CARTILHA DE CIBERSEGURANÇA DA QUALIMAX

LGPD

Lei nº 13.709/2018

(Lei Geral de Proteção de Dados Pessoais)

OBJETIVOS DA CARTILHA:

01 **Introduzir** o assunto CIBERSEGURANÇA de maneira simples e didática.

02 **Esclarecer** quanto aos fundamentos de SEGURANÇA E CIBERSEGURANÇA.

03 **Informa**r os recursos disponibilizados e como navegar de modo seguro no mundo digital.

04 **Fornecer** exemplos adequados à realidade da instituição.

05 **Conscientizar** sobre os colaboradores e público sobre o tema.

1. Conceitos

CIBERSEGURANÇA e SEGURANÇA DA INFORMAÇÃO

Informação + Segurança

Antes de tudo, devemos lembrar de duas frases:

- **A segurança depende de TODOS, seja consciente.**
- **Sem proteção, não existe privacidade.**

É dever de todos NÓS ajudar a conquistar e manter a Segurança da Informação na Empresa e em nossas vidas privadas.

INFORMAÇÃO :

É um conjunto organizado de dados que formam uma mensagem com significado e uso.

Exemplos de Dado:

Nome: José

Endereço: Rua Bom Dia, 45

Exemplo de Informação:

O sr. José é morador da Rua Bom dia, 45.

SEGURANÇA DA INFORMAÇÃO :

É um conjunto de ações destinadas a manter as informações seguras contra o acesso não autorizado e alterações indevidas.

De forma simples, entender a segurança da informação é compreender como proteger informações pessoais e corporativas de ameaças como invasores, vírus e outros tipos de ataques físicos ou cibernéticos.

A segurança da informação trata da proteção de dados e informações contra acessos não autorizados, alterações, divulgação ou destruição, garantindo a confidencialidade, integridade e disponibilidade da informação. É importante entender conceitos básicos, como:

- **Confidencialidade:**

  Garantir que a informação seja acessível somente por pessoas autorizadas.

- **Integridade:**

  Assegurar que os dados não sejam alterados de forma não autorizada.

- **Disponibilidade:**

A informação deve estar disponível quando necessário somente pelos usuários autorizados.

OS TRÊS PILARES PRINCIPAIS DA SEGURANÇA DA INFORMAÇÃO :

É o conjunto de três PILARES que garantem a Segurança da Informação.

São eles:

- Confidencialidade
- Integridade
- Disponibilidade

CONFIDENCIALIDADE :

Propriedade da Informação de não ser divulgada para partes não autorizadas, incluindo indivíduos, entidades ou processos.

Exemplos comuns em empresas:

- Empregados desligados com acesso aos conteúdos corporativos da empresa;
- Vazamentos de dados de usuários e clientes;
- Arquivos sensíveis em servidores não protegidos;
- Acesso de terceiros a planejamentos estratégicos da empresa.

Controles:

Segregação de Acesso

Criptografia

Politica de Controle de Acesso

INTEGRIDADE :

A Propriedade da informação deve ser completa e exata. Ou seja, a informação mantém sua origem e ela não pode ser alterada, assim somente pessoas autorizadas poderão ter o acesso.

Exemplos comuns em empresas:

- Quando o processo é executado estrategicamente é possível utilizar ferramentas para realizar a recuperação de informações danificadas ou perdidas. (Exemplo: Backup)

Controles:

Monitoramento, Logs e auditoria

Criptografia

Politica de Controle de Acesso

DIPONIBILIDADE :

A Propriedade da informação deve ser acessível e utilizável por entidades autorizadas.

