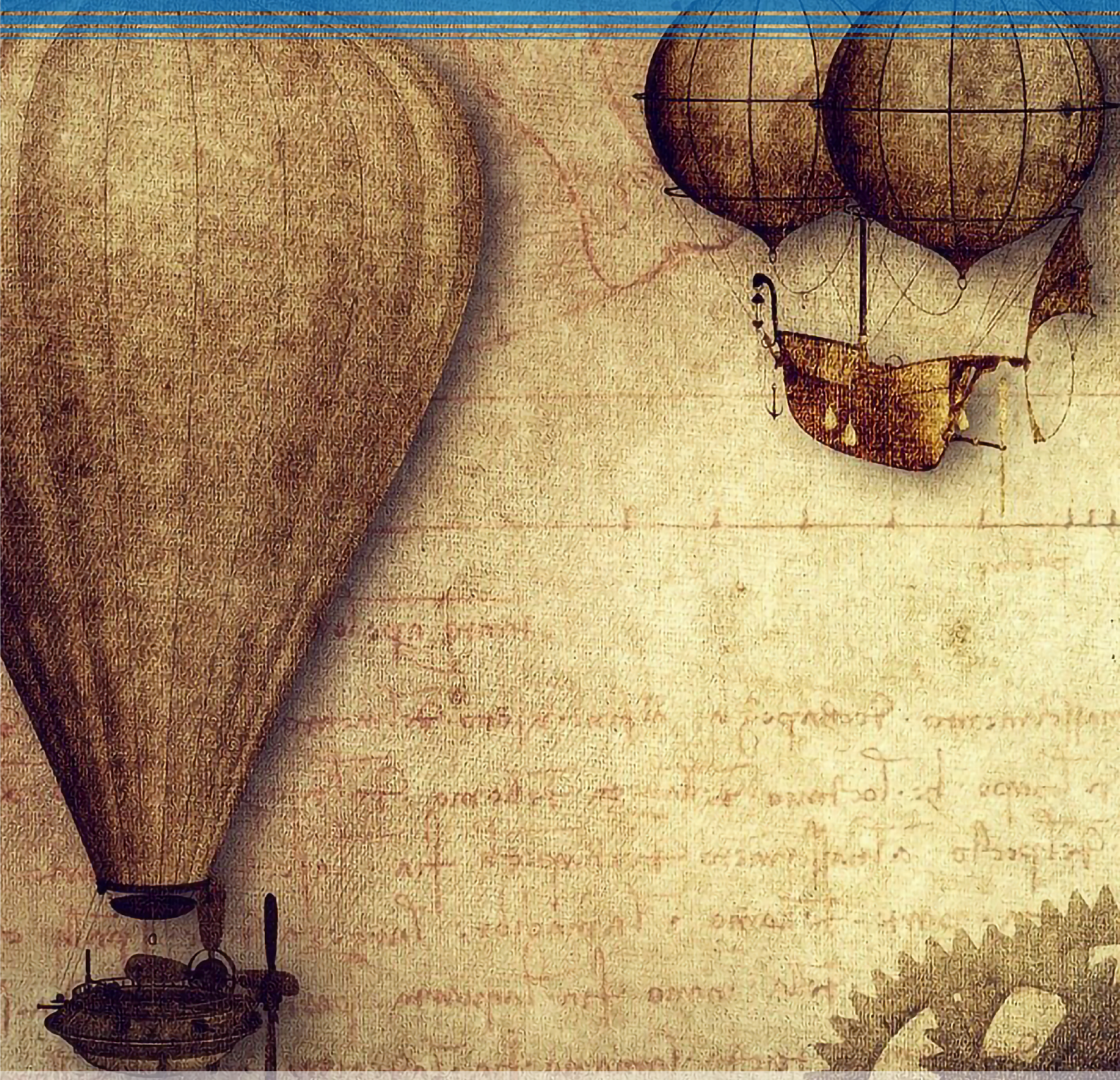
Núm. 1 - 2022

REVISTA ConCiencia Joven

Facultad de Ingeniería | Universidad Católica de Salta



INGENIERÍA
UNIVERSIDAD CATÓLICA DE SALTA

REVISTA ConCiencia Joven

Facultad de Ingeniería
Universidad Católica de Salta
Salta - Argentina

Número 1, 2022

INGENIERÍA
UNIVERSIDAD CATÓLICA DE SALTA

REVISTA
ConCiencia Joven

COMITÉ EDITORIAL

CONTENIDOS

EDITORIAL

ARTÍCULOS

SOBRE LA REVISTA

EDITORIAL

Editorial

Todas las cosas tienen un inicio, el de esta revista resulta muy gratificante porque viene a llenar un espacio en la difusión de los resultados de las investigaciones realizadas por alumnos.

Recordemos que, como institución universitaria, debemos cumplir diversos objetivos en la formación de los futuros profesionales; el primero sería promover que logren experiencias significativas que produzcan efectos positivos en su accionar futuro a fin de que interpreten que están insertos en un mundo globalizado que merece ser estudiado y a cuya mejora todos podemos contribuir. El segundo objetivo es despertar vocaciones en los estudiantes, entre ellas, la de la investigación; se trataría entonces de propiciar que visualicen como modo de vida la investigación, que con dedicación y trabajo se puede interpretar la realidad.

La Facultad de Ingeniería incluye estos propósitos como objetivos estratégicos con el fin de garantizar su cumplimiento, ya que ello permitirá que se generen recursos humanos calificados comprometidos con la realidad e insertos en el medio local. Se abre para ellos, de esta manera, un camino en la investigación, desde su condición de alumnos hasta cuando, como profesionales con títulos de grado, busquen completar posgrados en áreas que esta unidad académica defina como prioritarias. Serán los futuros directores de los proyectos de investigación, conocedores de las potencialidades y de los inconvenientes que el estudio de la ciencia conlleva.

En todos los niveles de la formación se genera conocimiento; así, las investigaciones de cátedra son el germen de nuevos temas, del despertar de las vocaciones y de los grupos de investigación. Hay un proceso escalonado de crecimiento que se debe estimular con la publicación de los resultados. Fruto del trabajo de mucha gente, esta revista que hoy se inicia resulta muy valiosa por todo lo dicho.

Mg. Ing. Néstor Lesser
Decano de la Facultad de Ingeniería
UCASAL

ARTÍCULOS

Agregado de valor a la producción de maní en el norte argentino

Pablo L. Reina
reina_pablo@hotmail.com

Juan M. Larrahona
juanlarrahona@gmail.com

Ingeniería Industrial, Facultad de Ingeniería, UCASAL

Resumen

Buscando evaluar la factibilidad y viabilidad de instalar una fábrica productora de maní saborizado y con chocolate, con abastecimiento de materia prima local y comercialización en la Provincia de Salta- Argentina, se llevó a cabo el estudio de contexto, de mercado (contemplando las 5 fuerzas de Porter, plan de marketing, estudio y proyección de la demanda), técnico (albergando la diagramación y planificación del proceso productivo, maquinaria, logística externa e interna, lay out y dimensiones del proyecto), ambiental, y económico/ financiero (obteniendo precio de venta y costo unitario del producto, costos fijos, flujo de fondos y análisis de sensibilidad) del proyecto. Dando como resultado que con una inversión inicial de USD $420.121, contemplando maquinaria, instalaciones, bienes de uso, adquisición de terreno y construcción, se obtuvo dos flujo de fondo, uno con aportes propios y otro con inversionistas a una tasa de interés del 59,90%, dando como resultado un VAN de -USD $398.041 o -USD $409.324, una TIR del 10% o -16% y un periodo de repago en el año N°9 o N°10 respectivamente, lo que volvió al proyecto inviable económicamente, no así en lo que respecta al resto de los estudios que se demostró su factibilidad. En el análisis final se podrá observar datos a tener en cuenta para mejorar la viabilidad económica del proyecto.

Palabras Clave

Maní, Salta, Factibilidad, Proyecto.

Abstract

Seeking to evaluate the feasibility and viability of installing a factory producing chocolate- flavored peanuts, with local raw material supply and marketing in the Province of Salta- Argentina, it was carried out with the study of context, market (considering the 5 forces de Porter, marketing plan, study and projection of demand), technical (hosting the establishment and planning of the production process, machinery, external and internal logistics, layout and dimensions of the project), environmental, and economic / financial (obtaining sale price and unit cost of the product, fixed costs, cash flow and sensitivity analysis) of the project. As a result, with an initial investment of USD $ 420,121, considering machinery, facilities, fixed assets, land acquisition and construction, it were obtained two cash flows, one with own contributions and the other with investors at an interest rate of 59, 90%, resulting in a NPV of -USD $ 398,041 or -USD $ 409,324, an IRR of 10% or -16% and a repayment period in year N° 9 or N° 10 respectively, which made the project economically unfeasible , not so with respect to the rest of the studies that were demonstrated to be feasible. In the final analysis, it will show data to be taken into account to improve the economic viability of the project.

Keywords:

Peanut, Salta, Feasibility, Project.

Introducción

Si Argentina, un gran exportador de commodities del mundo, tiene tanto potencial de desarrollo ¿Por qué no tomar la iniciativa de darle agregado de valor a algún insumo que se produzca en la zona?.

Con esta impronta y notando un relevante crecimiento del consumo de picadas en adición de que gran parte del maní que se produce en el norte argentino se destina a Córdoba o al exterior sin proceso alguno [1] es el puntapié inicial para abordar un estudio que permita evaluar la factibilidad y viabilidad [2] de instalar una fábrica productora de maní saborizado y con chocolate con materia prima local y cuya comercialización sea en la provincia de Salta.

Entre los principales beneficios de llevar a cabo el proyecto se pueden encontrar:

- Determinar la factibilidad de montar la industria,
- Fomentar el crecimiento del sector manisero en la provincia dándole un valor agregado al maní.

2. Contexto

Dentro de lo más destacado del análisis de macroentorno PESTEL existía una situación política polarizada en una época de elecciones que generaba inestabilidad en todos los sentidos y donde se hallaba una alta carga impositiva como también nuevos recortes de subsidios para empresas. Por su parte en la situación económica existía una especulación bursátil y de mercados bastante alta que se traduce en las divisas y a su vez en precios de todos los rubros, esto también afectó a las empresas elevándose las tasas de interés entre otros factores llegando a niveles muy complicados para generar rentabilidad. Es por eso que para evitar inconvenientes inflacionarios se tomó como moneda de análisis el dólar estadounidense.

3. Estudio de Mercado

Por maní saborizado se entiende que es un snack compuesto con un corazón de maní tostado, rodeado de una gruesa capa hecha de harina de trigo junto a un jarabe para empanizar y saborizado con jarabe saborizante. Por su parte el maní con chocolate posee un corazón de maní tostado recubierto de un jarabe a base de agua, azúcar y saborizantes que favorecen la adherencia del chocolate.

3.1. Principales agentes de mercado

Se consideró como clientes objetivos a todas las personas de cualquier clase social en la provincia de Salta a partir de los 4 años de edad excluyendo los que están contraindicados médicamente.

En cuanto a los proveedores se los buscó de la forma más estratégica posible minimizando costos, distancias y tiempos de respuesta. De los mismos se realizó un resumen de todos (precios sin IVA) en la Tabla 1.

A pesar de que la empresa no contaba con competidores directos en Salta Capital que elaboren los mismos productos a escala industrial, se consideró como competencia principalmente a aquellos productos que se importan a la provincia desde otra o de otros países para el caso del maní con chocolate y que se venden a través de distribuidoras o supermercados mayoristas o minoristas como es el caso de las marcas reconocidas como J.L. SA y Maní King para los manies saborizados y Maní King, Georgalos, Dulcim, Palmesano para con chocolate. Y cuyos precios de venta de acuerdo a lo relevado en el mercado minorista rondaban entre los USD $0,41 - $0,95 para los 100 g y USD $3,54 - $4,90 para 1 Kg de maní saborizado y USD $1,65 - $3,50 y USD $10 - $12 para los 100 g y 1 kg de maní con chocolate respectivamente dependiendo de la marca.

Tabla 1: Proveedores

Producto	Ubicación	Proveedor	Lead time	Precio (USD)	Cant. por precio	MOQ
Maní con cascara	Luis Burela - Anta	De la zona	2 días	$0,38	1 Kg.	-
Paquete 1 Kg.	Pje. Ing Clement 1243 - Salta	Petit Plast	30 Días	$636,75	100 kg	100 kg
Paquete 80 g.				$611,65	100 kg	100 kg
Bolson (30 U x 80 g)				$21,10	1000 uds.	20000 uds
Cajas de cartón	Dean Funes 455 - CABA.	Mazaranz	25 Días	$0,65	unidad	1000 uds

Producto	Ubicación	Proveedor	Lead time	Precio (USD)	Cant. por precio	MOQ
Harina	km 1.153 de la Ruta Nacional 34 - Jujuy	Molino Pampa Blanca	7 Días	$20,89	50 kg	50 kg
Azúcar	Salta	Maxi Consumo	-	$14,25	25 kg	-
Sal	Salta	UMA	1 Día	$3,33	50 kg	-
Bicarbonato de Sodio	Oncativo 101- Córdoba	La Reposterita	7 Días	$2,15	1 kg	$14
Manteca	Ruta 26 Km 2 - Salta	La Rotonda Lacteos	1 Día	$12,50	2,5 kg	-
Salsa de soja				$8,70	3 L	-
Agua	España 887	Aguas del Norte	-	$0,60	1 mt³	-
Chocolate para cobertura	Oncativo y Rivadavia - Córdoba	La reposterita	7 Días	$43,20	10 kg	$14
Goma arábiga atomizada				$15,20	1 kg	$14

distancias y aprovechando la capacidad de carga del vehículo al máximo.

Se priorizo la capital salteña para abastecer realizando luego de esto viajes desde la planta al interior a lugares estratégicos de distribución tales como General José de San Martín, General Güemes, Oran, La Caldera, Rosario de la Frontera, Metan, Cafayate, Cachi, Cerrillos, Rosario de Lerma, Rivadavia y Anta. Dónde localidades cercanas se abastecerán de esos puntos y de esta forma evitar incurrir en gastos de transportes atendiendo la máxima cantidad de lugares posibles sin necesidad de viajar a ellos.

3.2. Plaza

Se diagramó un plan de distribución donde una vez almacenados los productos en la fábrica se distribuirán a los centros de consumos mediante transporte propio o tercerizado en base a los pedidos, distancias y plazos de entrega acordados con los clientes tales como Supermercados, Mayoristas, Minoristas, Eventos, Restaurantes, Boliches y Bares siguiendo un ruteo determinado optimizando

3.3. Proyección de la demanda

Para determinar la proyección de la demanda se tuvo en cuenta el análisis poblacional de acuerdo a la estadística obtenida en la Dirección General de Estadísticas y las encuestas [3] que se realizó a 400 personas de la provincia de Salta a través de 14 preguntas objetivas, de los cuales se puede observar los resultados más relevantes en la Tabla 2.

Tabla 2: Resultados relevantes de las encuestas

3-Apto para comer maní		
Opciones	Cantidad	Porcentaje
Si	381	95,3%
No	9	2,3%
Tal vez	10	2,5%
Total	400	

7- Consumo de maní saborizado		
Opciones	Cantidad	Porcentaje
Si	240	62,3%
No	145	37,7%
Total	385	

5- Preferencias de maní		
Opciones	Cantidad	Porcentaje
Garrapiñada	175	20,33%
Saborizado	125	14,52%
Salado	223	25,90%
Frito Saldado	43	4,99%
Con chocolate	227	26,36%
Mantequilla	51	5,92%
Al natural	6	0,70%
Otro	11	1,28%
Total	861	

8-Consumo de maní con chocolate		
Opciones	Cantidad	Porcentaje
Si	287	74,5%
No	98	25,5%
Total	385	

14-Preferencia sobre producción		
Opciones	Cantidad	Porcentaje
Si	194	49,6%
No	60	15,3%
Tal vez	137	35,0%
Total	391	

Obteniendo como resultado final la Tabla 3 que indica todas las características de la demanda:

Tabla 3: Proyección de la Demanda

Concepto		2019	2020	2021	2022	2023	2024	2025	2026	2027	2028
Población de salta		1.302.035	1.319.066	1.334.800	1.350.898	1.366.783	1.382.435	1.397.837	1.413.012	1.427.980	1.442.730
Población de Salta hasta 4 años		137.012	136.701	136.313	135.858	135.346	134.807	134.256	133.706	133.167	132.646
Población de salta a partir de 4 años		1.165.023	1.182.365	1.198.487	1.215.040	1.231.437	1.247.628	1.263.581	1.279.306	1.294.813	1.310.084
Población sin extrema pobreza (96,5%)		1.124.247	1.140.982	1.156.540	1.172.514	1.188.337	1.203.961	1.219.356	1.234.530	1.249.495	1.264.231
Aptos para consumir maní (96,5%)		1.084.899	1.101.048	1.116.061	1.131.476	1.146.745	1.161.822	1.176.678	1.191.322	1.205.762	1.219.983
Consumo Per capita de maní (kg)		1,00	1,00	1,00	1,00	1,00	1,00	1,00	1,00	1,00	1,00
Turismo en Salta		1.869.276	1.909.270	1.949.265	1.989.260	2.029.254	2.069.249	2.109.244	2.149.239	2.189.233	2.229.228
Consumo M.S. per capita Turismo (kg)		28.039	28.639	29.239	29.839	30.439	31.039	31.639	32.239	32.838	33.438
Cuota de mercado		20%	20%	20%	20%	20%	20%	20%	20%	20%	20%
Mercado turistico a abastecer		5.608	5.728	5.848	5.968	6.088	6.208	6.328	6.448	6.568	6.688
Consumo total de maní (kg)		1.084.899	1.101.048	1.116.061	1.131.476	1.146.745	1.161.822	1.176.678	1.191.322	1.205.762	1.219.983
Preferencias	Sobre Maní Saborizado (14,52%)	157.506	159.850	162.030	164.268	166.484	168.673	170.830	172.956	175.053	177.117
	Sobre Maní con chocolate (26,36%)	286.030	290.288	294.246	298.310	302.336	306.311	310.228	314.088	317.896	321.645
Consumo	De maní saborizado (62,3%)	98.185	99.647	101.006	102.401	103.783	105.147	106.492	107.817	109.124	110.411
	De maní con choclate (74,5%)	213.222	216.396	219.347	222.377	225.378	228.341	231.261	234.139	236.977	239.772
Preferencias local (67,1%)	De maní saborizado	67.293	69.692	72.058	74.488	76.948	79.433	81.941	84.472	87.025	89.599
	De maní con choclate	146.136	151.345	156.483	161.760	167.102	172.500	177.946	183.442	188.987	194.577
Cuota de mercado		17,5%	20,0%	22,5%	25,0%	27,5%	30,0%	32,5%	35,0%	37,5%	40,0%
Mercado a abastecer	De maní saborizado	11.776	13.938	16.213	18.622	21.161	23.830	26.631	29.565	32.635	35.840
	De maní con choclate	25.574	30.269	35.209	40.440	45.953	51.750	57.833	64.205	70.870	77.831
TOTALES	Total de maní a abastecer	42.958	49.935	57.269	65.030	73.201	81.788	90.791	100.218	110.073	120.358
	Total maní con cascara a consumir	54.976	63.905	73.291	83.222	93.680	104.668	116.190	128.254	140.866	154.029
	Total de cascara para desecho	12.018	13.970	16.021	18.192	20.478	22.880	25.399	28.036	30.793	33.671
Consumo total de los productos (en kg)											
Maní saborizado (46,33%)		39.189	44.333	49.731	55.432	61.426	67.713	74.298	81.183	88.373	95.869
Maní con Chocolate (45,05%)		56.768	67.190	78.154	89.767	102.005	114.872	128.374	142.519	157.315	172.765

4. Estudio Técnico

4.1. Proceso Productivo

El proceso productivo constó de las partes señaladas en la Figura 1.

En lo que respecta al proceso en común para ambos productos se consideró la recepción como el primer control de calidad de estado y cantidades de materia prima para pasar posteriormente a la zona de limpieza que busca eliminar toda partícula excedente al maní con cáscara a través de una zaranda, una vez limpio se extraerán los granos de su vaina a través de una máquina descascaradora. La selección se pensó como el 2° control de calidad donde se eliminan los granos defectuosos por medio de recogida manual a través de una correa de clasificación, los granos en buen estado se secarán hasta una lograr la humedad del 9% en horno a temperatura entre 160 y 170 °C, dado que esta etapa es fundamental para el siguiente proceso que consta en la eliminación de la piel de maní, se decidió realizar un control de humedad. Finalmente, una vez que se logra la preparación de la materia prima para poder ser almacenada, se envasará en Big Bags y se almacenará en depósitos con temperatura y humedad controlada hasta ser requerida por producción.

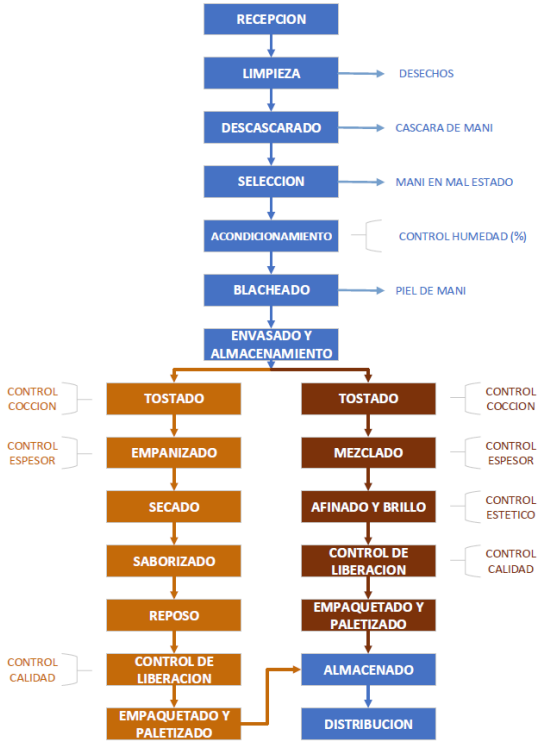


Figura 1: Proceso

Dado que ambos productos poseen procesos distintos y no se pueden mezclar por la contaminación de sabor y/o olor que generaría se los consideró como procesos aislados.

Respecto a la línea dulce se determinó comenzar con un tostado de maní hasta un color marrón claro que es el punto óptimo para sacarle las propiedades nocivas para la salud, dado que este factor es importante para

la calidad del producto se determinó colocar un control de color superficial. Posteriormente pasa a las grageadoras donde se mezcla el maní con chocolate (previamente calentado en fundidora a 45°C) 3 o 4 veces hasta tener el espesor deseado, una vez seco se introducirá a otra grageadora para darle brillo superficial con un jarabe (goma arábiga con agua) previamente preparado hasta adquirir una forma esférica y un brillo uniforme. A fines de contar con altos estándares de calidad, se planteó contar con un control de liberación que consta en la búsqueda de imperfecciones como falta de recubrimiento, espesor inadecuado, brillo indebido, granos rotos, etc. Por último, se empaquetan en bolsas 80 g y 1 kg en una empaquetadora automática con sensor de peso, luego se colocarán en cajas 10 bolsones de 30 unidades de 80 g o 20 paquetes de 1 kg y se paletiza para su correspondiente almacenamiento.

