PROGRAMA CUORE | Apoio ao Colaborador
Formação Contínua

Programa I:

Fundamentos Gerais relativos a Proteção e Segurança de Dados em contexto de Trabalho

Gi Group HOLDING

Bem Vindo(a) à sua Formação

Na sequência de celebração de Contrato de Trabalho, a GI GROUP vem por este meio enviar o seu Programa de Formação de Colaborador.

Esta formação é de consulta obrigatória e corresponde à modalidade de formação inicial, a qual consideramos ser uma mais-valia, quer para o seu desenvolvimento pessoal e profissional, quer para a sensibilização dos princípios orientadores do presente Módulo, considerados de maior relevância, na garantia de um exercício profissional de excelência.
Estes cursos estão organizados em formação à distância e, na modalidade de auto formação, modalidade de aprendizagem individual que permite ao indivíduo aprender ao seu próprio ritmo, utilizando recursos específicos para o efeito e, que contribua para o aumento das suas competências pessoais e profissionais sem a necessidade do acompanhamento contínuo de um tutor ou formador.

Ao aceder a este Módulo, o/a Colaborador/a declara que se compromete a:
1. Aceder ao material formativo e dedicar o tempo necessário, para o seu desenvolvimento de competências e conclusão do presente Módulo;
2. Não transmitir a terceiros, sob qualquer forma, os materiais formativos recebidos.

Em caso de necessidade de suporte, p.f. contacte: formacao.colaborador@gigroup.com

Conteúdo Programático

A importância da Confidencialidade e da Privacidade
Cultura de Proteção de Dados
Regulamento Geral sobre Proteção de Dados (RGPD):
- Enquadramento Legal
- Aplicabilidade

Definições
- Dados Pessoais
- Tratamento de Dados
- Fundamentos para o Tratamento de Dados

Princípios Orientadores da Lei
Direitos dos Titulares de Dados
Violação de Dados Pessoais
Segurança de Informação
- Conceitos Básicos
- Classificação e Etiquetagem de Informação
- Transmissão Segura de Informação

Debriefing de Formação – O que Aprendi

A importância da Confidencialidade e da Privacidade

Confidencialidade

A confidencialidade garante que a informação é acedida apenas por pessoas que têm autorização para tal, respeitando as regras instituídas a este respeito.

A informação confidencial não deve ser utilizada em benefício próprio ou de terceiro e não pode ser divulgada qualquer informação que não tenha sido previamente autorizada.

Exemplos de conteúdo de Confidencialidade:

- **Dados pessoais;**
- **Informação financeira;**
- **Planos estratégicos e comerciais;**
- **Contratos;**
- **Fusões e aquisições;**
- **Especificações técnicas, entre outros.**

A importância da Confidencialidade e da Privacidade

Privacidade

A privacidade é um conceito associado à confidencialidade e que compreende a proteção da informação que dispõe, com o objetivo de garantir o cumprimento das normas legais aplicáveis e do direito fundamental de cada individuo de decidir quem deve ter acesso, em cada momento, aos seus dados.

O não cumprimento de todas as normas e boas práticas na privacidade de dados pessoais pode:

Constituir uma violação dos direitos previstos na Lei da proteção de dados pessoais (Lei 67/1998) e o Regulamento Geral sobre a proteção de dados (679/2016 da EU).
Constituir um ilícito, passível de sanção disciplinar, civil e/ou penal.
Comprometer seriamente a imagem e reputação da Empresa.

Cultura de Proteção de Dados

Apresentamos abaixo algumas sugestões de modo a que possa ativamente contribuir para a promoção de uma cultura de proteção de dados, a partir do seu posto de trabalho:

1. Se não se encontra no seu posto de trabalho, garanta que remove todos os documentos em papel da sua mesa ou de outros locais (impressoras, aparelhos de fax, etc.) de modo a impedir o acesso não autorizado.

2. Sempre que se ausenta do seu posto de trabalho, garanta que bloqueia o acesso ao seu computador ou outros equipamentos, que realizem tratamento de dados pessoais.

3. O ecrã do seu computador não deve permitir a visualização, nem o acesso não autorizado, a informação considerada restrita e/ou sensível.

4. Não partilhe a sua password ou credenciais de acesso. Todas as passwords são encaradas como um dado confidencial.

5. O arquivo que contenha informação restrita e/ou sensível, deverá ser mantido reservado e fechado, sempre que não esteja em uso.

