UNIVERSIDAD ORT
Uruguay

El Gobierno de TI en la era de la empresa digital

Dra. Helena Garbarino
garbarino@ort.edu.uy

Felix Baumgartner (Salzburgo, Austria, 20 de abril de 1969) es un exmilitar, paracaidista y un saltador BASE. Es conocido por la particular peligrosidad de las maniobras que ha realizado durante su carrera. Baumgartner pasó algún tiempo en el ejército austriaco, donde practicó paracaidismo, incluyendo entrenamiento para aterrizar en zonas pequeñas.
El 14 de octubre de 2012 batió tres récords históricos al lanzarse en caída libre desde los **39.068 metros de altura**, después de haber ascendido en globo tripulado a la **estratosfera.**

Cloud computing is revolutionizing how organizations use technology worldwide and for a good reason, it leverages on economies of scale more than any application of technology in recent history. And with the economic stability of the world swaying back and forth, organizations and businesses are forced to embrace that which makes them more stable and compete in a shaky market. Cloud computing allows them to do just that as it leverages their business processes with high returns and low costs. But the aggregation of data and information in a single virtual space has its own risks –it becomes a prime target for attackers and opportunists. This is more in line with the concept of data gravity. As data becomes more massive, the faster it attracts other services, application, customers, and yes even attackers. It also becomes harder to move which only assures attackers that the data they want is in the same place at any given time.

Cloud computing has received the brunt of most recent high-profile security attacks and data breaches, giving cloud computing a bad reputation of being unsecure, which now makes it a scapegoat for any failed security measure. But cloud computing can become very secure no matter the architecture or type used, but this would require a strong governance framework.

The Solution: Security Governance Framework

A governance framework is essential for any concept of technology to succeed. There are different types of governance frameworks for most concepts like how to run the organization itself, as well as the different departments in an organization, and of course a dedicated governance framework for IT. But for cloud computing, perhaps the most important governance framework would be that for security.

As with IT governance which stretches across all of its facets, from the people to the whole organization, the cloud computing security governance framework must do the same. The framework must allow the CSO and CIO to oversee and assess all risks and manage them accordingly, as well as the security and compliance of the organization's cloud environment.

This **governance framework** must allow for security, compliance, and all of IT and the rest of the organization to be synergized to make the cloud secure. And therefore must do some of the following things.

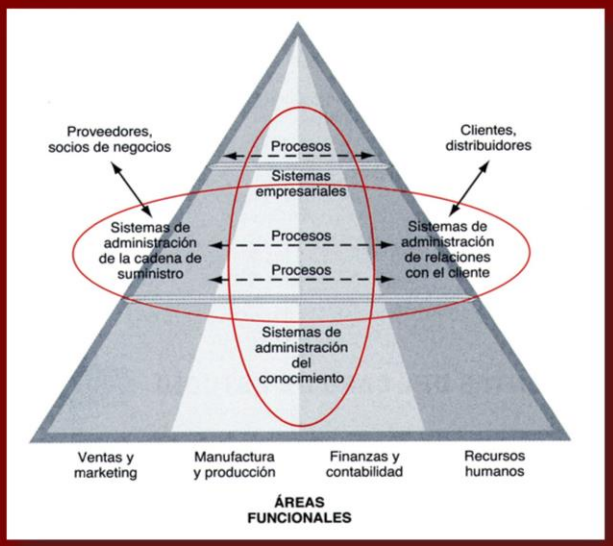
1. Educate your workforce. Most security breaches and attacks stem from negligence or ignorance from the basic building block of the organization, the rank and file. Most breaches are a result of something that internal users have done or failed to do, and to prevent such things from happening again or at all, they must be made aware of the dangers of some actions and must be educated with security measures which they should always comply with.
2. Audit compliance. Use an audit tool which can view the organization's vulnerabilities across the board. It is common for departments to be without contact with each other because they are not related whatsoever, and the solution to this is to create a framework for compliance across the organization which combines the different streams of information from different groups, giving security administrators a single overview.
3. Employ Identity and Access Management (IAM). This is one of the best ways to keep track of people who have access to sensitive data. This prevents or at least mitigates breaches and attacks from internal sources. Access management must be paired with a data logging solution which allows administrators to know who does what, when and where and that all changes are logged and audited properly.
4. Employ **Security Information and Event Management** (SIEM). The ideal cloud security solution should integrate the organization's access management to secure a complete view of where the organization stands in terms of security. Security as a service is one solution that organizations may avail if they cannot provide their own.
5. Look for guidance but ensure your own security. Many organizations both government, academic, or private like the **European Network and Information Security Agency** (ENISA) and the Cloud Security Alliance (CSA) have published papers and guidance protocols for securing cloud environments. Organizations can consider them as guidance and must form their own way for securing their cloud based on the recommendations and incorporate their own twists into those depending on their needs.

