

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

1. INTRODUÇÃO

A Política de Segurança da Informação, também referida como PSI, é o documento que orienta e estabelece as diretrizes corporativas da UX Innovation para a proteção dos ativos de informação e a prevenção de responsabilidade legal para todos os usuários. Deve, portanto, ser cumprida e aplicada em todas as áreas da organização.

2. OBJETIVOS

Estabelecer diretrizes que permitam aos colaboradores, associados, clientes e prestadores de serviços da UX Innovation seguirem padrões de comportamento relacionados à segurança da informação adequados às necessidades de negócio e de proteção legal da empresa, das informações e do indivíduo.

Nortear a definição de normas e procedimentos específicos de segurança da informação, bem como a implementação de controles e processos para seu atendimento.

Preservar as informações da UX Innovation quanto à:

- **Integridade:** garantia de que a informação seja mantida em seu estado original, visando protegê-la, na guarda ou transmissão, contra alterações indevidas, intencionais ou acidentais.
- **Confidencialidade:** garantia de que o acesso à informação seja obtido somente por pessoas autorizadas.
- **Disponibilidade:** garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário, com as devidas autorizações.

3. APLICAÇÕES DA PSI

As diretrizes aqui estabelecidas deverão ser seguidas por todos os colaboradores, bem como os prestadores de serviço, e se aplicam à informação em qualquer meio ou suporte. Esta política dá ciência a cada colaborador de que os ambientes, sistemas, computadores e redes da empresa



poderão ser monitorados, auditados e gravados, com prévia informação, conforme previsto nas leis brasileiras.

É também obrigação de cada colaborador se manter atualizado em relação a esta PSI e aos procedimentos e normas relacionadas, buscando orientação do seu gestor ou da Gerência de Planejamento e Sistemas de Informações sempre que não estiver absolutamente seguro quanto à aquisição, uso e/ou descarte de informações.

4. PRINCÍPIOS DA PSI

Toda informação produzida ou recebida pelos colaboradores como resultado da atividade profissional contratada pela UX Innovation pertence à referida organização. As exceções devem ser explícitas e formalizadas em contrato entre as partes, caso seja aplicável.

Os equipamentos de informática e comunicação, sistemas e informações são utilizados pelos colaboradores para a realização das atividades profissionais. O uso pessoal dos recursos é permitido desde que não prejudique o desempenho dos sistemas e serviços, porém, fica a cargo da UX Innovation realizar eventuais monitoramento, auditoria e inspeções sem prévio aviso.

5. REQUISITOS DA PSI

Para a uniformidade da informação, a PSI deverá ser comunicada a todos os colaboradores, clientes, prestadores de serviços a fim de que a política seja cumprida dentro e fora da empresa.

Tanto a PSI quanto às normas deverão ser revistas e atualizadas periodicamente, sempre que algum fato relevante ou evento motive sua revisão antecipada, conforme análise e decisão do Comitê de Segurança.

Deverá constar em todos os contratos da UX Innovation a Cláusula de Confidencialidade, como condição imprescindível para que possa ser concedido o acesso aos ativos de informação disponibilizados pela organização.

A responsabilidade em relação à segurança da informação deve ser comunicada na fase de contratação dos colaboradores, prestadores de serviços e parceiros, que devem ser orientados sobre os procedimentos de segurança, bem como o uso correto dos ativos, a fim de reduzir possíveis riscos. Eles devem assinar um termo de responsabilidade e não poderão utilizar as informações e dados da Emissora fora do contexto ao qual elas se destinam, sempre prezando pela confidencialidade das informações.

Um plano de contingência e a continuidade dos principais sistemas e serviços deverão ser implantados e testados no mínimo anualmente, visando reduzir riscos de perda de confidencialidade, integridade e disponibilidade dos ativos de informação.

A UX Innovation exonera-se de toda e qualquer responsabilidade decorrente do uso indevido, negligente ou imprudente dos recursos e serviços concedidos aos seus colaboradores, associados, clientes e prestadores de serviços reservando-se o direito de analisar dados e evidências para



obtenção de provas a serem utilizadas nos processos investigatórios, bem como adotar as medidas legais cabíveis.

