Rodorei
TRANSPORTAMOS O FUTURO

Boas Práticas em Segurança da Informação

Programa OEA – Proteção de Sistemas, Bases de Dados e Segurança Eletrônica

PROTEGER DADOS É PROTEGER A OPERAÇÃO

Rodorei
TRANSPORTAMOS O FUTURO

OBJETIVO

Do Treinamento

Estabelecer diretrizes e boas práticas de segurança da informação para todos os colaboradores que utilizam sistemas corporativos da empresa e/ou acessem a bases de dados compartilhada **SHAREPOINT**, em conformidade com os requisitos do **Programa OEA - Operador Econômico Autorizado** e padrões internacionais de segurança (ISO 27001, NIST e WCO SAFE).

Rodorei
TRANSPORTAMOS O FUTURO

FOCO DO TREINAMENTO

Foco nas pessoas e cuidados com acesso a sistema e informações, além de equipamentos eletrônicos:

PÚBLICO

Colaboradores, prestadores de serviço ou parceiros que tenham acesso autorizado ao sistema corporativo da empresa e/ou de sua base de dados.

DISPOSITIVO

Dispositivos e recursos eletrônicos (computadores, notebooks, celulares e impressoras) utilizados em operações logísticas, administrativas e financeiras.

PADRÃO INTERNACIONAL DE SEGURANÇA

O que é? O que faz?

- Norma internacional para Gestão da Segurança da Informação (SGSI).
- Define requisitos para criar, implementar, manter e melhorar continuamente processos de proteção da informação,
- Foco em confidencialidade, integridade e disponibilidade.

ISO 27001 (International Organization for Standardization)

- Fornece o Cybersecurity Framework (CSF),
- Organiza boas práticas em cinco funções principais: Identificar, Proteger, Detectar, Responder e Recuperar.
- Muito usado como guia para gestão de riscos cibernéticos.

NIST (National Institute of Standards and Technology – EUA)

- Estrutura global para garantir a segurança e facilitação do comércio internacional.
- Na OEA, foca em gestão de riscos, segurança de cargas, integridade da cadeia logística
- Confiança mútua entre operadores e autoridades aduaneiras.

WCO SAFE Framework (World Customs Organization)

PROTEGER DADOS É PROTEGER A OPERAÇÃO

Rodorei
TRANSPORTAMOS O FUTURO

PRINCÍPIOS BÁSICOS DE SEGURANÇA DA INFORMAÇÃO

- **CONFIDENCIALIDADE** = Proteger informações contra acessos não autorizados.
- **INTEGRIDADE** = Garantir que os dados não sejam alterados de forma indevida, ou seja são registro.
- **DISPONIBILIDADE** =Assegurar que o sistema e informações estejam acessíveis sempre que necessário.
- **AUTENTICIDADE** = Confirmar a identidade de usuários, dispositivos e informações, sempre com senhas individuais e pessoais.
- **RASTREALIBILIDADE** = Registrar e monitorar os acessos e transações para auditoria e conformidade.

CONFIDENCIALIDADE + INTEGRIDADE + DISPONIBILIDADE + AUTENTICIDADE + RASTREALIBILIDADE = SEGURANÇA DA INFORMAÇÃO

PROTEGER DADOS É PROTEGER A OPERAÇÃO

Rodorei
TRANSPORTAMOS O FUTURO

GESTÃO SEGURA DE SENHAS E AUTENTICAÇÃO

- Sempre utilizar senhas com caracteres especial, misturando letras maíusculas e minúsculas, além de caracteres especiais.
- Troca sua senha de acesso pelo menos a cada **90 dias**, ou em caso de incidente de segurança registrado, mesmo que não seja com seu usuário.
- Não utilizar dados fáceis na senha, como datas de aniversário, nomes próprios pessoais.
- Nunca utilizar nas senhas numeração sequencial, como por exemplo: **1234**.
- Nunca utilizar a palavra **SENHA** em suas senhas
- Nunca repetir a mesma senha.
- Não utilizar para senhas de acesso da empresa, senhas de e-mails ou de redes pessoais. Lembresse o acesso é professional e não pode ter sua segurança fragilizada.
- Nunca anotar sua senha em papel, post-it, bloco de notas notas, ou outros aplicativos que não sejam criptografados.
- Nunca compartilhar credenciais, mesmo com gestores ou equipe de TI.
- Utilizar autenticação multifator (MFA) em sistemas críticos sempre que solicitado.