Regulamento Geral da Proteção de Dados (RGPD)

Enquadramento Legal

- 1995 – A União Europeia aprova a Diretiva de Privacidade de Dados Pessoais.
- Abr. 2016 - A União Europeia aprova o Regulamento Geral de Proteção de Dados (RGPD), uma revisão substantiva e o fortalecimento dos princípios de privacidade da União Europeia - para entrar em vigor em Maio de 2018.
- Jul. 2016 -EU-EUA anunciam o substituto do agora extinto Safe Harbor: o EU-US Privacy Shield Framework (mecanismo que garante o fluxo transfronteiriço de dados da EU para Fora EU).
- O Regulamento Geral sobre Proteção de Dados Pessoais (Regulamento UE 2016/679) passará a ser aplicado diretamente em todos os Estados Membros da U.E. a partir de 25 de Maio de 2018, substituindo a diretiva em vigor, até à data.

Regulamento Geral da Proteção de Dados (RGPD)

Aplicabilidade

O Regulamento Geral sobre a Proteção de Dados (RGPD) 2016/679 do Parlamento Europeu e do Conselho de 27 de Abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados, revoga a anterior Diretiva 95/46/CE e representa uma legislação destinada a harmonizar as leis de privacidade de dados em toda a Europa.

Aplicação do RGPD a todas as entidades públicas e privadas.

Aplicável ao tratamento de dados, realizado na União Europeia e fora da União Europeia.

Definições

Dados Pessoais

Para efeitos de legislação em vigor, entende-se por dados pessoais qualquer informação de qualquer natureza e independentemente do respetivo suporte, incluindo som e imagem, relativa a uma pessoa singular identificada ou identificável (“titular de dados”). É considerada identificável a pessoa que possa ser identificada direta ou indiretamente, a partir de um determinado dado.

Alguns exemplos:

- Nome
- Numero de identificação
- Testemunhos de conexão (cookies)
- Identidade física, fisiológica, genética, mental, económica, cultural ou social da pessoa singular, entre outros.

Definições

Dados Pessoais * *NOVO*

O RGPD passa a incluir:

Dados de Localização

Os consumidores que transportam os seus smartphones ou tablets podem não perceber quantos dados de geolocalização estão a ser captados ou o que está a ser usado.

Identificadores por Via Eletrónica

Os dados pessoais incluem agora endereços de email , informações sobre hábitos de navegação na internet, endereços de IP, cookies, entre outros.

Definições

Tratamento de Dados

Uma operação ou um conjunto de operações efetuadas sobre dados pessoais, por meios automatizados ou não automatizados, tais como a recolha, o registo, a organização, a estruturação, a conservação, a adaptação ou alteração, a recuperação, a consulta, a utilização, a divulgação por transmissão, difusão ou qualquer outra forma de disponibilização, a comparação ou interconexão, a limitação, o apagamento ou a destruição.

Definições

Tratamento de Dados - Fundamentos

Para que o tratamento de dados pessoais seja conforme a Lei, é necessário estar verificado um dos seguintes fundamentos:

- **Consentimento do Titular de Dados (livre, informado, expresso e escrito);**
- **Obrigação (execução) contratual ou diligências pré contratuais, a pedido do Titular de Dados;**
- **Obrigação jurídica a que o Responsável pelo Tratamento esteja sujeito;**
- **Defesa dos interesses vitais do Titular de Dados ou de outra pessoa singular;**
- **Interesse público;**
- **Interesse legítimo prosseguido pelo Responsável pelo Tratamento ou por terceiros.**

Princípios Orientadores da Lei

Princípio do tratamento lícito, leal e da transparência.
As Empresas necessitam de garantir que as suas práticas, processos e sistemas internos de tratamento de dados, estão baseados na lealdade e transparência de tratamento. Reforçamos a necessidade que consulte a Declaração de Privacidade GI GROUP para que conheça em detalhe a nossa orientação, a este nível.

Princípio da especificação e da limitação da finalidade.
As Empresas deverão recolher e tratar dados pessoais, em função de uma finalidade específica. Igualmente, os dados deverão ser reservados pelo tempo estritamente necessário, considerando essa finalidade.

Princípio da minimização dos dados.
As Empresas apenas deverão processar os dados pessoais considerados necessários, para atingir os seus objetivos de tratamento.

