Business Intelligence

Muchas empresas tienen datos, pero carecen de información, y por tanto de conocimiento. Por supuesto que es importante recopilar y almacenar datos de los clientes, empleados, compras, ventas, etc. pero de nada nos servirán si no conseguimos algo útil de esos datos. Necesitamos tratarlos, procesarlos de forma que nos puedan dar esa información que resulta tan importante para la compañía. Y una vez que se hayan tratado esos datos, les daremos valor, ya sea comparándolos con otros, usándolos como predicción de consecuencias, etc. de esta forma, pasaremos de tener información a tener conocimiento. Para todo ese proceso existe el Business Intelligence:

> *"El BI es aquello que abarca los procesos, las herramientas, y las tecnologías para convertir datos en información, información en conocimiento y planes para conducir de forma eficaz las actividades de los negocios."*
>
> The Data Warehouse Institute

Leyendo por Internet he encontrado algunas tendencias que están teniendo mayor impacto y de las cuales se hablará en 2018. La primera de ellas es cómo el aprendizaje automático mejorará el trabajo del analista. El analista ya no necesitará hacer el trabajo arduo, ya que el asistente lo podrá hacer por él, además aumentará notablemente su eficiencia, y ayudará a este a explorar y mantenerse en el flujo de análisis de datos, porque ya no tendrá que detenerse para hacer cálculos. Debemos tener en cuenta que el aprendizaje automático permite explorar muchas posibilidades cuando uno necesita ayuda para encontrar una respuesta.

Otra de las tendencias es la promesa del procesamiento del lenguaje natural (NPL), del cual hemos hablado en clase. Según Gartner, hacia el año 2020, el 50 % de las consultas analíticas se generará mediante búsquedas, procesamiento del lenguaje natural o voz. El procesamiento del lenguaje natural permitirá a las personas hacer distintos tipos de preguntas sobre los datos y recibir respuestas relevantes. Así obtendrán la información de una forma más rápida, pudiendo convertirla en conocimiento para posteriormente tomar las decisiones que consideren. De todas formas, debemos tener en cuenta que la ambigüedad es un problema grave de esta tendencia, ya que pueden aparecer problemas a la hora de hacer la misma pregunta. A veces solo existe una manera correcta para formular la pregunta y el usuario no quiere pensar cual puede llegar a ser esa manera, el simplemente quiere la respuesta. Por lo tanto, debemos tener en cuenta que el uso tiene que ser natural.

La última tendencia que me ha parecido interesante es la de que la ubicación de las cosas impulsará la innovación en el Internet de las cosas (IoT). Todos

los dispositivos tienen capacidad de interacción y recopilan datos que ofrecen una mejor experiencia de conexión. De hecho, Gartner predice que, en el año 2020, el número de dispositivos conectados con la IoT y disponibles para los consumidores será más del doble del actual. Y aunque hay una cosa que preocupa a personas y empresas: la seguridad de los datos, se observa una tendencia positiva que consiste en el uso de los datos de los dispositivos con IoT y los beneficios de ese uso. A esto se le llama la ubicación de las cosas, y permite a los dispositivos con IoT detectar y comunicar su posición geográfica. Gracias a esto, se podrá comprender mejor la situación y predecir lo que sucederá en ese lugar específico. [1]

Bankia ha sido una de las últimas empresas que ha transformado su inteligencia de negocio. El nuevo motor de gestión de acciones comerciales está dando servicio a todos los clientes y a todos los canales de la organización, y gracias a la explotación de la información, ya están constatando los beneficios tangibles. *"Queda camino por recorrer, es un proyecto estratégico a largo plazo. El nuevo sistema de Business Intelligence tiene una gran capacidad de evolución y aprendizaje, y a finales de este año ya notaremos de forma muy importante los beneficios reportados a Bankia por su implantación",* prevé Luis Bernardo García, director de actividades comerciales. Además, tienen otras líneas de trabajo como la creación de algoritmos predictivos y el Machine Learning. En definitiva, van a continuar con la transformación del área de BI en Bankia. [2]

Lo que está claro es que tanto el BI como el IoT ofrecen un sinfín de posibilidades y capacidades, y es imprescindible para una empresa que busca crecer sostenidamente y destacar por su competitividad. ¿Acaso no queremos todos formar parte de una organización inteligente y de alta rentabilidad?

Bibliografía

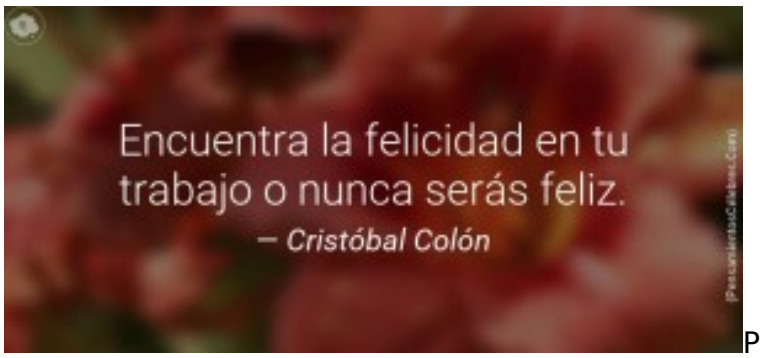
[1] Tableau. <<Las 10 tendencias principales de inteligencia de negocios para 2018.>> Accedido el 1 de enero de 2018. https://www.tableau.com/es-es/reports/business-intelligence-trends#loc-iot