Respecto a la línea salada, el tostado y su correspondiente control se realiza igual que la línea dulce, una vez tostado el maní se mezcla en una grageadora con un jarabe para empanizar y harina de trigo unas 3, 4 o 5 veces dependiendo del espesor deseado siempre que el mismo sea homogéneo y uniforme. Para mejorar la absorción del jarabe saborizante el producto empanizado se lo tuesta ligeramente en el horno evitando que se pase y se agriete el recubrimiento por estar demasiado seco, el jarabe saborizante se mezclara junto con el producto empanizado en otra grageadora. Luego, se lo dejará secar de forma natural en bandejas mientras se realiza el control de liberación con el fin de detectar imperfecciones como falta de recubrimiento, espesor inadecuado, saborizado irregular, granos rotos, etc. El empaquetado, encajonado y paletizado se realiza de igual forma que la línea dulce.

Paralelamente al proceso principal, ocurren una serie de procesos secundarios que deben ser tenidos en cuenta, tales como la higiene de operarios previo ingreso a la planta, la eliminación de desechos en bolsa de consorcio y posteriormente en contenedores plásticos, la limpieza en cambio de turno de todos los equipos, instalaciones y herramientas que se ensucien y la preparación de insumos, como el jarabe para empanizar, saborizante o de brillo o chocolate líquido, en el mismo día que su uso para evitar algún tipo de contaminación o pérdida de propiedades.

Conociendo en detalle el proceso productivo-logístico del proyecto y la producción diaria teórica para abastecer la proyección de la demanda, fue lo que sirvió a modo guía para determinar la capacidad de las máquinas y elegir correctamente una balanza industrial, limpiadora de granos, descascaradora, cinta transportadora, peladora, grageadora, horno tostador industrial, empaquetadora automática, compresor de aire, fundidora de chocolate industrial, bandeja de manipulación, contenedor de plástico, medidor de humedad de grano digital, freezer industrial, auto elevador, transpaleta hidráulica, Furgón Renault Master 2.3, rack para almacén, big bag y pallet plástico.

4.2. Localización

Para determinar la localización del proyecto se utilizó el método de calificación por puntos considerando como factores principales la cercanía de materia prima y consumidores, la disponibilidad de mano de obra, servicios y espacios, planes de desarrollo e incentivo, estado de acceso y sentimiento de afecto a la zona obteniendo como mejor localización el Parque industrial de Salta (propuesto por su cercanía a gran parte de los consumidores finales) frente a otras variantes como el parque industrial de Güemes o terrenos en Anta o la Merced propuestos por su punto estratégico de salida a toda la provincia, cercanía a la materia prima y evitar problemas de sobrepoblación a futuro respectivamente.

4.3. Logística

4.3.1. Logística Externa

Realizado el análisis de logística externa, el aprovisionamiento más crítico fue el de maní con cáscara y es por ello que se creó una política de abastecimiento de 19 tn de acuerdo al consumo productivo:

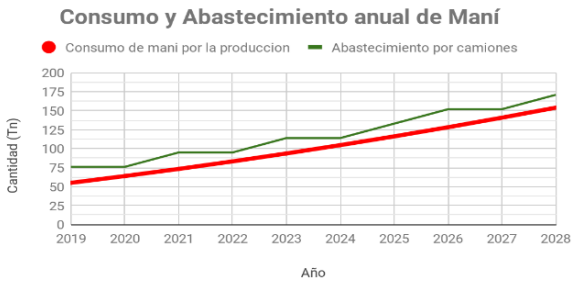


Figura 2: Consumo y abastecimiento anual de maní

Figura 3: Indicadores de Almacenamiento de maní

Para el resto de los materiales se determinó la Tabla 4 de stock teórico mínimo anual:

Tabla 4: Requerimiento mínimo de M.P e insumos

Cantidades Mínimas a Abastecer		Año 2019	Año 2020	Año 2021	Año 2022	Año 2023	Año 2024	Año 2025	Año 2026	Año 2027	Año 2028
Materia Prima (tn)	Maní pelado	43,0	49,9	57,3	65,0	73,2	81,8	90,8	100,2	110,1	120,4
	Harina	26,3	29,8	33,4	37,2	41,2	45,5	49,9	54,5	59,3	64,4
	Azúcar	2,8	3,1	3,5	3,9	4,3	4,8	5,2	5,7	6,2	6,8
	Sal	0,4	0,4	0,5	0,6	0,6	0,7	0,7	0,8	0,9	1,0
	Bicarbonato de sodio	0,4	0,4	0,5	0,6	0,6	0,7	0,7	0,8	0,9	1,0
	Salsa de soja	1,2	1,3	1,5	1,7	1,8	2,0	2,2	2,4	2,7	2,9
	Manteca	1,2	1,3	1,5	1,7	1,8	2,0	2,2	2,4	2,7	2,9
	Chocolate	30,1	35,6	41,4	47,5	54,0	60,8	68,0	75,5	83,3	91,5
	Goma Arábiga	1,1	1,3	1,6	1,8	2,0	2,3	2,6	2,9	3,1	3,5

En lo que respecta a la política de abastecimiento se determinó que quedará a cargo del gerente de producción buscando tener una relación óptima de costo/disponibilidad estando sujeta a modificaciones en base a variables como costos de transporte optimizando cantidades de carga, costos de almacenamiento, cantidades mínimas de pedido, tiempos de respuesta del proveedor, caducidad, mantenimiento de stock y stock de seguridad.

Para determinar la política de distribución se realizó un análisis de las ciudades más estratégicas para aprovisionar teniendo en cuenta costos de transporte, distancias, cantidades, demanda afectada, entre otros factores. Ello se informa en la Tabla 5

Tabla 5: Rutas logísticas de distribución

Ruta	Porción representativa de la demanda	Recorridos aproximados	Localidades alcanzadas
Norte	30,22%	401 km	Orán - José de San Martín - Gral. Güemes - Iruya
Sur	5,74%	180 km	Metán - Rosario de la Frontera - La Candelaria
Este	6,47%	320 km	Anta - Riadavia
Suroeste	9,51%	517 km	Cerrillos - Chicoana - Rosario de Lerma - La Viña - Guachipas - Cafayate - Cachi
Capital	47,28%	10 km	Capital
La Caldera	0,78%	25 km	La Caldera

4.3.2. Logística Interna

Debido a que se trataban de recursos comestibles, estos poseen caducidad y por cuestiones de salud, higiene y calidad se decidió utilizar el sistema FIFO para el consumo de stock y un sistema de almacenamiento en racks convencionales de dos niveles más piso, asegurando condiciones de limpieza, humedad y temperatura óptimas, a excepción de la manteca (ya que requiere temperaturas más bajas que el resto de los materiales) o insumos para embalaje y empaquetamiento. A fines de determinar el requerimiento de m^2 de almacén y racks a comprar, se realizó el cálculo volumétrico [4] utilizando pallets de 1.300 x 1.100 x 120 mm como unidad de manipulación los cuales soportan hasta 1.500 kg.

Tabla 6: Requerimiento palletizado

Cantidad Acumulada de Pallets a Almacenar (sin stock seguridad)		Año 2019	Año 2020	Año 2021	Año 2022	Año 2023	Año 2024	Año 2025	Año 2026	Año 2027	Año 2028
Materia Prima	Mani Pelado (Big Bag 500 kg)	85,9	99,9	114,5	130,1	146,4	163,6	181,6	200,4	220,1	240,7
	Harina (30 bolsas de 50 kg)	17,5	19,8	22,3	24,8	27,5	30,3	33,3	36,3	39,6	42,9
	Azúcar (60*25 kg)	1,8	2,1	2,3	2,6	2,9	3,2	3,5	3,8	4,2	4,5
	Sal (75*20 kg)	0,3	0,3	0,3	0,4	0,4	0,5	0,5	0,5	0,6	0,6
	Bicarb. de sodio (50*25 kg)	0,3	0,4	0,4	0,4	0,5	0,5	0,6	0,6	0,7	0,8
	Salsa de soja (160*5 L)	1,5	1,7	1,9	2,1	2,3	2,5	2,8	3,0	3,3	3,6
	Manteca (300*2,5 kg)	1,6	1,8	2,0	2,2	2,5	2,7	3,0	3,2	3,5	3,8
	Chocolate (30*50 kg)	20,0	23,	27,6	31,7	36,0	40,5	45,3	50,3	55,5	61,0
	Goma Arábiga (50*25 kg)	0,9	1,1	1,3	1,4	1,6	1,8	2,1	2,3	2,5	2,8
Producto terminado	Maní Saborizado (Bulto) (50*10 Bulto)	12,3	14,0	15,7	17,5	19,3	21,3	23,4	25,6	27,8	30,2
	Saborizado (1 kg) (50* 20 kg)	24,4	27,6	30,9	34,5	38,2	42,1	46,2	50,5	55,0	59,6
	Maní c/ chocolate (Bulto) (50*10 Bulto)	33,7	39,8	46,4	53,2	60,5	68,1	76,1	84,5	93,3	102,5
	Con chocolate (1 kg) (50* 20 kg)	16,4	19,4	22,5	25,9	29,4	33,1	37,0	41,1	45,4	49,8
TOTAL (Pallets)		216,6	251,4	288,0	326,8	367,5	410,4	455,3	502,3	551,5	602,8

Considerando un stock de seguridad del 20% para la materia prima y una rotación mensual para el producto terminado se determinó la cantidad máxima de pallets a almacenar por año alcanzando el máximo de producción con un pico de 59 pallets según se señala en la Figura 4.

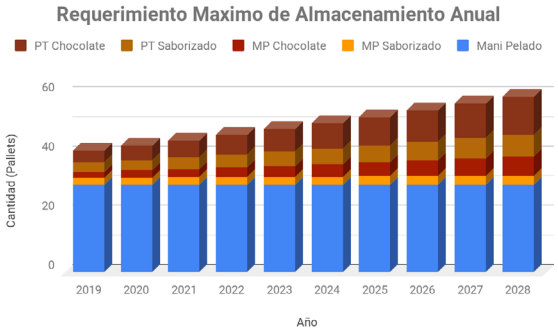


Figura 4: Requerimiento máximo de almacenamiento anual

4.4. Tamaño y terreno

El proyecto se establecerá en el Parque Industrial de Salta en un terreno con la superficie mínima necesaria de 1.353,5 m2, contemplando áreas administrativas, de almacenamiento, de producción, oficinas y las distancias mínimas exigidas por parte del APIS, con un costo de USD 55,56 el m2 definido por el mercado inmobiliario.

Para el área más importante, la de producción, se estimó un total a requerir de 222 m2 el cual incluye todo el proceso productivo del último año del proyecto junto con todos los equipos necesarios para que se lleve a cabo el mismo, un pequeño sector de tránsito para personal y otro para auto elevador.

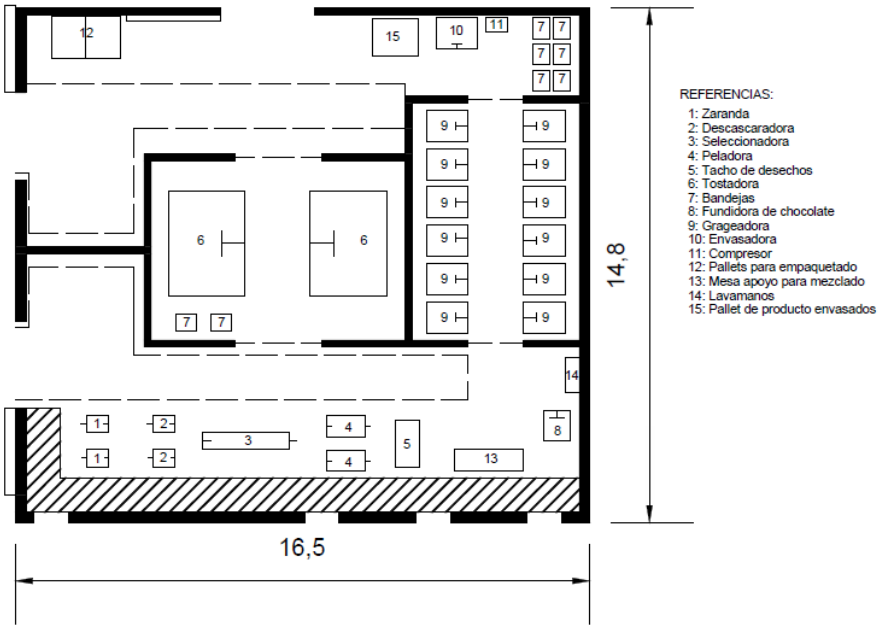


Figura 5: Plano de producción

A continuación, se detalla todo el edificio en conjunto con el terreno, junto con sus medidas correspondientes (Figura 6).

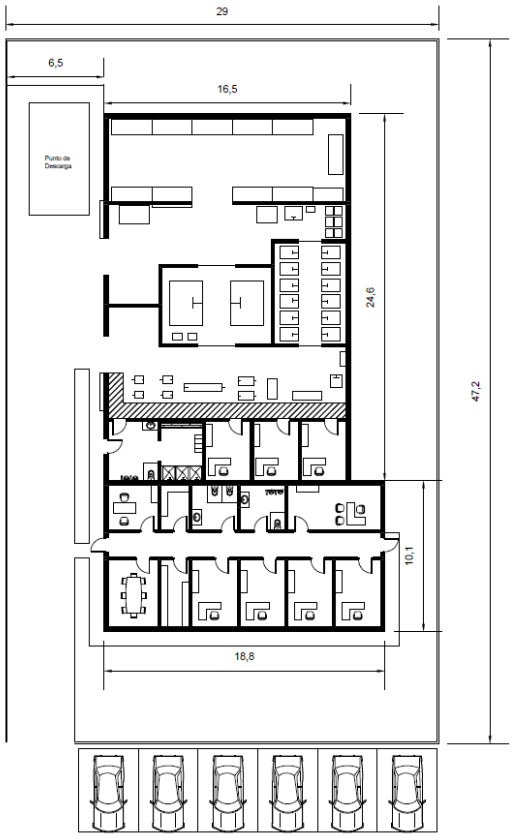


Figura 6: Plano General

En cuanto a su naturaleza jurídica se determinó constituir una Sociedad de Responsabilidad Limitada bajo el nombre de "Llamani" con una duración de 10 años, un aporte igualitario entre los socios al igual que la distribución de los resultados y una fiscalización externa.
A fines de poder desarrollar de manera óptima el trabajo administrativo se tuvieron en cuenta las inversiones de amoblado (por ejemplo, mueble y sillas), instalaciones (por ejemplo, aire acondicionado) y tecnología (programas como paquete Office, paquete adobe, sistema tango, entre otros) necesarias.

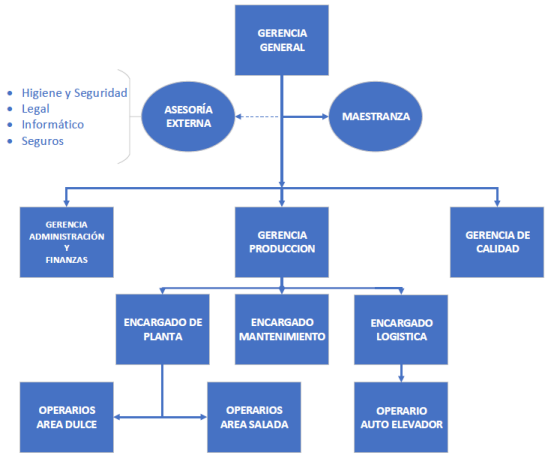


Figura 7: Organigrama

4.5. Planificación de la producción

La planificación de la producción [5] se tuvo en cuenta la capacidad máxima efectiva de las máquinas, la demanda diaria, los tiempos operativos preestablecidos de 9 hs diarias con 1 hora de almuerzo diagramando la producción diaria que determinó el número de personal ideal, cantidad y capacidad teórica de la maquinaria y el estimado de producción diaria promedio a lo largo de la vida del proyecto. Además, se notó la factibilidad de realizar la producción en paralelo recién al 5° año del proyecto.

5. Estudio Organizacional

Adoptando el siguiente esquema organizacional [6] se determinó la necesidad de un total de 12 personas al principio del proyecto y culminando con 15 considerando todos los niveles jerárquicos (ver Figura 7).

6. Estudio Ambiental

Se realizó un análisis de IA con el método Matriz Causa-Efecto – Vicente Conesa Fernández donde se pudo determinar que las actividades desarrolladas se encuentran entre compatibles y moderados lo cuales implicarán tomar medidas de control, prevención y mitigación para reducirlos al mínimo.
Para ello se propusieron una serie de mejoras como ser:

- Buscar corregir con los instrumentos correspondientes el coseno Phi del establecimiento y llevar una medición mensual de los valores eléctricos consumidos para poder reducirlos al mínimo.
- Realizar los mantenimientos correspondientes a las maquinarias así estas trabajan de manera óptima y no incurren en mayores gastos energéticos por funcionamiento mecánico y/o eléctrico indebido.

- Realizar los controles y mantenimientos correspondientes al horno de tostado para evitar lo máximo posible cualquier pérdida de calor que este genere.
- Colocar tacos de goma en los apoyos fijos de las máquinas que producen movimiento para disminuir el ruido que generan.
- Alejar lo máximo posible la circulación del auto elevador respecto a donde se encuentran los operarios de producción para poder disminuir el ruido generado por este.
- Exigir a los proveedores logísticos como así también a los rodados propios los mantenimientos correspondientes y que dispongan de tecnología EURO 5 la cual permite reducir el 80% del humo que emite el caño de escape.

7. Estudio Financiero

Arribando al análisis económico financiero donde se determinó que el costo unitario y precio de venta industrial del maní saborizado y con chocolate fue de USD $1,24-$2,11 y USD $3,13-$4,85 dando un margen de ganancia del 70% y 55% respectivamente, además se llegó a determinar el calendario de inversiones, así como el cálculo de las amortizaciones, costos fijos y variables, ingreso por ventas proyectadas, gastos administrativos, capital de trabajo y valor de desecho a lo largo de la vida útil de proyecto, se obtuvo como resultado los siguientes flujos de caja junto a su análisis de rentabilidad, según se muestra en las Tablas 7 y 8.

Tabla 8: Análisis del flujo de fondo con inversión propia

Flujo de caja con fondos propios:

Tabla 7: Flujo de fondos con inversión propia

Concepto	0	2019	2020	2021	2022	2023	2024	2025	2026	2027	2028
Ingresos		357.923	419.314	483.873	552.213	624.199	699.861	779.228	862.346	949.261	1.039.997
Venta Activo											
Costos Variables		226.218	265.208	306.211	349.618	395.342	443.402	493.817	546.616	601.827	659.468
Costos Fijos		92.926	92.926	92.926	92.926	111.691	111.691	111.691	111.691	111.691	111.691
Gastos Administrativos		36.030	36.030	36.030	36.030	36.030	36.030	36.030	36.030	36.030	36.030
Depreciaciones											
Amortizaciones		28.115	28.119	28.155	28.159	28.163	29.521	29.525	29.529	29.565	29.569
Valor libro											
Utilidad Antes de Imp.		25.367	2.970	20.550	45.480	52.973	79.216	108.164	138.480	170.147	203.239
Impuesto		-	-	-	15.918	18.540	27.726	37.858	48.468	59.551	71.134
Utilidad Desp Imp.		25.367	2.970	20.550	29.562	34.432	51.490	70.307	90.012	110.596	132.105
Depreciaciones											
Amortizaciones		28.115	28.119	28.155	28.159	28.163	29.521	29.525	29.529	29.565	29.569
Valor libro											
Inversión Inicial	420.121										
Inver. De Reemplazo		39	357	39	39	53.205	39	39	357	39	39
Invers. De Ampliación											
Invers.Capital de Trabajo	29.192	3.205	3.370	3.568	5.300	3.950	4.144	4.340	4.538	4.738	
Recupero CT											66.344
Valor de desecho											185.889
Flujo de Caja	449.313	495	21.422	45.098	52.381	5.440	76.830	95.454	114.646	135.384	413.869
Flujo de Caja Acumulado	449.313	449.808	428.385	383.287	330.906	325.465	248.636	153.182	38.536	96.848	510.717

Tabla 8: Análisis del flujo de fondo con inversión propia

VAN (USD)	$ -398.041,39
TIR	10%
Periodo de repago	9

Flujo de caja con fondos de inversores:

Tabla 9: Flujo de Fondos con inversión de terceros

Concepto	0	2019	2020	2021	2022	2023	2024	2025	2026	2027	2028
Ingresos		357.923	419.314	483.873	552.213	624.199	699.861	779.228	862.346	949.261	1.039.997
Venta Activo											
Costos Variables		226.218	265.208	306.211	349.618	395.342	443.402	493.817	546.616	601.827	659.468
Costos Fijos		92.926	92.926	92.926	92.926	111.691	111.691	111.691	111.691	111.691	111.691
Gastos Administrativos		36.030	36.030	36.030	36.030	36.030	36.030	36.030	36.030	36.030	36.030
Gastos Comerciales											
Gastos Financieros		162.772	161.871	160.431	158.129	154.447	148.560	139.146	124.094	100.025	61.539
Depreciaciones											
Amortizaciones		28.115	28.119	28.155	28.159	28.163	29.521	29.525	29.529	29.565	29.569
Valor libro											
Utilidad Antes de Imp.		188.138	164.841	139.881	112.649	101.474	69.343	30.982	14.386	70.122	141.700
Impuesto		-	-	-	-	-	-	-	-	24.543	49.595
Utilidad Desp Imp.		188.138	164.841	139.881	112.649	101.474	69.343	30.982	14.386	45.579	92.105
Depreciaciones											
Amortizaciones		28.115	28.119	28.155	28.159	28.163	29.521	29.525	29.529	29.565	29.569
Valor libro											
Inversión Inicial	420.121										
Inver. De Reemplazo		39	357	39	39	53.205	39	39	357	39	39
Invers. De Ampliación											
Préstamo	271.739										
Amortizaciones del capital		1.503	2.404	3.844	6.147	9.828	15.716	25.129	40.182	64.250	102.736
Invers.Capital de Trabajo	29.192	3.205	3.370	3.568	5.300	3.950	4.144	4.340	4.538	4.738	
Recupero CT											66.344
Valor de desecho											185.889
Flujo de Caja	177.574	164.770	142.853	119.177	95.976	140.294	59.720	30.964	1.161	6.118	271.133
Flujo de Caja Acumulado	177.574	342.344	485.197	604.373	700.349	840.643	900.363	931.327	932.488	926.371	655.238

Tabla 10: Análisis del flujo de fondos con inversión de terceros

VAN (USD)	$ -409.324,16
TIR	-16%
Periodo de repago	10

Viendo en primera instancia que el proyecto no era rentable, se decidió realizar un análisis de sensibilidad (ver Tabla 11) en base al precio de venta del producto a fines de observar a partir de qué punto es viable económicamente el proyecto.

