POLÍTICA DE SEGURANÇA e CÓDIGO DE CONDUTA

2009

TECNISA

Mais construtora por m²

POLÍTICA DE SEGURANÇA e CÓDIGO DE CONDUTA

2009

TECNISA

Mais construtora por m²

Política de Segurança e Código de Conduta TECNISA
Ed. 2009

Autoria:
FGV Projetos – SP - Prof. João Roberto Peres (coordenador do projeto)

Realização e Aprovação:
CEST - Comitê de Ética e Segurança – Tecnisa
FGV Projetos – SP

Presidente CEST: Roberto Moliner (DTI)

Membros CEST: Denilson Novelli (e-business), Denise Bueno (RHU), Ivam Marcelo Torres (CTB), Jaqueline Guerra (DQP), Maurício Bortoli (FIN), Neil Amereno (DRI), Paola Carrara Dsamby Gomes (JUR), Tatiane Pereira (JUR – VND), Wagner Souza (COM)

Suplentes CEST: Bruno Gigliote (COM), Cecília Dantas (DTI), Cristiane Sampaio e Sampaio (JUR), Crystiane Silva (JUR – VND), Denize Nunes (DQP), Fernando Fernandez (CTB), Geraldo Colonhezi (DRI), Paulo Schiavon (e-business), Priscilla Rosa (RHU) e Thatiana Senna (FIN).

Escritório de Segurança Corporativa: André Rodrigues de Almeida e Carlos Wagner B. Lima.

Presidente Tecnisa: Carlos Alberto Julio

Diretores Tecnisa: Douglas Duarte, Fabio Villas Boas, José Carlos Lazaretti, Joseph Meyer Nigri, Leonardo Paranaguá, Romeo Busarello e Tomas Banlaky.

ÍNDICE

POLÍTICA DE SEGURANÇA

TECNISA

Mais construtora por m²

POLÍTICA DE SEGURANÇA TECNISA

1.1 OBJETIVO

A Política de Segurança Corporativa da TECNISA S.A. tem como objetivo apresentar as estratégias definidas pela alta direção no tocante à segurança corporativa e das informações na organização, para atender aos requerimentos dos negócios, considerando:

a) Definir abrangência da segurança da organização;

b) Definir as responsabilidades e autoridades;

c) Definir, por meio de suas diretrizes, todas as ações de segurança corporativa reduzindo os riscos e garantindo a integridade, o sigilo e a disponibilidade das informações e dos sistemas, das instalações, dos recursos e das pessoas;

d) Direcionar a adoção de soluções de segurança integradas e gerenciadas continuamente;

e) Servir de referência para operação, auditoria, apuração e avaliação de responsabilidades.

1.2 ABRANGÊNCIA

A Política de Segurança Corporativa da TECNISA nesta nova versão abrange os seguintes aspectos:

a) Requisitos de Segurança Pessoal;

b) Requisitos de Segurança Patrimonial, Física e Eletrônica;

c) Requisitos de Segurança Lógica e da Informação;

d) Requisitos de Segurança Operacional.

1.3 RESPONSABILIDADES E AUTORIDADES

Responsáveis pelo Fórum de SC – Presidente e Corpo diretivo da TECNISA.

Diretor responsável por SC: Dr. Tomas Laszlo Banlaky.

Designado – Governança da Segurança Corporativa – CIO: Roberto Moliner.

Designado – Gestão do Escritório de Segurança Corporativa – SO: André R. Almeida

1.4 DEFINIÇÕES E DIRETRIZES

Definições

O tema "Segurança da Informação" passou a ser assunto estratégico nos meios empresariais.

A TECNISA com suas ações pioneiras e inovadoras vem há mais de 8 (oito) anos aperfeiçoando sua Política de Segurança Corporativa, com divulgação periódica a todos os seus funcionários, colaboradores, parceiros, fornecedores, clientes e acionistas.

Nesta nova edição do tema Política de Segurança Corporativa, buscou-se ampliar os horizontes e ajustar novas diretrizes capazes de antecipadamente elevar a segurança empresarial a níveis mais avançados (3.0), integrando sistemas, processos e usuários, na busca de reduzir ao máximo as ameaças, que constantemente afrontam a inteligência de sua equipe técnica que convive com os constantes desafios do mercado.

A segurança corporativa é um tema que representa um processo contínuo de trabalho e é essencial para a própria sobrevivência dos negócios e da organização. Todos os funcionários, prestadores de serviços, fornecedores e parceiros e demais envolvidos, devem conhecer, entender e aplicar os controles de segurança em suas atividades diárias.

"A contínua melhoria da segurança corporativa depende de todos."

O que é Informação?

O conceito de informação e definido como o conjunto de dados associados que, quando devidamente interpretados, geram conhecimento e permitem ações efetivas. Tais ações podem ser positivas ou não, de forma que podem acarretar exposição de clientes, fraudes e deturpação na imagem da organização perante o mercado. As informações alojadas nas instalações físicas, Rede de Dados e de comunicações, meios magnéticos ou óticos, em documentos impressos e até verbais na TECNISA são de sua exclusiva responsabilidade e propriedade.

A obtenção de informações pode ocorrer através da leitura de um Relatório Gerencial ou Contábil, de documentos e instruções, manuais e documentos diversos, e até mesmo nas telas das estações de trabalho. A informação pode estar impressa, escrita, armazenada em diversos meios ou em transito em Redes Locais ou em grandes distâncias, em e-mail ou correio de voz. O importante sobre as informações é que elas devem ser guardadas ou divulgadas conforme a sua importância e valor estratégico para os negócios da TECNISA, portanto elas devem ser protegidas desde a sua geração, armazenamento, manipulação, integração, compartilhamento, processamento, divulgação e descarte.

O que é segurança corporativa da informação?

O termo segurança corporativa da informação vem sendo empregado para designar um conjunto de controles sobre o tratamento das informações, baseados em uma política previamente determinada pela alta direção das organizações.

As principais características que devem ser consideradas sobre a segurança das informações, de forma que se garanta que toda a informação deve possuir, compreendem:

• **Integridade** – permite estabelecer a garantia de que uma determinada informação não foi violada ou tenha sofrido adulteração ou modificações não autorizadas em relação a sua forma original.

• **Confidencialidade** – é a característica que permite estabelecer a garantia de que uma determinada informação só possa ser empregada ou acessada por pessoas cuja identificação e permissão sejam autorizadas.

• **Disponibilidade** – estabelece a garantia de que as pessoas devidamente identificadas e autorizadas possam ter acesso às informações a qualquer tempo.

• **Rastreabilidade** – é uma das características que garantem que as informações possam ter o seu fluxo de hospedagem, transmissão e acessos registrados para futuras auditorias.

• **Auditabilidade** – compreende as características que garantem que as informações possam ser examinadas quanto as suas demais características de Integridade, Confidencialidade, Disponibilidade e Rastreabilidade de forma a se obter a certificação que essas características de fato estão ativas e efetivas.

Todas as características (controles) devem ser estabelecidas com o objetivo de garantir que o padrão determinado, de segurança da informação possa ser aplicado em uma organização. A segurança das informações é uma atribuição de todos os funcionários,

contratados, prestadores de serviços, fornecedores, parceiros e cliente, que devem colaborar para que se possa atingir um alto grau de confiabilidade e privacidade no tratamento das informações.

O que é Segurança Corporativa ou Orgânica?

O conceito de segurança corporativa ou modernamente chamada de segurança orgânica compreende a aplicação de todas as disciplinas sobre Segurança Patrimonial, Eletrônica, Pessoal, Trabalho, das Informações, Contingênciais, de Continuidade dos Negócios, de Redes, Inteligência e Contra-Inteligência, Criptográfica, etc.

O que é Política de Segurança?

Política de Segurança representa a determinação de princípios sobre segurança empresarial ou corporativa, estabelecida pela alta direção de uma organização, para orientar o desenvolvimento de medidas e controles que garantam a segurança das informações, dos bens patrimoniais tangíveis e intangíveis e das pessoas.

A Política de Segurança Corporativa da Informação TECNISA foi desenvolvida por Consultoria Externa, e vem sendo ajustada continuamente desde 1999, aprovada pelo "Comitê de Ética e Segurança TECNISA" e homologada pela Diretoria executiva.

O que significa “princípios e Diretrizes” da Política de Segurança?

O termo “princípios e Diretrizes” são empregados para especificar as determinações aprovadas pela alta direção da organização, quanto seus anseios em relação a controles e processos de segurança, que garantam a efetiva proteção dos bens da “informação – patrimônio – pessoas”. A Política de Segurança da Informação TECNISA está expressa em Princípios, Diretrizes e Atribuições.

Qual o significado de Normas?

Normas representam um conjunto de regras específicas que descrevem o que deve ou não ser praticado ou executado por um grupo de pessoas ou ambiente, processo, serviço, que será adotada como base para sua aplicação ou avaliação.

Qual o significado de Procedimentos?

Procedimentos representam as descrições da maneira de se proceder em atividades, serviços, processos, estabelecidos por uma Norma ou designados em “princípios” de uma política.

