Dicas e Aprendizados

Baixe e salve este PDF na sua área de trabalho.

Fique atento aos quatro escudos e dicas de segurança!

Nunca envie informações confidenciais para seu endereço de e-mail pessoal

Poste prudentemente – Rever as diretrizes de mídia social da Deloitte e as obrigações contratuais aplicáveis.

Mantenha-o profissional – Não envie documentos da Deloitte, cliente ou terceiros para seu endereço de e-mail pessoal.

Mantenha-o no ambiente da Deloitte – Não envie arquivos da Deloitte ou clientes para seu endereço de e-mail pessoal ou sites pessoais de colaboração na nuvem.

Classifique corretamente os dados para proteger informações

Não se atrase – Relatar o potencial incidente mais cedo ou mais tarde é crucial para alcançar os melhores resultados.

Defina corretamente – Saiba identificar os diferentes tipos de informações confidenciais e informações pessoais para a devida proteção de dados.

Use apenas tecnologia aprovada

Tecnologia com confiança – Use apenas tecnologias aprovadas.

Verifique o plano – Os CIMPs (Confidential Information Management Plans, planos de gerenciamento de informações confidenciais) estabelecem estratégias de equipe de conta, equipe de engagement, negócios e linhas de serviço para gerenciar informações confidenciais e ajudar a prevenir, detectar, conter e mitigar o risco de possíveis incidentes de confidencialidade.

Você não pode perder o que você não tem

Mantenha-o enxuto – Agende um tempo semanalmente para revisar sua caixa de entrada e excluir mensagens que não são mais necessárias para um propósito comercial, observando, ao mesmo tempo, manter registros oficiais e documentos sob guarda de documentos de acordo com as políticas de retenção de registros de sua empresa.

Arquivar em tempo hábil – arquive corretamente arquivos de projeto, a partir de seu laptop ou site de colaboração dentro dos cronogramas de arquivamento especificados da sua empresa e exclua arquivos não mais necessários para um propósito comercial.

Cortar o acesso – Avise os proprietários de sites de colaboração quando você não precisar mais de acesso.

Dicas de segurança

Mantenha-se diligente – ao trabalhar em casa, seja consciente sobre a manutenção da confidencialidade e das salvaguardas de privacidade.

Não facilite os ataques de phishing – Fique atento às tentativas de engenharia social e não clique em links suspeitos em e-mails.

Não seja anônimo – Mantenha seu crachá de segurança visível o tempo todo no escritório, mesmo que você esteja apenas sentado em sua mesa.

Relate oportunamente – Denuncie possíveis incidentes usando o processo de reporte da sua empresa assim que você suspeitar de uma possível perda ou divulgação de qualquer tipo de informação confidencial ou informação pessoal.

Conheça seu ambiente – Evite trabalhar ou discutir informações confidenciais em público sempre que possível.

Sem utilização não autorizada – Todos são obrigados a fazer o seu próprio crachá na Deloitte e nas instalações dos clientes. Não permita que ninguém o siga por uma porta de segurança sem um crachá, mesmo que você conheça.