- ✓ Tratamento lícito, leal e transparente
- ✓ Limitação da finalidade
- ✓ Minimização de dados
- ✓ Exatidão de dados
- ✓ Conservação dos dados
- ✓ Segurança e Confidencialidade

Princípios Orientadores da Lei

Princípio da exatidão dos dados.
O Regulamento afirma que “cada passo razoável deve ser dado” para apagar ou retificar dados que são imprecisos ou incompletos. Os Titulares de dados têm o direito de solicitar que dados imprecisos ou incompletos sejam apagados ou retificados.

Princípio relativo à conservação dos dados.
As Empresas necessitam de desenvolver mecanismos internos de eliminação de dados pessoais, quando estes não se revelem necessários, salvaguardando a sua conservação pelo período estritamente necessário.

Princípio da segurança e da confidencialidade.
Os dados pessoais devem ser “processados de forma a garantir a segurança apropriada dos dados pessoais, incluindo proteção contra processamento não autorizado ou ilegal e contra perda, destruição ou dano acidental, usando medidas técnicas ou organizacionais apropriadas”.

- ✓ Tratamento lícito, leal e transparente
- ✓ Limitação da finalidade
- ✓ Minimização de dados
- ✓ Exatidão de dados
- ✓ Conservação dos dados
- ✓ Segurança e Confidencialidade

Direitos dos Titulares de Dados

Direito à Informação: O Titular de Dados tem o direito de receber a informação necessária ao seu conhecimento e esclarecimento, relativa à política de privacidade aplicável ao seu tratamento.

Direito ao Acesso: O Titular de Dados tem direito a aceder à informação que a Empresa/Entidade detém a seu respeito.

Direito à Edição/Rectificação: O Titular de Dados tem o direito de solicitar a alteração ou rectificação dos seus dados pessoais, com vista à atualização da sua informaçao.

Direito à Objeção: O Titular de Dados tem o direito a opor-se à recolha e/ou tratamento dos seus dados, para fins de marketing e publicidade.

Direito ao Esquecimento: O Titular de Dados tem o direito de solicitar a eliminação dos seus dados pessoais, dos sistemas da Empresa/Entidade.

Direito à Portabilidade: O Titular de Dados tem o direito a solicitar, em ficheiro acessível, os dados pessoais que transmitiu e que constem da posse da Empresa/Entidade.

- ✓ A resposta ao Titular de Dados é obrigatória e deve ocorrer no prazo de 30 dias, após a solicitação inicial.

- ✓ Na qualidade de Titular de Dados, caso necessite de exercer qualquer um dos direitos previstos, solicitamos que aborde directamente o Consultor GI GROUP ou, alternativamente, através do endereço: pt.privacy@gigroup.com

Regulamento Geral da Proteção de Dados (RGPD)

Violação de Dados Pessoais

O novo regulamento obriga a que, por padrão (by default), os novos bens, serviços, produtos, sistemas, dispositivos e processos sejam construídos, desde a fase de desenvolvimento, de acordo com os requisitos de privacidade e proteção (privacy by design), de modo a garantir máxima proteção da informação.
Violação de Dados Pessoais: o que é? Significa, antes de mais, uma violação de segurança que leva à destruição acidental ou ilegal, perda, alteração, divulgação não autorizada ou acesso a dados pessoais. É mais do que apenas perder dados pessoais.

Violação de Dados Pessoais: Alguns exemplos:

- Acesso a dados pessoais, por pessoas não autorizadas para tal;
- Ação deliberada ou acidental do Responsável de Tratamento ou Subcontratante;
- Enviar informação com dados pessoais a destinatários incorrectos, entre outros.

Sempre que tiver conhecimento de alguma situação que possa ser reconhecida como “Violação de Dados Pessoais”, deverá comunicar de forma imediata à GI GROUP, via: pt.privacy@gigroup.com

Regulamento Geral da Proteção de Dados (RGPD)

Segurança de Informação

A informação pode existir em vários formatos: impressa, armazenada eletronicamente, verbal, transmitida pelo correio convencional...

É da responsabilidade da segurança de informação protegê-la de vários tipos de ameaças, para garantir a continuidade do negócio e minimizar riscos.

A segurança de informação compreende a proteção de informação, sistemas, recursos e demais ativos contra desastres, erros, e manipulação não autorizada.

Assim, a segurança da informação deverá também ser aplicada em todas as fases do ciclo de vida nas atividades que desenvolve diariamente.

Porque se deve preocupar com a segurança de informação?