Termos Aplicáveis neste documento

a) **Ativo de Informação** – é o patrimônio composto por todos os dados e informações geradas e manipuladas durante a execução dos sistemas e processos das organizações, clientes, investidores e acionistas vinculados à TECNISA S.A.;

b) **Ativo de Processamento** – é o patrimônio composto por todos os elementos de hardware e software necessários para a execução dos sistemas e processos das entidades relacionadas à TECNISA S.A., tanto os produzidos internamente quanto os adquiridos;

c) **Controle de Acesso** – são restrições ao acesso físico ou às informações de um sistema exercidas pela gerência de segurança das organizações relacionadas à TECNISA S.A.;

d) **Custódia** – consiste na responsabilidade de se guardar um ativo para terceiros.
Entretanto, a custódia não permite automaticamente o acesso ao ativo, nem o direito de conceder acesso a outros;

e) **Direito de Acesso** – é o privilégio associado a um cargo, pessoa ou processo para ter acesso a um ativo;

f) **ESC** - Escritório de Segurança Corporativa – conjunto de pessoas designadas para atuar exclusivamente em processos de segurança corporativa;

g) **Ferramentas** – é um conjunto de equipamentos, programas, procedimentos, normas e demais recursos através dos quais se aplicam a Política de Segurança vinculada à TECNISA S.A.;

h) **Incidente de Segurança** – é qualquer evento ou ocorrência que promova uma ou mais ações que comprometam ou que possam significar uma ameaça à integridade, autenticidade, ou disponibilidade de qualquer ativo da TECNISA S.A.;

i) **Integrantes** – são pessoas físicas ou jurídicas, que de alguma forma se relacionam com a TECNISA, sejam como prestadores de serviços, fornecedores, parceiros, etc.

j) **Proteção dos Ativos** – é o processo pelo qual os ativos (bens) devem receber classificação quanto ao grau de sensibilidade. O meio de registro de um ativo de informação deve receber a mesma classificação de proteção dada ao ativo que o contém;

k) **Responsabilidade(s)** – são as obrigações e os deveres da pessoa que ocupa determinada função;

l) **Senha Fraca ou Óbvia** – é aquela na qual se utilizam caracteres de fácil associação com o dono da senha, ou que seja muito simples ou pequena, tais como: datas de aniversário, casamento, nascimento, o próprio nome, o nome de familiares, seqüências numéricas simples, palavras com significado em qualquer língua, dentre outras.

m) **SO** – Security Officer – profissional qualificado e dedicado a Segurança;

1.5 REQUISITOS DE SEGURANÇA DE PESSOAL

1.5.1 Definições

Segurança das Pessoas compreende uma das missões mais importantes da organização. Ela estabelece um conjunto de medidas e procedimentos de segurança a serem observados por todos os funcionários/colaboradores e pelos prestadores de serviço (terceiros ou integrantes), necessários à proteções dos ativos da TECNISA S.A..

1.5.2 Objetivos

Reduzir os riscos de erros humanos, furto, roubo, apropriação indébita, fraude, infiltração e uso não apropriado dos ativos da TECNISA S.A.;

Prevenir e neutralizar as ações de pessoas que possam comprometer a segurança da TECNISA S.A.;

Orientar e estabelecer os parâmetros de capacitação de todo o pessoal envolvido na realização de trabalhos diretamente relacionados aos controles de segurança da TECNISA S.A., assim como o pessoal em desempenho de funções de apoio, tais como a manutenção das instalações físicas e a adoção de medidas de proteção compatíveis com a natureza da função que desempenham;

Orientar o processo de avaliação de todo o pessoal que trabalhe na TECNISA S.A. e nas empresas a ela vinculadas, mesmo em caso de funções desempenhadas por prestadores de serviço.

1.5.3 Diretrizes

1.5.3.1 Processo de Admissão

Compete à área de RHU adotar critérios rígidos para o processo de recrutamento seletivo de candidatos em funções ligadas ao ciclo de vida dos serviços administrativos e produtivos, com o propósito de selecionar para os quadros das entidades integrantes e da TECNISA S.A. pessoas reconhecidamente idôneas e sem antecedentes que possam vir a comprometer a segurança ou credibilidade da TECNISA S.A.;

A TECNISA S.A. executará rigoroso critério seletivo de estagiários que venham atuar em atividades críticas da organização, atribuindo a eles apenas as atividades coerentes com a capacitação avaliada.

O funcionário ou prestador de serviços assina um termo de compromisso assumindo o dever de cumprir a Política de Segurança da TECNISA S.A. e o Acordo de Confidencialidade e Exclusividade de Propriedade das Informações da TECNISA S.A.. Nesses documentos cada funcionário ou terceiro assume o dever de manter sigilo, mesmo quando desligado, sobre todos os ativos de informações e de processos operacionais exclusivos da TECNISA.

1.5.3.2 Atribuições da Função

As atribuições de cada função devem ser relacionadas de acordo com a característica das atividades desenvolvidas, a fim de determinar-se o perfil necessário do funcionário ou prestador de serviço, considerando-se os seguintes itens:

a) **A descrição sumária das tarefas inerentes à função;**
A descrição sumária das tarefas inerentes a cada função deve ser descrita pelos gestores da TECNISA S.A.. e encaminhadas à área de RHU, sempre que houver mudanças de requerimentos;

b) **As necessidades de acesso a informações sensíveis;**
Nesse tópico são descritas as razões pelas quais é justificado o acesso do funcionário ou terceiros às informações sensíveis à TECNISA S.A.. São priorizadas as tarefas e as diferentes funções que o respectivo cargo desempenhará. Devem ser descrita pelos gestores da TECNISA S.A.. e encaminhadas à área de RHU, sempre que houver mudanças de requerimentos;

c) **O grau de sensibilidade do setor onde a função é exercida;**
Esse tópico diz respeito ao setor ou nível físico ao qual o funcionário ou terceiro tem acesso e está intimamente ligado ao item b. Os funcionários ou terceiros cujas funções são diretamente ligadas a informações estratégicas ou confidenciais, devem trabalhar em nível 3, sendo que os demais funcionários podem trabalhar em nível 2 (informações de uso interno). Nível 1 apenas para as informações públicas.

d) **As necessidades de contato de serviço interno e/ou externo;**
Esse tópico, também relacionado ao cargo do funcionário ou terceiro diz respeito à necessidade do mesmo em manter contatos de serviço interno e/ou externo à TECNISA S.A.. Os funcionários ou terceiros com contatos externos seguem procedimentos que incluem a assinatura de acordo de confidencialidade antes do acesso a qualquer informação classificada em nível 2 e 3.

e) **As características de responsabilidade, decisão e iniciativas inerentes à função;**
Nesse tópico serão descritas as funções operacionais, gerenciais e administrativas de cada cargo. Todas as exceções que tenham impacto na segurança devem sempre ser submetidas, para aprovação prévia, ao Escritório de Segurança Corporativa.

f) **A qualificação técnica necessária ao desempenho da função;**
Nesse tópico serão levantadas as qualificações técnicas necessárias ao desempenho da função. As informações contidas nesse tópico têm origem no Departamento de Recursos Humanos. Esse item é sensivelmente crítico para as áreas diretamente relacionadas com infraestrutura, atividade técnica de TI&C, Segurança e Engenharia, sendo necessária, portanto, a comprovação de capacitação através de experiência ou de curso e/ou certificação específica.

1.5.3.3 Levantamento de Dados Pessoais

O levantamento de dados pessoais é elaborado através de pesquisa, feita por empresa especializada, do histórico da vida pública do candidato, com o propósito de verificação de seu perfil.

1.5.3.4 Entrevista de Admissão

Deve ser realizada, por profissional qualificado, com o propósito de confirmar e/ou identificar dados não detectados ou não confirmados durante o levantamento de dados pessoais do candidato;

Deverão ser avaliadas, na entrevista inicial, as características de interesse e motivação do candidato, sendo que as informações veiculadas na entrevista do candidato são apenas aquelas de caráter público;

1.5.3.5 Desempenho da Função

Periodicamente, o desempenho dos funcionários e integrantes deverá ser acompanhado e avaliado com o propósito de detectar a necessidade de atualização técnica e de segurança;

É dado aos funcionários ou prestadores de serviços da TECNISA S.A. acesso às informações, mediante o fornecimento de instruções e orientações sobre as medidas e procedimentos de segurança;

1.5.3.6 Credencial de Segurança

O funcionário e ou integrantes são identificados por meio de uma credencial (crachá apropriado) que habilita o acesso às informações sensíveis, de acordo com a classificação do grau de sigilo da informação e, conseqüentemente, com o grau de sigilo compatível ao cargo e/ou à função a ser desempenhada;

A Credencial de Segurança somente é concedida pelo Escritório de Segurança Corporativa e é fundamentada na necessidade de conhecimento técnico dos aspectos inerentes ao exercício funcional e na análise da sensibilidade do cargo e/ou função;

A validade é de um ano de concessão a um indivíduo de uma credencial de segurança. Este prazo poderá ser prorrogado por igual período, quantas vezes forem necessárias, por solicitação da Gerencia, enquanto exigir a necessidade do serviço.

1.5.3.7 Treinamento em Segurança Corporativa

Nos treinamentos de segurança, a Política de Segurança Corporativa (inclusive da informação) e procedimentos específicos, são apresentados aos funcionários e prestadores de serviço, com o propósito de desenvolver e manter uma efetiva conscientização de segurança, assim como promover o seu fiel cumprimento.

Todo funcionário e integrante é treinado na ocasião de sua admissão na companhia e passa por uma reciclagem ao menos uma vez por ano.

