir para o desenvolvimento de atividades relacionadas à empresa. Os acessos à internet serão monitorados através de identificação e autenticação do usuário. O acesso às páginas e web sites é de responsabilidade do colaborador, sendo proibido a visualização, transferência (downloads), cópia ou qualquer outro tipo de acesso a sites:

- De conteúdo pornográfico ou relacionados a sexo.
- Que defendam atividades ilegais.
- Que menosprezem, depreciem ou incitem o preconceito a qualquer classe social, raça, religião, crença ou gênero.
- Que promovam a participação em salas de discussão de assuntos não relacionados aos negócios da ELR-SI.
- Que promovam discussão pública sobre os negócios da ELR-SI, a menos que autorizado pela Diretoria.
- Que possibilitem a distribuição de informações de nível “Confidencial”.
- Que permitam a transferência (downloads) de arquivos e/ou programas ilegais.

15. Política de uso de estações de trabalho e equipamentos da ELR-SI

Os recursos que permitem o acesso à informação são auto - rizados e disponibilizados exclusivamente para o usuário desempenhar suas funções na ELR-SI ou para outras situações formalmente permitidas.

Quando o usuário se comunicar através de recursos de tecnologia da ELR-SI, a linguagem falada ou escrita deve ser profissional, de modo que não comprometa a imagem da Empresa.

Os conteúdos acessados e transmitidos através dos recursos de tecnologia da ELR-SI devem ser legais, de acordo com o Código de Ética da entidade, e devem contribuir para as atividades profissionais do usuário.

O uso dos recursos de tecnologia da ELR-SI pode ser examinado, auditado ou verificado pela Empresa, mediante autorização expressa da Diretoria Executiva, sempre respeitando a legislação vigente.

Cada usuário é responsável pelo uso dos recursos que lhe foram fisicamente entregues e estão sob sua custódia, devendo garantir a conservação, guarda e legalidade dos programas (softwares) instalados.

Em caso de roubo ou furto de recursos físicos de tecnologia, o usuário deve fazer o registro da ocorrência em unidade policial, comunicar ao seu gestor imediatamente.

Os recursos de tecnologia da ELR-SI, disponibilizados para os usuários, não podem ser repassados para outra pessoa interna ou externa da organização.

Ao identificar qualquer irregularidade no recurso de tecnologia o usuário deve comunicar imediatamente à Assessoria de Segurança da Informação.

16. Uso De Computadores Pessoais

Qualquer equipamento computacional particular a serem usados dentro da rede ou ambiente interno da ELR-SI precisam ser avaliados pelo equipe de segurança, cabendo a equipe de segurança de TI da ELR-SI permitir ou negar a utilização destes equipamentos nas premissas restritas da empresa.

Os recursos de tecnologia da informação, disponibilizados para os usuários, têm como objetivo a realização de atividades profissionais, mesmo quando utilizados em equipamentos pessoais, sendo que a proteção do recurso computacional de uso individual é de responsabilidade do colaborador que detém sua posse.

É de responsabilidade do colaborador assegurar a integridade de seus equipamentos pessoais, assim como a confidencialidade e disponibilidade da informação contida no mesmo, para tanto, toda informação não classificada como “Pública” referente à ELR-SI e seus Parceiros contida em equipamentos de uso pessoal dos colaboradores deverá ser criptografada.

Em caso de furto o colaborador deverá alertar imediatamente a ocorrência em uma delegacia de polícia e também à equipe de segurança da ELR-SI.

17. Política Social

Os Colaboradores da ELR-SI deverão estar atentos quanto à ataques de Engenharia Social, que é um termo utilizado para representar a habilidade de enganar pessoas, visando obter informações sigilosas. Os colaboradores devem estar cientes que ataques de engenharia social podem ser caracterizados pelo contato direto entre o engenheiro social e o colaborador vítima através de telefonemas e até mesmo pessoalmente, pois engenheiro social nem sempre é alguém desconhecido. Mas também podem ser caracterizados pela utilização de softwares ou ferramentas para invasão, como, por exemplo, vírus, cavalos de Tróia ou através de sites e e-mails falsos para assim obter informações desejadas.