- Problemas mais comuns:
- Destruição de informações e outros recursos
- Modificação ou deturpação de dados
- Roubo, remoção ou perda da informação
- Revelação de informações
- Interrupção de serviços

Regulamento Geral da Proteção de Dados (RGPD)

Segurança de Informação – Conceitos Básicos

Ativo de Informação: A informação é elemento essencial para todos os processos de negócio da organização, sendo, portanto, um bem ou ativo de grande valor
Vulnerabilidade: São as fraquezas presentes nos ativos de informação, que podem causar, intencionalmente ou não, a quebra de um ou mais dos três princípios de segurança da informação: confidencialidade, integridade, e disponibilidade
Ameaça: A ameaça é um agente externo ao ativo de informação, que aproveitando-se das vulnerabilidades deste ativo, poderá quebrar a confidencialidade, integridade ou disponibilidade da informação suportada ou utilizada por este ativo
Probabilidade: A probabilidade é a chance de uma falha de segurança ocorrer levando-se em conta o grau das vulnerabilidades presentes nos ativos que sustentam o negócio e o grau das ameaças que possam explorar estas vulnerabilidades.
Impacto: O impacto de um incidente são as potenciais consequências que este incidente possa causar ao negócio da organização e demais envolvidos
Risco: O risco é a relação entre a probabilidade e o impacto. É a base para a identificação dos pontos que requerem investimentos em segurança da informação

As pessoas são o elemento central de um sistema de segurança da informação. Os incidentes de segurança da informação envolvem, quase sempre, pessoas, quer no lado das vulnerabilidades exploradas, quer no lado das ameaças que exploram estas vulnerabilidades. Mantenha-se atento e garanta a sua conformidade máxima com os procedimentos e práticas instauradas no seu local de trabalho, neste âmbito.

Regulamento Geral da Proteção de Dados (RGPD)

Segurança de Informação – Classificação e Etiquetagem de Informação

Os Titulares de Informação são responsáveis por classificar a informação que criem ou adquiram segundo os padrões de classificação de dados em vigor nas empresas em que se encontram colocados.

- Os Titulares ficam depois responsáveis por assegurar que o acesso a tal informação seja gerido com base nos padrões instituídos por tais Entidades.
- Os Titulares de Informação devem trabalhar com funções de apoio apropriadas, como as TI, com vista a assegurar a manutenção dos controlos apropriados para limitar o acesso à informação com base no princípio da necessidade.
- Os Titulares de Informação são responsáveis por assegurar que os respetivos documentos sejam mantidos em conformidade com o Plano de Retenção de Registos, em vigor na Entidade.

Todos os Colaboradores são responsáveis por se manterem conscienciализados acerca de vulnerabilidades e ameaças, como a engenharia social, a mistificação de interfaces (*pishing*) e outros ataques/explorações, e por se protegerem do acesso e do uso não autorizados dos Sistemas de Informação com que interagem profissionalmente.

Os Colaboradores que violem tais procedimentos poderão ser sujeitos a medidas disciplinares que podem ir até à rescisão do contrato de trabalho e à instauração de um processo civil ou criminal.

Regulamento Geral da Proteção de Dados (RGPD)

Segurança de Informação – Classificação e Etiquetagem de Informação

Classificação da Informação Confidencial
informação que a Empresa tem a obrigação legal de manter em confidencialidade ou que deve ser considerada informação comercial ou concorrencial sensível.

Dados Pessoais, Comerciais, Financeiros, Exclusivos

- **Acesso:** O acesso a visualização e edição será concedido apenas aos funcionários que dele necessitem para realizar o seu trabalho.
- **Transferência:** Os utilizadores devem adotar medidas proativas para proteger a transferência; por exemplo, usar métodos aprovados de transferência de ficheiros encriptados, evitar mensagens eletrónicas sempre que possível e nunca enviar informação para um destinatário que não necessite de tal informação.
- **Armazenamento:** Os utilizadores devem armazenar os documentos físicos em locais fechados. Os dados eletrónicos devem ser armazenados em locais seguros, como um armazenamento em nuvem aprovado ou um armazenamento em rede aprovado com controlos de acesso adequados.

Além disso, subconjuntos de Informação Confidencial podem também ser regulados ou controlados nos termos da legislação, de normas sectoriais ou de acordos comerciais. A Empresa pode impor requisitos de processamento adicionais em relação a tais dados, em consistência com os requisitos estabelecidos pela autoridade competente. Mantenha-se atento e procure informação relevante neste âmbito, no seu local de trabalho.