1.5.3.8 Acompanhamento no Desempenho da Função

São realizados processos de avaliação de desempenho da função que documentam a observação do comportamento pessoal e funcional dos funcionários e integrantes. A avaliação é realizada pela chefia imediata dos mesmos;

São registrados os atos, atitudes e comportamentos positivos e negativos relevantes, verificados durante o exercício profissional;

Os comportamentos incompatíveis ou que possam gerar comprometimentos à segurança devem ser averiguados e comunicados à chefia imediata;

As chefias imediatas asseguram que todos os funcionários ou prestadores de serviços tenham conhecimento e compreensão das normas e procedimentos de segurança em vigor;

1.5.3.9 Processo de Desligamento, Férias e Licenças.

O acesso de ex-funcionários às instalações da TECNISA S.A. é restrito às áreas de acesso público;

Sua credencial, sua identificação, seu crachá, o uso de equipamentos, mecanismos e acessos físicos e lógicos devem ser revogados;

1.5.3.10 Processo de Encerramento

O funcionário ou prestador de serviço assina, antes do desligamento, declaração de que não possui qualquer tipo de pendência junto às diversas unidades que compõem a TECNISA S.A..

1.5.3.11 Entrevista de Desligamento

É realizada entrevista de desligamento para orientar o funcionário ou prestador de serviço sobre sua responsabilidade na manutenção do sigilo de dados e/ou conhecimentos sigilosos de sistemas críticos aos quais teve acesso durante sua permanência na TECNISA S.A.;

1.5.3.12 Deveres e Responsabilidades

Deveres dos funcionários ou prestadores de serviços

São deveres dos empregados ou prestadores de serviço (integrantes);

a) Preservar a integridade e guardar sigilo das informações de que fazem uso, bem como zelar e proteger os respectivos recursos de processamento de informações;

b) Cumprir a Política de Segurança Corporativa, sob pena de incorrer nas sanções disciplinares e legais cabíveis;

c) Utilizar os sistemas de informações da TECNISA S.A. e os recursos a ela relacionados somente para os fins previstos pela Gerência de Segurança;

d) Cumprir as regras específicas de proteção estabelecidas aos ativos da empresa;

e) Manter o caráter sigiloso da senha de acesso aos recursos e sistemas da TECNISA S.A.;

f) Não compartilhar, sob qualquer forma, informações confidenciais com outros que não tenham a devida e similar autorização de acesso;

g) Responder, por todo e qualquer acesso, aos recursos da TECNISA S.A. bem como pelos efeitos desses acessos efetivados através do seu código de identificação ou outro atributo para esse fim utilizado;

h) Respeitar a proibição de não usar, inspecionar, copiar ou armazenar programas de computador ou qualquer outro material, em violação da legislação de propriedade intelectual pertinente;

i) Comunicar, imediatamente, ao seu superior imediato e/ou Escritório de Segurança Corporativa o conhecimento de qualquer irregularidade ou desvio.

1.5.3.13 Responsabilidades dos cargos de chefias

A responsabilidade das chefias compreende, dentre outras, as seguintes atividades:

a) Gerenciar o cumprimento da Política de Segurança Corporativa da TECNISA S.A. por parte de seus funcionários e prestadores de serviços.

b) Identificar os desvios praticados e adotar as medidas corretivas apropriadas;

c) Impedir o acesso de funcionários demitidos ou demissionários aos ativos de informações, utilizando-se dos mecanismos de desligamento contemplados pelo respectivo plano de desligamento do funcionário;

d) Proteger, no nível físico e lógico, os ativos de informação e de processamento da TECNISA S.A. relacionados com a sua área de atuação;

e) Garantir que o pessoal sob sua supervisão cumpra, compreenda e desempenhe a obrigação de proteger as informações da TECNISA S.A. e todas as políticas e normas relacionadas à segurança corporativa;

f) Comunicar formalmente ao Escritório de Segurança Corporativa ESC quais os funcionários e prestadores de serviço, sob sua supervisão, que podem acessar as informações da TECNISA S.A., seguindo as normas de classificação de informações e os perfis de cada cargo;

g) Comunicar formalmente ao Departamento de Recursos Humanos RHU quais os funcionários e prestadores de serviço demitidos ou transferidos, para exclusão no cadastro dos usuários;

h) Comunicar formalmente ao Departamento de Recursos Humanos RHU aqueles que estejam respondendo a processos, sindicâncias ou que estejam licenciados, para inabilitação no cadastro dos usuários.

1.5.3.14 Responsabilidades Gerais

São responsabilidades gerais:

a) Cada área que detém recursos e ativos é responsável por eles, provendo a sua proteção de acordo com a Política de Segurança Corporativa e de classificação da informação da TECNISA S.A.;

b) Todos os ativos deverão ter claramente definidos os responsáveis pelo seu uso;

c) Todos os ativos deverão estar relacionados no Plano de Continuidade do Negócio;

1.5.3.15 Responsabilidades do Escritório de Segurança Corporativa ESC.

São responsabilidades da Gerencia designada:

a) Estabelecer e seguir as regras de proteção dos ativos da TECNISA S.A.;

b) Decidir quanto às medidas e reações a serem tomadas no caso de violação das regras estabelecidas, utilizando mecanismos do Departamento de Recursos Humanos RHU para comunicação oficial com os colaboradores;

c) Revisar, anualmente, a Política de Segurança Corporativa e as regras de proteção estabelecidas, seguindo-as continuamente;

d) Restringir e controlar o acesso e os privilégios de usuários remotos e externos;

e) Elaborar e manter atualizado os Planos de Continuidade do Negócio;

f) Executar as regras de proteção estabelecidas pela Política de Segurança Corporativa;

g) Detectar, identificar, registrar e comunicar aos canais superiores as violações ou tentativas relevantes e significativas de acesso não autorizadas ou incidentes;

h) Definir e aplicar, para cada usuário de TI&C, restrições de acesso à rede, como horários autorizados, dias autorizados, entre outras;

i) Manter registros de atividades de usuários de TI&C (logs) por 6 (seis) anos. Os registros devem conter a hora e a data das atividades, a identificação do usuário de TI&C, comandos (e seus argumentos) executados, identificação da estação local ou da estação remota que iniciou a conexão, número dos processos e condições de erro observadas (tentativas rejeitadas, erros de consistência, etc.);

j) Limitar o prazo de validade das contas de prestadores de serviço ao período da contratação.

k) Verificar a exclusão das contas inativas.

l) Autorizar o fornecimento de senhas de contas privilegiadas somente aos funcionários que necessitem efetivamente dos privilégios segundo sua descrição de cargos, mantendo-se o devido registro e controle.

m) Executar mensalmente a Avaliação de Risco e apresentar relatório trimestral a direção;

n) Elaborar semestralmente, com base nos relatórios de Riscos, a Avaliação de Impacto para os Negócios, colhendo valorização e posicionamento da Diretoria quanto às prioridades de mitigação;

o) Executar todas as rotinas de segurança estabelecidas para os Planos de Contingência, Continuidade e Reação a Incidentes de Segurança;

p) Desenvolver Normas, Procedimentos e publicações ligadas a Segurança Corporativa, assim como manter na Intranet (Portal Corporativo) publicado tudo o que for necessário;

q) Realizar a gestão de todas as tarefas relativas à integração de ações da Segurança Patrimonial, Pessoal, Eletrônica entre outras, mesmo que sejam terceirizadas;

r) Gerenciar e realizar todas as tarefas ligadas às campanhas de conscientização e disseminação cultural sobre Segurança Corporativa, bem como promover a produção de Indicadores de gestão que apontem à compreensão, aceitação e aplicação da Política e do Código de Conduta;

s) Promover processos de Auditoria sobre Segurança, seja interno ou externo;

t) Desenvolver todas as tarefas designadas pela Gerencia e Diretoria responsável por Segurança Corporativa na TECNISA S.A..

Responsabilidades dos prestadores de serviço

São previstas no contrato cláusulas que contemplem a responsabilidade dos prestadores de serviço no cumprimento desta Política de Segurança da Informação e suas normas e procedimentos;

Todo prestador de Serviço deve assinar o Termo de Responsabilidade ao receber o Crachá de identificação, que o habilita ingressar nas instalações da TECNISA S.A..

1.5.3.16 Responsabilidades do Comitê de Ética e Segurança

Compete aos integrantes do Comitê apreciar a Política de Segurança Corporativa, validando seus preceitos, bem se oporem formalmente as clausulas, promovendo em comum acordo entre os participantes a mudança de redação, inclusão ou exclusão. Cuidado especial deve ser tomado quanto a questões técnicas e estratégicas.

1.6 REQUISITOS DE SEGURANÇA PATRIMONIAL, FÍSICA E ELETRÔNICA.

1.6.1 Definições

Ambiente Patrimonial ou físico é aquele composto por todo o ativo permanente ou temporário empregado pela TECNISA S.A., sejam próprios ou locados.

1.6.2 Diretrizes Gerais

As responsabilidades pela segurança patrimonial da TECNISA S.A. são definidas e atribuídas ao Escritório de Segurança Corporativa (ativos corporativos) independente de estas atividades serem delegadas a terceiros por questões operacionais ou de responsabilidade condominial;

A localização das instalações e dos ativos críticos da TECNISA S.A. não deve ser publicamente identificada;

Existem sistemas de segurança para acesso físico, permitindo controlar e auditar o acesso às instalações;

São estabelecidos controles duplicados sobre o inventário de Cartões de acesso a áreas restritas. Uma lista atualizada do pessoal que possui cartões é mantida pelo Escritório de Segurança Corporativa;

Chaves físicas são mantidas sob custódia das áreas e fisicamente protegidas contra acesso não-autorizado, uso ou duplicação;

a) Todo uso autorizado de chaves ou Cartões de acesso a áreas restritas deve ser registrado em formulário apropriado e controlado pelo Escritório de Segurança Corporativo.

b) Todos os Cartões de acesso revogados deverão ter suas chaves lógicas descartadas;

Perdas de cartões de acesso devem ser imediatamente comunicadas ao Escritório de Segurança Corporativa (ESC) da TECNISA S.A.. Os responsáveis pelo ESC devem tomar as medidas apropriadas para prevenir acessos não-autorizados;

Os sistemas críticos estão localizados em área protegida (ambientes de nível 4) e afastada de fontes potentes de magnetismo ou interferência de rádio freqüência;

Recursos e instalações críticas ou sensíveis devem ser fisicamente protegidos de acesso não autorizado, dano, ou interferência, com barreiras de segurança e controle de acesso. A proteção deve ser proporcional aos riscos identificados; Elas devem ser fisicamente protegidas de acesso não autorizado, dano, ou interferência.