Portanto é de extrema importância que os colaboradores:

- Não falar sobre a política de segurança da empresa com terceiros ou em locais públicos.
- Somente aceitar ajuda técnica de um membro de nossa equipe técnica previamente apresentado e identificado, com atenção para os critérios da cláusula 11.
- Nunca executar procedimentos técnicos cujas instruções tenham sido recebidas por e-mail, também visando todas os critérios estabelecidos na cláusula 13.
- Relatar à Equipe de Segurança pedidos externos ou internos que venham a discordar dos tópicos anteriores.

18. Termos e Definições

TI: Tecnologia da Informação

Software: É a parte lógica executada por um hardware, o conjunto de instruções e dados processados nos servidores e computadores. Toda interação dos usuários de computadores é realizada através de softwares.

Hardware: É a parte fisica que executa as instruçoes em baixo nivel composta por placas e dispositivos logicos: chips , circuitos integrados etc

Backup: É a cópia de dados de um dispositivo de armazenamento a outro para que possa ser restaurado em caso da perda dos dados originais, o que pode envolver apagamentos acidentais ou corrupção de dados.

Mídias Removíveis: Dispositivos de armazenamento portáteis que permitem a leitura e gravação de dados tais como: CD, DVD, Disquete, Pen Drive, cartão de memória entre outros.

USB: É um tipo de conexão "ligar e usar" que permite a conexão de periféricos sem a necessidade de desligar o computador.

VPN (Virtual Private Network): Modalidade de acesso à rede corporativa, que possibilita a conectividade, via internet, de um equipamento externo à rede interna da corporação, provendo funcionalidades e privilégios como se o mesmo estivesse conectado física e diretamente à rede interna. Comumente é utilizado por colaboradores em trânsito.

Softwares de Mensagens: São programas que permitem a usuários se comunicarem remotamente (à distância), através de conexão com a Internet. Por meio destes programas, é possível enviar mensagens de texto entre equipamentos fisicamente distantes. Também é possível enviar arquivos ou iniciar sessões de conversação com áudio e/ou com vídeo, em tempo real.

Firewall: É um dispositivo de uma rede de computadores que tem por objetivo aplicar uma política de segurança a um determinado ponto da rede.

Modem 3G/4G: É um dispositivo sem fio, com saída USB para conexão em outro dispositivo tais como Tablets (com suporte 3G/4G), notebooks, netbooks, desktops, etc. objetivando conexão com a internet. O modem 3G/4G recebe e decodifica o sinal digital de alta velocidade transmitido pelas operadoras de celulares para aparelhos portáteis (celulares, smartphones e notebooks) compatíveis com a tecnologia 3G/4G.

Servidor: é um sistema de computação centralizada que fornece serviços a seus usuários (clientes).

Ativo: Qualquer elemento importante para os negócios da empresa, que tem um valor para a organização e, consequentemente, necessita ser adequadamente protegido.

Endomarketing: divulgação interna de campanhas por meio do sistema de comunicação formal ou informal da ELR-SI.

19. Propriedade Intelectual

É de propriedade da ELR-SI, todos os “designs”, criações ou procedimentos desenvolvidos por qualquer colaborador durante o curso de seu vínculo empregatício com a ELR-SI.

20. Penalidades

A quebra do sigilo e/ou da confidencialidade das informações, devidamente comprovada, possibilitará a imediata aplicação de penalidades previstas conforme disposições contratuais e legislação em vigor que trata desse assunto, podendo culminar na rescisão do CONTRATO PRINCIPAL firmado entre as PARTES. Neste caso, a CONTRATADA, estará sujeita, por ação ou omissão, ao pagamento ou recomposição de todas as perdas e danos sofridos pela CONTRATANTE, inclusive as de ordem moral, bem como as de responsabilidades civil e criminal, as quais serão apuradas em regular processo administrativo ou judicial, sem prejuízo das demais sanções legais cabíveis, conforme Art. 87 da Lei nº. 8.666/93