Tabla 11: Análisis de sensibilidad

ANÁLISIS DE SENSIBILIDAD EN MILES DE USD										
VAN del proyecto		PRECIO MANÍ SABORIZADO								
	-$398.04	$1,50	$2,11	$2,50	$3,50	$4,50	$5,50	$6,50	$7,50	$8,50
PRECIO MANÍ CON CHOCOLATE	$4,00	-$563,55	-$505,80	-$470,29	-$392,03	-$315,61	-$239,20	-$162,78	-$86,37	-$9,95
	$4,85	-$444,41	-$398,04	-$368,00	-$291,58	-$215,17	-$138,75	-$62,34	$14,08	$90,49
	$5,50	-$367,73	-$321,36	-$291,32	-$214,90	-$138,49	-$62,07	$14,34	$90,76	$167,17
	$6,50	-$249,65	-$203,28	-$173,23	-$96,82	-$20,40	$56,01	$132,43	$208,84	$285,26
	$7,50	-$131,57	-$85,19	-$55,15	$21,26	$97,68	$174,09	$250,51	$326,92	$403,34
	$8,50	-$13,48	$32,89	$62,93	$139,35	$215,76	$292,18	$368,59	$445,01	$521,42
	$9,50	$104,60	$150,97	$181,01	$257,43	$333,84	$410,26	$486,67	$563,09	$639,51
	$10,50	$222,68	$269,05	$299,10	$375,51	$451,93	$528,34	$604,76	$681,17	$757,59
	$11,50	$340,76	$387,14	$417,18	$493,60	$570,01	$646,43	$722,84	$799,26	$875,67

8. Conclusiones

Concluyendo con el objetivo general de este proyecto, se llegó a plasmar la factibilidad tanto de mercado, como técnica, organizacional, ambiental y legal, así como la no viabilidad económica del mismo ya que la BADLAR se encuentra en un 45% aproximadamente.

Siendo la parte económica el único factor que impediría la factibilidad económica del proyecto, no implica que alguien por cuenta propia que desee emprender, pueda realizarlo cobrando el salario del gerente general, es por ello que realizando un análisis extenso del proyecto se detectó que el mismo se podría volver más rentable si se redujeran los precios de abastecimiento de maní, harina y chocolate, poder abastecerse de materia prima totalmente local o si el alcance del proyecto se extendiera a otras provincias.

Referencias Bibliográficas

[1] Secretaría de Agroindustria-Ministerio de Agricultura, Ganadería y Pesca. (Marzo 2019). Cadena de Maní - Resumen. Recuperado de: http://www.alimentosargentinos.gob.ar/HomeAlimentos/Cadenas%20de%20Valor%20de%20Alimentos%20y%20Bebidas/informes/Resumen_Cadena_2019%20Mani_MARZO_2019.pdf

[2] Nassir Sapag Chain, Reinaldo Sapag Chain. (2008). Preparación y Evaluación de Proyectos 5°Edición. Editorial: Mc Graw-Hill.

[3] Carl McDaniel Jr., Roger Gates. (2005). Investigación de mercados, sexta edición. Editorial Thomson. México.

[4] Comité Costarricense de Logística. (2003). Manual De Logística De Paletización Edición Nº 2 .

[5] Stephen N. Chapman. (2006). Planificación y control de la producción. Pearson Education

[6] Arias Galicia, Fernando. (1990). Administración de Recurso Humano. Editorial Trillas. México.

Análisis de sentimiento y minería de opiniones en Twitter

José Medrano
joseignacio18@gmail.com

Agustina Monge
agum_96@hotmail.com

Ingeniería en Informática, Facultad de Ingeniería, UCASAL

Resumen

En los últimos años las redes sociales se han vuelto un lugar en el cual volcar nuestras más variadas opiniones. Actualmente se encuentra a Twitter como uno de los espacios más utilizados a la hora de expresar nuestros sentimientos sobre distintas temáticas debido a que dicha herramienta es una plataforma de uso gratuito y de fácil acceso. A partir de esta situación, se pueden utilizar técnicas de Procesamiento de Lenguaje Natural (PLN) para identificar comportamientos y opiniones colectivas e inferir su polaridad, definiendo qué palabras se consideran de carácter positivo y cuáles de carácter negativo. Este tipo de análisis tiene un amplio campo de aplicación ya que el mismo puede ser aplicado tanto por empresas, quienes buscan saber la opinión de los clientes respecto a un producto determinado, por organizaciones políticas que buscan determinar cuál es la postura de los ciudadanos con respecto a un candidato y a su propuesta, como por agencias de turismo para determinar qué lugar es el más popular entre los turistas y a partir de eso ofrecer paquetes, etc. Con este artículo se desea describir, mediante una investigación, qué es análisis de sentimiento, cómo se realiza actualmente su práctica y qué podemos esperar a partir de ella.

Palabras Clave

NLP, Procesamiento del lenguaje natural, Análisis de sentimientos, Big Data, Machine Learning, Aprendizaje supervisado, Diccionario

Abstract

In recent years social networks have become a place to give our most varied opinions. Currently, Twitter is one of the most used spaces to express our feelings on different topics because this tool is a platform for free use and easy to access. From this situation, Natural Language Processing (NLP) techniques can be used to identify collective behaviors and opinions and infer their polarity, defining which words are considered positive and negative. This type of analysis has a broad field of application since it can be applied both by companies, who seek to know the opinion of customers about a particular product, by political organizations that seek to determine what is the position of citizens regarding a candidate and their proposal, as for tourism agencies to determine which place is the most popular among tourists and from there offer packages, etc. With this article we want to describe, through a research, what is sentiment analysis, how it is practiced nowadays and what can we expect from it.

Keywords:

NLP, Natural Language Processing, Sentiment Analysis, Big Data, Machine Learning, Supervised Learning.

Introducción

Es muy difícil saber con certeza lo que piensan las personas en su totalidad, o al menos un gran porcentaje, con una precisión considerable, sobre los temas por los que se ven afectados en su vida cotidiana.

En general, las encuestas realizadas por organizaciones dedicadas a estas tareas se ven sesgadas por la pequeña cantidad de gente entrevistada, o por no ser esta selección de personas una muestra representativa de toda la sociedad en conjunto.

En la actualidad gran cantidad de adultos y la mayor parte de los jóvenes utilizan al menos una red social ya sea para compartir su actividad cotidiana, informarse o formular opiniones.

Según diario Clarín, en abril del 2018 Twitter contaba con 336 millones de usuarios activos mensuales alrededor del mundo, siendo la red más popular en cuanto respecta a compartir opiniones [1].

Por estas razones es que se elige como foco de este artículo la red social Twitter y las opiniones que los usuarios vierten en ella, que proveen gran cantidad de información, con representación de casi todas las edades y estratos sociales.

Entonces, la información provista por las opiniones y comentarios en esta plataforma se puede utilizar para percibir o rescatar tendencias en las inclinaciones del pensamiento social.

Esta necesidad de conocer las magnitudes reales de los sentimientos y reacciones de las personas ante los sucesos que influyen en ellos no se puede satisfacer sin encontrar la manera de ser capaces de captar, conservar y analizar grandes cantidades de comentarios y opiniones de forma eficaz, extrayendo de ellos la mayor cantidad de información posible.

Se define el término Big Data como: "*Conjunto de técnicas que permiten analizar, procesar y gestionar conjuntos de datos extremadamente grandes que pueden ser analizados informáticamente para revelar patrones, tendencias y asociaciones, especialmente en relación con la conducta humana y las interacciones de los usuarios*" [2].

Si queremos identificar grandes cantidades de personas con pensamientos u opiniones con inclinaciones similares debemos enfocar nuestro esfuerzo en investigar, asimilar y utilizar nuevas herramientas que cuenten con la capacidad de manejo de este volumen masivo de datos.

Entonces, al concepto de Big Data debemos sumar el concepto de Data Mining (DM) o minería de datos. Sas Institute Inc. define a la minería de datos como:

"*Proceso de encontrar anomalías, patrones y correlaciones dentro de grandes conjuntos de datos para predecir resultados. Usando una amplia gama de técnicas, se puede utilizar esta información para aumentar los ingresos, reducir costos, mejorar las relaciones con clientes, reducir riesgos y más*" [3].

Uno de los derivados de la minería de datos tradicional, utilizada sobre bases de datos relacionales con datos estructurados, es la minería de texto, que busca extraer información sobre datos no estructurados, en distintos formatos de documentos.

A su vez, de la minería de texto surge otra rama conocida como análisis de sentimiento o minería de opinión, que es la parte de la minería en la cual se enfoca este artículo.

Entonces, el uso minería de opiniones para determinar la existencia o el cambio de comportamientos sociales se basa en herramientas de procesamiento de lenguaje natural (PLN), capaces de dar una connotación positiva o negativa del lenguaje utilizado en el texto escrito.

Clasificar la polaridad de un comentario u opinión se encuentra como la tarea primordial en análisis de sentimientos: se determina si la opinión es positiva, negativa o neutra según las palabras utilizadas para expresarse y su asociación con otros casos ya clasificados.

Con clasificaciones más avanzadas podemos determinar estados sentimentales, tanto positivos (felicidad, alegría), como negativos (ira, enojo, tristeza).

2. Twitter: el auge del microblogging

Desde su creación en 2006, esta plataforma fue adquiriendo más relevancia hasta llegar a ser lo que es en la actualidad, en donde millones de usuarios de todas partes del mundo comparten

sus experiencias, opiniones y visiones con respecto a una variedad notable de temas o sucesos.

A medida que fue evolucionando paulatinamente con el paso de los años se fueron incorporando distintas formas de enriquecer las publicaciones realizadas en esta red social, pudiendo ahora encontrar dentro de un tweet información en distintos formatos como vídeos, imágenes, GIFs, emojis, hashtags y texto.

Debido a estas características nombradas se puede considerar a Twitter como la fuente más importante de opiniones a la hora de llevar a cabo un proyecto de análisis de sentimiento sobre una determinada temática, gracias al enorme abanico de posibilidades que posee la gente a la hora de expresarse.

En la Figura 1 se pueden observar algunas de las relaciones de Twitter [4].

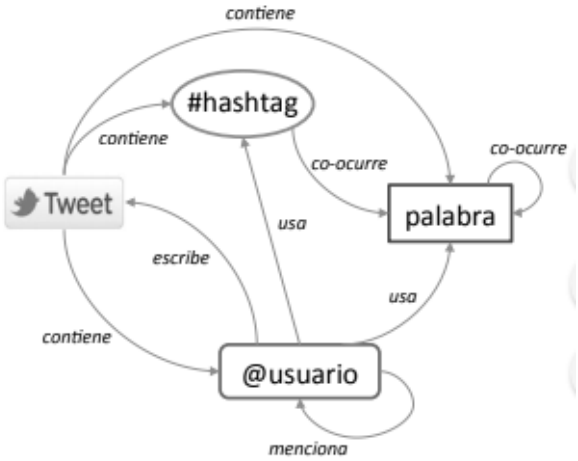


Figura 1: Relaciones en Twitter

publicado en redes sociales, principalmente Twitter, por su formato de microblogging.

Las aplicaciones en la vida real son sólo parte del porqué el análisis de sentimiento se ha vuelto un tópico popular de investigación.

Adicionalmente, es visto como un gran desafío en lo que respecta al PNL, creciendo exponencialmente el interés en esta problemática desde su aparición [6].

Luego de definir el nivel de análisis se debe determinar la técnica de análisis de sentimiento a utilizar.

Los dos enfoques más populares se tratan de técnicas de Machine Learning y el uso de un Diccionario léxico-emocional, como muestra la Figura 2 [7].

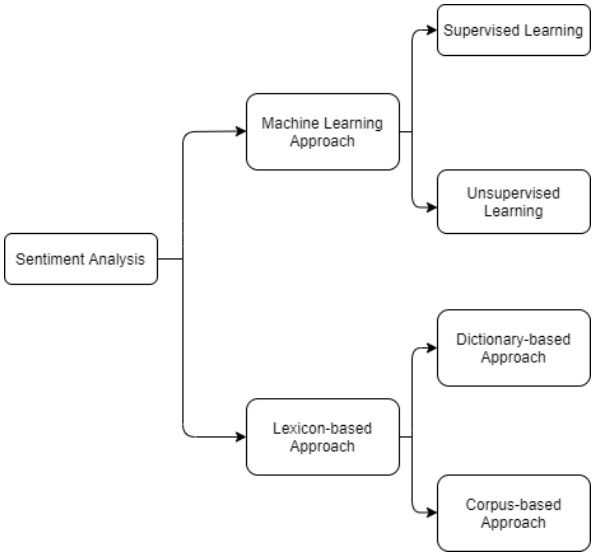


Figura 2: Tipología de las técnicas de Análisis de Sentimiento en Twitter

3. Análisis de sentimiento en la comunicación

Análisis de sentimiento (también conocido como minería de opinión) se refiere al uso de procesamiento de lenguaje natural, análisis de texto y lingüística computacional para identificar y extraer información subjetiva de los recursos.

"*Desde el punto de vista de la minería de textos, el análisis de sentimientos es una tarea de clasificación masiva de documentos de manera automática, en función de la connotación positiva o negativa del lenguaje ocupado en el documento.*" [5]

Actualmente, esta práctica se realiza mayoritariamente para la interpretación de lo

3.1. Aprendizaje Automático (Machine Learning)

El aprendizaje automático o también conocido como Machine Learning se divide en dos grandes tipos según haya o no retroalimentación, por un lado, está el aprendizaje automático no supervisado y por el otro el aprendizaje automático supervisado.

Los algoritmos utilizados por el aprendizaje automático no supervisado realizan el procesamiento en base únicamente a las entradas, es decir que el programa se va configurando a medida que procesa las observaciones que va recibiendo, en cambio, los algoritmos utilizados por el aprendizaje

automático supervisado cuentan con un corpus manualmente clasificado, sobre el cual se llevan a cabo dos procesos: encontrar los mejores parámetros para el algoritmo, y evaluar el nivel de fiabilidad con esos parámetros.
A esta fase se le llama de aprendizaje o entrenamiento.
A la hora de analizar tweets el algoritmo más adecuado de utilizar es del aprendizaje automático supervisado, a su vez este se divide en algoritmos de regresión o de clasificación.
Es conveniente utilizar este último ya que la tarea del mismo es asignar una categoría al texto de entrada, la cual puede ser dividida en tres (positivo/negativo/neutro) o en dos (positivo/negativo) [7].
Una vez definido cada uno de los puntos citados anteriormente, se debe proceder a extraer los atributos de cada uno de los tweets recolectados. Es por ello que se debe realizar un preprocesamiento de los mismos, en donde el objetivo principal es reducir la dimensionalidad y así, poder captar los conceptos más importantes a través de la eliminación de las *stopwords* o palabras vacías y la lematización. Las *stopwords* son aquellas palabras que no aportan información, mientras que la lematización consiste en reducir las palabras a su lema [8].
Luego, se debe definir si un atributo estará compuesto por una palabra o por varias (en general dos o tres) y a partir de ello seleccionar el algoritmo más adecuado, un ejemplo de ellos es Support Vector Machine (SVM) el cual es uno de los más utilizado a la hora de realizar este tipo de análisis ya que al utilizarlo como clasificador da buenos resultados. Cabe destacar que estos algoritmos serán aplicados al conjunto de entrenamiento y luego al conjunto de prueba que se quiera clasificar.

3.2. Diccionario léxico:

La alternativa más popular al aprendizaje supervisado es el uso de diccionario para la orientación semántica. En este caso no es necesario entrenar un modelo y supervisarlo. El uso de esta técnica se basa en algoritmos mucho más sencillos y en la utilización de un diccionario comúnmente llamado lexicón, en el cual encontramos generalmente una importante cantidad de palabras polarizadas y ponderadas, según su índole positiva o negativa y la intensidad del sentimiento que infieren las mismas.
Es posible también encontrar diccionarios en los cuales se clasifiquen a las palabras según la emoción que connotan.
El algoritmo usado por estos métodos es de características mucho más simples que los anteriormente nombrados.
La evaluación de un tweet implica solamente la detección de coincidencias en el texto con elementos del conjunto del diccionario, y realizar una ponderación final según todas las palabras encontradas, su concurrencia y la fuerza del sentimiento, para determinar entonces la orientación sentimental de la oración.
Existen varios diccionarios presentes en la web. La mayor parte de éstos (y los más refinados) están diseñados para el inglés. Existen diccionarios en español, pero no tan precisos y todavía faltos de maduración. Otra desventaja detectada a la hora de llevar a cabo esta técnica para realizar análisis de sentimientos es que la misma no considera el contexto en el que fue escrito un tweet en particular, ya que consiste solo en ponderar el mismo a partir del valor de cada una de las palabras que lo integran que se encuentran en el diccionario, es por ello que un tweet que fue escrito con una connotación negativa podría ser considerado positivo por el modelo y viceversa.
Algunos de los diccionarios más reconocidos son *Linguistic Inquirty and Word Count (LIWC), SentiWordNet, Q-WordNet, MPQA Subjectivity Lexicon, Big Liu Opinion Lexicon, AFINN y The General Inquirer.*

4. Conclusión

El análisis de sentimientos basado en la extracción de opiniones realizadas por las personas en redes sociales es una de las prácticas más utilizadas dado a su múltiple aplicación en diferentes temáticas, y por el hecho de que la misma es más económica que realizar encuestas en forma física y nos permite abarcar un gran segmento del mercado ya que las redes sociales

no discriminan las edades de sus usuarios ni los estatutos sociales.

Como se fue describiendo a lo largo del artículo, el análisis de sentimientos conlleva la aplicación de técnicas de Procesamiento del Lenguaje Natural el cual está muy relacionado al idioma y territorio en el cual se realizará el análisis. A partir del español se identifican los siguientes problemas [8]:

- Ambigüedad a nivel palabra: una palabra puede tener más de un significado.
- Ambigüedad sintáctica: Por ejemplo "María se encontró con Raquel para calmar su preocupación" no se puede definir si la preocupación es de María o de Raquel
- Resolución de la anáfora: se define anáfora al uso de una expresión cuya interpretación depende de otra expresión presente en el contexto del discurso (llamado su antecedente).
- Presuposición: "Ha dejado de fumar" implica que antes fumaba
- Ironía- Sarcasmo: "Había olvidado que tú eras el más inteligente, y que todos los demás éramos unos tontos."

Sin embargo, considerando dichos problemas y utilizando las técnicas y algoritmos adecuados se puede llegar a resultados muy beneficiosos para la persona u organización que realiza el análisis.

Un trabajo futuro a realizar en este ámbito sería el desarrollo de herramientas fiables para el análisis de sentimiento en tiempo real en base a *keywords* o palabras claves dadas utilizando cualquiera de las técnicas más conocidas nombradas en este artículo

Referencias Bibliográficas

[1] *Twitter crece en ganancias y usuarios, y supera las expectativas.* (25 de abril de 2018). Diario Clarín. Obtenido de:https://www.clarin.cim/tecnologia/twitter-crece-ganancias-usuarios-supera-expectativas_0_H1NnFZ02G.html

[2] Real Academia Española y Diccionario del Español Jurídico. (2019). *Big Data*. Obtenido de: https://dej.rae.es/lema/big-data.

[3] Delwiche, L. D., & Slaughter, S. J. (2019). *The little SAS book: a primer.* SAS Institute.

[4] Cotelo J.M, Cruz F., Ortega F.J, Troyano J.A. (2015). *Explorando Twitter mediante la integración de información estructurada y no estructurada*. Sociedad Española para el PNL (55), 75-82.

[5] Liu, B. (2007). *Web Data Mining. Exploring Hyperlinks, Contents, and Usage Data*. Chicago, Estados Unidos: Springer.

[6] Liu, B. (2012). *Sentiment Analysis and Opinion Mining*. doi:10.2200/S00416ED1V01Y201204HLT016.

[7] Baviera, T. (2017) *Técnicas para el Análisis de Sentimientos en Twitter: Aprendizaje Automático Supervisado y SentiStrength*. Dígitos (3),33-50. Recuperado de: https://www.researchgate.net/publication/317256429_Tecnicas_para_el_Analisis_de_Sentimiento_en_Twitter_Aprendizaje_Automatico_Supervisado_y_SentiStrength .

[8] Hernández Orallo, J. (2004) *Introducción a la minería de datos.* Madrid, España:Pearson.

Aplicación del diseño por capacidad al cálculo estructural de edificio destinado a hostal – comparación con normas anteriores

Omar Rodríguez
osr610@gmail

Andrés A. Saavedra
ingandressaavedra@ingenieria-sys.org

Ingeniería Civil, Facultad de Ingeniería, UCASAL

Resumen

Se diseñó la Arquitectura del edificio, bajo la normativa vigente – Código de Edificación, Código de Planeamiento Urbano y Ambiental de la ciudad de Salta y Decretos del Ministerio de Turismo de la Nación para la categorización de Hoteles. El cálculo estructural se realizó siguiendo dos filosofías. Primeramente, se establece un cálculo siguiendo los lineamientos de las normas sísmicas INPRES CIRSOC 103/I edición 1991, INPRES CIRSOC 103/II edición 1991, además de las INPRES CIRSOC 101 edición 1982 e INPRES CIRSOC 201 edición 1996. La filosofía del diseño sísmico predominante en este marco, es el de resistencia (rotura), y se modeló la Estructura mediante el software ECALC 2004. Posteriormente se aplicaron las normas INPRES CIRSOC 103/I edición 2013, INPRES CIRSOC 103/II edición 2013, INPRES CIRSOC 101 edición 2005 e INPRES CIRSOC 201 edición 2005. Lo primero que se realiza, es el Análisis Sismorresistente a partir del Método Estático. Luego, se efectúa el Diseño por Capacidad de la estructura, develando el comportamiento estructural en rotulación (de acuerdo al mecanismo de colapso planteado). Finalmente, se hace uso de las rigideces y las armaduras determinadas para elaborar el Análisis Estático No Lineal (Norma FEMA440).

Palabras Clave

Cálculo Estructural, Normas Sísmicas.

Abstract

The architecture of the building was designed, under current regulations - Building Code, Urban and Environmental Planning Code of the city of Salta and Decrees of the Ministry of Tourism of the Nation for the categorization of Hotels. The structural calculation was carried out following two philosophies. First, a calculation is established following the guidelines of the seismic standards INPRES CIRSOC 103 / I edition 1991, INPRES CIRSOC 103 / II edition 1991, in addition to INPRES CIRSOC 101 edition 1982 and INPRES CIRSOC 201 edition 1996. The predominant seismic design philosophy Within this framework, it is that of resistance (breakage), and the Structure was modeled using the ECALC 2004 software. Subsequently, the standards INPRES CIRSOC 103 / I edition 2013, INPRES CIRSOC 103 / II edition 2013, INPRES CIRSOC 101 edition 2005 and INPRES CIRSOC 201 2005 edition. The first thing that is carried out is the Earthquake Analysis from the Static Method. Then, the Capacity Design of the structure is carried out, revealing the structural behavior in labeling (according to the proposed collapse mechanism). Finally, the stiffnesses and reinforcements determined are used to develop the Nonlinear Static Analysis (Standard FEMA440).

Keywords:

Structural Calculation, Seismic Standards.

Introducción

1. Acerca del Diseño de Arquitectura

El Diseño se planteó, a partir de un eje de simetría central (para la distribución de las habitaciones), es decir perpendicular a la Línea Municipal. Esto es, para lograr una adecuada y simplificada distribución de las habitaciones (ver Figura 1).

