Revista Posgrado y Sociedad
Sistema de Estudios de Posgrado
Universidad Estatal a Distancia

ISSN: 2215-2172
Volumen 17, Número 1, 2019, 75-79
RevistaSEP-PyS@uned.ac.cr

Apuntes universitarios:

Día Internet Segura

Notas sobre la conferencia Estrategias de atención a nuevos retos de seguridad en línea y protección de datos

Mag. Salatiel Hernández Porras

Unidad de Tecnología de Información
Agencia de Protección de Datos de los Habitantes de Costa Rica*

*www.prodhab.go.cr, prodhab@rnp.go.cr

Desde 2004, gracias a una iniciativa impulsada por la Unión Europea como parte del proyecto SafeBorders, el segundo martes de febrero de cada año se conmemora el Día de Internet Segura. En esa fecha, más de 130 países de todo el mundo se unen en diferentes acciones orientadas a promover, debatir e impulsar cambios positivos en las condiciones de seguridad de las tecnologías digitales y en espacios virtuales, sobre todo para niñas, niños y adolescentes.

La Revista Posgrado y Sociedad y la Maestría en Tecnología Educativa del Sistema de Estudios de Posgrado (SEP) de la Universidad Estatal a Distancia, con el apoyo de la Dirección de Tecnologías de Información y Comunicación y organizaciones externas, desarrollaron una serie de actividades y eventos que incluyó una campaña de sensibilización en redes sociales de la institución, talleres "Junto a TIC" impartidos por personas colaboradoras del SEP y la conferencia Estrategias de atención a nuevos retos de seguridad en línea y protección de datos, dictada por don Salatiel Hernández Porras, jefe de la Unidad de Tecnología de Información de la Agencia de Protección de Datos de los Habitantes de Costa Rica (PRODHAB).

Sobre esta conferencia se presentan algunas notas de interés[1] .

La Agencia de Protección de Datos de los Habitantes de Costa Rica

En su participación, el experto ubica al público respecto a la institución que representa: la Agencia de Protección de Datos de los Habitantes de Costa Rica (PRODHAB) es una entidad pública adscrita al Ministerio de Justicia y Paz creada en 2011 para brindar apoyo legal y técnico teniendo como objetivo y fin garantizar a cualquier persona, independientemente de su nacionalidad, residencia o domicilio, el respeto a sus derechos fundamentales, concretamente, su derecho a la autodeterminación informativa en relación con su vida o actividad privada y demás derechos de la personalidad, así como la defensa de su libertad e igualdad con respecto al tratamiento automatizado o manual de los datos correspondientes a su persona o bienes.

Además, entre las atribuciones de la PRODHAB, se pueden destacar las siguientes: -Velar por el cumplimiento de la normativa en materia de protección de datos, tanto por parte de personas físicas o jurídicas privadas como por entes y órganos públicos. -Llevar un registro de las bases de datos reguladas por esta ley. -Resolver sobre los reclamos por infracción a las normas sobre protección de los datos personales. -Fomentar entre los habitantes el conocimiento de los derechos concernientes al acopio, el almacenamiento, la transferencia y el uso de sus datos personales. Lo anterior se establece según la Ley N.° 8968 de Protección de Datos de la Persona frente al Tratamiento de sus Datos Personales.

Aclara que PRODHAB no protege la información como tal, sino a las personas en relación con el uso irregular de los datos personales en sus diferentes tipos, sean datos de uso irrestricto (aquellos que pueden obtenerse de fuentes de acceso público como el Registro Nacional o el Tribunal Supremo de Elecciones: nombre, cédula, teléfono, dirección, entre otros); datos de carácter restringido (como información sobre salud, dirección física o datos salariales, por ejemplo) o datos sensibles (aquellos que pueden generar algún tipo de discriminación: religión, sexualidad, aspectos cognitivos, raza, etnia, entre otros, para su uso, se requiere el consentimiento del titular de esos datos).

Cinco conceptos básicos

El conferencista clarifica aspectos claves relacionados con la temática que nos convoca:

[1] Entrevista radial con don Salatiel esta accesible en Vivir con Valor, https://soundcloud.com/search?q=vivir%20con%20valor%202019

1. Ley N.° 8968, de Protección de Datos de la Persona frente al Tratamiento de sus Datos Personales, publicada en el Diario Oficial La Gaceta el 5 de setiembre del 2011. Su objetivo es garantizar a toda persona el respeto a sus derechos fundamentales y derechos de la personalidad, concretamente su derecho a la autodeterminación informativa y la defensa de su libertad e igualdad con respecto al tratamiento automatizado o manual de los datos sobre si misma o sus bienes.

2. Los datos personales son todos aquellos que asociados a la persona y permiten su identificación y caracterización: características físicas (color de piel, cabello, estatura, peso, tipo de sangre), datos biométricos (huella dactilar, patrón de la voz, forma de la mano, iris del ojo), datos académicos (estudios, expedientes); datos de identificación (nombre, dirección, fecha de nacimiento, teléfono); datos de contactos (domicilio, dirección electrónica, número telefónico); datos patrimoniales (propiedades, seguros, historial crediticio, cuentas bancarias, ingresos y egresos).

3. Tratamiento de datos personales: cualquier operación o conjunto de operaciones, efectuadas mediante procedimientos automatizados o manuales y aplicadas a datos personales, tales como recolección, registro, organización, conservación, modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma que facilite el acceso a estos, el cotejo o la interconexión, así como su bloqueo, supresión o destrucción, entre otros.