A entrada e saída, nestas áreas ou partes dedicadas, devem ser registradas com data e hora definidas e serem revisadas

periodicamente pelos responsáveis do ESC e mantidas em local adequado e sob sigilo;

O acesso aos componentes da infraestrutura, atividade fundamental ao funcionamento das operações da TECNISA, como painéis de controle de energia, comunicações e cabeamento, é restrito ao pessoal das áreas das áreas designadas;

São utilizados sistemas de detecção de intrusão para monitorar e registrar os acessos físicos aos ambientes críticos nas horas de utilização:

a) São mantidos pelos gestores dos Condomínios sistemas de Detecção e de Alarme de fumaça e Incêndio – o ESC é responsável por verificar periodicamente o perfeito funcionamento destes:

b) Em todas as instalações da TECNISA S.A. são mantidas equipes treinadas em brigadas de Incêndio;

c) Todos os funcionários e integrantes da TECNISA S.A. devem participar dos exercícios de evacuação dos ambientes;

d) Compete ao ESC vistoriar os sistemas e extintores de incêndio e suas validades em conformidade com os regulamentos do Corpo de Bombeiro da localidade da instalação da TECNISA S.A. .

e) Compete ao ESC manter planos emergenciais e de Continuidade operacional para todas as instalações da TECNISA S.A. .

O inventário de todo o conjunto de ativos é registrado e mantido atualizado, mensalmente por sistema de inventário automatizado;

Quaisquer equipamentos de gravação, fotografia, vídeo, som ou outro tipo de equipamento similar, só serão utilizados a partir de autorização do ESC e mediante supervisão contínua;

Nas instalações da TECNISA S.A. todos utilizam crachá de identificação e devem informar ao ESC sobre a presença de qualquer pessoa não identificada ou de qualquer estranho não-acompanhado;

Visitantes as instalações da TECNISA S.A. são supervisionados. Suas horas de entrada e saída e o local de destino são registrados. Essas pessoas têm acesso apenas às áreas específicas, com propósitos autorizados, e esses acessos seguem instruções baseadas nos requisitos de segurança da área visitada;

a) Visitantes que tem ingresso pelas garagens, também devem ser identificados e receberem autorização específica para ingressarem nas instalações da TECNISA S.A..

Os ambientes onde ocorrem os processos críticos da TECNISA S.A. são monitorados, em tempo real, com as imagens registradas por meio de sistemas de CFTV, com gravação remota;

Sistemas de detecção de intrusos foram instalados e são testados regularmente de forma a cobrir os ambientes, as portas e janelas acessíveis nos ambientes onde ocorrem processos críticos. As áreas não ocupadas possuem um sistema de alarme que permanece sempre ativado, desligando-se quando o sistema de controle de acesso identifica a entrada de alguém autorizado.

1.7 REQUISITOS DE SEGURANÇA LÓGICA E DA INFORMAÇÃO

1.7.1 Definição

Ambiente lógico é composto por todos os ativos de informações da TECNISA S.A..

1.7.2 Diretrizes gerais

A informação é protegida de acordo com o seu valor, sensibilidade e criticidade. Para tanto, a TECNISA S.A. possui um sistema de classificação da informação.

Os dados, as informações e os sistemas de informação da TECNISA S.A. que estão sob sua guarda são protegidos contra ameaças e ações não-autorizadas, acidentais ou não, de modo a reduzir riscos e garantir a integridade, sigilo e disponibilidade desses bens;

As violações de segurança devem ser registradas e esses registros são analisados periodicamente para os propósitos de caráter corretivo, legal e de auditoria;

Cada tipo de registro é classificado e analisado com forma e periodicidade própria de acordo com sua natureza, procedimento este realizado tanto pelo Escritório de Segurança Corporativa como

pelas demais áreas operacionais da organização. Os registros são protegidos e armazenados de acordo com a sua classificação e mantidos sob custódia da área de TI&C;

Os tipos de registros mantidos pela TI&C da TECNISA S.A. englobam:

• Registros de Sistemas Operacionais – login, logout, acesso a arquivos do sistema, dentre outros. Tais registros devem ser avaliados mensalmente.

• Registros de Aplicativos – registros de transações realizadas por servidores Web, Bancos de Dados. Tais registros devem ser avaliados mensalmente.

• Registros de Firewall e Roteadores– pacotes e conexões aceitas e rejeitadas.
Tais registros devem ser avaliados semanalmente.

• Registros do Sistema de Detecção de Invasão – tentativas de invasão da rede externa para a rede interna e vice-versa. Tais registros devem ser avaliados on-line permanentemente.

Os sistemas e recursos que suportam funções críticas para operação da TECNISA S.A. asseguram a capacidade de recuperação nos prazos e condições definidas em situações de contingência;

O inventário sistematizado de toda a estrutura que serve como "base" para manipulação, armazenamento e transmissão dos ativos de processamento, deverá estar atualizado mensalmente.

1.7.3 Diretrizes específicas

1.7.3.1 Sistemas

As necessidades de segurança são identificadas para cada etapa do ciclo de vida dos sistemas TECNISA S.A.. A documentação dos sistemas é mantida atualizada. A cópia de segurança é testada e mantida atualizada.

Os sistemas possuem controle de acesso de modo a assegurar o uso apenas a usuários ou processos autorizados. O responsável pela autorização ou confirmação da autorização é claramente definido e registrado.

As autorizações devem ser realizadas segundo sua criticidade:

• Usuários só poderão ter acesso a sistemas uma vez que tenham autorização do Departamento de RHU, com o devido consentimento do ESC e aprovação da Chefia imediata.

• Exceções só poderão ser autorizadas pelo gerente responsável pelo ESC ou por seu substituto em caso de impedimento.

Os arquivos de logs devem ser criteriosamente definidos para permitir recuperação nas situações de falhas, auditorias nas situações de violações de segurança e contabilização do uso de recursos. Os logs devem ser periodicamente analisados, no máximo mensalmente, para identificar tendências, falhas ou usos indevidos.

O log do sistema de detecção de invasão deve ser avaliado preferencialmente on-line e imediatamente após a constatação do início de um incidente;

Os logs devem ser protegidos e armazenados de acordo com sua classificação.

São estabelecidas e mantidas medidas e controles de segurança para verificação crítica dos dados e configuração de sistemas e dispositivos quanto à sua precisão, consistência e integridade.

Os sistemas são avaliados com relação aos aspectos de segurança (testes de vulnerabilidade) antes de serem disponibilizados para a produção. As vulnerabilidades do ambiente são avaliadas periodicamente e as recomendações de segurança adotadas.

1.7.3.2 Máquinas Servidoras

O acesso lógico ao ambiente ou serviços disponíveis em Servidores é controlado e protegido. As autorizações são revistas, confirmadas e registradas continuadamente. O responsável pela autorização ou confirmação da autorização é claramente definido e registrado. Todas as exceções devem ser aprovadas pelo ESC.

Os acessos lógicos são registrados em logs, que são analisados mensalmente. Tais arquivos de log são armazenados em servidor específico. Neste servidor o sistema de controle de acesso aos logs é feito através de mecanismos nativos do sistema operacional;

São adotados procedimentos sistematizados para monitorar a segurança do ambiente operacional, principalmente no que diz respeito à integridade dos arquivos de configuração do sistema operacional.

Os eventos são armazenados em relatórios de segurança (logs) de modo que sua análise permita a geração de trilhas de auditoria a partir destes registros. Todos os registros são mantidos pelo ESC em local seguro e centralizado;

As máquinas são sincronizadas para permitir o rastreamento de eventos;

Proteção lógica adicional (criptografia) deve ser adotada para evitar o acesso não-autorizado às informações, segundo classificações de segurança definidas para as informações.

A versão do sistema operacional, assim como outros softwares básicos instalados em máquinas Servidoras, deverá ser mantida atualizada, em conformidade com as recomendações dos fabricantes;

São utilizados somente softwares autorizados pela TECNISA S.A. nos seus equipamentos. É realizado o controle da distribuição e instalação dos mesmos;

O acesso remoto a máquinas servidoras é realizado adotando os mecanismos de segurança definidos para evitar ameaças à integridade e sigilo do serviço;

Os procedimentos de cópia de segurança (backup) e de recuperação estão documentados, atualizados e são regularmente testados, de modo a garantir a disponibilidade das informações;

1.7.3.3 Redes da TECNISA

O tráfego das informações no ambiente de rede (LAN, MAN, WAN, WLAN...) é protegido contra danos ou perdas, bem como acesso, uso ou exposição indevidos.

