

Primer Hito

Ingeniería en computación e Informática

Universidad Andrés bello

Campus Antonio Varas

T1: Seguridad de la información

Integrantes: Rodrigo Bustos

Ricardo Cesped

Cristopher Herrera

Fernando Olivares

Profesor: Eduardo Quiroga

Fecha: 06-04-2018

Tabla de contenidos

- Introducción
- Contexto - Rubro
- Organigrama
- Criterios utilizados en evaluación GAP
- Identificación de entrevistados
- Conclusión

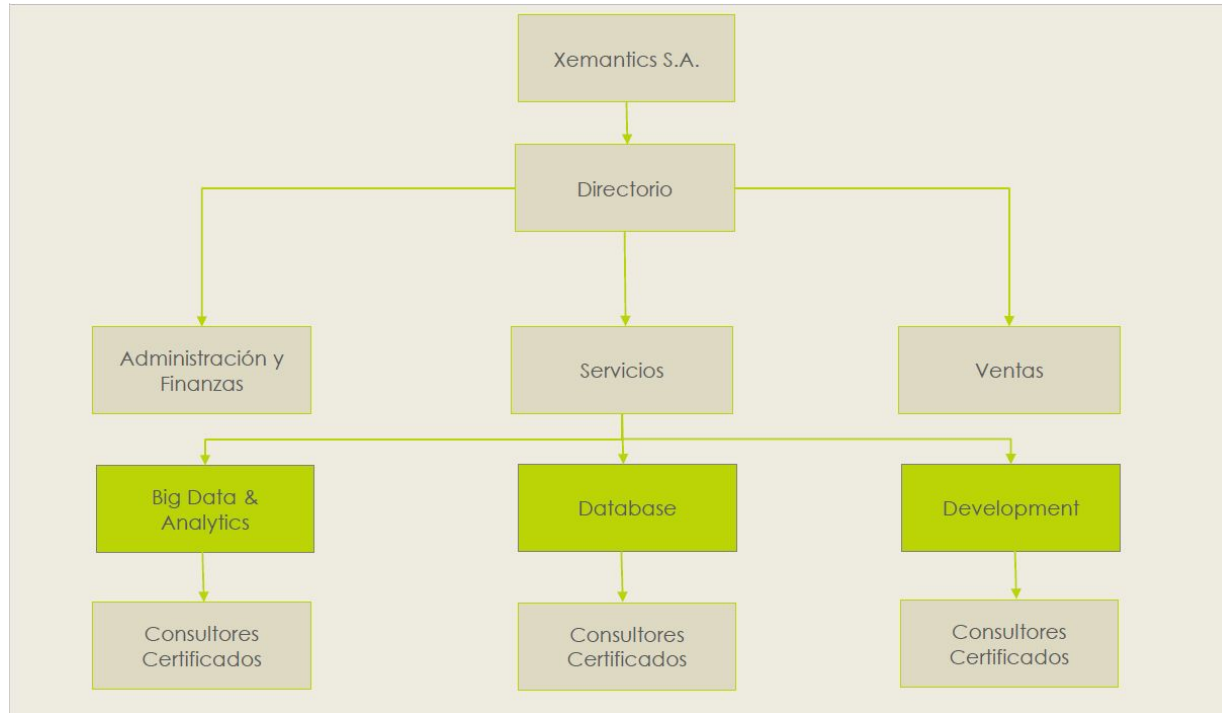
Introducción

La empresa Xemantics será el objetivo de la realización del análisis GAP.

“Empresa de carácter innovador, enfocada en el almacenamiento, diseño, procesamiento y descubrimiento de los datos desde un punto de vista moderno” Xemantics S.A.

Servicios como BI, Big Data, Development y Advanced Analytics

Organigrama



Criterios utilizados

Se entrevistó a dos personas, el entrevistado 1 tiene mayor ponderación dentro de la entrevista.

Resultados

Checklist	Estándar	Dominio	Indicador del análisis	Porcentaje Cumplimiento	Porcentaje NO Cumplimiento
1	5	Política Seguridad	71%	71%	29%
2	6	Organización de la Seguridad Informática	88%	88%	13%
3	7	Administración Activos	83%	83%	17%
4	8	Seguridad Recursos Humanos	100%	100%	0%
5	9	Seguridad Física y Ambiental	41%	41%	59%
6	10	Administración Comunicaciones y Operaciones	71%	71%	29%
7	11	Control de Accesos	71%	71%	29%
8	12	Adquisición, desarrollo y mantenimiento de Sistemas de Información	60%	60%	40%
9	13	Administración de Incidentes de Seguridad Informática	77%	77%	23%
10	14	Administración Continuidad de Negocios	70%	70%	30%
11	15	Cumplimiento	92%	92%	8%
Resultado de Evaluación			75%	75%	25%

Identificación de entrevistados

E1

Nombre: Pedro Cespéd

Cargo: Gerente de Servicios

E2

Nombre: Desconocido

Cargo: Gerente comercial

**Nota: A pedido del Entrevistado 1 se omitió el nombre del Entrevistado 2*

Conclusión

Gracias al análisis GAP se logró identificar las diferencias existentes entre la situación actual y la deseable, se identificó un 25% de no cumplimiento con la situación de cumplimiento deseable.

Los dominios más críticos identificados fueron la “seguridad física y ambiental” con un 59% de no cumplimiento y “ Adquisición, desarrollo y mantenimiento de sistemas informáticos” con un 40% de no cumplimiento.

Dentro del primer dominio crítico mencionado, no es posible mejorar la seguridad física y ambiental ni el control de acceso debido a la organización física de la empresa.

Los puntos en que buscamos entregar mejoras son, la revisión política de seguridad informática por parte de los gerentes, y, la posibilidad de la continuidad de los procesos de los negocios ante posibles ataques informáticos.