El Edificio consta entonces de 30 habitaciones con baño privado, dispuestas en 3 bloques. Las correspondientes al bloque N°1 y N°4, poseen una dimensión interior de 15,20 m²; ahora bien, respecto a las habitaciones del bloque N°2, estas poseen una dimensión interior de 14,00 m² (en todos los casos se respeta las dimensiones mínimas estipuladas por el código de edificación). Los 3 bloques, conforman una Estructura en forma de "U". Esto es para garantizar la iluminación y ventilación de todos los locales habitacionales del hostal, y para facilitar la circulación de las personas. Por otro lado, en el sector del Frente, se ubica la recepción, un pequeño restaurante, baños (de varones y mujeres independientemente), cocina y dormitorio de servicio en la Planta alta (con acceso independiente desde la Galería).

Se proyectó una playa de estacionamiento, para el acceso y permanencia transitoria de los vehículos de los pasajeros (en ciertos casos). Se tuvo en cuenta la aplicación de todas aquellas restricciones y normativas pautadas por los Códigos de Edificación y Planeamiento Urbano para el Diseño y ubicación de los Locales del Edificio [1], [2].

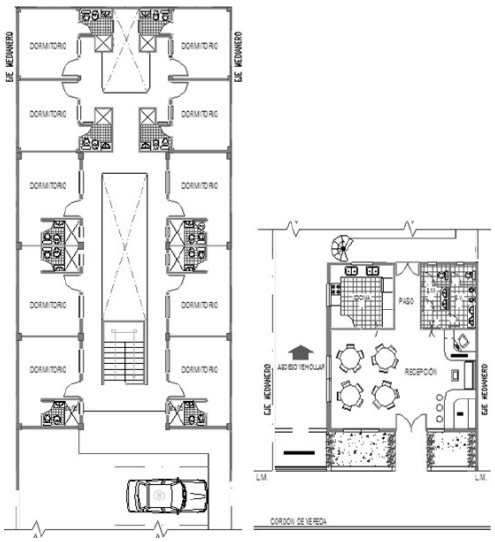


Figura 1: Planta tipo – Sector habitaciones - Recepción

2. Sobre las Acciones Sísmicas

Para la determinación de las solicitaciones sísmicas se aplicó el Método Modal Espectral a partir del programa ECALC 2004, también verificado mediante un cálculo a mano. Para ello se siguieron los lineamientos del reglamento CIRSOC 103 parte I edición 1991 [3].

Este procedimiento se basa en el análisis dinámico aproximado, en el que la respuesta de la estructura se obtiene mediante una combinación adecuada de las contribuciones modales, las cuales están caracterizadas por la máxima respuesta de cada modo afectada por los coeficientes de participación modal. Este indica la extensión en que cada modo contribuye a la respuesta total de la estructura.

2.1. Determinación de las solicitaciones sísmicas: ECALC 2004

Cálculo sísmico dinámico según Normas CIRSOC 103/I edición 1991

Método: superposición modal - dirección "X"

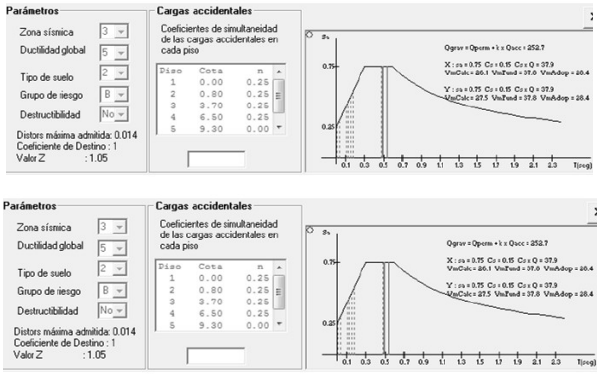


Figura 2: Parámetros para la determinación de las fuerzas sísmicas

Resultados Obtenidos:

		Piso	Cota (m)	Corte (t)	Corrim. (cm)	distor.
Corte en la base para modo fundamental:	37.8 t					
Corte en la base calculado:	28.1 t					
Corte en la base adoptado:	28.4 t	1	0.000	28.357	0.000	0.002
Pseudoaceleración modal:	0.75	2	1.000	27.990	0.034	0.009
Período modal:	0.50 seg	3	3.700	18.465	0.529	0.008
		4	6.500	2.639	0.950	0.004
		5	9.300	1.154	1.171	0.000
		6	9.470	0.000	1.172	0.000

Figura 3: Resultados del método Superposición Modal – Dirección X

2.2. Solicitaciones Sísmicas obtenidas - Método Dinámico Modal Espectral

Se consideró un modelo de 3 modos de vibración.

Esquema de cálculo (ver Figura 4)
Resultados obtenidos: Diagramas de corte en ambas direcciones (ver Figura 5)

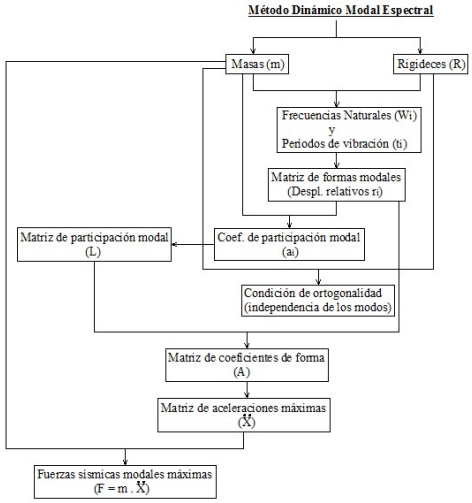


Figura 4: Esquema de Cálculo

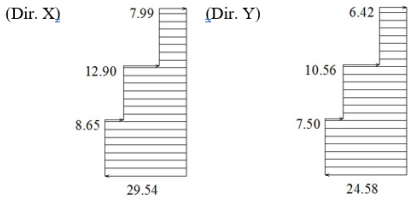


Figura 5: Diagramas de Corte

2.3. Solicitaciones Sísmicas obtenidas - Método Estático Equivalente

Se determinarán aquí las acciones globales de la Estructura en término de acciones
y deformaciones aplicando el Reglamento Argentino para Construcciones
Sismorresistente INPRES CIRSOC 103, Parte I, Construcciones en General, Año 2013 [4].
El análisis se realiza en dos direcciones independientemente y se supone que tanto los desplazamientos como los movimientos torsionales en cada dirección están desacoplados, es decir, que no influyen mutuamente.
Este método se basa en la simplificación de considerar la plastificación de la estructura por medio de un factor de modificación de la respuesta R, aplicado al espectro de diseño elástico.
Esto supone que la estructura puede plastificar más o menos uniformemente en toda su extensión.
Esquema de cálculo:
se muestra en la Figura 6

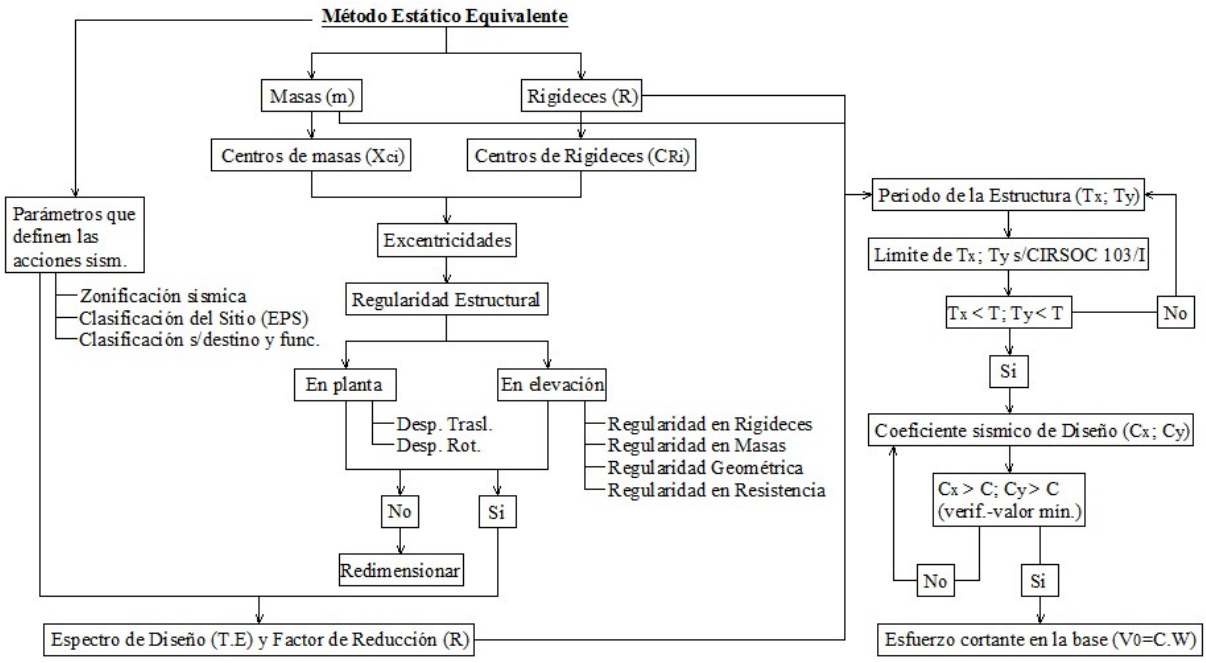


Figura 6: Esquema de Cálculo

Los resultados obtenidos se muestran en la Figura 7, en donde se observa que Dirección X = Dirección Y

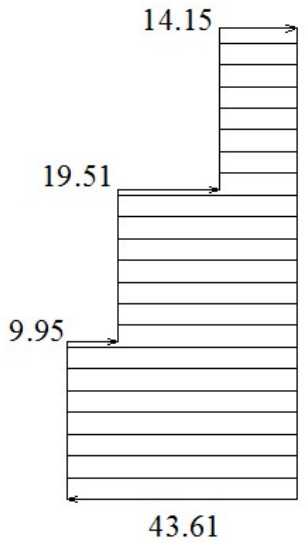


Figura 7: Diagrama de Corte

Verificación de la distorsión horizontal de piso (ver Figura 8):

Dirección "x"

NIVEL 1	θ_{skx}= (d_{ubk} - d_{ubk-1})/h_{sk} = Δ_{sk}/h_{sk}	0.006	<	0.015	verifica
NIVEL 2	θ_{skx}= (d_{ubk} - d_{ubk-1})/h_{sk} = Δ_{sk}/h_{sk}	0.000	<	0.015	verifica
NIVEL 3	θ_{skx}= (d_{ubk} - d_{ubk-1})/h_{sk} = Δ_{sk}/h_{sk}	0.000	<	0.015	verifica

Dirección "y"

NIVEL 1	θ_{skx}= (d_{ubk} - d_{ubk-1})/h_{sk} = Δ_{sk}/h_{sk}	0.001	<	0.015	verifica
NIVEL 2	θ_{skx}= (d_{ubk} - d_{ubk-1})/h_{sk} = Δ_{sk}/h_{sk}	0.000	<	0.015	verifica
NIVEL 3	θ_{skx}= (d_{ubk} - d_{ubk-1})/h_{sk} = Δ_{sk}/h_{sk}	0.000	<	0.015	verifica

Figura 8: Verificación de Dirección "x" e "y"

3. Acerca del Modelado

En esta etapa se realiza el modelo en un software representando la estructura del edificio para efectuar sobre el mismo el análisis estructural. El programa que se utiliza es el ECALC 2004, el cual se basa en la aplicación del método de rigidez matricial.

Es fundamental que el modelo sea lo más representativo posible a la realidad, ingresar de manera correcta los datos, y tener una idea aproximada de los resultados a obtener para evitar confusiones. Se analiza en 2 direcciones ortogonales el comportamiento del edificio frente a los estados límites últimos, el longitudinal (eje y) y el transversal (eje x); respecto de la dirección "x" se distribuyen 4 pórticos, y en la dirección "y" se dispuso de dos pórticos.

El método de análisis sísmico será el método modal espectral, que consiste en esquematizar la acción sísmica a partir de un valor calculado por la superposición modal; es aplicable a estructuras de configuración regular de distribución de rigideces y masas tanto en planta como en altura y con influencia en los modos de vibración.

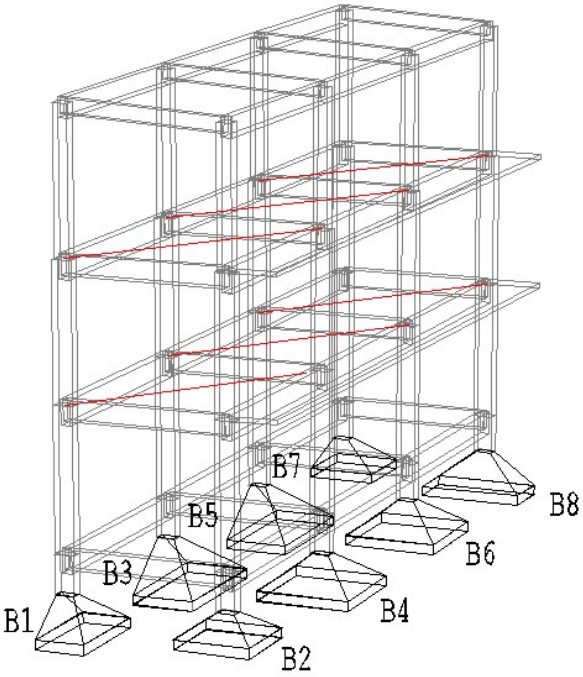


Figura 9: Modelo Estructural del Bloque N°1

4. Diseño Alternativo

Para modelar el bloque nº 1 (ver Figura 10) se utilizó el Software SAP 2000, tanto para la obtención de los esfuerzos que lo solicitan como para la realización de los análisis no lineales.

4.1. Reglamentos utilizados:

Reglamento CIRSOC 101-2005 [5]: Cargas permanentes y sobrecargas mínimas de diseño para edificios y otras estructuras.

Reglamento CIRSOC 101-1982 [6]: Cargas y Sobrecargas Gravitatorias para el Cálculo de las Estructuras de Edificios.

Reglamento CIRSOC 201-2005: Estructuras de Hormigón Armado.

Reglamento INPRES CIRSOC 103-2013: Construcciones sismorresistentes Parte I y Parte II.

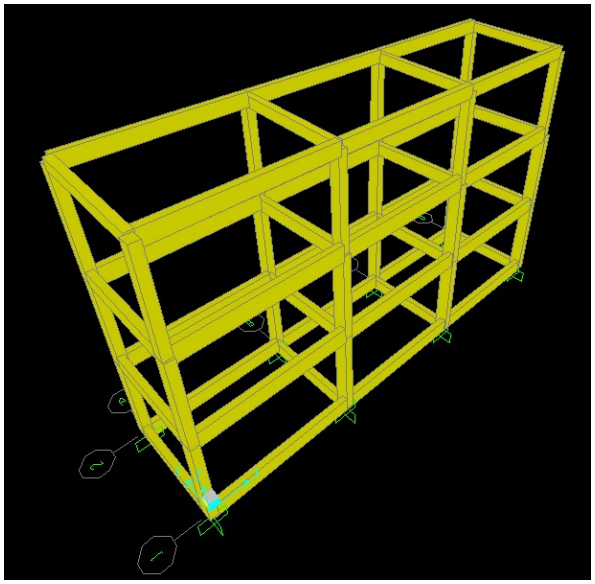


Figura 10: Estructura modelada en SAP2000

4.2. Cálculo Estructural aplicando el Método de Diseño por Capacidad

Primeramente, se definió un mecanismo de colapso que determina las zonas del sistema sismorresistente, que tendrán incursiones plásticas severas. Esas zonas se diseñaron y detallaron apropiadamente para que disipen energía bajo deformaciones inelásticas severas. Por otro lado, se diseñaron los sectores de los elementos que no se rotulan para que tengan la suficiente resistencia para asegurar su comportamiento elástico mientras las fuentes de disipación de energía desarrollan toda su capacidad.

4.3. Mecanismo de Colapso propuesto:

En ambas direcciones se forman rótulas en los extremos de vigas y base de columnas.

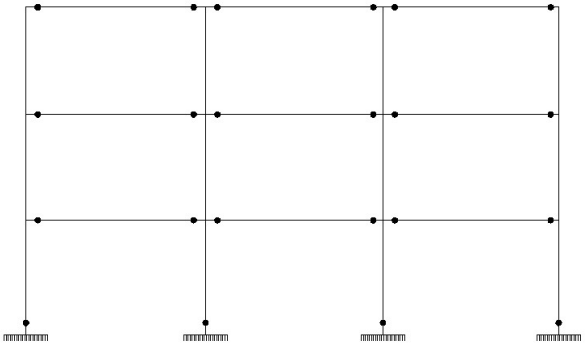


Figura 11: Mecanismo de colapso adoptado

Esquema de cálculo

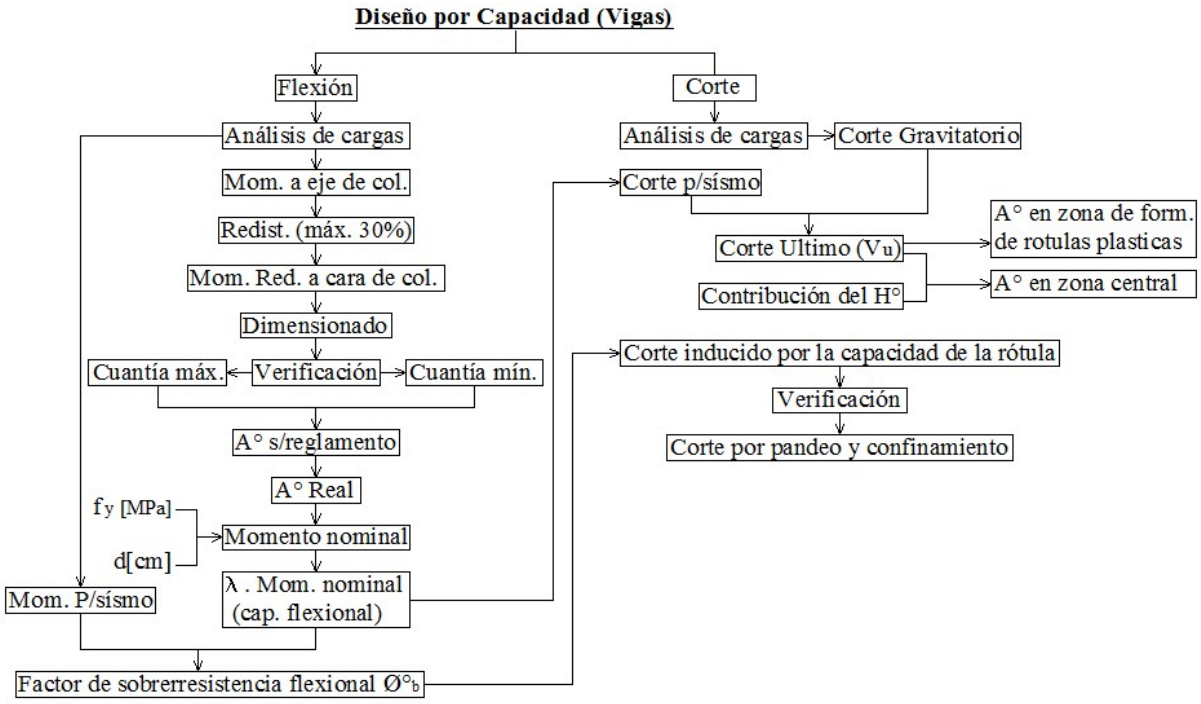


Figura 12: Esquema de cálculo

Para el diseño por capacidad de las columnas, es importante destacar que las solicitaciones de diseño para zonas donde se prevé la formación de rótulas plásticas, serán distintas que las correspondientes al resto de las columnas. En este caso, solo se deberá tener en cuenta esto en las columnas de la planta baja, ya que son las únicas que se van a rotular en la base.

En el primer caso, los momentos a considerar provienen de la combinación de estados de cargas más desfavorables; el corte de diseño se lo obtiene en función de la capacidad de sobrerresistencia de las rótulas que se forman en la columna; el cálculo del esfuerzo axial de diseño es indistinto para las columnas en donde se prevé o no la formación de rótulas plásticas y se calcula teniendo en cuenta el esfuerzo axial inducido por la sobrerresistencia flexional de las rótulas de todas las vigas considerando además las cargas gravitatorias. Por otro lado, en el resto de las columnas y capitel de las de planta baja, para la determinación de momentos de diseño, incidirá el factor de amplificación dinámica (que depende del período fundamental de la estructura), el factor de sobrerresistencia flexional de las vigas, el momento debido al sismo y el corte de diseño para dichas columnas. Con respecto al corte, éste estará en función del corte debido al sismo y al factor de resistencia flexional de las vigas.

Resultados Obtenidos (ver Figura 13)

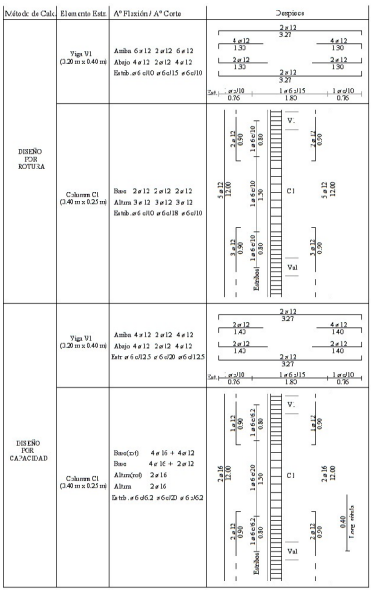


Figura 13: Resultados obtenidos

5. Resultados del PUSHOVER

$\Delta roof = 3\% He = 32\ cm$ (según Norma FEMA 440)

Al someter al bloque a las acciones del empuje lateral se observó un buen comportamiento global de la estructura, generándose las rótulas según el mecanismo de colapso seleccionado. A su vez las que se formaron no alcanzaron un grado de deformación que pueda llevar el edificio a la ruina.

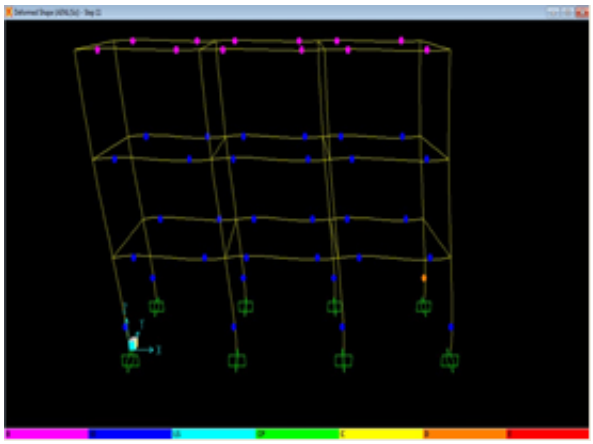


Figura 14: Comportamiento de la estructura – Empuje lateral según X

En los primeros pasos se comienzan a formar rótulas en las vigas del nivel más bajo subiendo hacia los pisos de arriba. También comienzan a aparecer las primeras rótulas en columnas de planta baja, en el sentido de aplicación de la carga lateral.

