POLÍTICA DE SEGURANÇA CIBERNÉTICA

Sumário

1. OBJETIVOS

Esta Política visa proteger os equipamentos, sistemas e dados de propriedade e/ou uso da FAR - Fator Adm. de Recursos ("FAR"); ORE Securitizadora, e Fator ORE Real Estate Holding Ltda e as sociedades por ela controlada (“FATOR ORE”), aqui definidas como (“Empresas”) contra fraudes, uso indevido, ataque de cibercriminosos, perda ou sequestro de dados.

O acesso, o uso indevido ou não autorizado aos referidos ativos das Empresas são tratados na Política de Segurança da Informação.

2. DIRETRIZES

Esta Política de Segurança Cibernética (“Política”) estabelece diretrizes aplicáveis a todos os Colaboradores Internos das Empresas.

Os Colaboradores devem cumprir as exigências desta Política e, além disso, assumem a responsabilidade profissional de agir de maneira ética em todos os atos que pratiquem.

Para fins da presente Política, serão aplicadas as definições listadas no Item I do Código de Ética e de Políticas Internas das Empresas, salvo se outro significado lhes for expressamente atribuído neste documento.

Adicionalmente ao disposto no presente documento, serão aplicadas as políticas do prestador de serviços de TI (Norma de Utilização de Recursos da Rede Corporativa e Diretrizes de Segurança da Informação desenvolvidos para as Empresas.

3. RESPONSABILIDADES

3.1. Diretoria

(i) Direcionar os esforços e recursos propostos para a segurança da informação, de acordo com a estratégia de negócios da empresa;

(ii) Aprovar as normas de segurança da informação e suas atualizações;

(iii) Aprovar os controles a serem utilizados para garantir a segurança das informações;

(iv) Acompanhar os indicadores de segurança e os incidentes reportados pela empresa prestadora de serviços de TI;

(v) Comunicar a Diretoria de *Compliance* os casos de violações das Políticas Internas relativas à informação para as providências necessárias;

(vi) Apoiar as iniciativas para melhoria contínua de medidas de proteção da informação da empresa, com vistas a reduzir os riscos identificados;

(vii) Aprovar o planejamento, alocação de verbas, os recursos humanos e de tecnologia, no que tange a segurança da informação;

(viii) Delegar as funções de segurança da informação aos profissionais responsáveis.

3.2. Empresa Prestadora de Serviços de TI

(i) Monitorar as violações de segurança e tomar ações corretivas visando saná-las e cuidando para que não haja recorrência;

(ii) Orientar os testes da infra-estrutura de tecnologia e de sistemas para avaliar os pontos fracos e detectar possíveis ameaças;

(iii) Assessorar as demais áreas da empresa no processo de classificação das informações;

(iv) Auxiliar as áreas de negócio na elaboração do Plano de Continuidade dos Negócios específico de cada uma;

(v) Assegurar que exista um processo apropriado para a comunicação dos incidentes e violações de segurança detectados pelos usuários da informação, independentemente dos recursos tecnológicos utilizados;

(vi) Identificar recursos e fornecer orientação para a tomada de ações rápidas caso sejam detectados incidentes de segurança;

(vii) Manter a infraestrutura que suporta o ambiente controlado;

(viii) Manter a infraestrutura e sistemas atualizados;

(ix) Garantir a implementação e operação dos indicadores de segurança;

(x) Notificar imediatamente os incidentes de segurança à diretoria;

(xi) Garantir a rápida tomada de ações em caso de incidentes de segurança;

(xii) Desenvolver programas de treinamento e de conscientização aos Colaboradores Internos e Externos sobre as normas de segurança da informação, a forma como ela está estruturada e os principais conceitos de segurança da informação e em conjunto com a área de RH e Compliance implementar e manter eses treinamentos;

(xiii) Revisar periodicamente a Norma de Segurança da Informação e sugerir as alterações necessárias.