Conclusion

A governance framework is essential for cloud computing but there shouldn't be just one good way to do it. Since no two organizations are alike, it would make sense that no two frameworks are alike, but they would have a lot of similarities. But no matter the difference all organizations need a security governance framework for any cloud infrastructure that they may be using.


Gobierno de TI
Empresa Digital

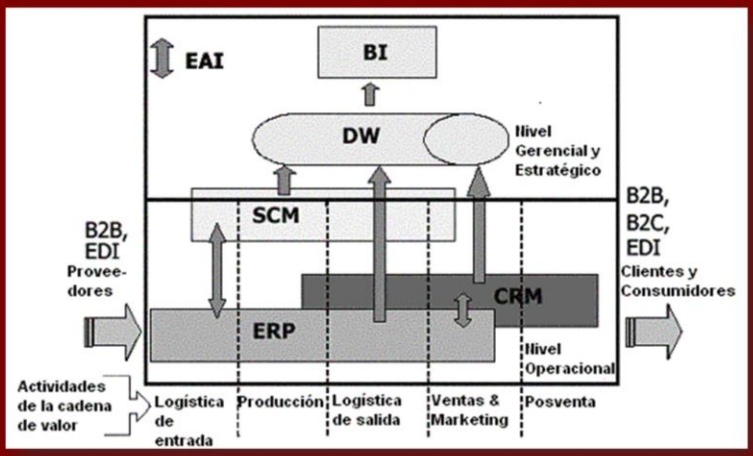
La empresa digital



Laudon, K; Laudon, J (2012). *Los sistemas de información gerencial*. Pearson: Mexico

La total utilización del los sistemas de información, por parte de una organización, para la realización de sus negocios. Para Laudon, la Empresa Digital sería aquella en donde prácticamente todos los procesos de negocio y las relaciones con clientes, empleados y otras entidades de su entorno, son realizados por medios digitales.