ACESSO SEGURO AO SISTEMA E AS BASES DE DADOS

- Cada usuário deve possuir um **perfil de acesso** com permissões exclusivamente relacionadas a sua utilização baseada na função a ser desempenhada.
- Bases de dados compartilhadas devem ser acessadas **somente em dispositivos autorizados** previamente pelo TI.
- Deve ocorrer bloqueio automático da tela a partir de 05 minutos de inatividade.
- O usuário não deve **em nenhuma hipótese** deixar sistemas abertos nos momentos de não utilização.
- Usuários devem **bloquear a tela** sempre que se afastarem do posto de trabalho.

PROTEGER DADOS É PROTEGER A OPERAÇÃO

Rodorei
TRANSPORTAMOS O FUTURO

PREVENÇÃO CONTRA AMEAÇAS CIBERNÉTICAS

PHISHING E ENGENHARIA SOCIAL

- **DESCONFIAR** de e-mails com erros de escrita, solicitações urgentes ou links suspeitos.
- **NUNCA CLICAR** em links ou abrir anexos de remetentes desconhecidos.
- **CONFIRMAR** com o remetente por outro canal antes de fornecer informações confidenciais.

Sempre acionar o Departamento de TI em qualquer caso suspeito

Rodorei
TRANSPORTAMOS O FUTURO

PREVENÇÃO CONTRA AMEAÇAS CIBERNÉTICAS

O que é? O que faz?

MALWARE E RANSOMWARE

- Manter **ANTIVÍRUS e FIREWALL ATIVOS** e atualizados, nunca desinstale ou desative a segurança do computador.
- **SEMPRE VERIFICAR** e informar mensagens de necessidade de atualizações não informadas pelo Departamento de TI.
- **NÃO CONECTAR** dispositivos USB desconhecidos e/ou não autorizados.
- **SUSPEITAR** mudanças nas páginas de acesso verificando com o TI a atualização e sempre checar os links de acesso.

Sempre acionar o Departamento de TI em qualquer caso suspeito

Rodorei
TRANSPORTAMOS O FUTURO

PREVENÇÃO CONTRA AMEAÇAS CIBERNÉTICAS

O que é? O que faz?

PHISHING = Tipo de GOLPE em que **HACKERS** enviam mensagens falsas (e-mails, SMS, links) se passando por pessoas ou empresas confiáveis, para enganar o usuário e **roubar senhas, dados bancários ou instalar vírus nos computadores**.

ENGENHARIA SOCIAL = Técnica de manipulação psicológica, em que criminosos **EXPLORAM A CONFIANÇA OU DISTRAÇÃO** da vítima para convencê-la a entregar informações sigilosas ou executar ações inseguras (como clicar em links, liberar acessos ou instalar programas).

Sempre acionar o Departamento de TI em qualquer caso suspeito

Rodorei
TRANSPORTAMOS O FUTURO

PREVENÇÃO CONTRA AMEAÇAS CIBERNÉTICAS

O que é? O que faz?

MALWARE São **PROGRAMAS MALICIOSOS** (vírus, trojans, spywares ou worms) que infectam computadores e sistemas com o objetivo de roubar dados, causar danos e/ou permitir acessos não autorizados.

•**RANSOMWARE** É um tipo específico de malware que **SEQUESTRA ARQUIVOS OU SISTEMAS**, criptografando-os e exigindo um pagamento (“resgate”) para liberar o acesso normalmento em BITCOIN para impossibilitar qualquer rastreio.

Sempre acionar o Departamento de TI em qualquer caso suspeito

USO CORRETO DE RECURSOS TECNOLÓGICOS

Mandamentos de Segurança

- Computadores e dispositivos móveis corporativos devem ser usados **exclusivamente** para atividades da empresa.
- É **proibido** instalar softwares não homologados pela equipe de TI.
- Controles, planilhas e documentos e dados devem ser armazenados **exclusivamente** em servidores oficiais.
- É **vedado** o uso de serviços de nuvem pessoais (Google Drive, Dropbox, etc.) para armazenamento de arquivos corporativos.
- Impressões de documentos sensíveis devem ser retiradas