[2]Computing. <<Bankia transforma su inteligencia de negocio>>. Accedido el 1 de enero de 2018. http://www.computing.es/analytics/casos-exito/1102192046201/bankia-transforma

-inteligencia-de-negocio.1.html

La felicidad laboral

La satisfacción en el trabajo ya no es una moda pasajera, si no una manera de pensar que ha llegado a las organizaciones para quedarse. Hace años, al introducirla en las empresas, muchas personas creían que era un tema frívolo, algo pasajero sin importancia. Pero en el momento en el que se dieron cuenta de que se vinculaba la felicidad con unos mayores índices de productividad y compromiso, estas compañías empezaron a tomar en serio el tema. Hoy en día es indispensable contar con el bienestar de nuestros equipos, ya que gracias a ello las personas estarán enganchadas y comprometidas con cada proyecto e idea. [1]



Pero… ¿Y qué es exactamente la felicidad en el trabajo? Es lograr el bienestar de los empleados en tu empresa a través de un buen clima laboral, un cómodo espacio de trabajo, motivación, oportunidad de desarrollo profesional y reconocimiento del trabajo. Hay que tener en cuenta que en muchos casos el sueldo hoy en día ya no es una prioridad, si no un factor más, por lo que hay que cuidar al trabajador para lograr atraerlo y retenerlo. [2]

Distintos estudios han demostrado que la felicidad laboral está directamente relacionada con disfrutar del trabajo que haces, sentirte orgulloso de la empresa, y trabajar con gente con la que exista una buena relación. [3]

¿Y cómo se puede medir el nivel de felicidad de una corporación?

Por un lado, debemos tener en cuenta como bien hemos comentado en clase, que tener un puesto de mayor jerarquía no quiere decir que nuestra motivación laboral sea diferente. Todos somos trabajadores, y como tales tenemos muchas cosas en común, y una de ellas podría ser el hecho de querer tener un buen ambiente de trabajo.

Por otro lado, si bien es cierto que no hay que dejar de lado los objetivos de la empresa, también es cierto que hay que mantener una comunicación clara, directa y concisa con todo el equipo de trabajo. Debemos tener en cuenta que es esencial lograr depositar confianza y responsabilidad, ya que esto aporta seguridad y motivación en el trabajador, aumentando así su productividad

exponencialmente. [4]

Aunque estemos hablando de la felicidad laboral, simple  mente es una forma de fomentar la productividad. A las empresas lo único que les interesa es el dinero, no les interesan las personas, simplemente quieren que a final de año cuando se haga el cierre de contabilidad se vea que han obtenido beneficios. Si la felicidad de los empleados no fuese vinculada con la productividad, las organizaciones no se preocuparían por ello, y eso se puede ver muy fácilmente echando la vista hacia atrás. Hace varios años no existía esta manera de pensar, y por tanto no se cuidaba a los empleados como se les cuida ahora.

Debemos tener en cuenta que la satisfacción laboral puede que no sea para siempre, ya que las personas igual que los puestos de trabajo, evolucionan. La base para que sea sostenible y verdadera es reinventar cada día nuestro puesto de trabajo. Aquí las expectativas son clave. Unas altas perspectivas acerca de las circunstancias favorables de nuestra vida quedan asociadas a una gran satisfacción vital. Las que son irreales o exageradas implican infelicidad. [5]

Por otro lado, leyendo sobre el tema me he encontrado con una encuesta lanzada por Adecco, la cual se ha realizado a más de 3500 trabajadores españoles, para conocer qué importancia tiene esta filosofía. Cabe destacar que 3 de cada 4 encuestados afirman ser felices en su trabajo. Y que los murcianos, vascos y canarios son los más felices en su trabajo. Aunque antes hemos dicho que la felicidad va de la mano de la productividad, también va de la mano de otros factores, como, la motivación, la implicación, la aceptación de responsabilidades y retos, una mayor tolerancia al estrés y una capacidad de adaptación mayor y mejor a los cambios. [1]

En mi opinión, lo malo de esta moda es que ha dado lugar a que surja todo un negocio alrededor de la felicidad en el trabajo. Hay empresas que consideran que la felicidad consiste en poner una mesa de pin pon o en dar comida gratis, pero al final los empleados siguen con la misma jornada interminable y con la misma jerarquía de trabajo.

Referencias

[1] Expansión. << ¿Hay una burbuja de la felicidad laboral? >>. Acceso el 16 y 17 de diciembre de

2017. http://www.expansion.com/emprendedores-empleo/desarrollo-carrera/2017/11/03/59fc858eca4741f44a8b4674.html

[2] Felicidad en el trabajo. << ¿Qué es la felicidad en el trabajo? >>. Acceso el 16 de diciembre de 2017. http://www.felicidadeneltrabajo.es/

[3] Connect Americas. << Los empleados felices ¡son más productivos!>>. Acceso el 16 de diciembre de 2017. https://connectamericas.com/es/content/los-empleados-felices-%C2%A1son-m%C3%A1s-productivos

[4] Edipe Galicia. << Felicidad laboral, un sueño que puede hacerse realidad>>. Acceso el 17 de diciembre de 2017. http://www.movimientofet.org/felicidad-laboral-motivacion-laboral/

[5] Expansión. <<La verdadera felicidad laboral>>. Acceso el 17 de diciembre de 2017. http://www.expansion.com/emprendedores-empleo/desarrollo-carrera/2017/12/07/5a2982b822601dfb428b4570.html

---

¿ViDChain: el futuro de la identidad digital?