La empresa digital

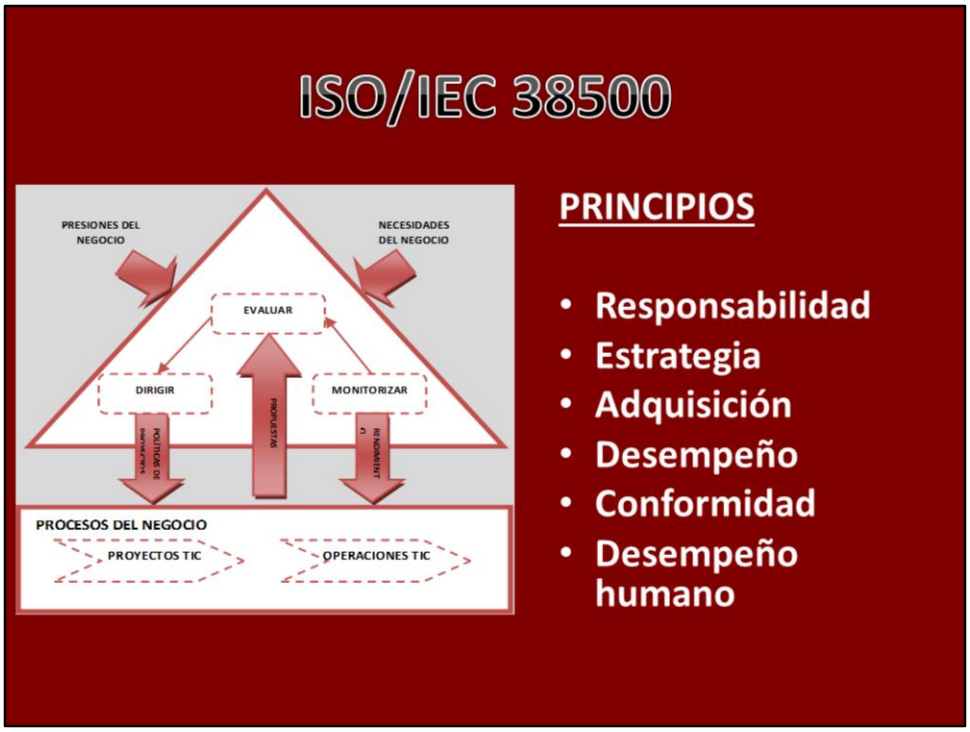


http://www.cyta.com.ar/

ISO/IEC 38500

La gobernanza corporativa de TI:

- *Es el sistema por el cual se dirige y controla el uso actual y futuro de TI.*
- *Implica evaluar y dirigir el uso de las TI para dar soporte a la organización y monitorizar el uso para lograr los planes.*
- *Incluye la estrategia y políticas para la utilización de las TI en la organización*

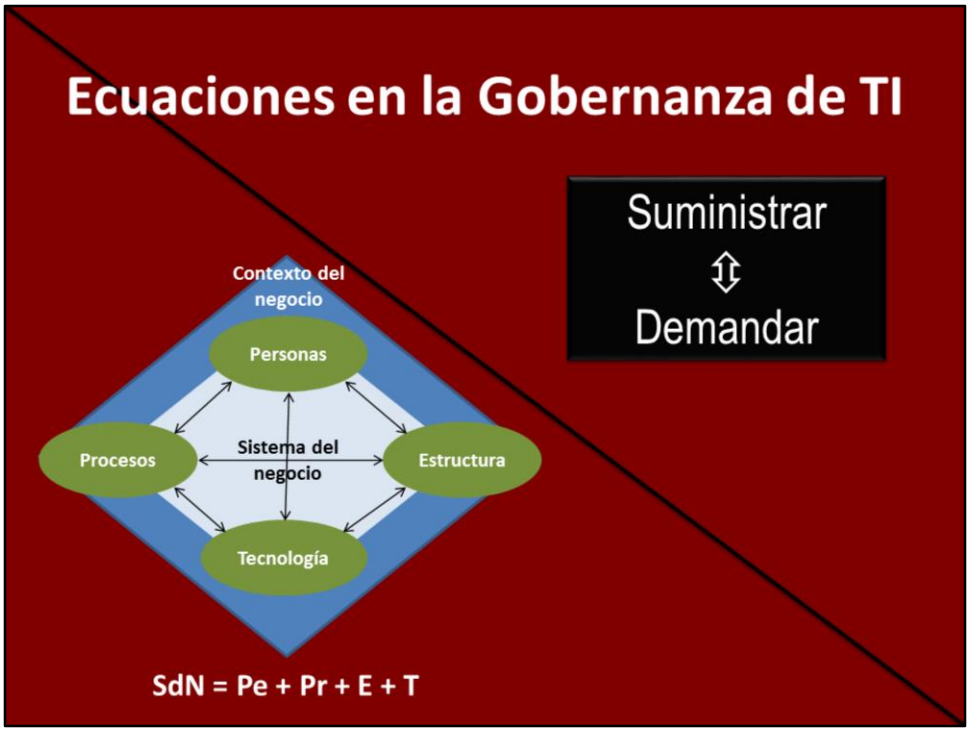


MODELO: los directores ejercerán el buen gobierno de TI a través de tres tareas principales:
•*Evaluar el uso actual y futuro de las TI.*
•*Dirigir la preparación e implantación de los planes y las políticas para garantizar que el uso de las TI satisface los objetivos del negocio.*
•*Supervisar la conformidad con las políticas y el desempeño frente a los planes.*