Sempre acionar o Departamento de TI em qualquer caso suspeito

Rodorei
TRANSPORTAMOS O FUTURO

CONDUTA EM CASOS DE INCIDENTES DE SEGURANÇA

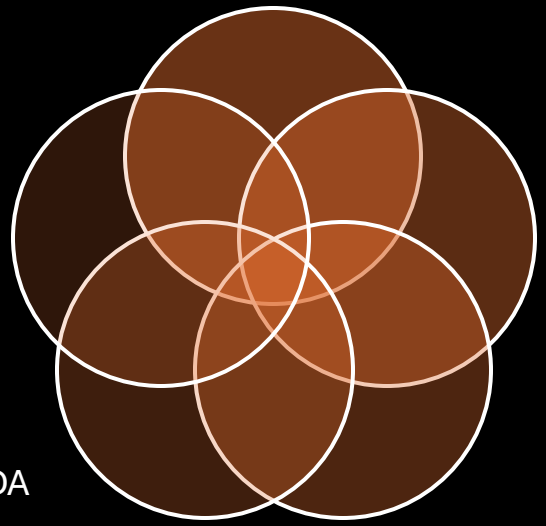
- O Departamento de TI e o Coordenador de qualidade isoladamente ou em conjunto podem auditar o atendimento as regras segurança.
- Incidentes de segurança serão relatados e tratados como Não Conformidade, podendo serar medidas disciplinares em caso de falhas de segurança.
- Os parâmetros e métodos utilizados estão em conformidade com o Programa OEA.
- Nunca tentar resolver sozinho incidentes suspeitos ou confirmados sobre segurança, sempre comunicar de imediato o Departamento de TI.
- Exemplos de Tipos de Incidentes:
  - Perda ou roubo de dispositivo corporativo.
  - Vazamento ou acesso indevido a informações.
  - Recebimento de e-mails suspeitos.
  - Erros de acesso em bases críticas.

Sempre acionar o Departamento de TI em qualquer caso suspeito

Rodorei
TRANSPORTAMOS O FUTURO

LGPD -
Lei Geral de Proteção de Dados

LGPD



Lei 13.709/2018

Proteção a dados pessoais

PROTEGER DADOS É PROTEGER A OPERAÇÃO

Rodorei
TRANSPORTAMOS O FUTURO

LGPD
Lei Geral de Proteção de Dados

PRINCÍPIOS

FINALIDADE
O uso dos dados somente deve ser feito com objetivos legítimos e legais

NECESSIDADE
A coleta de dados deve ser mínima se restringindo apenas ao necessário e sempre com anuência do titular

TRANSPARÊNCIA
Sempre demonstrar clareza sobre como os dados são tratados e armazenados

SEGURANÇA
Manter medidas técnicas e administrativas de segurança para proteção da informaçãop

Rodorei
TRANSPORTAMOS O FUTURO

LGPD
Lei Geral de Proteção de Dados

DIREITOS DOS TITULARES DAS INFORMAÇÕES

CONCEDER
Acesso, correção, exclusão e portabilidade de dados sempre que solicitado pelo titular

INFORMAÇÃO
Sempre informar sobre o compartilhamento dos dados (motivo e para que)

TRANSPARÊNCIA
Sempre demonstrar clareza sobre como os dados são tratados e armazenados

CANAIS DE CONTATO
Sempre manter canal de contato ativo entre os titulares e os detentores dos dados

Rodorei
TRANSPORTAMOS O FUTURO

LGPD
Lei Geral de Proteção de Dados

RESPONSABILIDADE SOBRE OS DADOS

TRATAMENTO

Tratar os dados pessoais de forma segura e exclusivamente para fins profissionais autorizados;

COMPARTILHAMENTO DE DADOS

Nunca compartilhar dados sem prévia autorização do titular

SEGURANÇA

Reportar incidentes ou suspeitas de incidente de vazamento de dados ao Departamento de TI

Rodorei
TRANSPORTAMOS O FUTURO

LGPD
Lei Geral de Proteção de Dados

INCIDENTES DE SEGURANÇA

ACIONAMENTOS

Em caso de vazamento de informações totais ou parciais deve ser relatado o incidente prontamente ao Departamento de TI para tratativas

NOTIFICAÇÕES

Na confirmação da suspeita comuinicar imediatamente os titulares afetuados com o vazamento das informações

Rodorei
TRANSPORTAMOS O FUTURO

FIM