3.3 Compliance

(i) Gerenciar os problemas disciplinares resultantes de violações dos controles de segurança da informação, juntamente com os gestores dos envolvidos;

(ii) Em conjunto com a área de de RH emitir o Termo de Compromisso, conforme modelo do Código de Ética e Políticas Internas;

(iii) Em conjunto com a área de RH gerenciar a assinatura do Acordo de Confidencialidade quando da contratação de terceiros ou prestadores de serviços;

(iv) Em conjunto com a Diretoria, determinar as sanções cabíveis de acordo com a legislação em vigor;

(v) Revisar periodicamente a Norma de Segurança da Informação e sugerir as alterações necessárias.

3.4 Colaborador

(i) Cumprir a Política e as Normas de Segurança da Informação;

(ii) Buscar orientação do superior hierárquico imediato em caso de dúvidas relacionadas à Segurança da Informação;

(iii) Proteger os ativos contra acesso, modificação, destruição ou divulgação não autorizados;

(iv) Não burlar ou tentar desativar qualquer controle de Segurança existente em equipamentos, nas estruturas físicas ou lógicas da rede das Empresas;

(v) Comunicar imediatamente à área de Segurança da Informação qualquer suspeita, evidência ou fato que possa acarretar o comprometimento da informação como e-mail suspeitos, instalação de programas desconhecidos, comportamentos inesperados, acessos ou copias indevidas ou qualquer anomalia no ambiente computacional;

(vi) Comunicar imediatamente à área de Segurança da Informação qualquer descumprimento ou violação desta Política e suas Normas;

(vii) Efetuar os treinamentos de Segurança da Informação.

4. EQUIPAMENTOS

Os equipamentos objeto desta Política são os de propriedade das respectivas Empresas definidas no item 1 deste política, tais como *desktops*, monitores, teclados, *mouses*, telefone, impressoras, desfragmentador de papéis e outros destinados ao uso pessoal ou comum dos Colaboradores.

Eles deverão ser utilizados exclusivamente para fins profissionais, estão sujeitos à monitoramento pela Diretoria de *Compliance* e o uso indevido está sujeito às penalidades.

Em caso de quebra ou indisponibilidade de equipamento (*desktops*, telefone), estarão disponíveis para uso imediato os equipamentos de contingência pré configurados.

Nas hipóteses em que for necessário acionar uma infraestrutura replicada - física ou virtualizada - que garanta a substituição de um servidor, roteador, *nobreak* e/ou outro equipamento de TI que falhe ou esteja inacessível (Redundância de TI) entrará em operação a Política de Continuidade dos Negócios das Empresas.

5. INSTALAÇÕES ELÉTRICAS E O SISTEMA DE REFRIGERAÇÃO

A fim de assegurar as condições ideais de funcionamento da Infraestrutura de TI, evitando perda de dados por falta ou sobrecarga de energia ou superaquecimento; e danos aos equipamentos de informática, é imprescindível instalações elétricas e sistema de refrigeração adequados.

Ambos foram dimensionados de acordo com a estrutura instalada sob orientação de profissionais especializados.

6. FUNCIONAMENTO CONTÍNUO DOS RECURSOS DE TI

Os Recursos de TI em sistema *no-stop* será feito por *nobreak,* que garante o funcionamento da infraestrutura por tempo suficiente para que nenhuma informação seja perdida quando ocorre falta de energia elétrica por até 12 horas. Os critérios de funcionamento e o procedimento para realização dos testes de verificação estão descritos na Política de Continuidade dos Negócios.

7. FIREWALL

As intrusões ou invasões são praticadas por pessoas que pretendem acessar, roubar ou sequestrar dados confidenciais e/ou informações privilegiadas, capturar dados para realização de fraudes, causar danos a sistemas e aplicativos.

A fim de evitar esses riscos, as Empresas contam com um mecanismo de controle do tráfego de dados entre os computadores de uma rede interna e desses com redes externas ("*Firewall*"). Ele trabalha segundo protocolos de segurança que garantem o correto funcionamento da comunicação entre as duas pontas, visando impedir intrusões.

Seu funcionamento é contínuo, as atualizações são programadas e realizadas automaticamente pelo sistema.

