Seguridad de la información

En la Seguridad Informática se debe distinguir dos propósitos de protección, la Seguridad de la Información y la Protección de Datos.

Se debe distinguir entre los dos, porque forman la base y dan la razón, justificación en la selección de los elementos de información que requieren una atención especial dentro del marco de la Seguridad Informática y normalmente también dan el motivo y la obligación para su protección.

Sin embargo hay que destacar que, aunque se diferencia entre la Seguridad de la Información y la Protección de Datos como motivo o obligación de las actividades de seguridad, las medidas de protección aplicadas normalmente serán las mismas.

Para ilustrar un poco la diferencia entre los dos, se recomiendo hacer el siguiente ejercicio.

En la Seguridad de la Información el objetivo de la protección son los datos mismos y trata de evitar su perdida y modificación non-autorizado. La protección debe garantizar en primer lugar la confidencialidad, integridad y disponibilidad de los datos, sin embargo existen más requisitos como por ejemplo la autenticidad entre otros.

El motivo o el motor para implementar medidas de protección, que responden a la Seguridad de la Información, es el propio interés de la institución o persona que maneja los datos, porque la pérdida o modificación de los datos, le puede causar un daño (material o inmaterial). Entonces en referencia al ejercicio con el banco, la pérdida o la modificación errónea, sea causado intencionalmente o simplemente por negligencia humana, de algún récord de una cuenta bancaria, puede resultar en pérdidas económicas u otros consecuencias negativas para la institución.

En el caso de la Protección de Datos, el objetivo de la protección no son los datos en si mismo, sino el contenido de la información sobre personas, para evitar el abuso de esta.

Esta vez, el motivo o el motor para la implementación de medidas de protección, por parte de la institución o persona que maneja los datos, es la obligación jurídica o la simple ética personal, de evitar consecuencias negativas para las personas de las cuales se trata la información.

En muchos Estados existen normas jurídicas que regulan el tratamiento de los datos personales, como por ejemplo en España, donde existe la “Ley Orgánica de Protección de Datos de Carácter Personal” que tiene por objetivo garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor, intimidad y privacidad personal y familiar [1]. Sin embargo el gran problema aparece cuando no existen leyes y normas jurídicas que evitan el abuso o mal uso de los datos personales o si no están aplicadas adecuadamente o arbitrariamente.

Existen algunas profesiones que, por su carácter profesional, están reconocidos o obligados, por su juramento, de respetar los datos personales como por ejemplo los médicos, abogados, jueces y también los sacerdotes. Pero independientemente, si o no existen normas jurídicas, la responsabilidad de un tratamiento adecuado de datos personales y las consecuencias que puede causar en el caso de no cumplirlo, recae sobre cada persona que maneja o tiene contacto con tal información, y debería tener sus raíces en códigos de conducta [2], [3] y finalmente la ética profesional y humana, de respetar y no perjudicar los derechos humanos y no hacer daño.

Si revisamos otra vez los resultados del ejercicio con el banco y en particular los elementos que clasificamos como “Información Confidencial”, nos podemos

preguntar, ¿de que manera nos podría perjudicar un supuesto mal manejo de nuestros datos personales, por parte del banco, con la consecuencia de que terminen en manos ajenas? Pues, no hay una respuesta clara en este momento sin conocer cuál es la amenaza, es decir quién tuviera un interés en esta información y con que propósito?

Referencias:

https://protejete.wordpress.com/gdr_principal/seguridad_informacion_proteccion/