Para este último post me ha parecido interesante dar a conocer un nuevo proyecto llamado ViDChain: una solución de gestión y validación de identidades basada en tecnología Blockchain. Actualmente está en fase beta y se dará a conocer durante esta semana de la mano de la organización Validated ID, la cual es además miembro de la Decentralized Identity Foundation (DIF), pero vayamos por partes. [1]

Validated ID nació en 2012 de la mano de varios entusiastas del mundo de la identidad digital y la firma electrónica. Cuando empezaron su objetivo era desplegar servicios en los que premiase la sencillez, pero con los niveles más altos de seguridad técnica y jurídica y con un modelo de negocio claro de prestación de servicios, no de producto. Hoy en día, centran sus esfuerzos en la creación de nuevos sistemas de identificación y firma aplicable a entornos de contratación que incorporan diversas tecnologías y pretenden facilitar la vida tanto a compradores como a vendedores. [2]

Por otro lado, la Decentralized Identity Foundation (DIF) de la cual forma parte la organización Validated ID y empresas como Microsoft, IBM o Accenture, es una fundación que crea un ecosistema de identidad descentralizada de fuente abierta para personas, organizaciones, aplicaciones y dispositivos. Es decir, la DIF está construyendo tecnología y estándares de identidad descentralizados. [3]

Ahora que ya estamos situados voy a explicar de qué trata ViDChain. Este proyecto es una apuesta decidida que abre el camino en el ecosistema de la identidad digital ligada a Blockchain. Se basa en agregar diferentes fuentes de identidad en una cartera de atributos de identidad. O sea, el usuario puede completar su cartera de identidad (identity wallet) con atributos muy variados y con distinto grado de confianza, desde fuentes relativamente poco confiables (redes sociales) a sistemas robustos (biometría). Todos estos atributos son válidos para operaciones distintas con distintos requerimientos de seguridad y en su conjunto permiten conformar una identidad digital amplia en función de los usos que se pretendan. Al tratarse de un proyecto en fase beta, la organización esta centrada en lanzar distintos pilotos a los potenciales consumidores, como universidades, bancos, administraciones públicas o aquellas empresas de servicios con especial interés en la gestión de usuarios. [1]

Y puede que os estéis preguntado… ¿Y qué aporta el Blockchain a la verificación de la identidad?

Primero tenemos que entender qué es el Blockchain: es un conjunto de tecnologías (P2P, sellado de tiempo, criptografía, etc.) que combinadas hacen posible que ordenadores y otros dispositivos puedan gestionar su información compartiendo un registro distribuido, descentralizado y sincronizado entre todos ellos, sustituyendo así a las tradicionales bases de datos. [4] Por lo que, esta tecnología permite que una vez introducidos códigos en ella permanezcan allí para siempre y “den fe” de una transacción, un acuerdo o una identidad, que puede ser encriptada en la parte que afecta a la privacidad.

Según Santiago Casas, el consejero delegado de Validated ID, en el futuro esta tecnología permitirá avanzar hacia una “identidad digital” en el que todas las personas tengan un documento que acredite su identidad sin necesidad de papeles. No obstante, ha reconocido que en el futuro una de las “guerras” estará en cómo se gestionan esos datos, con las grandes compañías de la Red implicadas en ser sus depositarios. [5]

Por lo tanto, lo que está claro es que, gracias a esta tecnología, y, sobre todo, gracias al peso que tiene el Blockchain en ella, los diferentes consumidores de la identidad digital (administraciones públicas, bancos, etc.) tendrán los datos de una forma más segura y ordenada. Y, además de que nosotros, los usuarios, no tengamos que ir de un lado para otro con los diferentes papeles, ellos podrán comunicarse de una forma más sencilla, teniendo concentrados todos los datos en un mismo sitio. Y lo que es más importante, nosotros mismos gestionamos nuestra cartera de identidad, lo cual nos hace sentir más seguros al conocer las medidas de seguridad empleadas. Pero quizás, como ya prevé Santiago Casas, el problema será cuando las distintas organizaciones tengan que gestionar los datos conjuntamente, ¿se podrá asegurar la integridad de los datos? ¿y su coherencia interna?