Se puede apreciar como continúan apareciendo rótulas hacia el último nivel, además se observa como el grado de deformación de las rótulas ya presentes, se va incrementando, desde el nivel inferior hacia arriba. Esto significa que existe una continua disipación de energía en la estructura de los elementos más débiles hacia los más fuertes; que es justamente lo que se pretende.

Se puede ver que solo las columnas de planta baja se rotulan, respetando el mecanismo de colapso adoptado al inicio del diseño por capacidad. Lo cual refleja que el bloque se comporta de manera apropiada ante las solicitaciones inducidas por el empuje lateral aplicado.

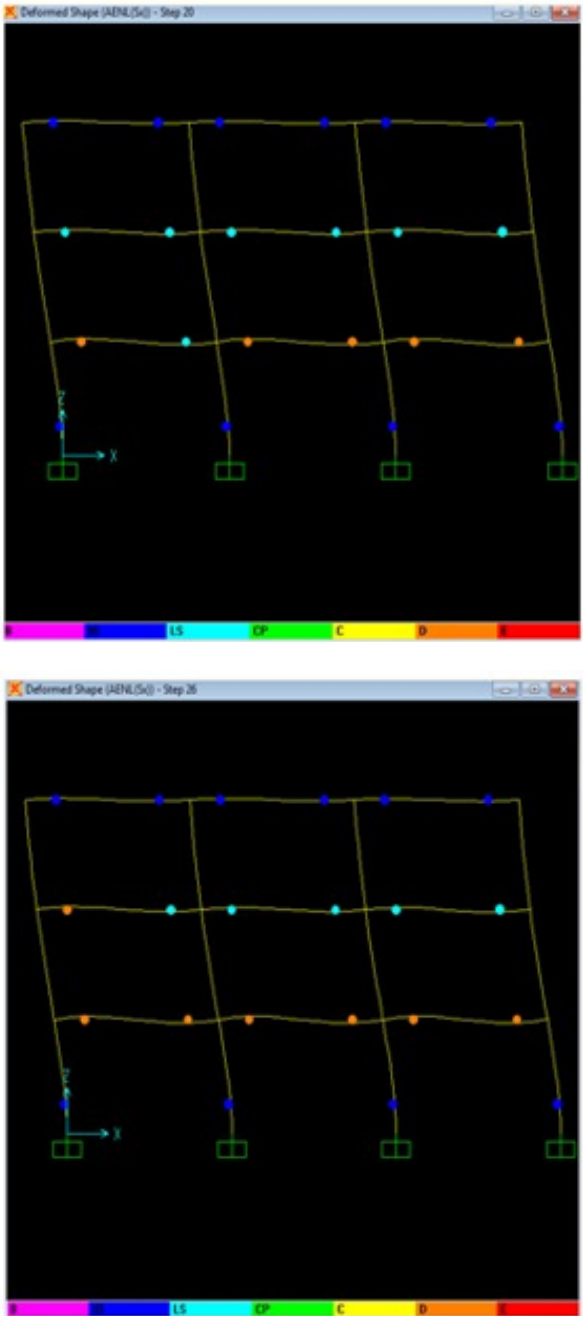


Figura 15: Secuencia de formación de rotulas plásticas – Step 20-26

El paso 26 representa el final de la secuencia de formación de rotulas plásticas, aquí el programa detiene el proceso iterativo, ya que se alcanzó el máximo desplazamiento estipulado por el usuario. Como podemos observar en la última imagen, no se produce el colapso de la estructura.

5.1. Comportamiento de la estructura diseñada por rotura

$\Delta roof = 3\% \; He = 32 \; cm$ (según Norma FEMA 440)

Realizando una comparación con el proceso de rotulación de la estructura diseñada por capacidad, respecto a la misma diseñada por rotura, se observa que, si bien ésta rotula con un mecanismo de colapso aceptable, la deformación alcanzada en las rótulas es mucho mayor que en el diseño por capacidad, mostrando así una menor capacidad de disipar energía.

Para tener una idea más apropiada de lo que sucede se mostrará a continuación una imagen del estado de la estructura diseñada por rotura al final de la secuencia de formación de rotulas plásticas.

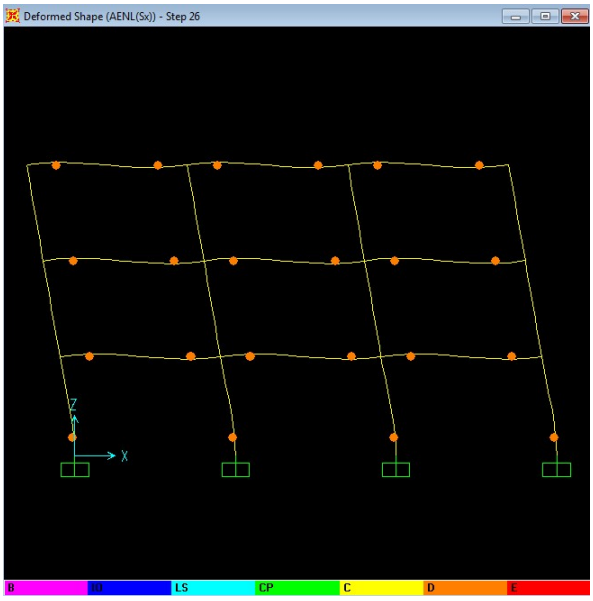


Figura 16: Estado final de rotulación – diseño por Rotura – Step 26

Como se puede apreciar, el grado de deformación de las rótulas es elevado en todos los elementos de la estructura. Ya no se cuenta con la reserva estructural que se tenía en las columnas de planta baja en el diseño por capacidad, recordando que, para ese caso, en la finalización de la secuencia de rotulación, las rótulas solo se deformaban hasta el valor IO (la parte azul de la escala).

6. Conclusiones

La aplicación del software de cálculo ECALC 2004, nos permite reemplazar sistemas de pórticos planos por espaciales. Se abandona

aquí el concepto de estructura plana con el flujo de tensiones a través de vigas y columnas de sección limitada, por estructuras con el flujo de tensiones repartido en superficies más amplias, las que al distribuirse en una zona mayor tienen una reducción de los valores unitarios y permiten obtener un notable ahorro de material.

El comportamiento de la edificación diseñada por capacidad refleja la facultad de disipación de energía de la misma, por medio de la formación de las rótulas plásticas. Durante los análisis no lineales realizados se observó que cuando la edificación alcanza su punto de desplazamiento máximo estipulado, las rótulas plásticas se formaron primero en las vigas, por lo tanto, se concluye que la edificación cumple con el criterio columna fuerte - viga débil.

Se observa que con el análisis no lineal se obtienen mecanismos de colapso exactamente iguales para el edificio diseñado por capacidad y por rotura. Con la diferencia de que, para el primer caso, el grado de deformación alcanzado en las rotulas plásticas, es mucho menor.

Comparación de las dos ediciones del reglamento CIRSOC 103/I:

La influencia del sitio de emplazamiento de la construcción en el reglamento 103/2013, impacta a diferencias del reglamento 103-1991 (que tenía en cuenta un solo factor de amplificación aplicable a la zona del espectro controlada por la velocidad) no sólo en la zona controlada por la velocidad de la onda de corte, sino también en la zona controlada por la aceleración, dando lugar entonces a los coeficientes Ca y Cv. Los mismos no solo son función del sitio, sino también del nivel de peligrosidad sísmica de la zona.

Críticas respecto al nuevo reglamento 103-2013: el periodo fundamental depende sólo de la rigidez de las componentes estructurales, y varía mucho si se trabaja con rigideces basadas en secciones brutas o en secciones agrietadas reglamentarias. De cualquier manera, se supone que conocidas las dimensiones de la estructura se conoce su periodo fundamental, esto es, la rigidez es independiente de la resistencia. Sin embargo, en el caso de estructuras que van a incursionar en el campo inelástico, esta suposición es inválida.

Referencias Bibliográficas

[1] Municipalidad de la Ciudad de Salta, s. d. (2017). *Código de Edificación* de la Ciudad de Salta

[2] Municipalidad de la Ciudad de Salta, s. d. (2017). *Código de Planeamiento Urbano y Ambiental* de la Ciudad de Salta

[3] INTI. (1991). *INPRES-CIRSOC 103 Normas Argentinas Para Construcciones Sismoresistentes.* Buenos Aires: INTI.

[4] INTI. (2013). *INPRES-CIRSOC 103 Reglamento Argentino para Construcciones Sismoresistentes*. Buenos Aires: INTI.

[5] INTI. (2005). *INPRES-CIRSOC 201 Reglamento Argentino de Estructuras de Hormigón Armado.* Buenos Aires: INTI.

[6] INTI. (1982). *INPRES-CIRSOC 101 Cargas y Sobrecargas Gravitatorias para el Cálculo de las Estructuras de Edificios.* Buenos Aires: INTI

Avances en las Interfaces Cerebro - Máquina

Joaquín A. Macaroff Pérez
jomax1398@gmail.com

Grupo IDEAS, Facultad de Ingeniería, UCASAL

Resumen

Imagine un mundo en el cual los seres humanos sean capaces de mover a voluntad las prótesis que necesiten, controlar los dispositivos móviles sin necesidad de "tocarlos", manipular un vehículo no tripulado desde la distancia como si fuese una extensión del cuerpo, detectar la falla que tiene algún dispositivo solo con hacer contacto físico; únicamente utilizando el poder de sus mentes y que además puedan recibir estímulos, de los elementos o programas que manipulen, para lograr tomar el mejor curso de acción. Suena a ciencia ficción ¿verdad?... pero resulta que ya existen diversas investigaciones que pueden convertir esta "ciencia ficción" en una realidad.

Las interfaces cerebro-máquina constituyen un conjunto de diversas tecnologías que permiten establecer un diálogo entre el hombre y la máquina, haciendo uso de las señales eléctricas producidas por el cerebro. Para abreviarlo se utiliza la nomenclatura anglosajona BMIs (brain-machine interfaces) y son el principal foco de estudio para intentar hacer realidad las ideas anteriormente expuestas.

Este trabajo busca como principal objetivo brindar conocimientos generales acerca de las BMIs para despertar el interés en el tema, que podría servir de guía para realizar futuros proyectos de investigación relacionados con el tema.

Palabras Clave

BMI, Interfase cerebro-máquina.

Abstract

Imagine a world in which human beings are able to move the prostheses they need at will, control mobile devices without having to "touch" them, manipulate an unmanned vehicle from a distance as if it were an extension of the body, detect failure who has a device just by making physical contact; only using the power of their minds and that they can also receive stimuli, from the elements or programs that they manipulate, in order to take the best course of action. It sounds like science fiction, right? ... but it turns out that there are already various investigations that can turn this "science fiction" into a reality.

Brain-machine interfaces constitute a set of various technologies that allow a dialogue between man and machine to be established, making use of the electrical signals produced by the brain. For short, the Anglo-Saxon nomenclature BMIs (brain-machine interfaces) are used and they are the main focus of study to try to make the above ideas come true.

The main objective of this work is to provide general knowledge about BMIs to awaken interest in the subject, which could serve as a guide to carry out future research projects related to the subject.

Keywords:

BMI, Brain-machine interface

Introducción

Las interfaces cerebro-máquina, en inglés brain-machine interfaces (BMIs) son tecnologías en desarrollo que emplean los continuos avances realizados en el campo de la neurociencia y ciencias de la computación para captar la actividad cerebral, interpretarla y poder transmitir la información obtenida a algunos dispositivos y probablemente también a medios virtuales que tengan algún impacto en el mundo externo (el que nos rodea), es decir, que el usuario pueda interactuar con los mismos a través de algún estimulo producido por sus pensamientos y pueda corregir el accionar de estos dispositivos mientras los usa, conforme a los resultados obtenidos.

El término BMIs fue acuñado por Jacques J. Vidal (1973) en [1], quien las describió a las BMIs como "formas de utilizar las señales cerebrales en un diálogo hombre-computadora" y "como un medio de control sobre procesos externos tales como computadoras o dispositivos protésicos". Por otra parte, en [2] se presentan la historia de las BMIs en 4 etapas principales: el origen, los pioneros, el surgimiento de un nuevo campo de investigación y la historia moderna.

En la actualidad, toda la comunidad científica acepta el hecho de que el cerebro emite señales eléctricas en variadas frecuencias que son conocidas como ondas cerebrales [3]. Estas frecuencias se clasifican en ondas Gamma, Beta, Alpha, Theta y Delta; las mismas se pueden presentar en diversas situaciones en las que se ve envuelta nuestra actividad cerebral de acuerdo con cómo se indica en la Figura 1.

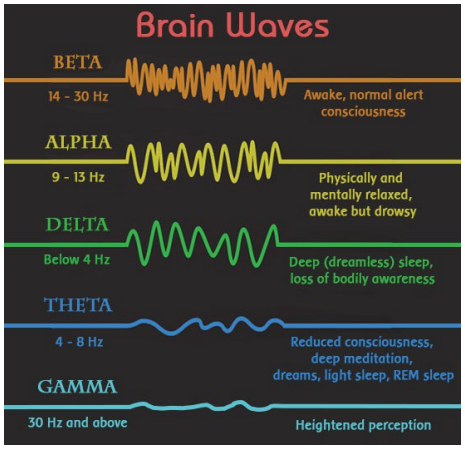


Figura 1: Actividad Cerebral

Las interfaces cerebro-máquina tiene el potencial de ayudar a las personas con una amplia gama de trastornos clínicos. Por ejemplo, se ha demostrado el control neuroprotésico humano de cursores informáticos [4], las extremidades robóticas o sea aquellos dispositivos que cumplen las mismas funciones, apoyando las actividades diarias del individuo [5] y los sintetizadores de voz que permiten la producción artificial del habla [6] utilizando no más de 256 electrodos que conectan al cerebro con dicha tecnología.

A medida que aumenta la comprensión de los aspectos neurocientíficos del cerebro, es probable que la tecnología vaya más allá del ámbito de las funciones motoras, tal vez, ayudando con la recuperación de la memoria, la toma de decisiones y algún otro tipo de funciones cognitivas como pueden ser la de orientación, las gnosias (capacidad que tiene el cerebro para reconocer información previamente aprendida como pueden ser objetos, personas o lugares a través de nuestros sentidos), entre otras.

De lo anteriormente expuesto, se puede deducir que las aplicaciones para las BMIs se encuentran limitadas por la imaginación humana y por el desarrollo de nuevas tecnologías producidas gracias al continuo avance de las investigaciones que se realizan sobre las mismas.

Este campo tiene un gran potencial de impacto social dado que puede mejorar la calidad de vida de las personas, pero existen serias preocupaciones éticas que se deben considerar [7] como la privacidad, la responsabilidad, identidad personal, el ámbito legal, entre otros.

Independientemente de lo que depare el futuro, las BMIs están marcando un camino en los campos de estudios en constante expansión de la neurociencia, la tecnología y la informática.

Este trabajo consta de 3 secciones, en la Sección 1 se explica el funcionamiento básico de una interfaz cerebro-máquina y luego en la Sección 2 se exponen las formas en las que se obtienen las señales producidas por la actividad cerebral, formas que muchas veces dan el nombre a las BMIs (BMIs invasivas, BMIs semiinvasivas o BMIs no invasivas) para finalmente en la Sección 3 brindar las conclusiones obtenidas acerca del trabajo realizado.

2. ¿Cómo Funciona?

El propósito de la BMIs es detectar y cuantificar las características de las señales cerebrales que indican las intenciones del usuario y traducirlas simultáneamente al lenguaje manejado por los dispositivos externos para que cumplan con la intención del usuario. La forma en la que esto se lleva a cabo se puede apreciar en la gráfica de la Figura 2 en la cual se muestran los equipos y etapas propias de las BMIs.

Por lo tanto, todo equipo y componente que forman parte de una interfaz cerebro-máquina se integra principalmente por sensores, decodificador y efectores o actuadores [8], los cuales se describen brevemente:

Sensores: son dispositivos que captan magnitudes físicas, en este caso variaciones eléctricas. Los sensores que usan las BMIs son dispositivos formados por electrodos que se encargan de captar la información procedente de la actividad cerebral en forma de señales digitales que puedan ser procesadas por ordenadores. Esta actividad cerebral puede involucrar un conjunto local de neuronas individuales o agregados de cientos, miles o millones de neuronas simultáneamente.

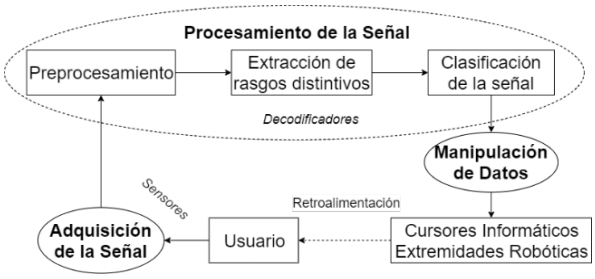


Figura 2: Etapas y equipos involucrados en las BMIs

Decodificadores: son algoritmos matemáticos encargados de procesar, filtrar el ruido y amplificar la señal obtenida por los sensores derivados del proceso neurofisiológico que refleja la intención del usuario. Estos componentes son esenciales para lograr garantizar el correcto funcionamiento de una interfaz cerebro-máquina.

Efectores o actuadores: son dispositivos que reflejan cual es la forma en la que interactúa el usuario con el entorno mediante las BMIs (prótesis, brazo robótico, cursores informáticos). Y además debe contemplar tres secuencias o etapas esenciales [9] tal y como se muestran en la Figura 2:

1° Secuencia: Adquisición de señal

El proceso de adquisición de señal requiere la obtención de las señales eléctricas procedentes del cerebro. Estas señales pueden ser registradas desde el cuero cabelludo, la superficie del cerebro o desde la actividad neuronal. Dado que la intensidad de las señales capturadas suele ser bajas, se necesita amplificarlas. Luego, para poder ser comprendidas por alguna aplicación del ordenador se las deben digitalizar. (Por ejemplo, registrar la señal de tomar un vaso de agua procedente de la actividad cerebral de un determinado sujeto).

2° Secuencia: Procesamiento de la señal

En esta etapa, las señales obtenidas de la secuencia anterior son analizadas y procesadas para obtener las señales de control. El procesamiento de la señal puede realizarse a través de las siguientes suboperaciones:

Preprocesamiento: La primera parte del procesamiento de la señal consiste en preparar el registro de la señal digital a procesar como una mejora para hacer que las características sean más claras de detectar. Algunas técnicas de filtrado pueden ser aplicadas. (Siguiendo con el ejemplo, se debe garantizar que las condiciones sean las adecuadas, preparando previamente al sujeto para que no se distraiga con algún otro evento)

Extracción de rasgos distintivos: Consiste en extraer señales con rasgos específicos. En general los sensores (como por ejemplo el EEG) registran no solo cierta señal eléctrica del cerebro, sino que también varias señales no deseadas. Esas señales no deseadas pueden sesgar (alterar) el análisis del sensor, obteniendo información errónea. Por lo tanto, las señales digitales se encuentran sujetas a los procedimientos de extracción. (Separar las señales procedentes de los demás sentidos para que se registren solo aquellas relacionadas con mover, agarrar y levantar el vaso para poder tomar agua)

Clasificación de la señal: algoritmo de traducción. En esta operación, un algoritmo de traducción, se ocupa de traducir la información obtenida a un lenguaje entendible por los dispositivos externos (efectores o actuadores) que cumplen la intención del usuario. Las señales son clasificadas en las diferentes frecuencias y formas que presentan; un algoritmo de clasificación puede utilizar métodos lineales o no lineales. (Esa señal es traducida por medio de un programa para que, por ejemplo, un brazo robótico pueda cumplirla).

3° Secuencia: Manipulación de datos

Una vez que las señales son clasificadas, la salida es manipulada para que se adapten a los efectores o actuadores. Estos proporcionan retroalimentación creando un bucle de control que cierra el ciclo. (Es decir, se operan esas instrucciones para que lleguen correctamente al brazo robótico en todo momento y para que no ocurra algún inconveniente).

La retroalimentación sensorial es muy importante para el control del movimiento. En las BMIs básicas la única retroalimentación que reciben los usuarios es la visual. Sin embargo, se ha demostrado que se puede utilizar un enfoque basado en el aprendizaje para proporcionar una señal más intensa de retroalimentación sensorial artificial [10]. Esto siguiere una nueva estrategia para restaurar la propiocepción a quienes utilizan las BMIs.

En el presente trabajo no se abordará este aspecto particular de las BMIs, aunque si se reconoce la complejidad de los componentes tecnológicos requeridos para que las BMIs puedan cumplir estas funciones.

3. Formas en las que se obtienen las señales eléctricas producidas por el cerebro

Hasta aquí se describió cómo funcionan las BMIs básicas; se aborda ahora abordaremos el análisis de la secuencia de adquisición de señal para entender cuáles son las diversas maneras que existen actualmente para obtenerlas.

La actividad neuronal se puede resumir como el movimiento de las cargas eléctricas que producen campos eléctricos y magnéticos debido a la interacción que ocurre entre las millones de neuronas que conforman el sistema nervioso. Las interfaces cerebro-máquina intentan detectar esa actividad cerebral, generada por ciertos estímulos, empleando los sensores adecuados, los que se conectan cerca de determinadas regiones del cerebro y facilitan la detección de los campos eléctricos y magnéticos para su posterior análisis.

Se emplean diferentes métodos para obtener las señales emitidas por el cerebro. Se dividen en invasivos, semi-invasivos (indicados por [11] y [12]) y no invasivos (según lo dicho por [13]) dependiendo de la capa del cerebro de donde se desee adquirir la señal. Esto se observa en la Figura 3 que muestra la relación entre los distintos métodos de obtención de señales y la capa del cerebro donde se toman los datos.

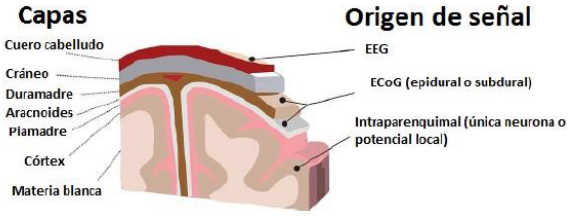


Figura 3: Señales y Capas del Cerebro Fuente: [13]

A continuación, se explican brevemente cada uno de estos métodos señalados.

Métodos invasivos

Los métodos invasivos requieren intervención quirúrgica dado que los electrodos deben estar en contacto directo con el cerebro para obtener la mejor calidad de señal en el área de córtex o materia blanca del mismo. Este tipo de intervención se suele utilizar en personas que sufren de parálisis o también podría utilizarse para restaurar la visión conectando el cerebro con cámaras externas.

Pese a presentar la mejor calidad de señal, los riesgos clínicos que tiene tal cirugía para el individuo lo hacen el método menos común y con mayores consecuencias adversas utilizado por las BMIs.

Métodos semi-invasivos

Los electrodos son implantados en el cráneo, pero afuera del cerebro. La electrocorticografía (ECoG) usa la misma tecnología que los EEG,

pero los electrodos están incrustados en una delgada almohadilla de plástico que se coloca por encima de la corteza.
Con este método se logra una buena calidad de señal, pero significativamente menor a la obtenida por los métodos invasivos. La ventaja es que no requieren de una intervención quirúrgica tan compleja por lo que el riesgo clínico es mucho menor.