Para comprender el modelo anterior, se debe seguir el "ciclo de gobernanza"[2]:
✓Gestión del negocio, como parte de su responsabilidad en los procesos de negocio, prepara propuestas para el uso de TI;
✓Las propuestas son evaluadas por el Gobierno Corporativo, teniendo debidamente en cuenta las presiones comerciales y las necesidades del negocio;
✓Sobre la base de su evaluación, los órganos del Gobierno Corporativo dirigen a los directores del negocio en las acciones específicas;
✓El Gobierno Corporativo dirige a los directores según los planes y las políticas aprobadas;
✓La Gerencia Corporativa de Proyectos se compromete a proporcionar la capacidad requerida a la organización;
✓Dichas capacidades, como operaciones de TI, se utilizan para operar el negocio;
✓El rendimiento de las TI y de la gestión empresarial en conformidad con las normas y políticas, se informa periódicamente al Gobierno Corporativo;
✓El órgano de Gobernanza Corporativa supervisa los informes para evaluar el rendimiento y la conformidad. El conocimiento en la organización de la vigilancia en el rendimiento hace que las propuestas que se evalúan con mayor detenimiento.

Principio 1: responsabilidad
Los individuos o grupos dentro de la organización entienden y aceptan sus responsabilidades (y la ejecución) con respecto al suministro y a la demanda de TI.
Principio 2: estrategia
La estrategia de negocios de la organización toma en consideración las capacidades actuales y futuras de TI, así como los planes estratégicos de TI satisfacen las necesidades actuales y futuras de la estrategia del negocio.
Principio 3: adquisición
En las adquisiciones de TI existe un equilibrio adecuado entre beneficios, oportunidades, costos y riesgos, tanto a corto como a largo plazo**.**
Principio 4: desempeño
TI es adecuada para brindar soporte a la organización, suministrando servicios con los niveles adecuados y con la calidad que se requieren para satisfacer las necesidades actuales y futuras del negocio.
Principio 5: conformidad
TI cumple con todas las leyes y los reglamentos obligatorios. Las políticas y las prácticas están definidas, implementadas y se hacen cumplir.
Principio 6: comportamiento humano
Las políticas, prácticas y decisiones con respecto a TI demuestran respeto por el comportamiento humano, incluyendo las necesidades actuales y evolutivas de todas las “personas en el proceso”.


ISO
27000
COBIT 5
AN ISACA® FRAMEWORK
ISO
International Organization for Standardization
ISO/IEC 20000
ITIL®
SSAE16
Completed Audit