---

[1] ValidateID. <<ViDChain, el futuro de la identidad digital>>. Acceso el 25 de noviembre de 2017, https://www.validatedid.com/es/vidchain-el-futuro-de-la-identidad-digital/

[2] ValidateID. <<Nuestra historia>>. Acceso el 25 de noviembre de 2017, https://www.validatedid.com/es/empresa/

[3] DIF. Acceso el 25 de noviembre de 2017, http://identity.foundation/

[4] CTIC. <<Qué es el “blockchain” del que todo el mundo habla?>>. Acceso el 26 de noviembre de 2017, http://www.fundacionctic.org/ctic/articulos-y-otras-publicaciones/que-es-el-blockchain-del-que-todo-el-mundo-habla?gclid=EAIaIQobChMItduwg6jc1wIVZyjTCh3tegyCEAAYASAAEgKaz_D_BwE

[5] EFE: Emprende. <<Blockchain, en el futuro de la firma electrónica y la identidad digital>>. Acceso el 27 de noviembre de 2017, http://www.efeemprende.com/noticia/blockchain-futuro-identidad-digital/

¿Podemos controlar nuestras identidades digitales?

Desafortunadamente, no podemos cuantificar la confiabilidad de un sistema, método o técnica, por mucho que existan distintas herramientas las cuales intentan darnos esa seguridad, nosotros lo único que podemos hacer es tratar de cuantificar el riesgo y equilibrarlo. Las empresas han estado analizando el riesgo durante años, y para ello se deben tener varios conocimientos sobre la misma, como por ejemplo, un resumen detallado del sistema, evaluaciones de la interacción requerida con los socios y su capacidad para realizar las tareas. Lo importante es cuantificar las pérdidas potenciales y sus probabilidades a un nivel de detalle que depende de la madurez de la infraestructura de identidad. Por lo que, con todo esto estamos hablando de una auditoría exhaustiva que nos ayude a mitigar esos riesgos de los que hablábamos en las publicaciones anteriores. [1]

Tanto las personas como las organizaciones deben tomar el control de su gestión de identidad, de forma que mejoren su seguridad y privacidad. Para ello pueden llevar a cabo una serie de estrategias:

1. Una auditoría de identidad personal para comprender donde acaba su huella digital, si cualquiera puede acceder a ella o no, etc.
2. Utilizar herramientas para mejorar la privacidad.
3. Mantenerse informado como ciudadano digital sobre cómo proteger su privacidad digital.

La siguiente matriz iría relacionada con el primer punto:

Riesgos	**Controles**
Suplantación de identidad	– Conocer en detalle la forma en la que se ha dado la suplantación de identidad. – Determinar que la organización ha definido una fuente de identidad confiable, como la base de datos de recursos humanos.
Registro abusivo de nombre de dominio	– Verificar que la empresa cuenta con una estrategia en caso de ciber ocupación. **–** Determinar que posee los recursos legales apropiados para reprimir este acto. [3]
Ataques de denegación de servicio distribuido o ataque «DDoS»	– Determinar si se puede soportar ese tipo de ataque. – Verificar que la empresa cuenta con una estrategia en caso de que el ataque le afecte.

Fuga de información	– Determinar que el sistema de manejo de identidad verifica cada solicitud de una identificación nueva o modificada contra la fuente confiable. – Determinar que las plataformas siguen la política de manejo de identidad de la organización. – Verificar que las aplicaciones heredadas que no se adhieren a la política de manejo de la identidad hayan sido formalmente aprobadas por un ejecutivo de TI en un nivel superior apropiado. – Determinar si un marco de gestión de seguridad apropiado, como ISO / IEC 27002 o la serie NIST 800, se utilizará como referencia de buenas prácticas. [4]
Publicaciones por terceros de informaciones negativas	– Determinar por qué han ocurrido esas publicaciones. – Determinar si existe una estrategia alternativa que solucione esa información negativa.
Utilización no consentida de derechos de propiedad industrial	– Comprobar que la organización conoce los métodos legales y que puede aplicarlos para evitar esa utilización no consentida.

Me parece interesante comentaros, con respecto al segundo punto, algo que he estado leyendo: La Estrategia Nacional para Identidades de Confianza en el Ciberespacio (NSTIC). Se trata de una organización que describe una visión del futuro, un **Ecosistema de Identidad**, donde individuos, empresas y otras organizaciones (comunidades) disfrutan de mayor confianza y seguridad mientras realizan transacciones confidenciales en línea. Y os preguntareis, pero ¿de qué se trata? Pues bien, es un entorno en el cual las tecnologías, las políticas y los estándares están acordados de manera que respaldan todas las transacciones (desde las que van de valores anónimos hasta totalmente autenticados, de altos a bajos). Los componentes de este ecosistema de identidad son los siguientes:

- El **Marco del Ecosistema de Identidad (Identity Ecosystem Framework – IDEF)** es el conjunto general de estándares de interoperabilidad, modelos de riesgo, políticas de privacidad y responsabilidad, requisitos y mecanismos de responsabilidad que estructuran el ecosistema de identidad.
- El **Servicio de Listado de Autoevaluación de IDEF (Self-Assessment Listing Service – SALS)** está diseñado para generar confianza en línea. Se trata de una página web donde los proveedores de servicios de

identidad en línea y las aplicaciones que autentican las credenciales pueden informar sobre su estado mediante una autoevaluación con un conjunto de estándares comunes.