Exemplos comuns em empresas:

- Servidor indisponível após falha da fonte de alimentação de energia.
- Site indisponível após um ataque. Exemplo: DDOS
- Serviços de comunicações indisponíveis após alguma ruptura de link

Controles:

Redundância e alta disponibilidade

Plano de continuidade e recuperação de desastres

Copias de Segurança e processo de restauração

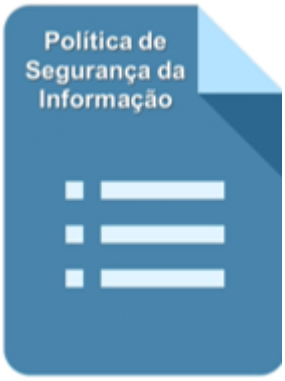
O TRIPÉ DA PROTEÇÃO DE DADOS:

O Tripé da Proteção de Dados é formado por:

- Pessoas
- Processos
- Tecnologia

“ Sem proteção não existe privacidade dos dados e informações.”

A POLÍTICA DE SEGURANÇA DA INFORMAÇÃO:



Política de segurança da informação é um conjunto de diretrizes que visa proteger as informações da empresa contra todo tipo de ameaça, seja ela interna ou externa, deliberada ou acidental.

Por que a Instituição precisa da Política de Segurança da Informação?

A Política é fundamental para prevenir, detectar e responder a incidentes de segurança que possam comprometer informações e temas confidenciais.

Todos devem compreender as diretrizes da instituição e seguir as determinações.

CIBERSEGURANÇA:

Cibersegurança

É um conjunto de diretrizes e ações que visam proteger as informações da empresa no mundo digital.

Cibersegurança é a segurança aplicada ao mundo digital, envolvendo a prática de proteger sistemas, redes e programas de ataques digitais. Esses ataques geralmente têm como objetivo acessar, alterar ou destruir informações, confidenciais, sensíveis; extorquir dinheiro de usuários; ou interromper a operação da empresa.

A **cibersegurança** pode ser dividida em algumas categorias:

- **Segurança de Rede:**

Proteger contra intrusos mal-intencionados, como hackers e malwares. É como ter um guarda-costas digital para sua rede, barrando os penetras indesejados.

- **Segurança de Aplicativos:**

Focar na manutenção de software e dispositivos livres de ameaças. Um pouco como um médico que verifica se não há nada de errado com seu aplicativo.

- **Segurança da Informação:**

Garantir a integridade e privacidade dos dados, tanto em trânsito quanto armazenados. Imagine um cofre superforte onde seus dados são guardados longe dos olhares curiosos.

- **Recuperação de Desastres:**

Planejar como responder a um incidente de segurança cibernética e como restaurar as operações e informações para voltar ao normal. É o plano de fuga para quando as coisas dão errado no mundo digital.

Defensor da Cibersegurança

É dever de todos ajudar a proteger as informações da empresa no mundo digital.

E como você se torna um defensor da cibersegurança?

- Mantendo-se informado sobre as melhores práticas de segurança.
- Acessar sites oficiais na internet, que contenham o cadeado do certificado de segurança e https. Ex.: https:
- Utilizar senhas fortes, com senha composta no mínimo de 10 caracteres com números, letras, símbolos, maiúsculo, minúsculo.
- Não utilizar a mesma senha para vários serviços. Cada sistema com sua senha.
- Utilizar antivírus atualizado no computador e smartphone.
- Atualizar regularmente seus sistemas, aplicativos , computador e celular.
- Não compartilhar a senha com ninguém. Sua senha, sua responsabilidade
- Não abrir e-mail ou mensagens e clicar em links suspeitos ou com teor de urgência.

Lembre-se, com acesso ao mundo digital, vêm grandes responsabilidades de segurança!

Então, da próxima vez que você digitar sua senha ou atualizar seu antivírus, pense em si mesmo como um defensor, mantendo o perigo digital à distância. Afinal, em um mundo onde os dados são o novo ouro, a cibersegurança é a armadura de defesa.

2. Colaboradores, Clientes, Usuários, Visitantes do Site

O PAPEL DE TODOS COMO DEFENSORES DA SEGURANÇA E CIBERSEGURANÇA:

Todos nós exercemos papel muito importante na proteção e preservação da informação no ambiente da instituição.

Além de usar os recursos tecnológicos como computador ou celular, é preciso que os todos estejam atentos as tentativas de golpes, falsos contatos, falsas ligações, falsos e-mails em diversas modalidades de cibercrime.