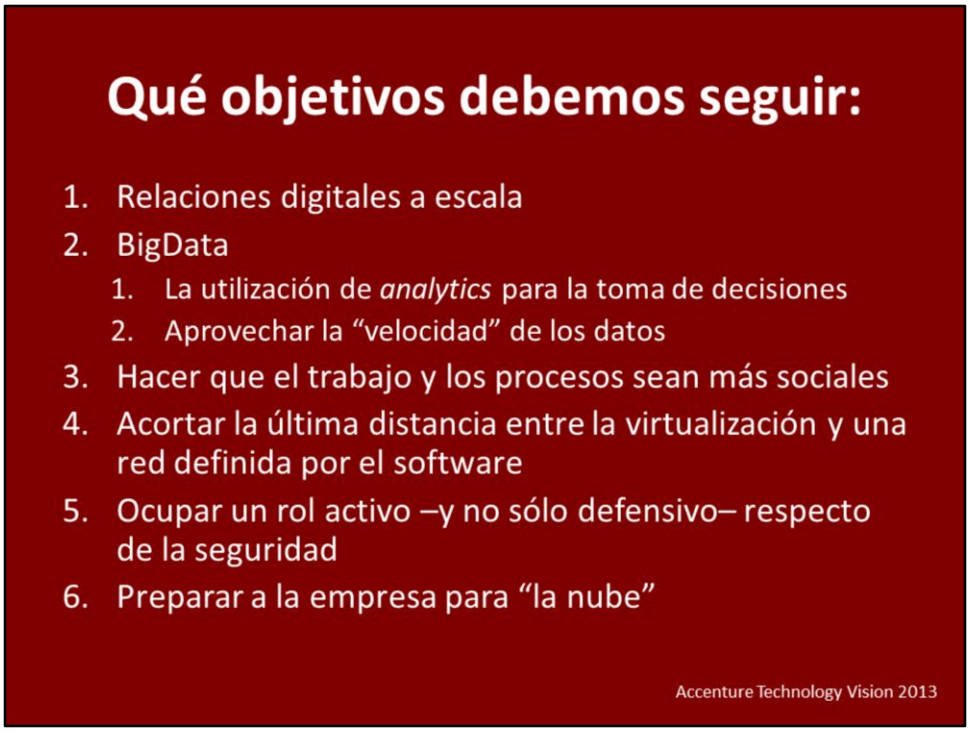


suministrar ↔ demanda

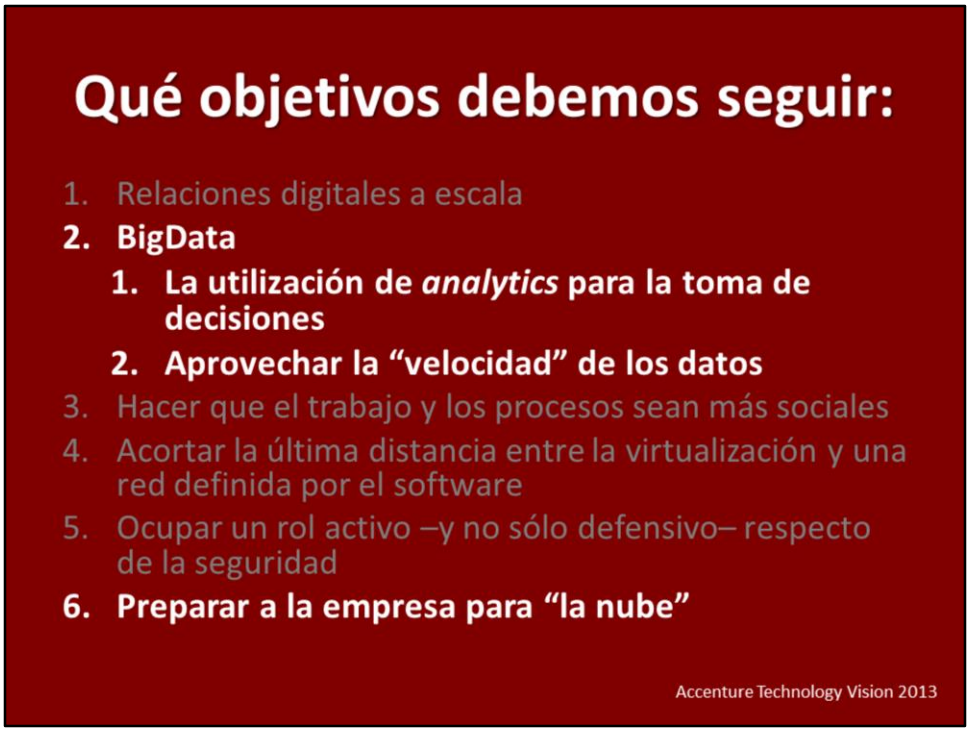
las demandas que realiza el negocio son las que originan los suministros que TI debe hacer para satisfacerlos. Las demandas que hace el negocio son el resultado de la planificación y ejecución del negocio, es decir, de qué negocio se trata y cómo opera el mismo. Como consecuencia, TI debe suministrar (planificar, organizar, implementar y ejecutar) lo que se le solicita de modo de habilitar al negocio a alcanzar sus objetivos tanto estratégicos como operativos de manera segura y efectiva reconociendo las capacidades y oportunidades en el uso de TI así como los riesgos asociados (tanto se utilice o no).