- El **Grupo Directivo del Ecosistema de Identidad (Identity Ecosystem Steering Group – IDESG)** administra el desarrollo de políticas, estándares y procesos de acreditación para el IDEF de acuerdo con los Principios Rectores en la Estrategia. El IDESG también asegura que las autoridades de acreditación validen la adherencia de los participantes a los requisitos del IDEF.
- Los **marcos de confianza** son desarrollados por una comunidad cuyos miembros tienen metas y perspectivas similares, como los Pilotos NSTIC. Un marco de confianza define los derechos y las responsabilidades de los participantes de esa comunidad, especifica las políticas y estándares específicos de la comunidad y define los procesos y procedimientos específicos de la comunidad que brindan seguridad. Un marco de confianza debe abordar el nivel de riesgo asociado con los tipos de transacción de sus participantes. Para ser parte del Ecosistema de Identidad, todos los marcos de confianza deben cumplir con los estándares de referencia establecidos por el IDEF.
- Las **autoridades de acreditación** evalúan y validan a los proveedores de identidad, proveedores de atributos, partes confiables y medios de identidad, asegurando que todos se adhieran a un marco de confianza acordado. Las autoridades de acreditación pueden emitir marcas de confianza a los participantes que validan.
- Los **esquemas de marca de confianza** son la combinación de criterios que se miden para determinar el cumplimiento del proveedor de servicios con el IDEF. El IDEF proporciona un conjunto básico de estándares y políticas que se aplican a todos los marcos de confianza participantes. Esta línea de base es más permisiva en los niveles más bajos de seguridad, para garantizar que no sirva como una barrera indebida a la entrada, y más detallada en niveles más altos de seguridad, para garantizar que los requisitos estén alineados con el riesgo de cualquier transacción dada. [2]

Por último, con respecto al tercer y último punto de estas posibles estrategias a seguir, os invito a que accedáis al Instituto Nacional de Ciberseguridad de España, y os leáis la guía de aproximación para el empresario sobre Ciberseguridad en la identidad digital y la reputación online. En ella encontramos, entre otras cosas, nuestro derecho (marco legal) y unas recomendaciones para la gestión de la identidad digital y la reputación online. Además, también me ha parecido interesante una página web del Gobierno de Australia (https://esafety.gov.au/) la cual se compromete a ayudar a los jóvenes a tener experiencias positivas y seguras en línea.

Por lo tanto, en algunas empresas más grandes se dispondrá de un Social Media Manager, el cual será el responsable de la identidad digital, sin embargo, en otras más pequeñas y con menos presupuesto, quizás se encargue el Community Manager. Lo que está claro es que el adecuado manejo de los riesgos, la gobernabilidad, etc. evita en gran medida esos problemas referentes a la

seguridad de la identidad digital, lo cual, según empresas como Deloitte, produce mucho valor para la misma.

Referencias

[1] Phillip J. Windley (2005). <<Digital Identity: Unmasking Identity Management Architecture (IMA)>>. Acceso el 16 de noviembre de 2017, https://books.google.es/books?id=o8mHSbDHgPsC.

[2] IDESG. <<Overview>>. Acceso el 15 de noviembre de 2017, https://www.idesg.org/The-ID-Ecosystem/Overview

[3] JUS. <<Disputa de nombres de dominio>>. Acceso el 16 de noviembre de 2017, https://jus.com.br/artigos/3977/disputa-de-nombres-de-dominio

[4] ISACA. <<Identity Management Audit/Assurance Program>>. Acceso el 15 de noviembre de 2017, https://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Identity-Management-Audit-Assurance-Program.aspx

---

Bichos, una aventura en miniatura

https://www.youtube.com/watch?v=XJovUZBAIkk

Siguiendo la manera didáctica de Pablo, me ha parecido interesante buscar un vídeo con el que pueda hablar de los diversos temas que hemos abarcado en clase. He encontrado este vídeo de la película “Bichos, una aventura en miniatura”, en el cual se pueden ver reflejadas varias cosas del día a día de una organización y de una persona.

En primer lugar, a partir del minuto 0:32, se puede escuchar la frase: “Sé que no acostumbramos a cambiar las tradiciones, pero …”. Esta frase nos enseña que las organizaciones y las personas necesitan actualizarse para ir avanzando, como dijo Miguel de Unamuno, “el progreso consiste en renovarse”, de ahí viene el dicho de “renovarse o morir”. Debemos darnos cuenta de que por mucho que funcione algo, seguramente exista otra forma mejor o simplemente diferente de hacerlo, por ello tenemos que buscarla. Muchas veces la gente cree que el cambio no es bueno, piensan… ¿Por qué voy a cambiar algo que funciona? Y es que es verdad que en la zona de confort se está muy bien, entonces… ¿Para qué salir de ella? Tienen razón, esa zona de confort nos da abrigo, nos hace sentir seguros, quizás porque abarca todo aquello que conocemos y controlamos. Pero eso mismo que nos protege también nos puede causar daño, si nos acomodamos nos estancamos, no buscamos estímulos, caemos

en la monotonía, por eso hay que ser valientes y olvidarse del miedo a lo desconocido, buscar nuevos aprendizajes, nuevas emociones. Me gustaría listar algunos consejos que he encontrado y que pueden ayudar a salir de esa zona de confort, espero que os sirvan:

- **Reconoce tus límites:** Debes reconocer tus barreras internas y externas. Acepta que no eres perfecto, pero reconoce que puedes llegar a donde desees. [1]