Componentes críticos da rede local são mantidos em salas protegidas e com acesso físico e lógico controlado, sendo protegidos contra danos, furtos, roubos e intempéries. Os servidores devem ser mantidos no mesmo nível de segurança das informações que eles armazenam. Todos os servidores da rede local estão em racks adequados;

São adotadas as facilidades de segurança disponíveis de forma inata nos ativos de processamento da rede;

A configuração de todos os ativos de processamento é averiguada quando da sua instalação inicial, para que sejam detectadas e corrigidas as vulnerabilidades inerentes à configuração padrão que se encontram nestes ativos em sua primeira ativação;

Serviços vulneráveis são eliminados ou trocados por similares mais seguros;

O uso de senhas é submetido a uma política específica para sua gerência e utilização;

O acesso lógico aos recursos da rede local é realizado por meio de sistema de controle de acesso. O acesso é concedido e mantido pela administração da rede, baseado nas responsabilidades e tarefas de cada usuário.

A utilização de qualquer mecanismo capaz de realizar testes de qualquer natureza, como por exemplo, monitoração sobre os dados, os sistemas e dispositivos que compõem a rede, só ocorrem a partir de autorização formal e mediante supervisão;

A conexão com outros ambientes de rede e alterações internas na sua topologia e configuração são formalmente documentadas e mantidas, de forma a permitir registro histórico, e tem a autorização da administração da rede e do ESC. O diagrama topológico, a configuração e o inventário dos recursos são mantidos atualizados.

São definidos relatórios de segurança (logs) periódicos de modo a auxiliar no tratamento de desvios, recuperação de falhas, contabilização e auditoria. Tais relatórios são disponibilizados e armazenados de maneira segura. As anormalidades identificadas nestes relatórios são tratadas segundo a sua severidade. Entre elas, inclui-se:

- Ataques Externos e Internos;
- Utilização indevida de Recursos;
- Falhas de subsistemas.

São adotadas proteções físicas adicionais para os recursos de rede considerados críticos;

Proteção lógica adicional deve ser adotada para evitar o acesso não-autorizado às informações;

A infraestrutura de interligação lógica está protegida contra danos mecânicos e conexão não autorizada;

A alimentação elétrica para a rede local é separada da rede convencional, sendo observadas as recomendações dos fabricantes dos equipamentos utilizados assim como as normas ABNT aplicáveis.

O tráfego de informações é monitorado, a fim de verificar sua normalidade, assim como detectar situações anômalas do ponto de vista da segurança;

São observadas as questões envolvendo propriedade intelectual quando da cópia de software ou arquivos de outras localidades;

Informações sigilosas, corporativas ou que possam causar prejuízo a terceiros estão protegidas e não são enviadas para outras redes sem proteção adequada;

Todo serviço de rede não explicitamente autorizado deve ser bloqueado ou desabilitado;

Mecanismos de segurança baseados em sistemas de proteção de acesso (firewall) são utilizados para proteger as transações entre redes externas e a rede interna da TECNISA S.A.;

Os registros de eventos são analisados periodicamente, no menor prazo possível e em intervalos de tempo adequados;

É adotado um padrão de segurança para todos os tipos de equipamentos servidores, considerando aspectos físicos e lógicos;

Todos os recursos considerados críticos para o ambiente de rede, e que possuam mecanismos de controle de acesso, fazem uso de tal controle;

Os serviços baseados em sistemas de proteção de acesso (firewall) são submetidos a uma avaliação complexa pelo ESC. No mínimo os seguintes aspectos são considerados:

- Requisitos de segurança definidos pelo serviço;
- Objetivo do serviço;
- Público-alvo;
- Classificação da informação;
- Forma de acesso;

- Frequência de atualização do conteúdo;

- Forma de administração do serviço;

- Volume de tráfego.

Ambientes de rede considerados críticos são isolados de outros ambientes de rede, de modo a garantir um nível adicional de segurança;

Conexões entre as redes da TECNISA S.A. e redes externas (parceiros/fornecedores/prestadores de serviços...) estão restritas somente àquelas que visem efetivar os processos necessários à operação da TECNISA S.A.;

As conexões de rede são ativadas: primeiro sistemas com função de certificação; segundo sistemas que executam as funções de registros e repositório. Se isto não for possível, empregam-se controles de compensação, tais como o uso de proxies que deverão ser implementados para proteger os sistemas que executam a função requerida contra possíveis ataques;

A segurança das comunicações intra-rede e inter-rede entre os sistemas da TECNISA S.A. é garantida pelo uso de mecanismos que asseguram o sigilo e a integridade das informações trafegadas;

As ferramentas de detecção de intrusos são implantadas para monitorar as redes, alertando periodicamente os administradores das redes sobre as tentativas de intrusão;

1.7.3.4 Controle de acesso lógico (baseado em senhas)

Usuários e aplicações que necessitem ter acesso a recursos da TECNISA S.A. são identificados e autenticados através de senhas;

O sistema de controle de acesso mantém as habilitações atualizadas e registros que permitem a contabilização do uso, auditoria e recuperação nas situações de falha;

Não é permitido a nenhum usuário obter direitos de acesso de outro usuário;

A informação que especifica os direitos de acesso de cada usuário ou aplicação é protegida contra modificações não-autorizadas;

O arquivo de senhas é criptografado e o seu acesso controlado;

As autorizações são definidas de acordo com a necessidade de desempenho das funções (acesso motivado) e considerando o princípio dos privilégios mínimos (ter acesso apenas aos recursos ou sistemas necessários para a execução de tarefas);

As senhas são individuais, secretas, intransferíveis e protegidas com grau de segurança compatível com a informação associada;

As seguintes características das senhas são definidas:

• O conjunto de caracteres permitidos deve incluir letras (maiúsculas e minúsculas), números e caracteres especiais;

• Tamanho mínimo é de 8 caracteres;

• Não existe tamanho máximo – recomendável até 40 caracteres;

• O prazo de validade máximo deve ser de 90 dias;

• As trocas são realizadas através dos mecanismos nativos dos sistemas operacionais;

• Restrições específicas para cada ambiente, aplicação ou plataforma poderão ser adotadas, se necessárias.

A distribuição de senhas (iniciais ou não) aos usuários de TI&C é feita de forma segura. A senha inicial, quando gerada pelo sistema, é trocada, pelo usuário de TI&C, no primeiro acesso.

O sistema de controle de acesso permite ao usuário alterar sua senha sempre que desejar. A troca de uma senha bloqueada só é executada após a identificação positiva do usuário. A senha digitada não é exibida;

Os usuários são bloqueados após 45 dias sem acesso e/ou 3 tentativas sucessivas de acesso mal sucedidas;

O sistema de controle de acesso solicita nova autenticação após 20 minutos de inatividade da sessão (time-out);

O sistema de controle de acesso exibe, na tela inicial, mensagem informando que o serviço só pode ser utilizado por usuários autorizados.

No momento de conexão, o sistema exibe para o usuário informações sobre o último acesso;

O registro das atividades (logs) do sistema de controle de acesso é definido de modo a auxiliar no tratamento das questões de segurança, permitindo a contabilização do uso, auditoria e recuperação nas situações de falhas. Os logs devem ser periodicamente analisados;

Os usuários e administradores do sistema de controle de acesso são formal e expressamente conscientizados de suas responsabilidades, mediante assinatura de termo de compromisso.

1.7.3.5 Computação de uso Pessoal e Mobilidade Corporativa

As estações de trabalho, incluindo equipamentos portáteis ou stand-alone e móveis (Pocketable Computing Devices (PCD*), Mobile Computing Devices (MCD), como celulares, smartphones, PDAs, sub-notebooks, notebooks, modems, placas, roteadores wireless e aplicações em firmwares), bem como informações, devem ser protegidos contra danos ou perdas bem com uso ou exposições indevidos;

Equipamentos que executem operações sensíveis devem receber proteção adicional, considerando os aspectos lógicos (controle de acesso e criptografia) e físicos (proteção contra furto ou roubo do equipamento ou componentes);

São adotadas medidas de segurança lógica referentes ao combate a vírus, backup, controle de acesso e uso de software não-autorizado;

As informações armazenadas em meios eletrônicos são protegidas contra danos, furtos ou roubos, sendo adotados procedimentos de backup, definidos em documento específico;

Informações sigilosas, corporativas ou cuja divulgação possa causar prejuízo as empresas parceiras ou integrantes, só são utilizadas em equipamentos da TECNISA S.A. onde foram geradas ou naqueles equipamentos por ela autorizados, com controles adequados.

O acesso às informações sempre deve atender aos requisitos de segurança, considerando o ambiente e forma de uso do equipamento (uso pessoal ou coletivo);

Os usuários de TI&C utilizam apenas softwares licenciados pelo fabricante nos equipamentos da TECNISA S.A., observadas as normas da legislação de software;

A TECNISA S.A. estabelece os aspectos de controle, distribuição e instalação de softwares utilizados;

A impressão de documentos sigilosos é feita sob supervisão do responsável emissor. Os relatórios impressos devem ser protegidos contra perda, reprodução e uso não-autorizado. Sua circulação deverá ocorrer sempre em envelope lacrado;

O inventário dos recursos de computação pessoal, inclusive os de mobilidade corporativa são mantidos atualizados e disciplinados pelo ESC;

Os sistemas em uso solicitam nova autenticação após 20 minutos de inatividade da sessão (time-out);

As mídias são eliminadas de forma segura, quando não forem mais necessárias. Procedimentos formais para a eliminação segura das mídias são definidos, para minimizar os riscos.

1.7.3.6 Combate contínuo a Vírus e Spywares

Os procedimentos de combate a processos destrutivos (vírus, cavalo-de-tróia e worms, spywares, bots entre outros) são sistematizados e englobam máquinas Servidoras, estações de trabalho, equipamentos portáteis e microcomputadores stand-alone. É dever de todos se certificarem da atualização dos mesmos.