Esta PSI foi implementada na UX Innovation por meio de procedimentos específicos, obrigatórios para todos os colaboradores, independentemente do nível hierárquico ou função na empresa, bem como de vínculo empregatício ou prestação de serviço.

O não cumprimento dos requisitos previstos nesta PSI acarretará violação às regras internas da organização e sujeitará o usuário às medidas administrativas e legais cabíveis.

6. DAS RESPONSABILIDADES ESPECÍFICAS

a. Dos Colaboradores em Geral

Entende-se por colaborador toda e qualquer pessoa física, contratada CLT ou prestadora de serviço por intermédio de pessoa jurídica ou não, que exerça alguma atividade dentro ou fora da organização.

Será de inteira responsabilidade de cada colaborador, todo prejuízo ou dano que vier a sofrer ou causar a UX Innovation e/ou a terceiros, em decorrência da não obediência às diretrizes e normas aqui referidas.

b. Dos Colaboradores em Regime de Exceção (temporários, estagiários)

Devem entender os riscos associados à sua condição especial e cumprir rigorosamente o que está previsto no aceite concedido pelo Comitê de Segurança da Informação.

A concessão poderá ser revogada a qualquer tempo se for verificado que a justificativa de motivo de negócio não mais compensa o risco relacionado ao regime de exceção ou se o colaborador que o recebeu não estiver cumprindo as condições definidas no aceite.

c. Dos Prestadores de Serviços

Deve se constar em contrato com todos os prestadores de serviços cláusulas de sigilo, confidencialidade e de responsabilidade a fim de atribuir e responsabilizar aqueles que fizerem o mal uso das informações e/ou cometerem atos ilícitos ou má conduta profissional.

d. Dos Gestores de Pessoas e/ou Processos

Ter postura exemplar em relação à segurança da informação, servindo como modelo de conduta para os colaboradores e prestadores de serviços sob a sua gestão.

Atribuir aos colaboradores, na fase de contratação e de formalização dos contratos individuais de trabalho, de prestação de serviços ou de parceria, a responsabilidade do cumprimento da PSI da UX Innovation.



Exigir dos colaboradores a assinatura, manual ou digital, do Termo de Compromisso e Ciência, assumindo o dever de seguir as normas estabelecidas, bem como se comprometendo a manter sigilo e confidencialidade, mesmo quando desligado, sobre todos os ativos de informações da UX Innovation.

Adaptar as normas, os processos, procedimentos e sistemas sob sua responsabilidade para atender a esta PSI, bem como outras políticas relacionadas.

e. Dos Custodiantes da Informação

i. Da Área de Tecnologia da Informação

Testar a eficácia dos controles utilizados e informar aos gestores os riscos residuais.

Acordar com os gestores o nível de serviço que será prestado e os procedimentos de resposta aos incidentes.

Configurar os equipamentos, ferramentas e sistemas concedidos aos colaboradores com todos os controles necessários para cumprir os requerimentos de segurança estabelecidos por esta PSI e pelas Normas de Segurança da Informação complementares.

Garantir segurança especial para sistemas com acesso público, incluindo o ambiente utilizado pelos associados e prestadores de serviços, fazendo guarda de evidências que permitam a rastreabilidade para fins de auditoria ou investigação.

Gerar e manter as trilhas para auditoria com nível de detalhe suficiente para rastrear possíveis falhas e fraudes. Para as trilhas geradas e/ou mantidas em meio eletrônico, implantar controles de integridade para torná-las juridicamente válidas como evidências.

Administrar, proteger e testar as cópias de segurança dos programas e dados relacionados aos processos críticos e relevantes para a UX Innovation. Implantar controles que gerem registros auditáveis para retirada e transporte de mídias das informações custodiadas pela TI, nos ambientes totalmente controlados por ela.

O gestor da informação deve ser previamente informado sobre o fim do prazo de retenção, para que tenha a alternativa de alterá-lo antes que a informação seja definitivamente descartada pelo custodiante.