- **Aprende a aceptar:** Al salir de nuestra zona de confort nos encontraremos con aspectos que no podemos manejar o controlar, es importante aceptar esas situaciones. Imagina lo que quieres y trabaja en ello: Cada pequeña acción que llevas a cabo te ayudará a ampliar tu perspectiva. [1]
- **Desafíate y rinde al máximo:** Según un estudio llevado a cabo por un grupo de psicólogos, un poco de ansiedad puede ser positivo para mejorar nuestro rendimiento y nos permite seguir creciendo profesionalmente. Por tanto, convierte esas situaciones que te provocan ansiedad en situaciones estimulantes y que nadie te pare los pies. No le llames nervios o inseguridad, llámale "emoción". [2]
- **Anticipa todas las excusas que te vas a poner:** Sé consciente de que, cuando te fijes metas que te resulten incómodas dentro de tu zona de confort, inconscientemente te vas a estar buscando un montón de excusas para no hacerlo. Juzga estas excusas como lo que son: invenciones cuyo único objetivo es racionalizar la aceptación de la comodidad. [2]

En mi opinión estos consejos son bastante útiles y constructivos, y pienso que se pueden seguir siempre y cuando sigas siendo fiel a ti mismo, lo cual sigue siendo uno de los retos más grandes en un mundo que quiere que todos sean iguales.

Por otro lado, siguiendo con el vídeo, a partir del minuto 1:35 podemos ver como los bichos trabajan en equipo para llegar al objetivo común: construir el pájaro. Se puede observar como cada una tiene su función, algunas hormigas guían a otras hormigas mientras trabajan, la araña teje en el momento en el que se la necesita, etc. Esto me ha recordado a que seguramente cuando trabajemos en una empresa cada uno de nosotros tendrá un trabajo específico, y que gracias a ese trabajo, y al del resto de nuestros compañeros

conseguiremos llegar al mismo objetivo. Trabajaremos en equipo, es decir, será un trabajo hecho por varios individuos donde cada uno hace una parte, pero todos trabajan con un objetivo común. Lo importante de todo esto, es que cada uno sepa que quiere hacer, que le gusta hacer, ya que en mi opinión, si todos remamos con las mismas ganas hacia el mismo sitio, se llegará antes y mejor al resultado final. ¿Y qué mejor forma que la de ir al trabajo con ganas de trabajar? [3]

Así mismo, en el minuto 3:42 podemos ver como la hormiga reina está recordando al resto de las hormigas lo bien que están trabajando. Esto me ha recordado a un momento de clase cuando comentamos que había que felicitar a las personas cuando hacían algo bien. Y es que un refuerzo positivo muchas veces ayuda más que regañar a alguien por algo que haya hecho mal. Esto se puede aplicar a una organización, por ejemplo, el jefe de proyectos debe exigir a sus empleados cierto grado de cumplimiento, pero a su vez también debe recordarles lo bien que lo están haciendo y ayudarles en todo lo que necesiten, como si fuera uno más, porque lo es.

Por lo tanto, lo que buscaba que sacarais de este post es que lo importante es ser feliz y que para eso hay que estar a gusto con uno mismo, con lo que está haciendo y con lo que tiene planeado hacer. Tenemos que darnos cuenta de que nadie nos va a allanar el camino, nosotros mismos tenemos que buscar ese camino y recorrerlo. Debemos recordar que tenemos suerte si contamos con gente a nuestro alrededor que nos ayude y a la que podamos ayudar, ya sea en un trabajo en equipo o en la vida personal. Y seguramente nos equivoquemos o lo pasemos mal al salir de esa zona de confort en la que estamos, pero debemos tener en cuenta en todo momento que el resultado final siempre va a merecer la pena.

Referencias

[1] La mente es maravillosa. <<Sal de tu zona de confort>>. Acceso el 31 de octubre de
2017. https://lamenteesmaravillosa.com/sal-de-tu-zona-de-confort

[2] Psicología y mente. <<Cómo salir de tu zona de confort: 7 claves para lograrlo>> Acceso el 31 de octubre de
2017. https://psicologiaymente.net/coach/salir-zona-de-confort-claves

[3] Wikipedia. <<Trabajo en equipo>>. Acceso el 1 de noviembre de
2017. https://es.wikipedia.org/wiki/Trabajo_en_equipo

Mobile Connect

En el post anterior hablaba de los diferentes riesgos y amenazas que existen y como afectaban a las organizaciones. Además, durante los anteriores posts hemos estado viendo como las contraseñas son una de las cosas más complicadas, ya que los usuarios pueden abandonar o dejar de utilizar los servicios que ofrece una compañía por el simple hecho del olvido de las mismas o por considerar que son poco seguras.