1.8 REQUISITOS DE SEGURANÇA OPERACIONAL

1.8.1 Inventário de ativos

Todos os ativos da TECNISA S.A. são inventariados, classificados, permanentemente atualizados, e possuem gestor responsável formalmente designado, conforme descrição a seguir:

Os ativos de TI&C são inventariados pelo DTI (ambiente da TECNISA S.A.) e Rede Local (ambiente corporativo). Os inventários de Segurança Física e materiais criptográficos são mantidos pelo ESC.

1.8.2 Gerenciamento de Riscos

Definição

Processo que visa à proteção dos serviços da TECNISA S.A., por meio da eliminação, redução ou transferência dos riscos. Os seguintes pontos principais são identificados:

a) O que deve ser protegido;

b) Análise de riscos (contra quem ou contra o quê deve ser protegido);

c) Avaliação de riscos (análise da relação custo/benefício).

Fases Principais

O gerenciamento de riscos consiste das seguintes fases principais:

a. Identificação dos recursos a serem protegidos – hardwares, rede, software, dados, informações pessoais, documentação, suprimentos;

b. Identificação dos riscos (ameaças) - que podem ser naturais (tempestades, inundações), causadas por pessoas (ataques, furtos, vandalismos, erros ou negligências) ou de qualquer outro tipo (incêndios);

c. Análise dos riscos (vulnerabilidades e impactos) - identificar as vulnerabilidades e os impactos associados;

d. Avaliação dos riscos (probabilidade de ocorrência) - levantamento da probabilidade da ameaça vir a acontecer, estimando o valor do provável prejuízo. Esta avaliação é feita com base em informações históricas ou em tabelas internacionais;

e. Tratamento dos riscos (medidas a serem adotadas) - maneira como lidar com as ameaças. As principais alternativas adotadas são: eliminar o risco, prevenir, limitar ou transferir as perdas ou aceitar o risco;

f. Monitoração da eficácia dos controles adotados para minimizar os riscos identificados;

g. Reavaliação cíclica dos riscos em intervalos de tempo não superiores a 90 (noventa) dias;

Riscos relacionados à operação da TECNISA S.A.

Os riscos avaliados para a TECNISA S.A. compreendem, dentre outros, os seguintes:

Segmentos de Risco

Dados e Informação: Indisponibilidade, Interrupção (perda), interceptação, modificação, fabricação, destruição.

Pessoas: omissão, erro, negligência, imprudência, imperícia, desídia, sabotagem, engenharia social, perda de conhecimento.

Redes: Hacker, acesso desautorizado, interceptação, engenharia social, identidade forjada, reenvio de mensagem, violação de integridade, indisponibilidade ou recusa de serviço.

Hardware: indisponibilidade, interceptação (furto ou roubo) ou falha.

Software e sistemas: interrupção (apagamento), interceptação, modificação, desenvolvimento ou falha.

Recursos criptográficos: falhas de Softwares criptográficos, Ciclo de vida dos certificados, gerenciamento das chaves criptográficas, falhas de hardware criptográfico, falhas de algoritmos (desenvolvimento e utilização) ou material criptográfico.

Considerações

Os riscos que não podem ser eliminados devem ter seus controles documentados e são levados ao conhecimento da direção da TECNISA S.A..

O efetivo gerenciamento dos riscos deve permitir decidir se o custo de prevenir um risco (medida de proteção) é mais alto que o custo das conseqüências do risco (impacto da perda); É necessária a participação e o envolvimento da alta administração da TECNISA S.A. nas decisões.

Implementação do Gerenciamento de Riscos

O gerenciamento de riscos na TECNISA S.A. deve ser conduzido de acordo com as melhores práticas do mercado, fundamentado em metodologia padrão ou proprietária, desde que atendidos todos os tópicos relacionados nesta política.

A TECNISA S.A. implementa análises de risco periodicamente através de sua própria estrutura e de terceiros. Os processos de gerenciamento de riscos devem ser revistos, no máximo, a cada 18 (dezoito) meses,

para prevenção contra riscos, inclusive aqueles advindos de novas tecnologias e novos negócios, visando à elaboração de planos de ação apropriados para proteção dos componentes ameaçados.

1.8.3 Planos de Continuidade do Negócio

Definição

É um conjunto de planos cujo objetivo é manter em funcionamento os serviços e processos críticos da TECNISA S.A., na eventualidade da ocorrência de desastres, atentados, falhas e intempéries.

Diretrizes Gerais

Sistemas e dispositivos redundantes devem estar disponíveis para garantir a continuidade da operação dos serviços críticos de maneira oportuna.

A TECNISA S.A. possui seu conjunto de Planos de Continuidade do Negócio que estabelece o tratamento adequado dos seguintes eventos de segurança:

a) Comprometimento das Bases de Dados Corporativa;

b) Invasão do sistema e da rede interna da organização;

c) Incidentes de segurança física e lógica;

d) Indisponibilidade da Infraestrutura; e

Todo pessoal envolvido com o Plano de Continuidade do Negócio recebe um treinamento específico para poder enfrentar estes incidentes;

A TECNISA S.A. possui um plano de ação de resposta a incidentes. Este plano prevê o tratamento adequado dos seguintes eventos:

a) Comprometimento de controle de segurança em qualquer evento referenciado no Plano de Continuidade do Negócio;

b) Notificação à todos os usuários, se for o caso;

c) Procedimentos para interrupção ou suspensão de serviços e investigação;

d) Análise e monitoramento de trilhas de auditoria; e

e) Relacionamento com o público e com meios de comunicação, se for o caso.

O Plano de Continuidade do Negócio da TECNISA S.A. é testado pelo menos uma vez por ano, garantindo a continuidade dos serviços críticos ao negócio;

A TECNISA S.A. possui planos de gerenciamento de incidentes e de

ações de resposta aos incidentes aprovados pela direção.

Todos os incidentes são reportados imediatamente, a partir do momento em que for verificada a ocorrência. Estes incidentes são reportados de modo sigiloso ao Gerente responsável pelo ESC, ao Diretor responsável por SC na TECNISA S.A..

1.8.4 Auditoria

As atividades da TECNISA S.A. estão associadas ao conceito de confiança plena. O processo de auditoria periódica representa um dos instrumentos que facilita a percepção e transmissão de confiança e transparência à comunidade de usuários, fornecedores, clientes e acionistas, dado que o objetivo desses processos é verificar a capacidade da TECNISA S.A. em atender aos requisitos legais inclusive os da CVM;

A aplicação e o resultado das auditorias internas promovidas pelo ESC é um item fundamental a ser considerado no processo operacional da TECNISA S.A., da mesma forma que o resultado das auditorias externas e fiscalizações são itens fundamentais para a manutenção da saúde corporativa;

Deverão ser realizadas auditorias periódicas na TECNISA S.A., pelo ESC ou por terceiros por ele autorizados ou designados.

1.8.5 Gestão da Segurança

A Política de Segurança Corporativa da TECNISA S.A. aplica-se a todos os recursos humanos, administrativos e tecnológicos a ela relacionados de modo permanente.

Esta política é comunicada para todo o pessoal envolvido e largamente divulgada através da TECNISA S.A. e as entidades a ela vinculadas, garantindo que todos tenham consciência da Política e a pratiquem na organização ou fora dela;

Todos os colaboradores, parceiros, terceiros, entre outros, recebem as informações necessárias para cumprir adequadamente o que está determinado na política de segurança corporativa;

Um programa de conscientização cíclico sobre segurança corporativa e da informação deve ser mantido através de treinamentos específicos, assegurando que todos os envolvidos sejam informados sobre os potenciais riscos de segurança e exposição a que estão submetidos os sistemas e operações da TECNISA S.A. e parceiros vinculados. Especificamente, o pessoal envolvido ou que se relaciona com os usuários estão informados sobre ataques típicos de engenharia social e como se proteger deles;

Os procedimentos são documentados e implementados para garantir que quando o pessoal contratado ou prestadores de serviços sejam transferidos, remanejados, promovidos ou demitidos, todos os privilégios de acesso aos sistemas, informações e recursos sejam

devidamente revistos, modificados ou revogados;

A TECNISA S.A. mantém mecanismo e repositório centralizado para manutenção de trilhas, logs e demais notificações de incidentes. O Gerente responsável por Segurança ou o ESC é acionado, uma vez que qualquer tentativa de violação seja detectada, tomando as medidas cabíveis para prover uma defesa ativa e corretiva contra ataques empreendidos contra esses mecanismos;

Os processos de aquisição de bens e serviços, especialmente os de Tecnologia da Informação – TI&C estão em conformidade com esta Política de Segurança Corporativa;

É considerada proibida qualquer ação que não esteja explicitamente permitida na Política de Segurança Corporativa da TECNISA S.A. ou que não tenha sido previamente autorizada pelo Gerente designado de Segurança da TECNISA S.A..

CÓDIGO DE CONDUTA

TECNISA

Mais construtora por m²

CÓDIGO DE CONDUTA TECNISA

CAPÍTULO 1

Seção I
Disposições Iniciais

Artigo 1 - Código de Conduta

1. A primeira Seção do presente Código de Conduta da TECNISA estabelece linhas de orientação em matéria de ética profissional para todos os colaboradores da TECNISA, constituindo também uma referência como padrão de conduta exigível no seu relacionamento com terceiros.