sistemas de negocio = personas + procesos + estructura + tecnología

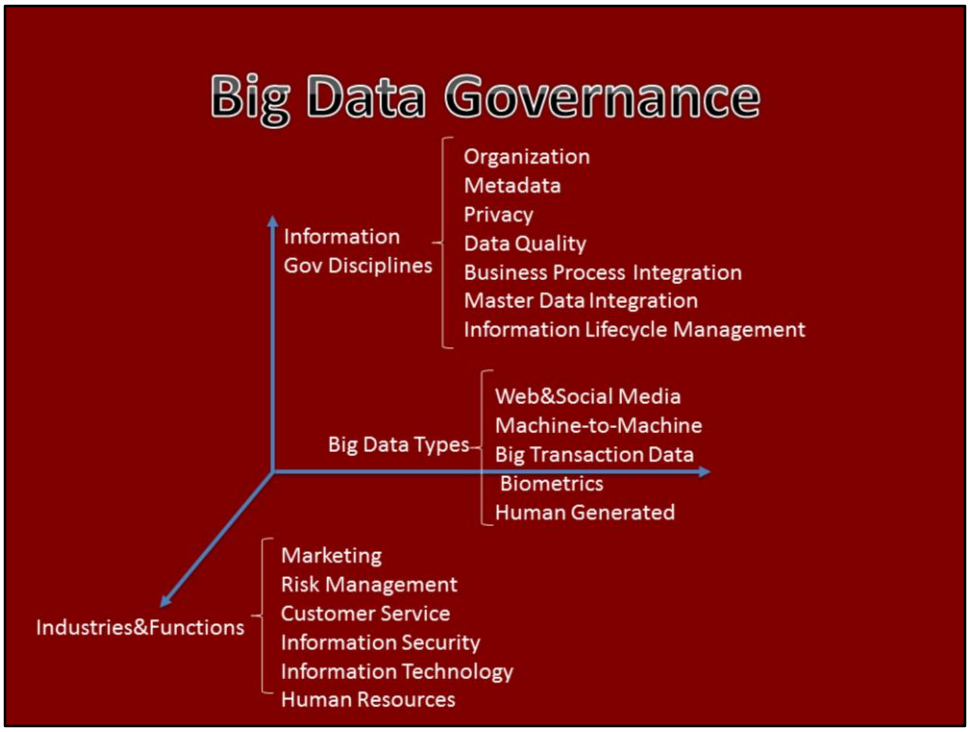
TI por sí sola no es suficiente, se obtienen resultados cuando TI es combinada con los otros tres elementos que conforman un sistema de negocio. Las personas son aquellas que trabajan en el sistema, los procesos (conjunto de tareas que deben ser realizadas para alcanzar los resultados esperados) los que pueden estar automatizados o no, la estructura que provee los límites de las operaciones y la autoridad para tomar decisiones y por último, la tecnología que habilita nuevas capacidades, mejora la performance, el control entre otros



Potenciar la tecnología para crear relaciones digitales a escala: La mayor parte de las empresas no aprovecha al máximo la tecnología para construir relaciones más profundas y enriquecidas que puedan mejorar la fidelidad de los clientes de manera significativa.
Diseñar para que por medio de *analytics* se obtengan los datos "correctos": Las empresas deben diseñar aplicaciones de software que les entreguen información estratégica para lo toma de decisiones, convirtiendo sus datos en un activo estratégico que impulsa los resultados de negocios.
Aprovechar la "velocidad" de los datos: Las empresas deben considerar no sólo la variedad y volumen de los datos, sino que también su velocidad. A medida que los datos sean cada vez más usados, las empresas buscarán aumentar sus ventajas competitivas acelerando el proceso "desde los datos al insight". Esto provocará que las aptitudes analíticas y relacionadas con el manejo de datos de una organización también se vuelvan más importantes .
Hacer que el trabajo y los procesos sean más sociales: Al incorporar herramientas de colaboración similares a las redes sociales a sus procesos de negocios, las empresas pueden aprovechar la mayor comodidad que sienten los empleados con ellas para alcanzar un nuevo nivel de productividad en donde el trabajo y los procesos se vuelven más sociales.
Acortar la última distancia entre la virtualización y una red definida por el software: Las organizaciones son capaces de reconfigurar la conectividad de sus sistemas y obteneruna mayor rentabilidad de sus inversiones en redes.
Ocupar un rol activo –y no sólo defensivo– respecto de la seguridad: Los puntos de acceso para un ataque están en constante expansión, por lo tanto, la seguridad óptima de TI debe ir más allá de la mera prevención. Las empresas deben estar siempre un paso adelante de sus enemigos, mediante la implementación de medidas inteligentes que les permitan comprender y atacarlo antes, logrando así que las defensas de la empresa se adpaten a la amenaza.
La nube ha llegado: este es el momento de preparar la empresa: Los beneficios de la nube son claros y es hora que las empresas se pregunten cómo deben usarla. Para esto, es necesario comprender con claridad y abordar las aptitudes, la arquitectura, el gobierno y la seguridad necesarios, ya sea para las aplicaciones, las plataformas o la infraestructura de TI que se encuentran en la nube.