En el apuro por abrir nuevos canales digitales, las empresas no pueden darse el lujo de perder de vista la necesidad de identificar y conectarse con aquellos individuos que usan una enorme cantidad de dispositivos móviles. El dominio de las identidades digitales puede transformar la posición de una organización en la economía digital. La simple verdad es esta: las empresas que logren aprovechar el tema de la identidad podrán sacar poderosos productos y servicios con más rapidez y efectividad que las que no lo logren. Un estudio de Oracle descubrió que casi dos tercios (64%) de los encuestados

dice que los canales digitales son altamente importantes para los ingresos de sus compañías (el 27% piensa que son fundamentales para la misión y el 37% que son muy importantes). 72% dice que el tema de la seguridad es el principal peligro para manejar la identidad personal y solo el 19% está muy bien preparado para cumplir con los requisitos de seguridad. Permitir que los clientes controlen sus propios datos de identidad es considerado como una medida altamente eficaz para el 48% de los adoptantes. [1]

Según diferentes líderes en seguridad biométrica, para 2020 las contraseñas

desaparecerán en países que realicen altas inversiones en mecanismos robustos de seguridad. [2] Y según la Asociación de operadores móviles y compañías relacionadas (GSMA), actualmente los gobiernos y empresas están buscando una autenticación más fuerte para reducir los riesgos, especialmente en los dispositivos móviles. Cuentan con un programa llamado Vision 2020 que tiene como objetivo encontrar una solución de autenticación basada en la red móvil para abolir el uso de contraseñas y dar paso a la autenticación digital desde dispositivos móviles. [2] Según datos de GSMA, el 87% de las personas abandonan los sitios web cuando se les pide que se registren, el 40% admite haber utilizado la función de "recuperar contraseña" al menos una vez al mes, y el 83% de los usuarios están preocupados por el uso de su información personal cuando acceden a Internet o a las apps. [3]

El Grupo de Trabajo Técnico y Terminales (TECT) de GSMA Latino América se reunió en marzo del año pasado en Río de Janeiro, Brasil, y sirvió como catalizador para seguir actualizando a los operadores móviles en los temas técnicos que la GSMA impulsa a nivel global. El encuentro atrajo a más de 60

ejecutivos de las áreas de las operadoras y los principales fabricantes del ecosistema móvil latinoamericano. Se habló sobre distintos temas, pero el que a nosotros nos importa es el seminario de servicios de identidad, en el cual se dio a conocer el Mobile Connect. Se trata de un servicio de autenticación que los operadores han lanzado en todo el mundo que pretende dar una alternativa a los numerosos usuarios y contraseñas del mundo digital. Además, se revisaron las evoluciones del servicio para dar servicios de autorización, atributos, pagos o identidad. [4]

Hoy en día muchas compañías telefónicas ofrecen el uso de esta tecnología de una forma gratuita y segura, simplemente tendrás que recordar tu número de teléfono para poder loguearte en todo tipo de páginas webs y apps, sin necesidad de recordar contraseñas. [5]

La inquietud que me surge es que si los mecanismos de autenticación más seguros son los biométricos (huellas, voz, etc.) y los menos seguros los basados en "algo que tú sabes o tienes" (contraseñas, tarjeta de proximidad, etc.). ¿Cómo sabemos que este método es seguro, si se trata de un mecanismo de autenticación basado en algo que tú tienes (el móvil)? Es decir, si en algún momento pierdo el móvil o me lo roban, pierdo esa seguridad y cualquiera podría entrar a cualquier portal que pueda activar con mi dispositivo. ¿No debería tener una estrategia de doble autenticación? En cualquier caso, me parece una buena idea siempre que las páginas que

necesiten un grado más elevado de seguridad lo combinen con otros mecanismos de autenticación.

Referencias

[1] Mercado. <<El gran problema de la identidad digital>>. Acceso el 31 de octubre de 2017. http://www.mercado.com.ar/notas/8019653

[2] Reporte digital. <<Autenticación digital, la tendencia que revoluciona la identidad digital>>. Acceso el 31 de octubre de 2017. http://reportedigital.com/seguridad/autenticacion-digital-identidad/

[3] El País. <<Movistar lanza el servicio que elimina las contraseñas para registrarse>>. Acceso el 1 de noviembre de 2017. https://elpais.com/economia/2016/04/14/actualidad/1460620789_925132.html

[4] GSMA. <<Reunión del TECT en Brasil: trabajo conjunto para traer la estrategia Vision 2020 de la GSMA a América Latina>>. Acceso el 1 de noviembre de 2017. https://www.gsma.com/latinamerica/es/reunion-del-tect-en-brasil-trabajo-conjunto-para-traer-la-estrategia-vision-2020-de-la-gsma-a-america-latina

[5] Orange. <<Mobile Connect: La solución universal, segura y cómoda para registrarse sin contraseñas>>. Acceso el 1 de noviembre de 2017. http://mobileconnect.orange.es/

Amenazas de la identidad digital

En el post anterior explicaba qué era la identidad digital o identidad 2.0, cuáles eran sus características, etc. Llegue a la conclusión de que la buena imagen lograda tras años de duro trabajo podía venirse abajo por cualquier brecha en la huella digital y que por ello debíamos tener cuidado y poner precauciones al respecto. Pero… ¿Cómo? ¿Cuántos riesgos existen? ¿Cuál es su magnitud? A continuación, voy a explicar las diferentes amenazas que he ido encontrando y cómo afectan a la entidad.