8. SENHAS

As Empresas adotam uma estrutura e configuração que induz a criação de senhas fortes, a fim de dificultar o acesso de pessoas mal intencionadas em seus sistemas. Há, ainda, um mecanismo automático que obriga a troca periódica de senhas pelos usuários ativos e cancela as senhas de usuários inativos/desligados da organização.

9. SOFTWARES

Aa Empresas possuem as licenças de uso de todos os *softwares* que utiliza. A Administração é responsável pelas renovações nos prazos e termos definidos em cada contrato.

É proibido o *download* de aplicativos e instaalar de qualquer natureza ou procedência sem o consentimento da Diretoria de Compliance.

O backup periódico de dados da rede, sua abrangência, armazenagem, metodologia e periodicidade é descrito na Política de Continuidade dos Negócios.

10. CORRESPONDÊNCIAS ELETRÔNICAS (“E-MAILS”)

Apenas os Colaboradores Internos e sócios da das Empresas possuirão conta de *e-mails* corporativas, que serão criadas pela empresa responsável pela Infraestrutura de TI no momento da contratação ou integralização de cotas sociais.

O responsável pela conta de *e-mail* individual ou do departamento deverá lhe atribuir uma senha de acesso pessoal, sigilosa e intransferível.

Essas correspondências poderão ser acessadas para fins de monitoramento pela Diretoria de *Compliance.*

Em caso de desligamento do Colaborador ou retirada do sócio, o acesso ao respectivo *e-mail* será imediatamente bloqueado pelo profissional de TI por orientação do Responsável por RH ou *Compliance*.

Os *e-mails* serão armazenados pela Microsoft, que proverá também os serviços de anti *spam,* anti vírus, recuperação de informação, *site* de recuperação de desastre e alertas relacionados ao vazamento de informações confidenciais e privilegiadas.

11. ARMAZENAMENTO DE DADOS EM NUVEM

Com vistas a evitar a perda de informações proprietárias, confidenciais e/ou privilegiadas, a Empresas adotam a armazenagem automática de dados em nuvem.

A responsabilidde de armazenamento corporativos de dados na rede no cloud sao dos usuários

12. TELEFONE

As Empresas definem os Colaboradores que terão acesso à linha telefônica corporativa de acordo com a atividade que desempenharão.

O uso do telefone deverá se restringir às atividades profissionais em prol das Empresas e estará sujeita à gravação automática que será mantida por até 180 dias, para fins de monitoramento e confirmação de operações.

O monitoramento será feito periodicamente à critério do Diretor de *Compliance,* mediante acesso ao portal de telefonia contratado, a fim de fazer cumprir o Código de Ética.

13. ERROS DE PROCEDIMENTOS INTERNOS

Procedimentos de gestão da segurança da informação mal-estruturados ou desatualizados podem acarretar vulnerabilidades e perdas de dados. Essas vulnerabilidades se manifestam por falhas no desenvolvimento, na implementação ou na configuração de mecanismos de segurança em *softwares,* no funcionamento dos *hardwares* ou em exposição a ameaças previsíveis.

As Empresas contam com equipe especializada para a execução dos protocolos de manutenção e segurança de seus Recursos de TI, como apontado acima.

Equipe de suporte de TI
e-mail suporte@tecnoqualify.com.br neste contato será direcionado para equipe responsável por cada atividade de TI e segurança da informação.

14. CRISES OU SITUAÇÕES CRÍTICAS

Na hipótese de situações não rotineiras em que os mecanismos descritos nesta Política se tornarem insuficientes ou ficarem indisponíveis, será acionada a Política de Continuidade dos Negócios, no que couber.

15. PENALIDADES

O não cumprimento desta ou da Política de Segurança da Informação implica em incidente de Segurança da informação e poderá resultar nas seguintes ações: advertência formal, suspensão, rescisão do contrato de trabalho, outra ação disciplinar e/ou processo civil ou criminal.

16. HISTÓRICO DE REVISÕES

1ª Versão (outubro/2022) = Criação do documento