Métodos no invasivos
Para adquirir las señales no se requiere ningún tipo de intervención quirúrgica dado que las mismas se obtiene con elementos que actúan por encima del cuero cabelludo por tal motivo las señales registradas no son tan precisas en comparación a los dos métodos anteriores.
Una de las formas más utilizadas para lograr la implementación de las interfaces cerebro-máquina es la electroencefalografía o el electroencefalograma (EEG – Electroencephalography), método de monitorización electrofisiológico que registra la actividad eléctrica del cerebro, a través de electrodos colocados directamente sobre el cuero cabelludo con ayuda de un gel líquido conductor, de modo que tome las medidas correspondientes a la actividad eléctrica presente en una amplia superficie del cerebro. Este es el más utilizado, dado que el montaje necesario para realizar las mediciones de las señales es sencillo, barato y los resultados que otorga son los suficientemente buenos para una gran parte de las aplicaciones que se pueden desempeñar con las BMIs. Algunos dispositivos como el casco Mindwave [14] constituyen alternativas más económicas basadas en la electroencefalografía.
Otro método no invasivo y de gran interés es la imagen por resonancia magnética funcional (fMRI - Functional Magnetic Resonance Imaging). Su funcionamiento se basa en el análisis de los cambios que se producen en el flujo de la sangre en el cerebro, teniendo siempre presente que el comportamiento de este flujo está ligado a la actividad cerebral. Para ello, se evalúa el diferente comportamiento magnético entre la sangre rica en oxígeno y la sangre pobre en oxígeno y volumen de sangre en ciertas zonas del cerebro. Para poder realizar estos análisis se hace uso de los escáneres basados en las propiedades de la resonancia magnética nuclear.
También cabe destacar como alternativa no invasiva la magnetoencefalografía (MEG Magnetoencephalography), que consiste en el análisis de la actividad magnética del cerebro a partir del fenómeno de la inducción magnética.
Los procesos neurofisiológicos que producen las señales analizables mediante MEG son los mismos que permiten un análisis mediante EEG. Las ventajas de MEG respecto de EEG se deben a que los campos magnéticos son menos afectados por el cuero cabelludo y huesos que los campos eléctricos, produciendo una mejor adquisición de señales. Sin embargo, el uso de MEG es poco viable debido al equipamiento electrónico necesario para realizarla.
Hasta aquí se expuso lo que se investigó y entendió respecto de cómo capturar la señal eléctrica neuronal y dejarla a disposición para procesarla e interpretarla mediante distintas tecnologías propias de las BMIs, pero no fue posible entender las formas en que estas señales pueden "volver" a la persona para que esta pueda tomar decisiones que permitan una mejor calidad de vida. El tema es muy complejo, y se debe avanzar detalladamente en las temáticas enunciadas para poder llegar a entender las BMIs en esta que sería su fase final.

4. Conclusión
Existen diversas líneas de investigación incipientes en las que se destacan los problemas éticos, el procesamiento de las señales, la manipulación de datos, las formas de lograr una retroalimentación efectiva, la aplicación de las BMIs para detectar fallas en alguna máquina, la implementación adecuada de BMIs para controlar un brazo protésico, la simulación de sentidos como podría ser el del tacto, el uso de inteligencia artificial (IA) para el apoyo de las BMIs, entre otros.
La tecnología de las BMIs cada vez está tomando mayor relevancia en el mundo. Existen empresas, universidades y grupos de investigadores que invierten una gran suma

de dinero y tiempo para seguirlas explorando y lograr una implementación adecuada de las mismas como es el caso de Neuralink y Facebook [15] o Brain and Cognitive Sciences research lab MIT, Biomedical Functional Imaging and Neuroengineering Laboratory of Carnegie Mellon University o The University of Tokyo, JP, Life Science Center of TARA [16].

No sería sorpresa que en los próximos años este tipo de tecnologías se conviertan en uno de los principales temas de investigación en el mundo debido a los grandes cambios que promete.

Luego de lo expuesto en el presente trabajo, como proyecto futuro se pretende investigar y avanzar en el estudio profundo de estas tecnologías para lograr implementar en su totalidad una interfaz cerebro-máquina básica que permita controlar un brazo protésico desarrollando o utilizando un sensor basado en EEG. También es intención avanzar en la investigación para desarrollar otras formas en las que se logre obtener una retroalimentación efectiva que apoye al funcionamiento de las BMIs, y de ser posible, lograr que por ejemplo al utilizar la prótesis de un brazo mediante las BMIs sea posible sentir la textura del objeto que se agarre o el calor que transmite para actuar en consecuencia, es decir, simular el sentido del tacto.

Una vez logrado un avance importante sobre lo dicho, la investigación puede continuar con la reducción o eliminación de los elementos físicos como los cables involucrados en las BMIs, de manera que su uso resulte más cómodo para el usuario.

Será un trabajo apasionante que demandará mucho tiempo, esfuerzo, recursos e investigaciones; existirán instancias para trabajar de forma colaborativa con otras universidades o instituciones interesadas en el tema y de seguro arroje diversos resultados prometedores acerca del desarrollo de las BMIs en la Argentina.

Este trabajo se elaboró en el Grupo IDEAS, de la Facultad de Ingeniería de la UCASAL, espacio creado para el desarrollo de capacidades de investigación e innovación, en aquellos alumnos interesados en estas actividades.

Referencias Bibliográficas

[1] Jacques J. Vidal, «Toward Direct Brain-Computer Communication,» *Annual Review of Biophysics and Bioengineering*, vol. 2, pp. 157-180, 1973.

[2] C. S. Nam, A. Nijholt and F. Lotte, "Introduction: Evolution of Brain-Computer Interfaces," Francis (CRCPress), 2018.

[3] GLOOM, «Mental Health Daily,» 15 04 2014. [En línea]. Available: https://mentalhealthdaily.com/2014/04/15/5-types-of-brain-waves-frequencies-gamma-beta-alpha-theta-delta. [Último acceso: 28 08 2019].

[4] T. Aflalo, «Decoding motor imagery from the posterior parietal cortex of a tetraplegic human,» *Science*, p. 906–910, 2015.

[5] C. I. Penaloza and S. Nishio, "BMI control of a third arm for multitasking," Science Robotics, 2018.

[6] G. K. Anumanchipalli, J. Chartier y E. F. Chang, «Speech synthesis from neural decoding of spoken sentences,» *Nature 568*, p. 493–498, 2019

.

[7] U. Asgher, N. S. Naz, K. Sardar, K. Sardar, Mehjabeen y A. Raza, «Ethical Issues of Brain-Computer Interface,» *IJCSNS*, vol. 18, nº 5, pp. 21-27, 2018.

[8] A. M. ASTOBIZA, T. AUSÍ, M. T. R. M. FERRER, M. A. PAYÁ y D. LÓPEZ, «Traducir el pensamiento en acción: Interfaces cerebro-máquina y el problema ético de la agencia,» *Revista de Bioética y Derecho*, nº 46, pp. 29-46, 2019.

[9] Rabie A. Ramadan, S. Refat, Marwa A. Elshahed y Rasha A. Ali, «Chapter 2 Basics of Brain Computer Interface,» 2017.

[10] O. J. S. P. Dadarlat MC, «A learning-based approach to artificial sensory feedback leads to optimal integration,» *Nat Neurosci*, nº 18, p. 138–144, 2015.

[11] Z. Koudelková y M. Stmiska, «Introduction to the identification of brain waves based on their frequency,» de *MATEC Web of Conferences 210*, 2018.

[12] «NeurotechEDU – Educational Materials for Neurotechnology,» [En línea]. Available: http://learn.neurotechedu.com/introtobci/#top-of-page. [Último acceso: 29 08 2019].

[13] Á. M. García, «Diseño de interfaces cerebro-máquina controlados mediante registros de EEG,» de 2.2.3. *Adquisición de señales*, Madrid, Escuela Politécnica Superior – Universidad Autónoma de Madrid, 2015, pp. 22-23.

[14] «Neurosky,» [En línea]. Available: https://store.neurosky.com/pages/mindwave. [Último acceso: 1 09 2019].

[15] GARFIELD BENJAMIN, 09 2019. [En línea]. Available: https://elpais.com/tecnologia/2019/08/23/actualidad/1566558959_777866.html.

[16] Jeff Coleman, «Medium,» 04 08 2018. [En línea]. Available: https://medium.com/@askwhy/brain-computer-interface-with-artificial-intelligence-and-reinforcement-learning-9c94b0454209. [Último acceso: 1 09 2019].

Diseño de un sistema de gestión de la seguridad informática para entorno de teletrabajo para el Instituto de Educación Superior N°2 Humahuaca- Jujuy

Ricardo C. Corimayo
ricardo_corimayo@yahoo.com.ar

Diplomatura en Seguridad de la Información Aplicada a Entornos Virtuales de Trabajo
Facultad de Ingeniería, UCASAL

Resumen

La seguridad de la información se ha convertido en un área esencial en cualquier organización, potenciado en este último tiempo por la implementación del teletrabajo. Por ello resulta importante diseñar un sistema de gestión de la seguridad de la información según las políticas marcadas por la organización, mejorando los procesos del negocio a través de metodologías adoptadas por la alta dirección que incluyen medidas organizativas, legales y técnicas; con esto se asegurará la confidencialidad, integridad y disponibilidad de la información y por, sobre todo, protegerá contra los riesgos de los activos, amenazas, vulnerabilidades e impactos. La seguridad informática en entornos virtuales se ha convertido en un factor importante en el diseño y puesta en funcionamiento del teletrabajo, donde los responsables deben implementar medidas eficaces para la seguridad de los procesos. En este trabajo se propone un plan de seguridad para el Instituto de Educación Superior N° 2 de nivel superior no universitario, donde se definirán la estructura organizacional (roles y funciones), y las políticas de seguridad para finalmente concluir con un plan de implementación, considerando aspectos tales como la virtualización, el trabajo colaborativo, servicios alojados en la nube, adecuados no solo a las políticas, sino a la implantación del teletrabajo.

Palabras Clave

Amenazas, Seguridad, Riesgos, Vulnerabilidades, Teletrabajo.

Abstract

Information security has become an essential area in any organization, enhanced in recent times by the implementation of teleworking. For this reason, it is important to design an information security management system with the policies set by the organization, improving business processes through methodologies adopted by senior management that include organizational, legal and technical measures; this will ensure the confidentiality, integrity and availability of the information, and mostly it will protect against the risks of the assets, threats, vulnerabilities and impacts. Computer security in virtual environments has become an important issue in the design and implementation of telework, where the manager of organizations must implement effective measures to keep processes safe. For this reason, in this project a security plan is proposed for the Higher Education Institute N ° 2 of a non-university higher level, where the organizational structure (roles and functions) and the security policies will be defined to finally conclude with a implementation plan, considering aspects such as virtualization, collaborative work, virtualization, services hosted in the cloud; all these are suitable not only for policies but also for the implementation of teleworking.

Keywords:

Threats, Security, Risks, Vulnerabilities, Telecommuting./

Introducción

Dentro de la estructura de cualquier organización, sea pequeña, mediana o grande se ha vuelto importante el hecho de incluir el manejo e implementación de nuevas tecnologías para automatizar sus procesos, manejo de personal, administración, capacitaciones, entre otras.

Cuando ocurre un problema dentro de la función informática en una organización, muchas de las actividades que están relacionadas con el sistema resultan afectadas, he ahí la importancia de tener una buena cultura informática y saber prevenir cualquier contingencia que se presente, para así no tener complicaciones de perder información importante.

En otros tiempos la seguridad de la información era fácilmente administrable, sólo bastaba con resguardar los documentos más importantes bajo llave y mantener instancias de seguridad de ingresos mediante guardias de seguridad. Hoy en día es más difícil.

Los sistemas electrónicos entraron en nuestra sociedad y obligaron a los sistemas de seguridad a evolucionar para mantenerse al día con la tecnología cambiante. Este trabajo se aplica al caso de una institución educativa. Hace unos años, estas, aún las más pequeñas, se conectaron a Internet (una amplia red pública con pocas reglas y sin guardianes), no quedando ajenas a los riesgos de seguridad informática.

La seguridad es sólo uno de los componentes de la administración de riesgos - minimizar la exposición de la organización y dar soporte a su capacidad de lograr su misión. Para ser efectiva, la seguridad debe estar integrada a los procesos del negocio y no delegada a algunas aplicaciones técnicas.

Los incidentes de seguridad más devastadores tienden más a ser internos que externos. Muchos de estos incidentes involucran a alguien llevando a cabo una actividad autorizada de un modo no autorizado. Aunque la tecnología tiene cierta injerencia en limitar esta clase de eventos internos, las verificaciones y balances como parte de los procesos de la organización, son mucho más efectivos.

El presente trabajo tiene como objetivo proponer un Plan de Seguridad para una institución educativa de nivel superior no universitario, que contemple diferentes aspectos tales como la virtualización, trabajo colaborativo, virtualización, servicios alojados en la nube y su adecuación a las políticas institucionales.

2. Situación del Instituto IES N°2

El Instituto de Educación Superior N° 2 (IES N°2) se ubica en la provincia de Jujuy y tiene sedes en las ciudades de Tilcara y Humahuaca. Es una institución de carácter púbico, que ofrece carreras técnicas y de profesorados, cuyo objetivo principal es la formación integral de sus estudiantes, propulsando el desarrollo sostenible de la comunidad en la cual se encuentra inserto.

En su estructura orgánica, dentro de la Secretaria Administrativa se encuentra un Área de Sistemas, que debe encargarse de mantener la funcionalidad permanente de los diferentes sistemas de información y servicios informáticos que actualmente tiene la institución, cumpliendo las normativas vigentes. Cuenta con una infraestructura tecnológica básica, una página web donde a través de sistemas "SISDES" se asisten a los procesos administrativos y pedagógicos y una plataforma virtual basada en Moodle para las aulas virtuales. Aunque se iniciaron los procesos para incrementar la capacidad técnica de la infraestructura informática, respondiendo a un plan a mediano plazo, como resultado del contexto de pandemia actual, se tuvieron que reconfigurar las expectativas de trabajo con estos sistemas, ya que no solo debía atenderse el funcionamiento de tareas administrativas y pedagógicas, sino que surgió la necesidad del correcto tratamiento de la información que resultan de las actividades de trabajo remoto de sus empleados. Sin embargo, estas transformaciones no siempre se abordan desde una perspectiva profesional sistémica y realista.

Se presentó una gran demanda hacia la institución; una cuestión urgente que tuvo que atender fue la heterogeneidad en la condición de partida de sus docentes en cuanto

a su experiencia en el uso de las herramientas virtuales o modalidades a distancia, capacidades que además están influenciadas por las condiciones familiares, que afectan el trabajo docente.

En un breve periodo de tiempo se debió atender tanto a estos problemas como generar un entorno de trabajo integrado mediante una plataforma y que los procesos administrativos, propios de la institución, mantengan el resguardo necesario en cuanto al tratamiento de la información.

En repuesta a la situación planteada, el instituto requiere que su sistema informático brinde un espacio de intercambio docente, se constituya en un repositorio virtual que apoye a las clases online, brinde un sistema seguro de gestión para los actos administrativos involucrados en el servicio educativo, como mesas de examen, actas volantes, libro matriz, datos estadísticos etc., y por último generar las condiciones adecuadas para que sus empleados realicen sus trabajos de forma remota, asegurando la información. En la actualidad, la seguridad de la información es un objetivo de primordial importancia para ésta y todas las organizaciones, ya que se refiere a garantizar la calidad, disponibilidad, integridad y confidencialidad de su activo más preciado: la información.

La información es un activo que, como otros activos comerciales importantes, es esencial para el correcto desempeño de una organización y en consecuencia necesita ser protegido adecuadamente. Como resultado de esta creciente interconectividad, la información ahora está expuesta a un número cada vez mayor y una variedad más amplia de amenazas y vulnerabilidades [1].

A partir de los desafíos actuales impuestos por la situación sanitaria, resulta importante ofrecer un proceso de mejora y estabilidad a estos servicios, de los que dependen las aplicaciones disponibles para satisfacer las actividades de la rectoría y el actuar tecnológico que en general apoya todas las actividades administrativas-pedagógicas del cuerpo docente. Por ello, desde el Área de Sistemas, se deben realizar ingentes esfuerzos para mantener una mejora continua y proveer sistemas siempre disponibles y con las mejores condiciones técnicas posibles para el actuar institucional [2].

3. Plan de Seguridad Propuesto

En este apartado se incluyen todos los aspectos técnicos involucrados en la definición de un Plan de Seguridad Informática, para una institución como la indicada.

3.1. Objetivo del Plan de Seguridad propuesto

Este trabajo se encamina a definir las bases para un plan integral que marque los lineamientos progresivamente aplicables, a fin de lograr un Plan de Seguridad Informática, partiendo desde las copias de seguridad, sus protecciones, integralidad, restricción de acceso y demás elementos para tener en cuenta.

Se enfoca principalmente en el aspecto de la Seguridad de la Información de los componentes relevantes del sistema de Información del IES N° 2, aplicable tanto al área administrativa como la académica y sirve como marco para el trabajo pedagógico de cada docente en el diseño de sus clases virtuales, al utilizar las plataformas virtuales del instituto. Las políticas expresadas serán de obligatorio cumplimiento para todo el personal del Instituto, incluyendo sus sedes, emplazadas en localidades cercanas; será liderada por el grupo de sistemas y proporcionan las bases para la implementación y ejecución efectiva de controles que velen por la seguridad de la información, reduciendo el nivel de riesgo a la cual está expuesta, clarificando las responsabilidades de los usuarios y las medidas que deben adoptarse para proteger la información.

3.2. Caracterización del Sistema Informático de la Institución

Actualmente se cuenta con grupo de personas, encargadas del desarrollo y mantenimiento de los sistemas y un piso tecnológico que consiste en acceso a internet con un servidor proporcionado por Programas Nacionales y se contrató un servidor virtual para alojar la web y plataforma Moodle de la institución.

La red implementada está compuesta por

40 Access Point con acceso a internet, que se encuentran ubicados en aulas, oficinas y salones comunes tanto en la sede central como el resto de las sedes.

Con respecto al área de seguridad informática recientemente constituida, los roles y responsabilidades no han sido formalizados y las tareas desempeñadas se limitan por ahora al control de acceso de la mayoría de los sistemas del Instituto. Las tareas correspondientes a la administración de seguridad son desarrolladas por el grupo de sistemas como la administración de red, firewalls y base de datos; otras tareas son realizadas directamente por las áreas de los usuarios, y finalmente otras responsabi-lidades, como la elaboración de las políticas y normas de seguridad, concientización de los usuarios, monitoreo de incidentes de seguridad, etc., no han sido asignadas formalmente a ninguna de las áreas.

En este sentido, en el presente trabajo se detallarán los roles y responsabilidades relacionadas a la administración de seguridad de la información que involucra, no solamente a miembros de las áreas de seguridad informática y sistemas, como administradores de seguridad de información y custodios de información, sino también a los directivos y coordinadores de las diferentes unidades como propietarios de información, y a los usuarios en general.

3.3. Diseño del plan de seguridad de la información

Para el diseño del Plan de seguridad de la información se desarrollarán un conjunto de acciones que se inician con la evaluación de riesgos y culminan con la administración de los incidentes de seguridad. A continuación, se detalla cada componente:

3.3.1. Evaluación de riesgos, amenazas y vulnerabilidades

Para la definición del alcance de las políticas - estándares y con el propósito de identificar las implicancias de seguridad del uso y estrategia de tecnología, amenazas y vulnerabilidades y nuevas iniciativas del instituto, se desarrolló un conjunto de entrevistas con la rectoría del Instituto, personal del área de sistemas y el área de seguridad informática.

Producto del análisis de la información obtenida en dichas entrevistas, surgen los siguientes indicadores:

Los bienes informáticos más importantes para proteger son:

- La red de trabajo interno de la Oficina
- El servidor de aplicaciones.
- Las bases de datos del sistema administrativo - académico SISDES (de importancia crítica)
- El servicio de correo electrónico

Las amenazas más importantes para considerar de acuerdo con el impacto que pudieran tener sobre la institución son:

- El acceso no autorizado a la red, tanto producto de un ataque externo como interno.
- Pérdida de disponibilidad.
- La sustracción, alteración o pérdida de datos.
- La introducción de programas malignos.
- El empleo inadecuado de las tecnologías y sus servicios.

Las áreas sometidas a un mayor peso riesgo y las amenazas que lo motivan son:

- El local de los servidores de la red (acceso no autorizado y pérdida de disponibilidad).
- El local de oficinas administrativas y de dirección (alteración o pérdida de datos, pérdida de disponibilidad, la introducción de programas malignos, fuga de información clasificada)

3.3.2. Políticas de seguridad de información.

Con el objetivo de contar con una guía para la protección de información del instituto, se elaboraron las siguientes políticas y estándares de seguridad de la información, tomando en cuenta el estándar de seguridad de información ISO 27001 y las normas establecidas internamente por el instituto.

- Las propuestas de iniciativas encaminadas a mejorar el sistema de seguridad informática se aprobarán por Rectoría.
- El acceso a las tecnologías de la entidad será expresamente aprobado en cada caso y el personal tiene que estar previamente

preparado en los aspectos relativos a la seguridad informática.
- Los usuarios de las tecnologías informáticas y de comunicaciones responden por su protección y están en la obligación de informar cualquier incidente o violación que se produzca a su jefe inmediato superior.
- Todos los bienes informáticos serán identificados y controlados físicamente hasta nivel de componentes.

Identificación, Autenticación y Control de Acceso

Toda la información debe ser clasificada como Restringida, Confidencial, Uso Interno o General.

La clasificación de información debe ser documentada por el Propietario, aprobada por el Director responsable y distribuida a los Custodios durante el proceso de desarrollo de sistemas o antes de la distribución de los documentos o datos.

La clasificación asignada a un tipo de información solo puede ser cambiada por el propietario de la información, luego de justificar formalmente el cambio en dicha clasificación.

La información que existe en más de un medio (por ejemplo, documento fuente, registro electrónico, reporte o red) debe tener la misma clasificación, sin importar el formato.

Frecuentemente, la información deja de ser sensible o crítica después de un cierto período de tiempo, verbigracia, cuando la información se ha hecho pública.

Seguridad ante software maliciosos.

El área de seguridad informática debe realizar esfuerzos para determinar el origen de la infección por virus informáticos, para evitar la reinfección de los equipos del instituto.

La posesión de virus o cualquier programa malicioso está prohibida a todos los usuarios. Se tomarán medidas disciplinarias en caso se encuentren dichos programas en computadoras personales de usuarios. Todos los archivos adjuntos recibidos a través del correo electrónico desde Internet deben ser revisados por un antivirus antes de ejecutarlos. Asimismo, está prohibido el uso de pendrivers provenientes de otra fuente que no sea la del mismo del instituto, a excepción de los provenientes de las interfaces con organismos reguladores, proveedores y el estado, los cuales necesariamente deben pasar por un proceso de verificación y control en el área de Sistemas (Help Desk), antes de ser leídos.

El programa antivirus debe encontrarse habilitado en todas las computadoras del instituto y debe ser actualizado periódicamente. En caso de detectar fallas en el funcionamiento de dichos programas éstas deben ser comunicadas al área de soporte técnico.