Quando ocorrer movimentação interna dos ativos de TI, garantir que as informações de um usuário não serão removidas de forma irrecuperável antes de disponibilizar o ativo para outro usuário.

Atribuir cada conta ou dispositivo de acesso a computadores, sistemas, bases de dados e qualquer outro ativo de informação a um responsável identificável como pessoa física, sendo que:



- Os logins (usuários) individuais dos funcionários serão de responsabilidade do próprio funcionário.
- Os logins (usuários) de terceiros serão de responsabilidade do gestor da área contratante.

Definir as regras formais para instalação de software e hardware em ambiente de produção corporativo, bem como em ambiente exclusivamente do associado, exigindo o seu cumprimento dentro da empresa.

ii. Da Área de Segurança da Informação

Propor as metodologias e os processos específicos para a segurança da informação, como avaliação de risco e sistema de classificação da informação.

Propor e apoiar iniciativas que visem à segurança dos ativos de informação da UX Innovation.

Publicar e promover as versões da PSI e suas normas aprovadas pelo Comitê de Segurança da Informação.

Promover a conscientização dos colaboradores em relação à relevância da segurança da informação para o negócio da UX Innovation, mediante campanhas, palestras, treinamentos e outros meios de endomarketing.

Apoiar a avaliação e a adequação de controles específicos de segurança da informação para novos sistemas ou serviços.

f. Do Monitoramento e da Auditoria do Ambiente

Para garantir as regras mencionadas nesta PSI, bem como seu devido cumprimento a UX Innovation poderá:

- implantar sistemas de monitoramento nas estações de trabalho, servidores, correio eletrônico, conexões com a internet, dispositivos móveis ou wireless e outros componentes da rede – a informação gerada por esses sistemas poderá ser usada para identificar usuários e respectivos acessos efetuados, bem como material manipulado;
- tornar públicas as informações obtidas pelos sistemas de monitoramento e auditoria, no caso de exigência judicial, solicitação do gerente (ou superior) ou por determinação do Comitê de Segurança da Informação;
- realizar, a qualquer tempo, inspeção física nas máquinas de sua propriedade;
- instalar sistemas de proteção, preventivos e detectáveis, para garantir a segurança das informações e dos perímetros de acesso.

7. CORREIO ELETRÔNICO - E-MAIL



O objetivo desta norma é informar aos colaboradores da UX Innovation quais são as atividades permitidas e proibidas quanto ao uso do correio eletrônico corporativo.

O uso do correio eletrônico da UX Innovation é para fins corporativos e relacionados às atividades do colaborador usuário dentro da organização. A utilização desse serviço para fins pessoais é permitida desde que feita com bom senso, não prejudique a UX Innovation e também não cause impacto no tráfego da rede.

Acrescentamos que é proibido aos colaboradores o uso do correio eletrônico da UX Innovation:

- enviar mensagens não solicitadas para múltiplos destinatários, exceto se relacionadas ao uso legítimo da organização;
- enviar mensagens por correio eletrônico pelo endereço de seu departamento, usando o nome de usuário de outra pessoa ou endereço de correio eletrônico que não esteja autorizado a utilizar;
- enviar qualquer mensagem por meios eletrônicos que torne seu remetente e/ou a UX Innovation ou suas unidades vulneráveis a ações civis ou criminais;
- divulgar informações não autorizadas ou imagens de tela, sistemas, documentos e afins sem autorização expressa e formal concedida pelo proprietário desse ativo de informação;
- falsificar informações de endereçamento, adulterar cabeçalhos para esconder a identidade de remetentes e/ou destinatários, com o objetivo de evitar as punições previstas;
- apagar mensagens pertinentes de correio eletrônico quando qualquer uma das áreas da UX Innovation estiver sujeita a algum tipo de investigação;
- produzir, transmitir ou divulgar mensagem que:
 - contenha qualquer ato ou forneça orientação que conflite ou contrarie os interesses da UX Innovation;
 - contenha ameaças eletrônicas, como: spam, mail bombing, vírus de computador;
 - contenha arquivos com código executável (.exe, .com, .bat, ou qualquer outra extensão que represente um risco à segurança);
 - vise obter acesso não autorizado a outro computador, serviços, servidor ou rede;
 - vise interromper um serviço, servidores ou rede de computadores por meio de qualquer método ilícito ou não autorizado;
 - vise burlar qualquer sistema de segurança;
 - vise vigiar secretamente ou assediar outro usuário;
 - vise acessar informações confidenciais sem explícita autorização do proprietário;
 - vise acessar indevidamente informações que possam causar prejuízos a qualquer pessoa;
 - inclua imagens criptografadas ou de qualquer forma mascaradas;
 - tenha conteúdo considerado impróprio, obsceno ou ilegal;
 - seja de caráter calunioso, difamatório, degradante, infame, ofensivo, violento, ameaçador, pornográfico entre outros;
 - contenha perseguição preconceituosa baseada em sexo, raça, incapacidade física ou mental ou outras situações protegidas;
 - tenha fins políticos locais ou do país;
 - inclua material protegido por direitos autorais sem a permissão do detentor dos direitos.