Regulamento Geral da Proteção de Dados (RGPD)

Segurança de Informação – Classificação e Etiquetagem de Informação

Classificação da Informação Interna
Informação da Empresa que não seja Confidencial ou Pública.

Páginas de Intranet, Correio eletrónico, Boletins Informativos/Memorandos
Acesso: O acesso a visualização e edição será limitado a grupos de pessoas em função do seu departamento ou classificação de trabalho.
Transferência: Os utilizadores devem adotar medidas proativas para proteger a transferência; embora a mesma possa ser enviada com precauções razoáveis sempre que aplicável e possível.
Armazenamento: A informação pode ser armazenada em locais seguros, como armários com fecho ou discos rígidos de utilizadores.

Além disso, subconjuntos de Informação Confidencial podem também ser regulados ou controlados nos termos da legislação, de normas sectoriais ou de acordos comerciais. A Empresa pode impor requisitos de processamento adicionais em relação a tais dados, em consistência com os requisitos estabelecidos pela autoridade competente. Mantenha-se atento e procure informação relevante neste âmbito, no seu local de trabalho.

Regulamento Geral da Proteção de Dados (RGPD)

Segurança de Informação – Classificação e Etiquetagem de Informação

Classificação da Informação Pública
informação cuja divulgação, alteração ou destruição não autorizadas causariam um risco reduzido ou nulo para a Empresa

Sítio Externo, Comunicados de Imprensa, Materiais de Marketing
Acesso: O acesso a visualização pode ser concedido livremente. O acesso a edição deve continuar a ser controlado pelo Titular da Informação.
Transferência: Os utilizadores devem adotar medidas proativas para proteger a transferência; embora a mesma possa ser enviada livremente por qualquer meio.
Armazenamento: A informação pode ser armazenada onde for necessário, salvo estipulação em contrário a definir pela empresa.

Além disso, subconjuntos de Informação Confidencial podem também ser regulados ou controlados nos termos da legislação, de normas sectoriais ou de acordos comerciais. A Empresa pode impor requisitos de processamento adicionais em relação a tais dados, em consistência com os requisitos estabelecidos pela autoridade competente. Mantenha-se atento e procure informação relevante neste âmbito, no seu local de trabalho.

Regulamento Geral da Proteção de Dados (RGPD)

Transmissão Segura de Informação

- Os utilizadores não usarão os seus computadores portáteis, computadores de secretária ou dispositivos móveis atribuídos pela Empresa (caso aplicável) para descarregar ou armazenar grandes volumes de fotos pessoais, canções, ficheiros ou outros dados e aplicações não relacionados com o trabalho. Nem a GI GROUP, nem a Empresa na qual se encontra a trabalhar, serão responsáveis pela perda de quaisquer desses dados.
- Os utilizadores não usarão os dispositivos atribuídos pela Empresa (caso aplicável) para receber a transmissão de grandes volumes de vídeo ou áudio nem para recorrer à tecnologia de hot-spotting para uso pessoal.
- As permissões de Gestão de Direitos da Informação (IRM, ou Information Rights Management) do Outlook deverão ser usadas sempre que ocorrer a transmissão de Informação Confidencial por correio eletrónico. A IRM possibilita que os utilizadores encriptem uma mensagem e especifiquem permissões de acesso para impedir a leitura, a impressão, o reencaminhamento ou a cópia de informação sensível por pessoas não autorizadas.
- A introdução de dispositivos não autorizados na rede empresarial global cria um risco de segurança ou uma potencial perturbação da infraestrutura tecnológica, não estando autorizada.

Resumimos-te os principais resultados alcançados através desta formação:

1. Saber identificar comportamentos a adotar, de modo a garantir a Confidencialidade e a Privacidade de informação
2. Saber compreender os conceitos associados à Proteção e Segurança de Dados
3. Saber identificar os Princípios Orientadores da Lei (RGPD), no âmbito do fluxo de tratamento de dados
4. Saber reconhecer as situações de potencial contexto de violação de dados pessoais e como as reportar, com vista à sua resolução
5. Saber atuar em contexto de segurança de informação, no que diz respeito ao acesso, transferência e armazenamento de dados

Agora que concluíste esta ação, acede ao questionário de satisfação da formação AQUI (**Passo obrigatório para a conclusão desta ação**).