- **Suplantación de identidad.**

La suplantación de identidad puede darse o bien creando o bien accediendo a un perfil no autorizado de una empresa o de una red social, es decir, se

trata de la usurpación de los perfiles por terceros malintencionados. Los atacantes intentan aprovecharse de la reputación del atacado para sacar beneficios, como, por ejemplo, el robo de información sensible para el chantaje. Para ello, recurren a las técnicas Phishing y/o Pharming.[1]

En la primera, el estafador (phisher) usurpa la identidad de una empresa o institución de confianza para enviar un email, SMS, etc. a los clientes, trabajadores, usuarios… y así conseguir engañarles para que revelen información personal, como contraseñas o datos de tarjetas de crédito y de la seguridad social y números de cuentas bancarias.[2] En la segunda, sin embargo, el estafador redirige a sus víctimas hacia una página web fraudulenta que suplanta a la original, incluso si escriben correctamente la dirección Web de su banco o de otro servicio en línea en el buscador.[3]

- **Registro abusivo de nombre de dominio.**

El nombre de dominio es la 'dirección' que utilizan las empresas para identificarse ante su público (por ejemplo deusto.es). Y el riesgo puede surgir al registrar este nombre, ya que, no existe ningún control o vigilancia durante este proceso, y en el caso de que se diese alguna infracción el único responsable sería el solicitante del registro. [1]

El ataque, conocido como cybersquatting, se produce cuando un tercero malintencionado registra un nombre de dominio existente con el propósito de extorsionarlo para que lo compre o bien simplemente para desviar el tráfico web hacia un sitio competidor o de cualquier índole.[4]

- **Ataques de denegación de servicio distribuido o ataque «DDoS».**

El objetivo de los ataques de denegación de servicio distribuido consiste en dejar un servidor inoperativo. Se lleva a cabo generando un gran flujo de información desde varios puntos de conexión hacia el mismo punto de destino, el cual acabará saturado y se colapsará. Todo esto le acarrea a la empresa un perjuicio a la identidad digital, ya que, ya no existe en la Red y la reputación online baja considerablemente al demostrar lo vulnerable que es.[1]

- **Fuga de información.**

La fuga de información tiene dos posibles orígenes, por un lado, desde el interior de la organización, bien por error o bien por una acción consciente e intencionada. Y, por otro lado, desde el exterior, utilizando diferentes técnicas para robar información de los equipos y sistemas de la entidad.

El objetivo de este ataque suele ser el lucro, haciendo que la buena imagen y el prestigio de la entidad se vea comprometida por la publicación de información sensible y/o confidencial.[1]

- **Publicaciones por terceros de informaciones negativas.**

Está claro que no solo se está en la red, sino que se conversa en ella, por lo que, las empresas obtienen sus feedback de los usuarios a través de los medios sociales. El hecho de que un mal comentario sea distribuido por las redes puede ser información valiosa para que la empresa sepa cómo mejorar, pero también puede perjudicar su honor y reputación. Hay que tener en cuenta que la información en Internet no desaparece con el tiempo, lo que hace que valoraciones negativas que posiblemente ya estén solucionadas sigan perjudicando gravemente a la entidad.[1]

- **Utilización no consentida de derechos de propiedad industrial.**

La utilización no consentida de derechos de propiedad industrial es un riesgo para la identidad y la reputación de una empresa. Esta acción puede estar motivada por una falsa sensación de que en Internet todo vale y no se vulnera ningún derecho, o por un empleado descontento que divulga elementos fundamentales para el negocio, como patentes o secretos industriales. [5]

Naturalmente, una combinación de herramientas de seguridad y buenas prácticas son fundamentales para evitar muchas de estas amenazas, pero las consecuencias de la suplantación de identidad en Internet son cada vez más y más negativas. Por ello debemos tener una responsabilidad compartida entre distintas partes: los usuarios al tomar las medidas adecuadas de seguridad, las empresas responsables de la protección de los datos y los gobiernos a través de la legislación en la materia, así como con la creación de instituciones enfocadas en atender estas problemáticas.[6] Con estos últimos se puede contactar por medio de la página web http://www.agpd.es (Agencia Española de Protección de Datos), donde además de facilitar herramientas a las empresas para que cumplan con la protección de datos, si tú como individuo sientes una amenaza, puedes denunciarlo.

Continuará…

Referencias

[1] Incibe. <<Guia ciberseguridad online>>. Acceso el 17 de octubre de 2017, https://www.incibe.es/extfrontinteco/img/File/empresas/guias/guia_ciberseguridad_identidad_online.pdf

[2] Avast. <<Phishing>>. Acceso el 17 de octubre de 2017, https://www.avast.com/es-es/c-phishing

[3] Wikipedia. <<Pharming>>. Acceso el 17 de octubre de 2017, https://es.wikipedia.org/wiki/Pharming

[4] Wikipedia. <<Ciberocupación>>. Acceso el 17 de octubre de 2017, https://es.wikipedia.org/wiki/Ciberocupaci%C3%B3n

[5] Fernando Amaro. <<Identidad Digital y Reputación Online (III)>>. Acceso el 18 de octubre de 2017, http://fernando-amaro.com/identidad-digital-reputacion-online-iii/

[6] We live security. << 3 amenazas que buscan robar tu identidad: ¡cuídate de ellas!>>. Acceso el 18 de octubre de 2017, https://www.welivesecurity.com/la-es/2015/09/30/3-amenazas-robar-identidad/

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