Es obligación del personal del IES emplear sólo los programas cuyas licencias han sido obtenidas por el instituto y forman parte de su plataforma estándar. Asimismo, se debe evitar compartir directorios o archivos con otros usuarios; en caso de ser absolutamente necesario, coordinar con los directores y/o coordinadores respectivos y habilitar el acceso sólo a nivel de lectura, informando al Departamento de Soporte Técnico.

Todo el personal debe utilizar los protectores de pantalla y/o papel tapiz autorizados por la Institución; el estándar es:

Papel Tapiz: IES N° 2 TILCARA JUJUY Protector de Pantalla: IES N° 2.

3.3.3. Diseño de arquitectura de seguridad de red.

Con el objetivo de controlar las conexiones de la red del IES N° 2 con entidades externas y monitorear la actividad realizada a través de dichas conexiones, se elabora una propuesta de arquitectura de red la cual incluye dispositivos de monitoreo de intrusos y herramientas de inspección de contenido.

Medidas y procedimientos

Son diversos los elementos considerados para implementar la seguridad de la información y la elección de los mismos depende de las características específicas del IES N° 2. Estas medidas y procedimientos persiguen identificar los bienes de acuerdo con su importancia, controlar y supervisar que sean utilizados en

funciones propias de trabajo y garantizar su protección.

Capacitación de usuarios

Es responsabilidad del área de seguridad informática promover constantemente la importancia de la seguridad a todos los usuarios de los sistemas de información. El programa de concientización en seguridad debe de contener continuas capacitaciones y charlas, adicionalmente se pueden emplear diversos métodos como afiches, llaveros, mensajes de log-in, etc., los cuales recuerden permanentemente al usuario el papel importante que cumplen en el mantenimiento de la seguridad de la información.

3.3.4. Resguardo y recuperación de la información

- Se define lo siguiente para este apartado:
- Se realizarán copias de seguridad de la información y del software que se determine y se comprobarán con regularidad.
- Garantizar un Servidor NextCloud[1] con carpetas particulares para cada usuario, en la cual se realizan backup de la información más importante de cada trabajador del IES N° 2.
- Cada trabajador será responsable de la información que guarde en el Servidor NextCloud y de la periodicidad con que realice las salvas personales.
- Los jefes de áreas son los responsables de organizar la salva de la información del área respectiva, definiendo la información a salvar y el trabajador encargado de esto.
- Cada área dispondrá de un disco externo para la salvaguarda de la información clasificada y/o limitada.

3.3.5. Administración de Incidentes de Seguridad.

Luego de reportado el incidente de seguridad, éste debe ser investigado por el área de seguridad informática. Se debe identificar la severidad del incidente para la toma de medidas correctivas.

El personal encargado de la administración de la seguridad debe realizar la investigación de los incidentes de forma rápida y confidencial. Se debe mantener una documentación de todos los incidentes de seguridad ocurridos en el instituto.

Se debe mantener intacta la evidencia que prueba la ocurrencia de una violación de seguridad producida tanto por entes internos o externos, para su posterior utilización en procesos legales, en caso de ser necesario.

4. El teletrabajo

El teletrabajo es una modalidad que unida al buen uso de las tecnologías de información y comunicación resulta muy efectiva para las organizaciones en el marco de la efectividad, calidad de vida, y productividad laboral.

"Se define el teletrabajo como el resultado de las aplicaciones de las tecnologías de información y comunicación, en donde no es importante el lugar geográfico ni la separación del empleador, por lo menos un 20% de las horas trabajadas" [3].

4.1. Implementación del teletrabajo en el IES N° 2

La implementación del teletrabajo requiere que la institución se organice y atienda a los siguientes requerimientos: Equipo de cómputo, conexión a internet (en caso de no ser trabajador offline), conexión a las bases de datos, seguridad informática (que resguardará la información de la comunidad educativa y dará confianza al colaborador de manejar esta información)

El mejor modelo que se ajusta a esta institución es el teletrabajo flexible, donde las personas puedan repartir su jornada laboral entre el instituto y su casa, de manera que exista cohesión del producto de su trabajo, que permita la integración con el equipo de trabajo, lo que genera importantes lazos que impactan positivamente en la realización de una tarea además de lograr consolidar el sentimiento de pertenencia. Otro tipo de teletrabajo que se propone, es el off line o desconectado,

1 https://nextcloud.com/

por el cual el personal del instituto trabaja desconectado del servidor central para luego hacer llegar los datos [4]. Aunque en pocas y especiales situaciones, accedan a la red mediante control de usuario y adecuándose a las recomendaciones de seguridad enunciadas.
En concordancia con lo expresado respecto a la norma de seguridad informática, se implementarán los siguientes ítems, desde el punto de vista de los dispositivos del Teletrabajador:

- Se implementará configuración sobre el firewall personal que responda a las políticas de control de la institución.
- Se mantendrá actualizado los Sistemas Operativos junto a las demás aplicaciones, haciendo hincapié en las actualizaciones de seguridad, como de los antivirus.
- En las computadoras portátiles se utilizará una segunda cuenta de usuario con privilegios limitados; se mantendrá la cuenta administrativa para tareas que así lo requieran.
- Se configurará el Bloqueo de Sesión para prevenir accesos no autorizados durante las ausencias temporales del Teletrabajador.
- Se limitará convenientemente la instalación de aplicaciones extra en el teléfono celular. También tendrán instalados software antivirus y antimalware.
- Se adoptará una política de renovación de contraseña segura, la cual podrá ser cambiada siguiendo los estándares de seguridad indicados en "Creación de Contraseñas Seguras".

4.2. Adecuaciones necesarias en la infraestructura para una virtualización segura.

Hoy más que nunca, la virtualización es una forma de simplificar el entorno de trabajo. La infraestructura informática no tiene por qué ser complicada: cada servidor, sistema operativo y aplicación satisface una necesidad en la organización. Sin embargo, gestionar todas esas licencias, el mantenimiento, los parches, las actualizaciones, la seguridad y los backups deja poco tiempo para mejorar las operaciones, añadir nuevas funciones y aportar un auténtico valor añadido a las tareas realizadas. Es factible el ahorro de tiempo gracias a la facilidad de administración o de clonación de los discos duros virtuales, que se realizarán como cualquier otro archivo, con las ventajas que esto tiene asociado [5].
El software de virtualización libera las aplicaciones de las ataduras y límites impuestos por el hardware con el que se ejecutan y permite compartir los recursos, lo que reduce enormemente la complejidad de TI.
Sin embargo, para el IES N° 2, debido a las carencias de recursos económicos y humanos, se propone la utilización de VMware[2]. Para empezar, ofrece licencias adaptadas al tamaño de la organización; además, la nueva tecnología de almacenamiento vSphere permite virtualizar el almacenamiento en sus propios servidores y la curva de aprendizaje es de solo unas horas. Tiene las siguientes ventajas:

- Simplicidad: VMware le ayuda a crear una infraestructura consolidada con menos servidores. Además, pone a su alcance herramientas automatizadas para optimizar y gestionar los entornos físicos y virtuales desde una única consola accesible desde un navegador web.
- Almacenamiento: Teniendo en cuenta que el Instituto no dispone de hardware de almacenamiento compartido.
- Mantenimiento sin interrupciones: llevando a cabo tareas de clonación, aplicación de parches, actualización, protección y reimplementación de máquinas virtuales sin interrupción del servicio

4.3. Servicio que se va a migrar en la nube

El concepto de "la informática en la nube" (conocido en inglés como "Cloud Computing") empezó en proveedores de servicio de Internet a gran escala, como Google, Amazon AWS, Microsoft y otros que construyeron su propia infraestructura. De entre todos ellos emergió una arquitectura: un sistema

2 https://www.vmware.com/ar.html

de recursos distribuidos horizontalmente, introducidos como servicios virtuales de tecnología informática escalados masivamente y manejados como recursos configurados y funcionando de manera continua [6].

Para la implementación de Cloud Computing en el IES N° 2 se propone utilizar una especie de "sistema hibrido", almacenando los datos más sensibles de forma local (que por lo general son pocos) y utilizando la nube para todo lo demás; por ello es necesario analizar para cada caso particular las necesidades propias de cada sede y departamento, para así saber si se puede utilizar con confianza la informática en la nube, estableciendo qué TICs locales se aplicarán y cuáles TICs en la nube servirán para el objetivo perseguido, logrando de esta manera una relación costo-beneficio-confidencialidad que se adapte a las exigencias requeridas.

En forma adicional a la utilización de la informática en la nube y con el fin de minimizar aún más los costos necesarios para comenzar a operar una solución basada en este modelo, se propone el uso de Sistemas Operativos "Open Source", como Linux, ya que la mayoría de los servicios en la nube funcionan en forma independiente a la plataforma o sistema operativo que se esté utilizando.

El servicio para migrar en la nube es el de almacenamiento, más específicamente el de Backup. "Copia de Seguridad" y se refiere a copiar, duplicar o multiplicar la información considerada lo suficientemente importante como para ser conservada, para poder recuperarla ante una catástrofe informática como la eliminación de archivos por un virus, crackers o bien accidentalmente [7]. Cuando sucede eso se pueda ejecutar procesos de recuperación de la información

Para llevar adelante el Backup es necesario considerar las siguientes recomendaciones:

- Es importante realizar una limpieza exhaustiva para liberar datos innecesarios u obsoletos, o sea, elegir la información o tipo de datos a almacenar.
- Otro aspecto destacado pasa por definir una estrategia de 'backup' y determinar con qué frecuencia realizar copias de seguridad en la nube (completa, incremental, diferencial o espejo).
- Asimismo, es posible elegir una configuración de 'backups' automáticos con tiempos e intervalos definidos (recordar que es una práctica que se debe hacer de forma periódica), de manera que no sea necesario hacer cada copia siempre de manera manual.

Consejos de seguridad cloud

- Comprobar en qué lugar van a estar alojados los datos: Uno de los aspectos que se debe tener en cuenta es en qué país van a estar ubicados los servidores en los que se encontrarán los archivos. Teniendo en cuenta que dicho país debe cumplir con las garantías adecuadas para la protección de datos y cumplir con las garantías que se deben aportar para la protección de la privacidad.
- Es necesario analizar que el proveedor de servicios garantiza la recuperación de los datos: La integridad y recuperación de los datos es otro asunto de gran relevancia. La empresa de servicios en la nube con la que se trabaje, debe garantizar la posibilidad de recuperar los datos y tener un buen sistema de copias de seguridad, diarias y programadas, y que facilite la recuperación de la información en caso de que se la necesite.
- Tener en cuenta las necesidades de uso de la nube: Si aumenta el peso del conjunto de datos con el que se va a trabajar, habrá que ampliar los planes (tener en cuenta el aspecto escalabilidad) para disfrutar de un rendimiento adecuado.
- Gestionar bien los permisos y el acceso al sistema: La gestión de permisos es uno de los ejes de la seguridad cloud. Se pueden proteger los archivos del sistema de almacenamiento y controlar la trazabilidad de estos, así como también establecer los permisos de usuario que se crea conveniente.
- Por último, es importante considerar el Cifrado de Datos: Una recomendación que no puede dejarse de lado es subir los datos cifrados (encriptados) para que ante un robo estos estén resguardados.

4.4. Sistemas colaborativos y redes sociales.
Las redes sociales son parte de los hábitos cotidianos de navegación de gran cantidad de personas. Por ello están presente dentro de las herramientas utilizadas en el Instituto para realizar sus tareas tanto pedagógicas como administrativas, logrando trabajos colaborativos y manteniendo una comunicación activa. Cualquier usuario de Internet hace uso de al menos una red social y muchos de ellos participan activamente en varias de ellas. En el instituto se mantiene activo el Facebook y el WhatsApp.
Sin embargo, a partir de su uso, los usuarios del IES se ven expuestos a un conjunto de amenazas informáticas, que pueden atentar contra su información o incluso su propia integridad.
Ante la creciente tendencia de los ataques informáticos a utilizar las redes sociales como medio para su desarrollo, se vuelve de vital importancia para el usuario estar protegido y contar con un entorno seguro al momento de utilizarlas [8].
En las redes sociales los integrantes de la comunidad educativa del Instituto pueden conectarse con otros para compartir información como fotografías, videos y mensajes.
Por ello se elaboró una serie de consejos para ayudar a proteger a los usuarios cuando usan redes sociales.

- Ser precavido al hacer clic en vínculos que recibe en mensajes de sus amigos en su sitio web social. Trate los vínculos en los mensajes de estos sitios de la misma manera que los vínculos en los mensajes de correo electrónico.
- Sepa qué ha publicado acerca de usted mismo; no use material que cualquiera pueda encontrar con una búsqueda rápida, respecto a datos laborales.
- Para evitar revelar las direcciones de correo electrónico de sus amigos, no permita que los servicios de redes sociales examinen su libreta de direcciones de correo electrónico
- Dé por sentado que todo lo que pone en una red social es permanente. Aún si elimina su cuenta, cualquiera en Internet puede fácilmente imprimir fotografías o texto o guardar imágenes y videos en una computadora.
- Tenga cuidado de instalar elementos adicionales en su sitio. Muchos sitios de redes sociales le permiten descargar aplicaciones de terceros que le permiten hacer más cosas con su página personal.

5. Conclusión
Del análisis realizado a la situación en cuanto a la seguridad informática del IES N° 2, se pudo observar una gran cantidad de amenazas (con origen en programa dañinos, o por vía remota) que reciben constantemente los sistemas informáticos y en particular los de entorno virtual.
Se partió del supuesto que un sistema de complejidad pequeña como es el del Instituto de Educación Superior, no posee muchos activos en riesgo, pero el trabajo condujo a cambiar este concepto, como lo dejó evidenciado en cada uno de los puntos desarrollados.
A pesar de que cualquier organización y en especial la del IES N° 2 se beneficia de todo lo que le provee las tecnologías de información, esto plantea un reto a los profesionales de la informática, de manera que se realicen esfuerzos encaminados a robustecer los aspectos de la seguridad, controles, integridad de la información, etc.
Un sistema seguro debe ser íntegro (con información modificable solo por las personas autorizadas), confidencial (los datos tienen que ser legibles únicamente por los usuarios autorizados), irrefutable (el usuario no debe poder negar las acciones que realizó) y tener buena disponibilidad (debe ser estable).
Por ello es necesario mantener un estado de alerta y actualización permanente: la seguridad es un proceso continuo que exige aprender sobre las propias experiencias. El Instituto no puede permitirse considerar la seguridad como un proceso o un producto aislado de los demás. La seguridad tiene que formar parte de ella.
La seguridad informática en entornos virtuales se ha convertido en un factor importante en el diseño e implementación del teletrabajo.

El encargado de la seguridad debe estar constantemente implementando medidas eficaces para mantenerlas seguras con el fin de tener sistemas confiables y estables.
Pero a pesar de esto y aun con las mejores medidas de seguridad que se adopten siempre habrá amenazas en contras de los sistemas.

Referencias Bibliográficas

[1] GALEANO VILLA, Jorge Luis - ALZATE CASTAÑEDA, Cristian Camilo, *Protocolo de Políticas de Seguridad Informática para las Universidades de Risaralda*, disponible en: http://ribuc.ucp.edu.co:8080/jspui/bitstream/handle/10785/1731/CDMIST65.pdf?sequence=1.

[2] Plan Estratégico de las Tecnologías de la Información y las Comunicaciones (PETIC). 2015-2019- Resolución 8213 de 07 de diciembre de 2015.

[3] Roche Tovar, I. (2007). *La gerencia de Recursos Humanos Ante la posibilidad de implantación de una iniciativa de trabajo.* Revista Informe de Investigaciones Educativas, 21, 93-113

[4] Ortiz Chaparro, Francisco, *El teletrabajo. Una nueva sociedad laboral en la era de la tecnología*, Madrid: McGraw-Hill/Interamericana de España, 1997.

[5] Shackleford D. *Virtualization Security: Protecting Virtualized Environments.* 2012

[6] http://tecnofilos.aprenderapensar.net/2010/02/03/trabajar-en-la-nube-modelos-actuales-en-cloud-computing) [Consultado el 25/08/2020].

[7] *Computación en nube, Beneficios, riesgos y recomendaciones para la seguridad de la Información*, ENISA, 2009 http://www.enisa.europa.eu/activities/risk-management/files/deliverables/cloud-computing-risk-assessment [Consultado el 25/08/2020]

[8] https://doble-efe.com/definicion-redes-sociales/ [Consultado el 25/08/2020]

Seguridad Informática en la transformación del Trabajo Presencial al Teletrabajo

Luciana Gervasoni
lucigervasoni.lg@gmail.com

Diplomatura en Seguridad Informática en Entornos Virtuales de Trabajo,
Facultad de Ingeniería, UCASAL

Resumen

Este trabajo muestra la resolución de una situación problemática que enfrenta una organización al tener que modificar su modalidad de trabajo presencial a modalidad de teletrabajo en tiempos de emergencia, apresurada por la pandemia mundial surgida a raíz del virus COVID-19.

En primer lugar, se tomaron decisiones teniendo en cuenta los recursos que se tenían al momento de la migración a la nueva forma de trabajo y, a partir de allí, se realizó un plan de seguridad que permite la integración gradual de políticas y recursos que refuerzan la seguridad de la información de la empresa.

Este programa de protección de activos de la organización contempla distintos vectores que se deben tener en cuenta para abarcar una solución sólida, incluyendo tareas continuas, mantenimiento del plan y concientización de los empleados, factores fundamentales para el éxito del procedimiento.

Palabras Clave

Seguridad teletrabajo, Políticas de seguridad, Evaluación de riesgos.

Abstract

This project shows a resolution of a problematic situation with which an organization deals by having to modify its face-to-face work modality to work from home in emergency times, rushed by the world pandemic arising from COVID-19 virus.

In first place, some decisions were taken considering the resources that the organization had at the moment of the migration and, starting from there, a security plan was made allowing the integration of policies and resources that reinforce the company information security.

This program of organization asset protection includes different vectors that must be taken into account to cover a solid solution, including continuous tasks, plan maintenance and employee training, fundamental factors for the success of the procedure.

Keywords:

Security in homework, Security policies, Risk assessment.

Introducción

En el presente trabajo se plantea una situación empresarial actual en la que una organización decide comenzar a trabajar con algunos de sus empleados fuera de la institución. Esta nueva modalidad de trabajo, llamada teletrabajo o home-office, es adoptada por aquellos empleados que realizan sus tareas diarias desde su casa.

La organización pone a disposición sus recursos humanos, materiales y financieros para lograr esta migración de la mejor manera y como principal objetivo mantener la seguridad, integridad y confidencialidad de los activos de la empresa.

El Departamento de Seguridad informática se hace cargo de las políticas de seguridad y del programa de seguridad que se presenta a la Gerencia de la empresa para su aprobación y puesta en marcha.

2. Situación de la empresa

Una obra social de la ciudad de Santa Fe tiene alrededor de 300 empleados y, en su cartilla médica, más de 1000 prestadores de servicios de la salud (médicos de distintas especialidades, kinesiólogos, oculistas, etc.). La cantidad de socios es de alrededor de 15000.

Al inicio del aislamiento social obligatorio, la empresa tuvo que adaptarse a las circunstancias y seguir operando de igual manera (dentro de lo posible). Parte de sus empleados continuaron trabajando en sus puestos de trabajo físico y otros tantos comenzaron a trabajar desde sus casas con los elementos que tenían.

Hoy en día, la obra social desea implementar el teletrabajo para los empleados de los sectores de Atención telefónica, Sistemas, Ventas y Socios, siendo un total de 150 trabajadores aproximadamente.

Sus tareas serán, según cada sector:

- Atención telefónica: recibir las llamadas de socios, atender sus inquietudes y despejar sus dudas. Transferir llamadas al sector correspondiente.
- Sistemas: encargados de la infraestructura y redes, desarrollo de la aplicación de la obra social, y seguridad de la información.
- Ventas: encargados de contactar nuevos posibles socios y vender los planes de salud.
- Socios: encargados del alta, baja, y modificación de datos de socios.

La empresa dotará de computadoras portátiles y teléfonos celulares a todos los empleados en modalidad de teletrabajo. Además, proveerá de escritorios y sillas a quienes lo soliciten. El presupuesto para esta operación y para fortalecer la infraestructura actual de la empresa es de U$S200.000.

3. Seguridad Informática

En los siguientes apartados se define la organización y estructura de la seguridad informática, considerando particularmente todo lo relativo a la política de seguridad que será necesario implementar, así como el programa de seguridad pertinente.

3.1. Política de Seguridad

Se define en términos de los objetivos, alcance, comunicación, propietarios de las políticas y normas, que se describen detalladamente a seguir:

Objetivos:

- Desarrollar la estrategia necesaria para cuidar de los activos de la información de la organización al momento de tener a sus recursos humanos trabajando desde sus hogares.
- Mantener los estándares de seguridad de la información que se encuentra tanto dentro como fuera de la empresa respondiendo a su integridad, confidencialidad, no repudio y autorización de acceso.

Alcance:

Esta política establece normativas para alcanzar y mantener la seguridad de la información de la empresa al momento de tener a sus empleados trabajando en sus casas.

Comunicación:

La política de seguridad para el teletrabajo será comunicada a la totalidad de empleados,

luego de ser aprobada por la alta gerencia y presentada por el Departamento de Seguridad de la Información. Este departamento será el encargado, no sólo de comunicar la política, sino de capacitar a los distintos recursos humanos para su completo entendimiento.

Propietarios de las políticas:
El Departamento de Seguridad de la Información será el encargado de controlar si esta política es cumplida por todos los empleados. En caso de haber algún incumplimiento, se informará al jefe del departamento y se ejecutarán las acciones necesarias para corregir esta situación.

Normas:
Las normas abarcan los siguientes espacios: escritorios de trabajo, Conectividad, Políticas de contraseñas y Permisos de usuarios, y se definen en detalle a continuación:

a. Escritorio de trabajo:
- Cada empleado utilizará diariamente la notebook brindada por la empresa.
- Se entregará la misma con Windows 10 instalado. Se deben aceptar e instalar todas las actualizaciones que proponga el sistema operativo.
- La notebook tendrá instalado el sistema Antivirus de Kaspersky, controlado por el servidor Kaspersky Security Center instalado en la infraestructura de la empresa.
- Se podrá instalar software legal solamente necesario para actividades laborales y se debe mantener actualizado.
- Evitar descargar archivos y programas que no sean de páginas oficiales.
- Utilizar política de bloqueo de pantalla: la pantalla se bloqueará luego de 10 minutos de no haberse movido el cursor.
- Estará prohibido conectar dispositivos USB o discos externos a las notebooks. En caso de necesitar hacerlo exclusivamente por trabajo, se dará un permiso temporal.

b. Conectividad:
- La notebook puede conectarse por Ethernet o WiFi, siempre a redes privadas y seguras. No se permite conectarse a redes públicas.
- La conexión a la empresa será a través de la VPN que se puso a disposición. Cada empleado ingresará con su usuario y contraseña de Active Directory (Microsoft). Se utilizará un factor de doble autenticación: será un código enviado al celular empresarial del empleado, que luego escribirá en la notebook para completar la conexión.
- Al ingresar la contraseña para conectarse a la VPN, el sistema admitirá hasta 9 intentos de inicio de sesión erróneos, a la décima vez se bloqueará el usuario por 20 minutos. De ocurrir una vez más el bloqueo en un lapso de tiempo corto, se deberá pedir el desbloqueo de usuario a personal de Seguridad de la Información.

c. Política de contraseñas:
- Se solicitarán contraseñas robustas. Su longitud mínima será de 9 caracteres y deben poseer al menos una letra mayúscula, una minúscula, un símbolo y un número.
- Se deben cambiar las contraseñas cada dos meses.

d. Permisos de usuarios:
- Cada usuario en la VPN tendrá permisos para conectarse solamente a su escritorio remoto en la empresa. Desde este, se podrá mover dentro de la red, según corresponda y con los permisos que siempre tuvo.