Potenciar la tecnología para crear relaciones digitales a escala: La mayor parte de las empresas no aprovecha al máximo la tecnología para construir relaciones más profundas y enriquecidas que puedan mejorar la fidelidad de los clientes de manera significativa.
Diseñar para que por medio de *analytics* se obtengan los datos "correctos": Las empresas deben diseñar aplicaciones de software que les entreguen información estratégica para lo toma de decisiones, convirtiendo sus datos en un activo estratégico que impulsa los resultados de negocios.
Aprovechar la "velocidad" de los datos: Las empresas deben considerar no sólo la variedad y volumen de los datos, sino que también su velocidad. A medida que los datos sean cada vez más usados, las empresas buscarán aumentar sus ventajas competitivas acelerando el proceso "desde los datos al insight". Esto provocará que las aptitudes analíticas y relacionadas con el manejo de datos de una organización también se vuelvan más importantes .
Hacer que el trabajo y los procesos sean más sociales: Al incorporar herramientas de colaboración similares a las redes sociales a sus procesos de negocios, las empresas pueden aprovechar la mayor comodidad que sienten los empleados con ellas para alcanzar un nuevo nivel de productividad en donde el trabajo y los procesos se vuelven más sociales.
Acortar la última distancia entre la virtualización y una red definida por el software: Las organizaciones son capaces de reconfigurar la conectividad de sus sistemas y obteneruna mayor rentabilidad de sus inversiones en redes.
Ocupar un rol activo –y no sólo defensivo– respecto de la seguridad: Los puntos de acceso para un ataque están en constante expansión, por lo tanto, la seguridad óptima de TI debe ir más allá de la mera prevención. Las empresas deben estar siempre un paso adelante de sus enemigos, mediante la implementación de medidas inteligentes que les permitan comprender y atacarlo antes, logrando así que las defensas de la empresa se adpaten a la amenaza.
La nube ha llegado: este es el momento de preparar la empresa: Los beneficios de la nube son claros y es hora que las empresas se pregunten cómo deben usarla. Para esto, es necesario comprender con claridad y abordar las aptitudes, la arquitectura, el gobierno y la seguridad necesarios, ya sea para las aplicaciones, las plataformas o la infraestructura de TI que se encuentran en la nube.


Big Data Governance
Information
Gov Disciplines
Organization
Metadata
Privacy
Data Quality
Business Process Integration
Master Data Integration
Information Lifecycle Management
Big Data Types
Web&Social Media
Machine-to-Machine
Big Transaction Data
Biometrics
Human Generated
Industries&Functions
Marketing
Risk Management
Customer Service
Information Security
Information Technology
Human Resources

Cloud Governance

1. ¿Existe un plan? ¿Se han sopesado el valor y los costos?
2. ¿Los planes de computación en la nube respaldan la misión de la empresa?
3. ¿La organización está preparada para el cambio?
4. ¿En la planificación, se han evaluado las inversiones existentes? ¿Alguna se podría perder?
5. ¿Existen estrategias para medir y dar seguimiento al valor de la inversión y a los riesgos?

Felix Baumgartner (Salzburgo, Austria, 20 de abril de 1969) es un exmilitar, paracaidista y un saltador BASE. Es conocido por la particular peligrosidad de las maniobras que ha realizado durante su carrera. Baumgartner pasó algún tiempo en el ejército austriaco, donde practicó paracaidismo, incluyendo entrenamiento para aterrizar en zonas pequeñas.
El 14 de octubre de 2012 batió tres récords históricos al lanzarse en caída libre desde los **39.068 metros de altura**, después de haber ascendido en globo tripulado a la **estratosfera.**

UNIVERSIDAD ORT
Uruguay

¡Muchas gracias!

Dra. Helena Garbarino
garbarino@ort.edu.uy