8. INTERNET

Todas as regras atuais da UX Innovation visam basicamente o desenvolvimento de um comportamento eminentemente ético e profissional do uso da internet. Embora a conexão direta e permanente da rede corporativa da organização com a internet ofereça um grande potencial de benefícios, ela abre a porta para riscos significativos para os ativos de informação.

Qualquer informação que é acessada, transmitida, recebida ou produzida na internet está sujeita a divulgação e auditoria. Portanto, a UX Innovation, em total conformidade legal, reserva-se o direito de monitorar e registrar todos os acessos a ela.

Os equipamentos, tecnologia e serviços fornecidos para o acesso à internet são de propriedade da organização, que pode analisar e, se necessário, bloquear qualquer arquivo, site, correio eletrônico, domínio ou aplicação armazenados na rede/internet, estejam eles em disco local, na estação ou em áreas privadas da rede, visando assegurar o cumprimento de sua Política de Segurança da Informação.

A internet disponibilizada pela organização aos seus colaboradores, independentemente de sua relação contratual, pode ser utilizada para fins pessoais, desde que não prejudique o andamento dos trabalhos nas unidades e que não prejudique a imagem da UX Innovation.

O uso da Internet e dos recursos de tecnologia pelos colaboradores da UX Innovation é permitido, sugerido e incentivado, desde que seu uso esteja relacionado aos objetivos e atividades fins do negócio ou responsabilidades do colaborador.

9. REDE SEM FIO

O acesso específico às redes sem fio (WI-FI) da UX Innovation é de uso exclusivo de usuários com credenciais de acesso e/ou autorizados previamente pela Gerência de Sistemas de Informações.

A UX Innovation disponibilizará uma rede sem fio de eventos durante a realização dos mesmos, para visitantes onde há o exclusivo acesso à Internet e com regras de controle de conteúdo. Este ambiente é segregado do ambiente corporativo, e seus usuários utilizam credenciais de acesso temporárias;

A UX Innovation disponibiliza uma rede sem fio para dispositivos móveis apenas para usuários previamente autorizados. Este ambiente é segregado;

A utilização da rede sem fio é uma concessão da UX Innovation aos usuários que necessitem deste recurso para desempenhar suas funções e poderá ser suspensa, a qualquer momento, sem aviso prévio, caso sejam identificadas situações que possam comprometer a rede de dados da UX Innovation.

A responsabilidade de todos os acessos feitos durante sua disponibilização é atribuída ao solicitante.



10. MONITORAMENTO

A UX Innovation reafirma que o uso da tecnologia e da Internet é uma ferramenta valiosa para o desempenho das atividades da empresa e para todo o negócio. Dessa forma, o mau uso desses recursos pode ter impacto negativo sobre a produtividade dos colaboradores e os resultados do negócio.

Portanto, a UX Innovation se dá o direito de aplicar restrições de navegação e monitorar o uso da Internet na rede corporativa, de forma individual, aplicando a cada equipamento e colaborador.

11. SANÇÕES

Comprovada a utilização irregular, o colaborador envolvido terá o seu acesso à Internet bloqueado pela GPSI, sendo comunicado o fato à gestão imediata, podendo incorrer em processo administrativo disciplinar e nas sanções legalmente previstas.