2. Esta seção estabelece padrões de referência para o grau de cumprimento de obrigações assumidas por parte dos colaboradores, sem prejuízo de outras normas de conduta aplicáveis em áreas funcionais específicas da TECNISA.

Artigo 2 - Objeto

O presente Código de Conduta estabelece as regras fundamentais de conduta, organização e disciplina do trabalho, que devem ser respeitadas por todos os envolvidos com a TECNISA no exercício das suas funções.

Artigo 3 - Âmbito de aplicação

1. As disposições do Código de Conduta aplicam-se a todos Colaboradores e Integrantes, definidos este último como: terceiros, fornecedores e parceiros da TECNISA.

2. São Colaboradores da TECNISA, para o efeito do presente Código:
a) Os membros dos órgãos de administração;
b) Os trabalhadores / funcionários;
c) Os estagiários contratados;

3. Os colaboradores e demais integrantes que infringirem o presente Código de Conduta sujeitará às penalidades disciplinares previstas, sendo-lhe dados amplos direito de defesa.

Artigo 4 - Disposições legais e regulamentares

1. O presente Código de Conduta visa complementar as disposições legais e regulamentares em vigor, assim como o Código de Ética Corporativo TECNISA e os referentes à formação acadêmica dos integrantes.

2. A sujeição, pelos integrantes da TECNISA, ao presente Regulamento, não os exonera do dever de conhecimento e respeito das disposições legais e regulamentares a eles aplicáveis.

Seção II
Princípios e Deveres Gerais de Conduta

Artigo 5 - Princípios gerais de conduta

1. No desempenho das respectivas atividades, e nas relações com clientes, fornecedores, prestadores de serviços, entidades reguladoras, entidades externas em geral, concorrentes ou funcionários destes, os colaboradores da TECNISA em particular, bem como os demais integrantes devem assegurar níveis máximos de profissionalismo, seriedade, competência, lealdade, integridade, transparência e diligência.

2. No trato com fornecedores, parceiros, clientes e funcionários destes, os colaboradores e integrantes devem ainda comportar-se de forma correta, cortês, acessível, disponível e conscienciosa.

3. Os colaboradores e integrantes devem executar ou promover todas as medidas ao seu alcance para a defesa dos interesses da TECNISA e dos seus clientes.

Artigo 6 - Princípio da igualdade de tratamento

Os colaboradores e integrantes devem assegurar igualdade de tratamento a todos os fornecedores, parceiros e clientes da TECNISA.

Artigo 7 - Dever de lealdade

1. Para os colaboradores da TECNISA, o dever de lealdade implica não só o adequado desempenho das tarefas que lhes são atribuídas pelos seus superiores, o cumprimento das instruções destes últimos e o respeito pelos canais hierárquicos apropriados, mas também a transparência e abertura no trato pessoal com superiores e colegas.

2. Os colaboradores e integrantes da TECNISA devem designadamente manter outros colegas intervenientes interados no mesmo assunto, ao corrente dos trabalhos em curso e permitir-lhes dar o respectivo contributo, não lhes sonegando informações que possam prejudicar a execução dos mesmos.

3. São contrárias ao tipo de lealdade que se espera dos colaboradores e integrantes, a não revelação a superiores e colegas de informações que possam afetar o andamento e resultado dos trabalhos, sobretudo com o intuito de obter vantagens pessoais, ou fornecimento de informações falsas, inexatas ou exageradas, a recusa em colaborar com os colegas e a demonstração de uma atitude de obstrução.

4. Espera-se que os colaboradores e integrantes que desempenhem funções de direção, coordenação e chefia, sejam exemplares e instruam as suas equipes de uma forma clara e compreensível.

Artigo 8 - Dever de sigilo e colaboração com entidades externas

1. É dever fundamental dos colaboradores e integrantes o cumprimento e respeito pelo segredo profissional e pelo sigilo bancário, ou seja, os colaboradores e integrantes devem guardar sigilo sobre todos os serviços e negócios existentes com os clientes, bem como sobre fatos ou informações, relativos aos mesmos clientes, a TECNISA, a outros colaboradores, parceiros ou a terceiros, cujo conhecimento lhes advenha do exercício das suas funções, e que em nada prejudiquem a atividade da TECNISA.

2. Os colaboradores devem prestar às autoridades policiais, às autoridades judiciais e às autoridades de supervisão da CVM, ou outras, toda a colaboração necessária que for exigível, nos termos da lei.

Artigo 9 - Deveres de conduta interna

São deveres fundamentais de conduta interna, para colaboradores e integrantes:

a) Contribuir para o bom-nome, harmonia e respeito pela imagem da empresa;

b) Zelar pelo patrimônio material da TECNISA, preservando os materiais, instrumentos de trabalho, a segurança das instalações, móveis, equipamentos e softwares disponibilizados para uso; Os recursos de informática (desktop, notebooks, impressoras, etc.) que contenham informações da TECNISA, de clientes, parceiros e fornecedores, sendo que estes deverão ser utilizados de forma restrita com base nas normas de Segurança estabelecidas, pelo Escritório de Segurança Corporativa;

c) Utilizar recursos, de hardware e software, disponibilizados pelo departamento de Informática, para atender exclusivamente a realização do trabalho para a TECNISA, de acordo com as Normas internas;

d) Observar as normas internas e as práticas administrativas em vigor na TECNISA

e) O cumprimento das ordens dadas pela hierarquia ou as instruções da Administração, cujo conhecimento advenha por qualquer forma;

f) Pôr imediatamente termo a qualquer conduta ilícita praticada por colaboradores diretamente ou indiretamente sujeitos à sua fiscalização ou direção e no exercício das suas funções;

g) Comunicar de imediato à sua chefia hierárquica ou ao Comitê de Ética e Segurança da TECNISA qualquer conduta que viole, ou seja, suscetível de violar o disposto no presente Código de Conduta ou nas leis. Esta comunicação será mantida em sigilo de autoria;

h) Conservar e manter em perfeita organização todos os elementos e documentos relacionados com a atividade profissional;

i) Aplicar prontamente todas as recomendações geradas por Normas Internas ou publicadas como Manuais de procedimentos específicos da TECNISA, com atenção especial as relativas à segurança da informação, mantendo sempre a política de tela limpa ao se afastar do seu posto de trabalho e mesa limpa ao final do seu expediente.

j) Garantir, no exercício da sua atividade, a minimização dos riscos da atividade da TECNISA.

k) Respeitar e aplicar fielmente as metodologias e normas repassadas pela TECNISA.

l) Promover a cooperação e o respeito mútuo entre colegas.

m) Ao detectar uma falha em tecnologias da Informação, nunca censurar na presença de cliente, e sim trazer ao conhecimento do departamento DTI para avaliação e providências.

n) Não utilizar, indevidamente, bens da TECNISA em proveito próprio;

o) Abster-se de solicitar ou aceitar de terceiros quaisquer ofertas ou benesses, em dinheiro ou em espécie, que excedam um valor meramente simbólico, susceptíveis de comprometer a sua imparcialidade e a sua lealdade para com a TECNISA.

p) É vedada ao colaborador a cobrança de qualquer honorário particular dos clientes TECNISA.

q) Abster-se de utilizar a sua posição na hierarquia ou na estrutura da TECNISA para obter qualquer vantagem, para si próprio, para a sua família ou para quaisquer terceiros.

r) Não aceitar nenhuma procuração ou mandato pessoal, salvo nos casos expressamente autorizados pela Administração.

s) Abster-se de concorrer com a TECNISA.

t) Abster-se de conceder a qualquer órgão de comunicação, informações, entrevistas ou opiniões relativas à atividade da TECNISA, por iniciativa própria ou a pedido dos meios de comunicação, sem

que para isso tenham obtido autorização prévia da Administração, da Assessoria de Imprensa e do Escritório de Segurança Corporativa acumulativamente.

u) Tratar os clientes de uma forma educada, prestável, cordial e no cumprimento de todos os Códigos, Manuais e Procedimentos da empresa referentes a regras, comerciais, éticas e morais.

Artigo 10 - Outros deveres de conduta

1. No intuito de salvaguardar os direitos dos colaboradores, estes devem avisar o departamento de Recursos Humanos sempre que ocorra alguma alteração relativa ao seu estado civil, encargos familiares ou mudança de morada, fornecendo sempre que solicitado, cópia legível dos seus documentos.

2. Toda a informação prestada pelos colaboradores a TECNISA deverá ser rigorosa e verdadeira. Todas serão tratadas com confidencialidade.

3. É interdito aos colaboradores e integrantes reencaminharem ou receberem correspondência pessoal na sede ou em qualquer estabelecimento da TECNISA.

Artigo 11 - Injúrias e Difamação

1. É proibida a todos os colaboradores e integrantes a prática de qualquer forma de difamação.

2. Entende-se por difamação quem, dirigindo-se a terceiro, imputar a outra pessoa, mesmo sob a forma de suspeita, um fato, ou formular sobre ela um juízo, ofensivo da sua honra ou consideração, ou reproduzir tal imputação ou juízo.

3. É proibido a todos os colaboradores praticarem qualquer tipo de injúria a um terceiro, imputando-lhe fatos, mesmo sob a forma de suspeita, ou dirigindo-lhe palavras, ofensivas da sua honra ou consideração.

4. É vedado submeter outros colaboradores a intimidações, assédio sexual, moral, intelectual ou constrangimento de qualquer natureza;

5. A violação de qualquer um dos deveres decorrentes do presente artigo constitui falta disciplinar gravíssima.

Artigo 12 - Consumo de álcool e drogas

1. Não é permitida a entrada ou permanência na empresa de colaborador ou integrantes que se apresentem em estado de embriagues ou sob a influência de drogas.

