Riesgos de la identidad digital: Introducción

> *La identidad digital es todo lo que manifestamos en el ciberespacio e incluye tanto nuestras actuaciones como la forma en la que nos perciben los demás en la red.*

(Aparici y Osuna Acedo, 2013)

El término de la identidad digital también llamada identidad 2.0, empieza a emplearse en la década de 1990 con la introducción de los ordenadores personales. Se trata de una revolución anticipada de la verificación de la identidad en línea utilizando tecnologías emergentes centradas al usuario.

En resumen, todas nuestras actuaciones dentro del espacio digital (imágenes, comentarios, etc.) conforman nuestra identidad o perfil digital. Por tanto, es imprescindible tener en cuenta que a través de esto los demás nos verán de un modo u otro en el ciberespacio. [1]

Para que nos sigamos situando en qué es la identidad digital, a continuación, menciono cuáles son sus características y propiedades:

Social: En ningún momento se llega a comprobar si una identidad es real o no.

Subjetiva: Depende del reconocimiento de los demás y de cómo perciban a la persona.

Valiosa: Se utiliza para investigar cómo es esa persona o empresa y así ayudar a tomar decisiones sobre ella.

Indirecta: No permite conocer a alguien personalmente.

Compuesta: La huella digital se construye por las aportaciones de la persona y de las demás personas que la rodean, sin necesidad de dar consentimiento.

Real: La información de la identidad puede producir efectos tanto positivos como negativos en la vida real.

Contextual: La divulgación de información en un contexto erróneo puede tener un impacto en nuestra identidad digital y, por tanto, en nosotros.

Dinámica: La identidad digital está en constante cambio o modificación. [2]

En el caso de las organizaciones, los riesgos de la identidad digital son una de las cuestiones más importantes. Al igual que cada individuo debe tener cuidado con la huella que deja, las compañías deben cuidar mucho su reputación. Por ello, aunque que la identidad digital ayude notablemente a mejorar las calidades de los negocios o a que las empresas contraten a personas a través de Internet, hay que tener en cuenta que obtener una información falsa o incluso hacer un mal uso de los datos, nos lleva a una vulnerabilidad, tanto personal como empresarialmente hablando.

En la mayoría de los casos, y sobre todo en las multinacionales, los empleados tienen que seguir la política global, es decir, existe una estrategia digital corporativa la cual ayuda a reducir los riesgos de la identidad 2.0. Pese a eso, he encontrado una encuesta hecha a varios trabajadores de distintas compañías, en la que los encuestados consideran que la huella digital sólo es parcialmente controlable. En su opinión, el principal factor de riesgo es el "empleado", tanto para la imagen de la compañía como para la seguridad de la misma. [3]

Hoy en día existe una "fatiga de identidad", es decir, los usuarios tienen demasiadas cuentas, con demasiados usuarios y contraseñas. Para intentar evitar dicha fatiga, algunas compañías han conseguido que la experiencia del usuario sea más cómoda, migrando dicha conexión a sitios que ofrecen un proceso más rápido y sencillo (Facebook, Google, LinkedIn…). A este proceso se le llama BYOI (Bring Your Own Identity), 

pero a pesar de que se puede obtener beneficio de ello, como, por ejemplo, reducir los costes administrativos al evitar el olvido de contraseñas y nombres de usuario, también tiene riesgos. Uno de ellos sería en el caso de que la identidad digital subyacente se viese comprometida, lo que le llevaría al usuario a realizar esfuerzos considerables para restablecerla. Sin embargo, se pueden reducir esos riesgos, por ejemplo, creando un proceso de autenticación basado en el riesgo. Este proceso evaluará una variedad de factores configurables como la hora del día, la ubicación geográfica, etc. [4]

Por lo tanto, he llegado a la conclusión de que la huella digital radica

sobre todo en los comportamientos y acciones de los perfiles sociales de la propia organización y de los empleados. Lo que me lleva a reflexionar sobre la seguridad que existe en la red y como una violación de la privacidad o un robo de identidad podría dañar una reputación, ya sea de la organización como de la persona misma. Ante esta situación debemos tener cuidado con los riesgos que acarrea tener un perfil digital, y poner precauciones para evitar cualquier posible incidencia o problema. Pero… ¿Cómo? ¿Cuántos riesgos existen? ¿Cuál es su magnitud?

Continuará…

Referencias

[1] Wikipedia. <<Identidad 2.0>>. Acceso el 5 de octubre de 2017, https://es.wikipedia.org/wiki/Identidad_2.0

[2] Gobierno de Canarias. <<Características y propiedades de la identidad digital>>. Acceso el 5 de octubre de 2017, http://www3.gobiernodecanarias.org/medusa/ecoescuela/seguridad/identidad-digital-profesorado/caracteristicas-y-propiedades-de-la-identidad-digital/

[3] Ben Ayed, G. (2011). Digital Identity Metadata Scheme: A Technical Approach to Reduce Digital Identity Risks. *Advanced Information Networking and Applications (WAINA), 2011 IEEE Workshops of International Conference on,* 607-612.

[4] ISACA. http://www.isaca.org/Knowledge-Center/Blog/Lists/Posts/Post.aspx?ID=321