12. ACESSO REMOTO

O acesso remoto aos serviços corporativos somente deve ser disponibilizado aos colaboradores que, oficialmente, executem atividade vinculada à atuação institucional da UX Innovation e que necessitam do serviço para execução de suas atividades institucionais, desde que autorizados.

Os administradores da rede da UX Innovation, para o desempenho de suas atribuições, poderão ter permissão de acesso remoto a todos os recursos computacionais da UX Innovation quando necessário.

Os colaboradores da TECNOLOGIA DA INFORMAÇÃO, quando administradores de rede e sistemas das unidades da UX Innovation, poderão ter permissão de acesso aos servidores de rede e estações de trabalho de sua circunscrição quando necessário.

A liberação de acesso remoto, só será efetivada após avaliação e aprovação pela GPSI, para que se evitem ameaças à integridade e sigilo das informações contidas na rede da UX Innovation.

Todos os usuários são responsáveis pelas informações e pelos recursos de informática a que tenham acesso.

A solicitação de acesso remoto deve ser registrada via O.S. e conter, no mínimo, as seguintes informações:

- Tipo da solicitação;
- Tempo de validade do acesso remoto;
- Justificativa;

As conexões remotas à rede da UX Innovation devem ocorrer da seguinte maneira:

- Utilização de autenticação da VPN (Virtual Private Network);
- As senhas e as informações que trafegam entre a estação remota e a rede da UX Innovation devem estar criptografadas;



Cada usuário deve manter suas credenciais de acesso (login e senha) em sigilo absoluto e não fornecê-lo a outra pessoa, garantindo assim, a impossibilidade de acesso indevido por pessoas não autorizadas.

É vedada a utilização do acesso remoto para fins não relacionados às atividades do colaborador na UX Innovation.

13. DAS DISPOSIÇÕES FINAIS

Assim como a ética, a segurança deve ser entendida como parte fundamental da cultura interna da UX Innovation. Ou seja, qualquer incidente de segurança subentende-se como alguém agindo contra a ética e os bons costumes regidos pela organização.

14. ANEXOS

TERMO DE CONFIDENCIALIDADE E DE NÃO CONCORRÊNCIA

TERMO DE CONFIDENCIALIDADE E DE NÃO CONCORRÊNCIA

Eu,.....,brasileiro(a), estado civil, empregado(a) devidamente registrado(a) em face de UX INNOVATION LTDA. (“UX Innovation”), com CTPS n°....., ora Signatário do presente Termo de Confidencialidade, Não Concorrência e Privacidade, me comprometo e assim o faço, no sentido de seguir, fielmente e sob as penas da lei, as disposições abaixo contidas nas Cláusulas adiante estipuladas, a saber:

Cláusula 1ª. Comprometo-me, enquanto funcionário devidamente registrado perante a UX Innovation, a guardar e manter, de forma irrestrita, completa privacidade e confidencialidade quanto aos dados cadastrados e devidamente inseridos no programa (Software) Business Intelligence (BI), Comercial, de Análise de Mercado e Análise de Dados para Gestão Empresarial de Propriedade da UX Innovation e das empresas em que a UX Innovation tiver contrato para esse serviço, bem como, de forma alguma, tornar público ou divulgar a terceiros as informações inseridas no referido sistema, as quais são de titularidade e propriedade da empresa acima nominada, em caráter exclusivo, sob as penas da lei.

Cláusula 2ª. Comprometo-me a não realizar qualquer tipo de cópia, reprodução ou mesmo transmissão dos sistemas para outro usuário ou para outro endereço, sem autorização prévia da Diretoria.

Cláusula 3ª. Comprometo-me a não utilizar, explorar, revelar ou transmitir, em meu benefício ou de terceiros, sem prévia autorização por escrito, e a manter em absoluto sigilo todas as informações a que vier a ter acesso em função do exercício das atividades laborais prestadas em favor de UX Innovation, em qualquer circunstância, durante e após o vínculo contratual, qualquer que seja a causa, a não as revelar, total ou parcialmente, direta ou indiretamente.



