ПОЛИТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Эта Политика информационной безопасности определяет общие принципы, в отношении которых изложены организационные требования для достижения и поддержания информационной безопасности.

Объект

Понятие «Информационная безопасность» означает состояние, при котором организация может осуществлять и поддерживать с течением времени, уровень конфиденциальности, целостности и доступности информации в соответствии с требованиями, установленными:

a) действующим законодательством (в частности, защиты частной жизни и интеллектуальной собственности);

b) контрактные требования потребителей;

c) Любые дополнительные требования, установленные независимо от Группы Палладио.

«Конфиденциальность» указывает на характеристику недоступности для посторонних лиц; «целостность» информации указывает, что информации характерна не для редактирования, или удаления, за исключением уполномоченных лиц; и «доступность» указывается информация, характерная для доступа по требованию уполномоченного лица, в определенное время.

Обобщение

Группа Палладио, как часть управления бизнесом, имеет необходимость получать доступ к данным, и способ получения может быть различным, информация, которая может относиться к: поддержке проектов Клиента, персональных данных сотрудников, административных и бухгалтерских данных, полученных, подготовленных и сохраненных в целях соблюдения требований законодательства. Руководство Группы Палладио считает, в этой связи, что принятие организационной модели, направленной на обеспечение информационной безопасности является стратегическм решением и необходимостью создать организационную структуру, в состоянии:

a) Производить, использовать и правильно хранить информацию, необходимую для соблюдения нормативных или договорных обязательств;

b) Эффективно использовать имеющиеся ресурсы, в рамках соответствующей классификации критической информации;

c) Создать и поддерживать с течением времени, уверенность Группы Палладио и заинтересованных сторон в отношении надежности компании в области защиты информации, которая создается и используется.

ПРИНЦИПЫ

Информационная безопасность является стратегическим решением

Осознание важности и правильнго получения, использования и хранения информации, должна стать частью повседневной работы на всех уровнях. В идеале, все решения административного порядка Группы Палладио, которые связаны с производством, доступом и обработкой информации, должны быть структурированы таким образом, чтобы добиваться безопасности такой информации.

Информационная безопасность основывается на методе оценки риска

В обеспечении информационной безопасности не существует никаких «волшебных формул» или «лучшей практики», применимые к любой ситуации: как компания занимается Информационной безопасностью, тесно ли связаны угрозы и реализация возможностей, которыем организация может подвергаться. Дисциплина риск-ориентированного мышления является инструментом, который помогает выявить и дать должный приоритет различных угроз и возможностей: этот инструмент должен стать частью повседневной работы для всех решений участников в Группе Палладио.

Информационная безопасность начинается с соблюдения правил

Для обеспечения безопасности информации жизненно важным является то, чтобы сосредоточиться на знании, уважении, законодательных и контрактных требований. Если в целом решения по обеспечению безопасности информации должны быть приняты с риск-ориентированного подходом, т. е. путем оценки затрат и выгоды, то законодательные и договорные требования должны всегда рассматриваться как «чистый риск», а именно как только обнаружен источник угрозы (связанный с несоблюдением законодательства или договорных положений), так и используется возможность обеспечения безопасности. Поэтому организация должна обязать, чтобы на всех уровнях участники стремились к выявлению, пониманию и соблюдению законодательных и договорных требований к информационной безопасности.

В частности, необходимо понимание на всех уровнях организации, что организационная модель, принятая в Группе Палладио по защите информации определяется и осуществляется в соответствии с UNI CEI ISO / IEC 27001: 2014. Таким образом, в различных организационных уровнях необходимо понимание требований этих правил и важность их соблюдения.

Информационная безопасность необходима в деятельности по достижению целей

Имеется достаточная уверенность в том, что Информационная безопасность будет достигаться и поддерживаться в течение времени, для этого необходимо задать путь, отмеченный присутствием на различных организационных уровнях соответствующих целевых показателей.

Для определения конкретного содержания целей, оставляемых на различных уровнях управления, в целом необходимо, чтобы эти цели были:

a) Выражены в количественных показателях, насколько это возможно;
b) Совместимы с пропорциональными ресурсами организации;
c) Сопровождались соответствующими сроками, в отсутствие данного параметра не может рассматриваться как таковые;
d) Периодически контролировлись.

Информационная безопасность находится в постоянном совершенствовании

Структура организации (рынок, компания, потребности и ожидания клиентов, ...) постоянно изменяются. В таком состоянии не будет шансов и нет возможности для любой организации выжить, если он регулярно не ставит под сомнение и не совершенствует свои ценности и свою политику, чтобы гарантировать, что информационная безопасность по-прежнему соблюдается для решения тех изменений, с которыми неизбежно приходится сталкиваться.

Главный исполнительный директор

Мауро Марки