4. La autodeterminación informativa es un derecho fundamental que refiere a principios y garantías relativas al legítimo tratamiento de los datos personales para controlar el flujo de informaciones que conciernen a cada persona al evitar que se propicien acciones discriminatorias. Implica la protección del derecho fundamental al conocimiento sobre el uso que se le da a la información propia (derivado del derecho a la privacidad) de manera tal que se pueda ejercer sus derechos de acceso, actualización o eliminación de sus datos personales.

5. El consentimiento informado surge a partir de la obligación de notificar claramente a una persona sobre la captación de información personal, el uso que se le va a dar y el derecho propio de otorgar el consentimiento de uso de esos datos.

Sobre la forma en que una institución o empresa debe proteger la información de carácter personal contenida en sus bases de datos, señala que deben considerarse varios factores: 1. Garantizar un entorno que sea seguro, 2. El fin por el cual se solicita la información se mantenga en el tiempo, 3. La identificación de una persona que sea legalmente responsable del uso de la información que se le va a brindar y que pueda tomar decisiones sobre cuál es el fin de recuperar la información y cuáles medidas deben tomarse para asegurarla .

¡Nuestra información en línea es importante!

Aunque usted no sea una figura reconocida o una celebridad, existen personas que hacen negocios y lucran con la venta de base de datos para fines como spam, publicidad o campañas maliciosas, por ejemplo.

Cada persona va dejando una huella en todos los sitios web que visita, puesto que en la cotidianidad la mayor parte de los trámites son en línea y la información se recopila fácilmente. Además, la lista de contactos en redes sociales se

[1] La profesión del responsable de la base de datos o a quien se designe como tal debe estar ligada a lo que se busca, o sea, debería estar directamente relacionada con la información que se está recopilando. Por ejemplo, un profesional puede ser el mejor abogado o administrador, pero si le asignan la recopilación (dar tratamiento a información de carácter personal) de datos de salud, de ADN o datos clínicos de algún paciente, posiblemente no tenga el conocimiento, la experticia que un profesional en el área específica (Medicina, por ejemplo) pueda tener. Así, asegura la adecuada toma y tratamiento de datos personales.

expone a que la información sea manipulada en perfiles falsos; en especial, cuando alguien tiene más de 500 contactos.

El tratamiento de datos personales genera una serie de riesgos. Por ejemplo, para los derechos y las libertades de las personas por cuanto pueden generar discriminación, aislamiento social, daños y perjuicios físicos, usurpación de la identidad, daño reputacional.

Por eso, es necesario acatar las siguientes recomendaciones:

- Analizar lo que se quiere publicar, porque luego se perderá el control sobre la información y podría ser utilizada contra usted.

- Si se van a publicar fotografías o videos en los que aparecen otras personas, asegúrese de que puede hacerlo; es decir, de que cuenta con la autorización expresa; no etiquete. Cerciórese de que no contenga datos personales de un tercero tal como un número de placa. ¡Ni para hacer una denuncia! Usted podría ser sancionado.

- Cuide el hecho de compartir fotografías o videos de niños, niñas o adolescentes. Se requiere la autorización de sus familiares o representante legal.

- Asegúrese de que sus contactos en las redes sociales sean realmente quienes cree que son.

- Resguarde su privacidad. Pregúntese, por ejemplo, si la información que se le entregamos o trasladamos a terceros en cupones, rifas o cualquier coletilla que le entreguen para participar por un premio, puede ser difundida.

- Si se usan redes sociales hay que maximizar la seguridad: la forma más fácil de conocer una persona, sus gustos e intereses es buscarlo en una red social; allí, con mucha frecuencia, se publican fotografías que muestran información personal delicada; es el caso de la foto de un familiar menor de edad que viste uniforme del centro educativo, o que incluye la imagen del carro y la placa que se utilizan para transportarse.

Es muy importante que protejamos nuestros datos personales. Exijamos que instituciones y empresas también lo realicen. Si bien es cierto que la primera persona que puede asegurar un entorno de datos seguro es el ciudadano y la ciudadana, don Salatiel indica que la DIC es la triada fundamental: Disponibilidad, Integridad y Confidencialidad, que se sustenta en la formación ético moral. Alcanza a toda persona, empresa o institución y posibilita el adecuado tratamiento de datos y ayuda a evitar las fugas de información o las vulneraciones.

Un tema delicado: información en y desde el centro educativo

¿Pueden los centros educativos captar imágenes del estudiantado durante las actividades escolares?

Algunas líneas para la construcción de una respuesta parten de la necesaria distinción entre las imágenes como parte de la función educativa. En ese sentido, estarían legitimadas. Sin embargo, aquellas para la difusión del centro y de sus actividades requieren el consentimiento de los interesados, familiares encargados o tutores.

¿Pueden los familiares de los alumnos que participan en un evento abierto a las familias grabar imágenes del evento?

Sin consentimiento no se puede tomar fotografías ni grabar videos. No es legal ni correcto tomar fotografías sin autorización de las personas que allí aparecen. Por esto, es fundamental discernir sobre el momento adecuado para tomar una fotografía para no violentar información personal de alguien.

Cuando los centros educativos quieren realizar grabaciones de actividades desarrolladas fuera del centro escolar, es necesario contar con el consentimiento de los interesados, sus familiares o tutores, siempre que no se realice en ejercicio de la función educativa.

Dra Maricruz Corrales y Mag. Salatiel Hernández.
Conferencia, 26 de febrero 2019. Fotografía propia