COLABORE E SEJA UM GUARDIÃO DA INFORMAÇÃO.

Em qualquer suspeita ou dúvida, todos devem procurar seu gestor para apoiar e entender o cenário, ANTES DE CAIR NUM GOLPE E/OU FRAUDE.

3. Mantenha sempre o ambiente seguro

Todos os dias acontecem invasões, acessos indevidos, panes ou golpes causando prejuízos.

Cuidado ao acessar seu computador, notebook e celular:

- **Colabore e não abra links, mensagens ou ligações suspeitas com tom de urgência ou promoções absurdas.**
- **Pare e pense, antes de abrir a mensagem e tomar ação. Achou a mensagem suspeita, acione a área de TI para avaliar e ajudar.**

Problemas causados por apagão global podem levar dias até serem corrigidos

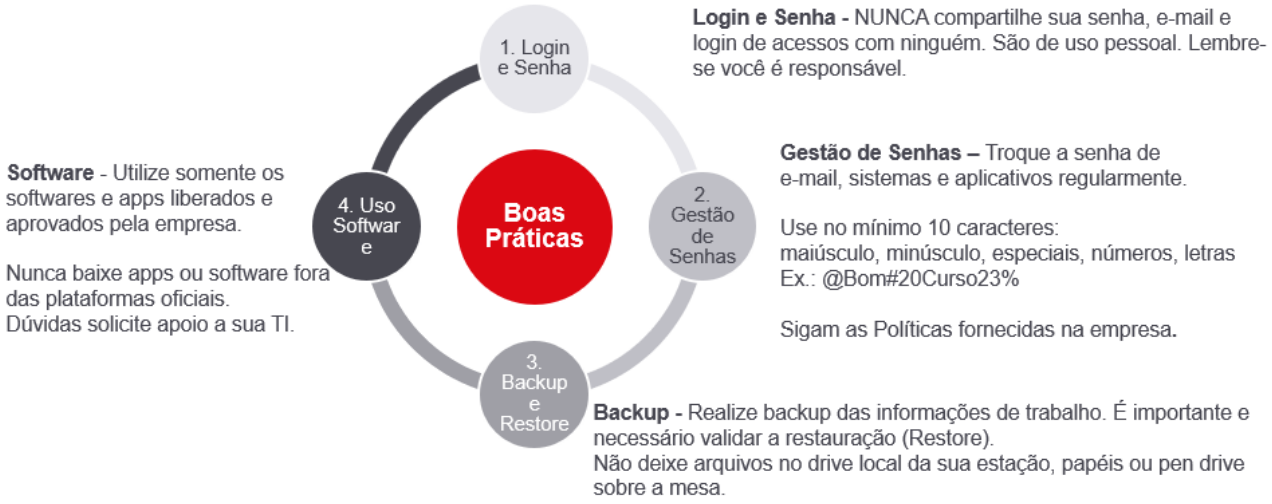
Correção manual necessária exigirá muito trabalho pela frente, dizem especialistas

- Voos são retomados após apagão da Microsoft; bancos e TVs foram afetados
- Falha global afeta hospitais de São Paulo e atrasa atendimentos

Boas práticas:

Dicas que todos devem seguir e praticar:

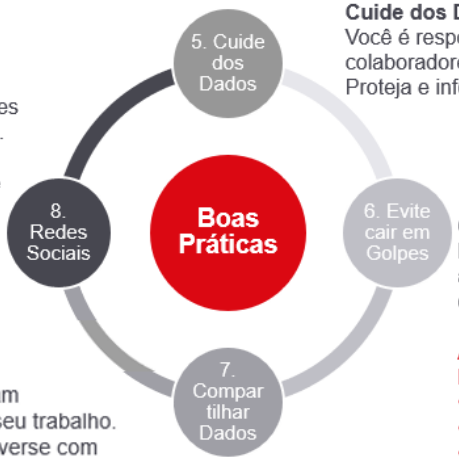
1.Login e senha
2.Gestão de senha
3.Backup
4.Softwares



Boas práticas:

Dicas que todos devem seguir e praticar:

5.Cuide dos dados privados e corporativos
6.Cuidado com as tentativas de golpes
7.Compartilhamento de dados
8.Redes Sociais



Cuide dos Dados Privados e Corporativos -
Você é responsável pelos dados (clientes, fornecedores, colaboradores) que utiliza nas tarefas e rotinas.
Proteja e informe seu gestor ou a TI caso perceba algo suspeito.