2. Não é permitido trazer, distribuir ou consumir, nas instalações da TECNISA quaisquer tipos de drogas ou álcool.

3. Excepcionalmente poderá ser permitido derrogar as normas relativas ao consumo de bebidas alcoólicas, em circunstâncias excepcionais, como eventos sociais promovidos pela TECNISA, sempre com prévia autorização do superior hierárquico.

Artigo 13 - Consumo de tabaco

Não é permitido fumar nas instalações da TECNISA bem como nos espaços comuns das instalações utilizadas pela TECNISA.

Seção III
Informações

Artigo 14 - Informações a clientes e/ou representantes destes

1. Os colaboradores e integrantes devem informar os clientes de acordo com o previsto na lei ou quando tal tenha sido unilateralmente ou contratualmente estabelecido pela TECNISA.

2. Qualquer informação prestada deverá ser rigorosa, completa, verdadeira, atual, clara, objetiva, lícita e devidamente autorizada.

3. A extensão e a profundidade da informação devem ter a necessária conformidade e classificação de segurança e ser adequada face ao grau de conhecimento, de experiência e de expectativas do cliente e/ou seus representantes.

Artigo 15 - Informações dos clientes

1. Os colaboradores e integrantes da TECNISA não podem revelar ou utilizar informações sobre fatos ou elementos referentes à vida da empresa ou às relações desta com os seus clientes cujo conhecimento lhes advenha exclusivamente do exercício das suas funções ou da prestação dos seus serviços.

2. O dever supra referido no parágrafo 1 não cessa com o término de funções ou serviços.

3. Os fatos referidos no parágrafo 1 só podem ser revelados:
a) A TECNISA;
b) Quando a lei o obrigue.

4. O envio de qualquer documentação ou correspondência a clientes deverá ser realizado com prudência e rigor na identificação do destinatário.

5. Os colaboradores e integrantes que trabalhem com dados pessoais devem respeitar os princípios legais aplicáveis, devendo, em especial, abster-se de tratar dados pessoais para fins não autorizados pela finalidade da recolha ou de transmiti-los a pessoas não autorizadas.

Seção IV
Atendimento

Artigo 16 - Atendimento direto a clientes e/ou colaboradores de clientes, fornecedores e parceiros.

1. O colaborador, ao atender diretamente um cliente e/ou funcionários de clientes, fornecedores e parceiros deve olhar as pessoas diretamente, mostrar-se atento, amável e acolhedor, bem como tratá-las pelos títulos que utilizem, se o colaborador os conhecer, e subsidiariamente utilizar o tratamento de "Senhor" ou "Senhora", consoante o sexo do interlocutor, confirmar se está a ouvindo e verificar se compreende bem o cliente e/ou funcionários de clientes, fornecedores e parceiros.

2. Os colaboradores e integrantes não podem utilizar documentos de identificação pessoal que não tenham sido emitidos pela TECNISA.

3. Sugerir aos clientes da TECNISA sempre que possível, as melhores soluções e apontar alternativas pertinentes aos produtos e serviços da TECNISA como primeira alternativa;

4. Os colaboradores não podem praticar qualquer tipo de discriminação, em especial, com base na raça, sexo, idade, incapacidade física, preferência sexual, opiniões políticas, idéias filosóficas ou convicções religiosas.

5. Os colaboradores devem demonstrar sensibilidade e respeito mútuo e abster-se de qualquer comportamento tido como ofensivo por outra pessoa.

Artigo 17 - Atendimento telefônico

1. O atendimento deve ser feito até ao terceiro toque impreterivelmente.

2. A linguagem deve ser correta, a voz simpática e sorridente, demonstrando sempre cortesia, compreensão e disponibilidade.

3. No atendimento telefônico quem atende deve sempre, e pela seguinte ordem, identificar a empresa, cumprimentar o cliente, identificar-se com o nome, perguntar quem fala, utilizar o título do cliente, se o houver, e o nome do cliente.

4. No atendimento telefônico o colaborador ou integrante nunca deve interromper o cliente e deve dar todas as informações úteis.

5. Todas as interrupções necessárias devem ser previamente explicadas. O colaborador deve "regressar à linha" no mínimo a cada 30 segundos ou solicitar o número para retornar a ligação.

6. Durante o atendimento telefônico o colaborador ou integrante não deve ingerir alimentos e/ou bebidas.

7. O colaborador ou integrante deve sempre aguardar que o interlocutor desligue primeiro.

Artigo 18 - Recepção de uma reclamação

1. Qualquer colaborador ou integrante que receber uma reclamação oral, telefônica ou pessoal, deve seguir os seguintes procedimentos éticos:

- Ouvir sem interromper;
- Não se desculpar ou culpar outros elementos da empresa;
- Resumir o que ouviu e transmitir a sua vontade de ajudar;
- Apresentar alternativas e soluções;
- Olhar para as pessoas diretamente e mostrar-se atento, amável e acolhedor;
- Tratar as pessoas pelos seus nomes;
- Não responder a linguagem de conflito.
- Manter o timbre de voz estável e equilibrado em qualquer circunstância.

2. Caso o colaborador não consiga resolver a situação, deve reportá-la de imediata ao superior hierárquico que deverá tomar as medidas necessárias.

3. No caso da recepção de uma reclamação escrita, seja qual for a sua proveniência, deve à mesma ser remetida de imediato para o Departamento Responsável pela reclamação do Cliente, que a tratará de acordo com os Procedimentos em vigor na empresa.

Seção V
Apresentação

Artigo 19 - Vestuário

1. Todos os colaboradores e integrantes devem adotar, no exercício das suas funções uma imagem, comportamento e atitudes que não seja sob nenhuma forma prejudicial à imagem da TECNISA.

2. Os colaboradores e integrantes obrigam-se a apresentarem-se com elevado aprumo e a cuidar da sua apresentação e higiene pessoal.

3. O vestuário a se utilizar devem ser discretos e formal, adaptado à imagem da empresa.

4. Os colaboradores e integrantes que desempenhem funções em contato direto com o público deverão ter um especial cuidado.

5. Os colaboradores e integrantes que não desempenhem funções em contato direto com o público poderão, às sextas-feiras, utilizar um vestuário tipo "business casual", desde que não tenham nesse dia qualquer reunião previamente agendada com clientes ou outras entidades externas.

CAPÍTULO 2

Artigo 20 - Sanções Disciplinares

1. Quando a TECNISA tiver conhecimento de procedimentos, por parte dos Colaboradores e Integrantes que representem violação às Normas Internas e deste Código, o assunto será encaminhado à Comissão de Ética e Segurança da TECNISA que analisará o caso e tomará as medidas disciplinares cabíveis.

2. O colaborador ou integrante será notificado formalmente pela TECNISA para apresentar defesa, sob pena de serem considerados verdadeiros os fatos imputados.

3. Os procedimentos adotados em casos de violação deste Código serão conduzidos pela Comissão de Ética e Segurança, a quem cabe também a recomendação final das respectivas sanções para aprovação da Diretoria.

4. As penalidades aplicáveis aos colaboradores resumem-se em advertência, suspensão temporária, afastamento definitivo e responsabilização civil ou penal, se for o caso, conforme segue:

• Falta: Será considerada falta à violação de qualquer artigo deste código que a critério da Comissão de Ética e Segurança da TECNISA, embora tenha ocorrido, não trouxe maiores prejuízos financeiros ou à imagem da empresa.

Penalidade: Advertência formal ou suspensão temporária a critério da comissão e com autorização da Diretoria.

• Falta Grave: Será considerada falta grave a violação de qualquer artigo deste código que a critério da Comissão de Ética e Segurança da TECNISA, que trouxer pequenos prejuízos financeiros ou à imagem da empresa ou se houver reincidência de alguma falta cometida anteriormente.
Penalidade: suspensão temporária com autorização da Diretoria.

• Falta Gravíssima: Será considerada falta gravíssima a violação de qualquer artigo deste código que a critério da Comissão de Ética e Segurança da TECNISA, trouxer grandes prejuízos financeiros ou à imagem da empresa ou se houver reincidência de alguma falta grave cometida anteriormente.
Penalidade: afastamento definitivo com autorização da Diretoria.

Para efeito dos Integrantes (terceiros, fornecedores e parceiros) a TECNISA fará as mesmas sugestões de penalidade aos representantes da Pessoa Jurídica da organização aonde participar o Integrante. Caso as imputações não sejam aceitas, a TECNISA reserva-se o direito de excluir o Integrante do seu quadro e das suas atividades na organização. Medidas legais e clausulas contratual pactuam esse comportamento.

CAPÍTULO 3

Artigo 21 - Entrada em vigor

1. O presente Código de Conduta vigorará 12 meses ou por tempo indeterminado, competindo a TECNISA a sua revisão sempre que o entender, e dentro dos limites exigíveis.

2. O presente Código de Conduta entra em vigor em 13 de Julho de 2009.

PROTOCOLO DE ACEITE

Eu, _____

portador do RG nº _____, recebi a publicação Política de Segurança e Código de Ética da Informação da Tecnisa S.A., com base na edição de 2009, e obtive informações sobre o seu teor de forma verbal e expositiva, além de ter lido em detalhes o seu conteúdo, concordando plenamente com o que está estabelecido pelo Comitê de Ética e Segurança com apoio integral do corpo diretivo da Tecnisa S.A.

São Paulo, _____ de _____ de 20_____.

_____

Assinatura

TECNISA

Mais construtora por m²