Parágrafo Único. Estou ciente de que a divulgação, exploração ou utilização de informação sigilosa, na forma descrita no caput, constitui crime de concorrência desleal, punido, de acordo com o disposto no artigo 196 do Código Penal, com pena de detenção, de três meses a um ano, ou multa, sem prejuízo de indenização por perdas e danos causados;

Cláusula 4^a. Comprometo-me a partir da data de assinatura deste Termo, a não concorrer com a UX Innovation no ramo de Análise de Mercado e Análise de Dados para Gestão Empresarial, em qualquer localidade da República Federativa do Brasil.

Parágrafo Único. Para fins da Cláusula acima narrada, serão considerados atos de concorrência ao negócio da empresa qualificada a participação deste Signatário ou de qualquer Pessoa a ele relacionada, direta ou indiretamente, como sócios, acionistas, quotistas, investidores, financiadores, administradores, consultores ou sob qualquer forma de operação, controle, associação e/ou aconselhamento de qualquer Pessoa que se dedique a negócio concorrente ao da empresa UX Innovation.

Cláusula 5^a. Por fim, considero-me advertido a respeito da obrigação de confidencialidade e de não concorrência prevista nesta Cláusula para todos os colaboradores, prestadores de serviço, parceiros e fornecedores, que serão instados a observarem as mesmas restrições aqui descritas, ficando assim responsável por qualquer descumprimento deste TERMO, respondendo civil e criminalmente, se for o caso, perante a empresa UX Innovation, inclusive pelas perdas e danos morais e materiais suportadas, bem como eventuais lucros cessantes.

Fernando Shiguero Shimada
Gestor de Segurança da Informação

Alexandre Lopes Ambrósio
Diretor de Operações



Política de Segurança da Informação UX docx

Código do documento 9411fff4-e637-4266-822e-6b21f805932c



Assinaturas



Fernando Shiguero Shimada
fernando.shiguero@uxinnovation.com.br
Assinou

Fernando Shiguero Shimada



Alexandre Lopes Ambrosio
alexandre.ambrosio@uxinnovation.com.br
Assinou

Alexandre Lopes Ambrosio

Eventos do documento

05 Nov 2024, 12:13:44

Documento 9411fff4-e637-4266-822e-6b21f805932c **criado** por ALEXANDRE LOPES AMBROSIO (623ed979-d47e-439d-92ea-bd1e4b98cd3b). Email: contato@uxinnovation.com.br. - DATE_ATOM: 2024-11-05T12:13:44-03:00

05 Nov 2024, 12:24:33

Assinaturas **iniciadas** por ALEXANDRE LOPES AMBROSIO (623ed979-d47e-439d-92ea-bd1e4b98cd3b). Email: contato@uxinnovation.com.br. - DATE_ATOM: 2024-11-05T12:24:33-03:00

05 Nov 2024, 12:30:14

ALEXANDRE LOPES AMBROSIO **Assinou** - Email: alexandre.ambrosio@uxinnovation.com.br - IP: 134.238.232.26 (134.238.232.26 porta: 25642) - **Geolocalização: -23.56825674956808 -46.68875275210087** - Documento de identificação informado: 286.056.418-78 - DATE_ATOM: 2024-11-05T12:30:14-03:00

05 Nov 2024, 12:36:44

FERNANDO SHIGUERO SHIMADA **Assinou** - Email: fernando.shiguero@uxinnovation.com.br - IP: 187.101.79.185 (187-101-79-185.dsl.telesp.net.br porta: 54672) - Documento de identificação informado: 326.434.668-02 - DATE_ATOM: 2024-11-05T12:36:44-03:00

Hash do documento original

(SHA256):a3538a067d4a25725350f792a0d71564bec49646e3a923f54baa4e99d02ab950

(SHA512):683243057de9ce815567a3791f7594835e35d6e46f4f8248431b367974f39e7648c3a09c2eef59b5a2b913864255940e1b0b091807d3172a87c93f7f1e2a8143

Esse log pertence **única e exclusivamente** aos documentos de HASH acima

Esse documento está assinado e certificado pela D4Sign