Redes Sociais -
- Faça o uso mínimo de informações e dados para atingir sua finalidade.
- Não compartilhe informações sigilosas/confidenciais nas redes e WhatsApp.
Lembre-se menos é mais

Cuidado com as tentativas de golpes
Na maioria das tentativas os golpistas utilizam a pressão ou urgência na mensagem, ligação ou abordagem para ter acesso a informações.

Assim, ao receber uma abordagem, e-mail ou ligação suspeita:
- Pare
- Pense
- Verifique

Valide quem está solicitando as informações!!!

Compartilhar Dados -
Evite compartilhar dados.
Os dados que você tem acesso foram disponibilizados para você realizar seu trabalho.
Caso necessite de informações converse com seu gestor, para validar a necessidade e depois solicitar o acesso a TI.

Boas práticas:

Dicas que todos devem seguir e praticar:

09.Atenção ao seu redor
10.Não salve senhas e logins
11.Whatsapp – siga as diretrizes e não misture WhatsApp Corporativo e Pessoal
12.Leia as Políticas e documentos oficiais da instituição

Leia as Politicas:

- É dever do colaborador ler e ter ciência das Políticas da empresa. Assim você seguirá as orientações e diretrizes da empresa.

- Principais políticas:

- Política de privacidade
- Política de cookies
- Política de segurança
- Demais políticas da empresa

Atenção ao seu redor -
- verifique se há pessoas em volta que possam estar olhando a tela do seu computador.
- não converse sobre assuntos sigilosos em locais públicos, ou naquele momento descontraído na hora do cafezinho.

Não salve senhas e logins –
Não use a opção "Salvar o login" ou "Login automático".
Com essa função habilitada, só facilita que pessoas mal-intencionadas consigam acessar a sua conta quando você estiver ausente do seu dispositivo.

WhatsApp –
- WhatsApp pessoal é para seu uso privado, fora da empresa.
- Não misture assuntos e conversas pessoais com assuntos de trabalho.
- Utilize senha e demais recursos de segurança disponíveis.
- Siga as políticas e diretrizes da empresa.

Seja um Defensor da LGPD, Privacidade e Proteção de Dados

Você está convocado(a) para ser defensor da LGPD, Privacidade e Proteção de Dados na empresa.

LGPD =

Privacidade
+
Segurança
+
Proteção dos dados

+

Tripé de Proteção

Conscientize-se

Participe

Divulgue...

4. Publicação e validade deste documento

A Liotécnica se reserva o direito, a seu exclusivo critério, de modificar, alterar, acrescentar ou remover partes deste documento a qualquer momento sem prévia consulta. Portanto, recomendamos que você verifique este documento periodicamente.

Esta documento foi alterada pela última vez e publicada em nossas plataformas em 13 de Dezembro de 2024.

5. Lei Aplicável

O presente documento será regida e interpretada segundo a legislação brasileira, no idioma português, sendo eleito o Foro da Comarca de Embu das Artes-SP para dirimir qualquer litígio ou controvérsia envolvendo o presente documento, salvo ressalva específica de competência pessoal, territorial ou funcional pela legislação aplicável.

6. Encarregado de Proteção de Dados

A Liotécnica segue as diretrizes estabelecidas pela Lei Geral de Proteção de Dados (LGPD) e de acordo com o artigo 41, comunica que o Encarregado pelo Tratamento de Dados na empresa é o sr. Lucas Muniz Machado, disponível para a comunicação através dos meios:

Encarregado de Proteção de Dados:
Sr. Lucas Muniz Machado
canallgpd@liotecnica.com.br

Endereço:
Avenida João Paulo I, 900
Embu das Artes-SP