3.2. Programa de seguridad
Este programa ofrece una forma de alcanzar las metas y objetivos de la organización, relacionados con la seguridad de la información, y se describe según las instancias de trabajo siguientes:

Evaluación de riesgos:
En el primer paso del programa de seguridad se deben identificar los riesgos a los que está expuesta nuestra organización al tener trabajando empleados en sus casas. A partir de esto, la información no sólo está almacenada en el interior de la empresa, sino que también está disponible en donde se encuentre cada una de

las notebooks y celulares distribuidos.

Para la evaluación de riesgos, primero se deben identificar los activos [1]: firewall, escritorios físicos en empresa, notebooks en home-office, celulares, empleados, información. En segundo lugar, se deben identificar las amenazas y vulnerabilidades a los que cada uno de estos activos está expuesto:

a. Firewall: puede ser atacado por hackers que intenten ingresar a la infraestructura de la empresa. Tipos de ataques: DoS, ataque de fuerza bruta.
b. Escritorios físicos en la empresa: al tener el protocolo RDP habilitado para la conexión de empleados en home-office, queda expuesto el puerto correspondiente y es más sencillo ingresar al mismo remotamente. También podría sufrir ataques de fuerza bruta si alguien quisiera ingresar como usuario.
c. Notebooks en home-office: si la red a la que se conectan no es segura, se corre el riesgo que accedan atacantes a la notebook y roben información. Además, si la notebook queda desbloqueada en algún momento, cualquier integrante de la casa podría acceder a la misma.
d. Celulares: la amenaza más grande se corre en el caso de pérdida o robo del celular. Éste debe tener bloqueo de pantalla (en lo posible biométrico) y de tarjeta SIM. También podría ser víctima de algún virus a través de la descarga de archivos.
e. Empleados: es el eslabón más débil de la cadena. Los empleados pueden ser engañados a través de métodos de ingeniería social y descargar distintos tipos de malware o entregar contraseñas sin saberlo [2].
f. Información: puede ser robada a través de los distintos métodos mencionados y más. Hay riesgo de que sea robada, de que se borre o que se divulgue.

El siguiente paso es calcular el nivel de riesgo de cada uno de ellos. Esto se logra a partir de la probabilidad de ocurrencia que tiene y del impacto que pueda llegar a tener en la organización el hecho de que el riesgo ocurra.

Para nuestra organización, los niveles de riesgo son los siguientes:

Tabla 1: Escala de riesgos

Impacto	Probabilidad de ocurrencia		
	Baja	Media	Alta
Bajo	Bajo	Bajo	Medio
Medio	Medio	Medio	Alto
Alto	Alto	Alto	Alto

Estrategia para mitigar riesgos:

Mitigar un riesgo es tomar una acción para disminuir el impacto del mismo [3]. A continuación, se establecen las estrategias para mitigar los riesgos:

a. Firewall: se deben activar todos los controles de antivirus y antimalware que posee el firewall. Se debe habilitar el acceso a su configuración (GUI) sólo para un usuario administrador y éste podrá ingresar solamente estando en la red local. Se habilitará el acceso para este mismo usuario por CLI a través de SSH. Se bloquearán todos los puertos que no sean exclusivamente utilizados por alguna aplicación. Se habilitará el acceso por VPN para empleados de home-office. Las contraseñas de usuarios y accesos deben ser seguras.
b. Escritorios físicos en la empresa: todos los escritorios físicos de la empresa se encontrarán en la red protegida por el firewall. Se cierran los puertos que no son utilizados. Las contraseñas de usuarios serán seguras. Se deshabilitan los puertos USB. Se bloquean las pantallas a los 10 minutos de no haber movimiento.
c. Notebooks en home-office: la conexión a internet será a través de una red segura y privada. Las contraseñas de usuarios serán seguras. Se deshabilitan los puertos USB. Se bloquean las pantallas a los 10 minutos de no haber movimiento.
d. Celulares: deben tener bloqueo de pantalla: numérico y biométrico (dentro de lo posible), puede ser a través de huella o de iris, según lo permita el dispositivo. La tarjeta SIM debe tener un PIN de bloqueo

para ocultar los contactos. El celular debe tener el antivirus de Kaspersky con el que se entrega.

e. Empleados: se capacitarán los empleados en cuanto a Seguridad Informática para que sepan responder a posibles ataques o evitar los mismos en caso de tener la posibilidad. Se distribuirá información periódicamente para reforzar los conocimientos.
f. Información: se establecerá la encriptación de la información almacenada en las notebooks y la información sensible de los celulares. Se hará backup de las notebooks: un full por semana y un incremental por día, el resto de los días.

Requerimientos de seguridad:

La empresa debe contar con la política de seguridad de la información y su respectivo programa de seguridad. Ambos deben estar aprobados por la alta gerencia de la organización. El Departamento de Seguridad debe constatar que se cumplan e informar sus estados periódicamente.

Recursos internos y externos necesarios:

La implementación del programa formulado requerirá de recursos para su desarrollo, entre los que se pueden indicar:

a. Recursos humanos encargados de llevar a cabo la gestión de la seguridad de la información: 2 analistas de seguridad y un jefe.
b. Recursos materiales: infraestructura de firewall para la conexión remota, notebooks, celulares. Licencias de Windows y antivirus Kaspersky. En algunos casos se pueden requerir elementos de escritorio: escritorio, silla.
c. Recursos financieros: para este proyecto se estimó un presupuesto aproximado de USD 200.000.

Infraestructura de seguridad y nuevas tecnologías:

La infraestructura de seguridad está compuesta principalmente por un firewall FortiGate 200E que se va a adquirir, que es el que permitirá la conexión de los 150 empleados en home-office a la infraestructura interna de la organización a través de la VPN SSL. Esta solución permite el monitoreo de conexiones, sesiones de usuarios y eventos que surjan durante cada jornada laboral.

La infraestructura de seguridad interna cuenta con un servidor anti-malware instalado en los servidores de la empresa, de la marca Kaspersky, que contará con políticas para las notebooks y celulares en home-office. Con la solución de Kaspersky, además, se podrá llevar un registro de eventos de seguridad que vayan sucediendo.

A partir de los dispositivos incorporados (notebooks y celulares) se aplicará la identificación de usuarios mediante biometría: reconocimiento de iris y de huellas digitales.

Para recuperar información perdida la empresa cuenta con la solución Veritas Backup Exec que se aplicará a notebooks y configuración del firewall.

Perímetro de seguridad:

En lo que respecta al perímetro de seguridad lógica, como se dijo anteriormente, va a estar a cargo de la solución de FortiGate. En lo que respecta a seguridad física, los equipos de la empresa se encuentran en un datacenter principal, ubicado en el interior de la empresa, cuidado de riesgos de intrusión y ambientales. Además, se cuenta con un datacenter secundario en otra ubicación y con los mismos cuidados.

Seguridad del equipamiento:

En cuanto a soluciones que se encuentran dentro de la empresa, como se aclaró anteriormente, cuentan con seguridad dentro de los datacenters. En cuanto a requerimientos de energía, cada uno de ellos contiene UPS APC para certificar su uso continuo.

Cada notebook y celular entregados a los empleados estarán anotados en un libro de registros. Si bien cuentan con seguro por robo, cada empleado deberá hacerse cargo del cuidado del equipamiento.

Políticas de seguridad y comunicación:

La empresa cuenta con una política de seguridad descripta en el apartado anterior. La comunicación de la misma y cada una de sus actualizaciones están a cargo del equipo de

Seguridad de la Información.

Documentación:
El equipo de Seguridad de la Información es el encargado de generar por primera vez la documentación de todo el plan y políticas de seguridad para el teletrabajo y mantenerla actualizada a medida que surjan distintos cambios.

Métricas:
Se crearán distintos indicadores que marquen la tolerancia máxima de eventos que pueden surgir mes a mes en lo que respecta al home-office. Cuando alguno de estos indicadores supere el límite, se revisarán los procesos nuevamente y se generará al menos un cambio que indique la supuesta mejora de la implementación. Los indicadores serán: cantidad de riesgos acontecidos (riesgos bajos, medios y altos por separado), cantidad de ataques de malware (internos y externos por separado), cantidad de equipos infectados, cantidad de daños en equipamientos por catástrofes naturales, cantidad de intentos de intrusión en la VPN, cantidad de intrusiones en la VPN, cantidad de equipos de home-office dañados por cualquier causa.

Tareas continuas:
- Concientización de los empleados: el equipo de Seguridad de la Información será el encargado de generar capacitaciones a cada uno de los empleados que comenzará a trabajar en home-office. Una vez que estén establecidos, se capacitará al resto de los empleados de la empresa.
- Monitoreo: el equipo de Seguridad Informática será el encargado de controlar los eventos almacenados en las distintas soluciones que son parte del teletrabajo y controlarán las métricas establecidas.
- Mantenimiento del programa: el equipo de Seguridad Informática será el encargado de reevaluar el programa y la política de seguridad de la empresa cada vez que los indicadores y la política de métricas así lo disponga.

4. Infraestructura de Red
En el programa de seguridad que se estableció para la empresa, en el apartado anterior, se muestran algunos riesgos de tener parte de la infraestructura fuera de la oficina. Además, se establece la importancia de cada riesgo: baja, media y alta, según su impacto y su probabilidad de ocurrencia. A partir de esto, se detallan algunas de las amenazas más importantes que tiene la infraestructura de red del negocio y su clasificación para, posteriormente, detallar su plan de mitigación:

a. Firewall: ingreso de atacantes a la VPN. Amenaza externa.
   Probabilidad de ocurrencia: media.
   Impacto: alto.
   Riesgo: alto.
   Mitigación: se deben activar todos los controles de antivirus, antimalware e IPS que posee el firewall. Se debe deshabilitar el acceso a su administración (mediante GUI y CLI) para usuarios que se encuentren fuera de la red interna y sólo para un usuario administrador. Se habilitará el acceso para este mismo usuario por CLI a través de SSH y de GUI a través de HTTPS.
   Se bloquearán todos los puertos que no sean exclusivamente utilizados por alguna aplicación. Ingreso a la VPN: se habilitará el acceso por VPN para empleados de home-office: las contraseñas de usuarios deben ser seguras, según lo estipulado en la política de seguridad presentada anteriormente. Esta última también estipula el bloqueo de usuarios luego de una cierta cantidad de intentos de ingresos erróneos.
b. Notebooks en home-office: infección de las notebooks a través de la descarga de archivos maliciosos.
   Amenaza interna.
   Probabilidad de ocurrencia: alta.
   Impacto: alto.
   Riesgo: alto.
   Mitigación: todas las notebooks tendrán el antivirus Kaspersky instalado y actualizado. Este reportará cualquier incidente al usuario y al administrador de la consola antivirus.
c. Notebooks en home-office: hackers podrían ingresar a la red de la notebook y a la información que hay en ella.

Amenaza externa.
Probabilidad de ocurrencia: media.
Impacto: alto.
Riesgo: alto.
Mitigación: en primer lugar, se concientizarán a todos los empleados que trabajen en home office sobre la importancia de la red a la que se conectan para trabajar: esta red debe ser segura y privada. Su contraseña de acceso debe ser compleja. Los discos de las notebooks poseerán encriptación para evitar que hackers se queden con información confidencial. Otra opción de mitigación es el mismo antivirus que tendrán instalado.

d. Correo electrónico: empleados pueden ser presa de correos de Phishing e ingresar a una web malintencionada las claves de usuario para acceder a la VPN y al equipo de trabajo.
Amenaza interna.
Probabilidad de ocurrencia: baja.
Impacto: alto.
Riesgo: alto.
Mitigación: concientización a los empleados que trabajen en home office y luego a todos los empleados de la empresa, sobre los ataques de ingeniería social. Se les enseñará a reconocer los distintos tipos de ataques y cómo defenderse.

5. Cloud Computing

Dentro de todos los servicios que se tienen en la red empresarial, se podría elegir la migración del servicio de backup a la nube. Como se comenta en el primer apartado (Seguridad Informática), la empresa posee la solución de backup Veritas Backup Exec [4] on-premise. Actualmente, los backups se guardan tanto en el datacenter principal, como en el secundario.

A partir de esto, se propone migrar el servicio de backup a la nube. Veritas posee en su software de backup, la posibilidad de realizar el backup en la nube, y también recuperarlo desde ahí mismo, desde donde sea que se esté ya que es administrable desde la nube también.

Recomendaciones de seguridad a tener en cuenta:

Veritas trabaja con la nube de AWS o Azure. Se debe elegir la solución indicada teniendo en cuenta las consideraciones de ambos proveedores (tanto Veritas como el que se elija):

a. Disponibilidad del servicio en la nube: el proveedor debe garantizar servicio continuo y demostrar que está preparado frente a caídas tanto en su infraestructura como de DoS provenientes de ataques informáticos. Deben tener un Plan de Contingencia adecuado en caso de que algo falle.
b. Los servidores de almacenamiento tanto de software (Veritas) como de los backups (AWS o Azure) realizados deben tener a su vez copias de backup en distintos servidores.
c. Revisar las políticas de seguridad de los proveedores y su cumplimiento.
d. Revisar que la infraestructura de los proveedores posea soluciones frente a ataques informáticos. Política de información de ataque: definir con anterioridad qué información deberá entregarse a la empresa cliente en caso de que la infraestructura de alguno de los proveedores sufra un ataque.
e. Establecer mecanismos de monitoreo y control de acceso de usuarios y tareas que se realicen en la plataforma.
f. Definir la ubicación de los servidores de los proveedores: las leyes en cuanto a protección de datos personales varían en cada país, por lo tanto, debe tenerse en cuenta que concuerden con las de Argentina.
g. Solicitar un contrato de privacidad y confidencialidad en cuanto a la información de nuestra empresa que ellos puedan tener desde la implementación del servicio en adelante y qué se realizará con ella una vez que el contrato finalice.
h. Tener en cuenta la experiencia y el conocimiento de las personas encargadas del soporte de la solución.
i. Solicitar el programa de actualizaciones de software en cuanto a parches de vulnerabilidades descubiertas.
j. Se debe tener en cuenta que exista la posibilidad de tener distintos tipos de usuarios en la plataforma de backup en la

nube, con diferentes permisos.

k. Se recomienda limitar las direcciones IP permitidas al acceso de la plataforma de backup.
l. Solicitar, en caso de tener la posibilidad, un doble factor de autenticación a la plataforma.

En cuanto a la integración de Veritas Backup Exec con el resto de la infraestructura, no habría problemas de ningún tipo ya que este proveedor soporta no solo multi-cloud sino también plataformas híbridas [5].

6. Virtualización

A continuación, se mencionan las distintas virtualizaciones que se realizarán en el proyecto para lograr que los empleados de la empresa realicen home-office:

- Virtualización de servicios: como se menciona en el apartado anterior, se virtualizará el servicio de backup de la organización para brindar un acceso seguro a los datos de la organización mediante el software Veritas Backup Exec (ver apartado 3 para más detalles).
- Virtualización de infraestructura: la virtualización más importante de toda la implementación de home-office es la de la red privada virtual (VPN) que permite la conexión de los empleados a la red interna de la empresa desde distintos puntos geográficos. De esta manera, el tráfico que se genera viaja cifrado dificultando a un tercero que pueda robar información confidencial [6].

Como se indicó anteriormente, el equipo que se adquiere para generar esta red virtual es el FortiGate 200E, que cubre y supera las necesidades para mantener la conexión de todos los empleados destinados a home-office.

6. Sistemas colaborativos

La empresa de salud publicitará sus Planes de Salud para las distintas edades y Planes Familiares tanto en Facebook como en Instagram. Además, se comunicará con los clientes o futuros socios a través de estas redes sociales y de WhatsApp. En primer lugar, se hacen recomendaciones en cuanto a las cuentas de la organización en estas aplicaciones y luego en lo que respecta a las publicaciones y envío de mensajes.

Recomendaciones a la hora de la creación de las cuentas de Facebook, Instagram y Whatsapp:

- Asociar las cuentas a un número de teléfono empresarial.
- Definir el tipo de cuenta como empresarial y realizar la verificación en caso de corresponder.
- Colocar una contraseña segura, como se explica en el apartado 1 de este proyecto (sección Seguridad Informática).
- Habilitar el doble factor de autenticación en cada una de las aplicaciones.
- Activar el monitoreo de inicio de sesión.

Se recomiendan los siguientes aspectos de seguridad en cuanto a las publicaciones:

- Subir fotos y/o videos de elaboración propia.
- No descargar cualquier tipo de archivo que pueda subir el público en general en los comentarios de las publicaciones.
- En caso de tener comentarios de cuentas extrañas, eliminarlos y bloquearlos.
- Tener instalado el antivirus Kaspersky en todos los dispositivos en los que se acceda a las redes sociales.

En lo que respecta a la comunicación con los clientes se realizan las siguientes recomendaciones de seguridad:

- Interactuar siempre con perfiles identificables.
- No entregar información confidencial ni personal a ningún usuario.
- En el caso de recibir mensajes inapropiados, denunciar el comentario y el perfil que corresponda.

7. Teletrabajo

Para esta nueva modalidad que adopta la empresa para algunos sectores de trabajadores, el modelo de teletrabajo más adecuado es el de Teletrabajador en Casa durante el período de la pandemia. Luego de finalizado el período se podría reversi pueden pasar a ser teletrabajadores flexibles.

Las características distintivas de este modelo son:

- Realización del trabajo en un lugar distinto al domicilio de la empresa: en la casa de cada empleado.
- Utilización de TICs para realizar el trabajo: notebook, celular, VPN, conexión a internet.
- Método de organización y ejecución de la actividad laboral: cada uno de los empleados, dependiendo del sector al que pertenezca deberá coordinar las actividades con su superior.

Recomendaciones de seguridad para el teletrabajador:

- Conectarse siempre a la VPN mediante redes privadas y seguras.
- Que la contraseña de sesión de la notebook cumpla con los requisitos mínimos de seguridad impuestos en la Política de Seguridad de la empresa.
- Que el celular posea factores biométricos para desbloquearlo.
- Permitir la actualización del sistema operativo de la notebook y del celular en cuanto estos dispositivos lo recomienden.
- No descargar programas que no sean de fuentes verídicas o páginas oficiales.
- Configurar el bloqueo automático en dispositivos luego de 10 minutos de actividad.
- Bloquear siempre los dispositivos cuando se dejen de usar o se pierdan de vista.
- Dejar habilitado el antivirus de los dispositivos en todo momento.
- Contactarse con el equipo de Seguridad Informática en caso de surgir algún incidente o tener alguna duda.

8. Conclusiones

Todo gran cambio merece grandes responsabilidades y grandes resultados. En este trabajo se detallaron todas aquellas responsabilidades y tareas que tendrán los equipos que sufrirán esta nueva modalidad de trabajo, desde los nuevos teletrabajadores hasta los equipos de Seguridad Informática y Sistemas que se harán cargo de la transición por completo. Se considera que este departamento está preparado y planificó las políticas y el programa de seguridad adecuados para comenzar con la implementación de este proyecto. A partir de este momento, la infraestructura de la empresa soportará modificaciones y se adaptará a todos los cambios logrando una nueva modalidad de trabajo mixta entre todos los empleados: empleados en oficinas y empleados en home-office.

Referencias Bibliográficas

[1] Las Claves del Éxito para la Gestión de Riesgos – ISOTools Excellence.

[2]Merce Molist (2014). El eslabón más débil en seguridad informática eres tú. https://www.elmundo.es/tecnologia/2014/01/18/52d-90707ca4741f2798b4570.html .

[3] 5 acciones para un proceso de Gestión de Riesgos eficaz. ISOTools Excellence. https://www.isotools.org/2017/10/08/5-acciones-proceso-de-gestion-de-riesgos-eficaz/#:~:text=Minimizar%20el%20impacto%20del%20riesgo,m%C3%ADnimo%20y%20f%C3%A1cil%20de%20subsanar .

[4] Software Backup Exec. Veritas. https://www.veritas.com/protection/backup-exec.

[5] Veritas Backup Exec. https://www.veritas.com/content/dam/Veritas/docs/data-sheets/V0276_GA_ENT_DS_BackupExec_20.1-EN.pdf.

[6] André Goujon (2012). ¿Qué es una VPN y cómo funciona para la privacidad de la información? https://www.welivesecurity.com/la-es/2012/09/10/vpn-funcionamiento-privacidad-informacion/.

SOBRE LA REVISTA

Sobre la Revista

ConCiencia Joven es una revista de la Facultad de Ingeniería de la Universidad Católica de Salta, Argentina, creada en el año 2022.

ConCiencia Joven brinda a la comunidad universitaria una plataforma de discusión, reflexión y exploración, teniendo como punto de partida la producción intelectual y material de alumnos vinculados a las carreras de grado, pre-grado y posgrado de la Facultad de Ingeniería de la UCASAL o de carreras de ingeniería de otras instituciones universitarias reconocidas.

La revista recibe artículos en español y en inglés.

Domicilio editorial – Facultad de Ingeniería. Sede Central: Campo Castañares - (Salta - Argentina)
Código Postal A4400EDD
Tel.: 54 - 0387 - 4268607
0810 555 822725 (UCASAL)
http://www.ucasal.edu.ar/eucasa

Política de acceso abierto y licencias de uso

incluir un reconocimiento a la publicación original realizada en esta revista, y por consiguiente al respectivo número donde se encuentra el artículo. En este sentido, el Autor/a asume el compromiso de informar al Editor/a, de manera formal, las autorizaciones y licencias pertinentes contraídas con terceros para el uso de la obra.

Apertura editorial

La revista mantiene y fomenta como política editorial la participación de autores, y miembros del equipo editorial, ajenos a la propia Universidad y unidades académicas vinculadas.

Autoría - Responsabilidad

La responsabilidad sobre las opiniones vertidas en los textos y sobre el respeto a la propiedad intelectual corresponde a los autores.

Asimismo, los autores declaran haber cumplido con las normas internacionales en materia de conflicto de intereses y normas éticas para la investigación y publicación de material académico y científico. En cualquier caso se debe informar sobre la existencia de vínculo comercial, financiero o particular con personas o instituciones que pudieran tener intereses relacionados con los trabajos que se publican en la revista.

Proceso editorial
Proceso de Evaluación

Los artículos basados en Proyectos finales, tesis, tesinas, etc. de grado o posgrado, además de la corrección correspondiente por parte del jurado académico en su momento, serán seleccionados para su publicación por el Comité Editorial, considerando la calidad académica sobresaliente y/u originalidad.

Los artículos que presentan resultados de investigaciones, deberán ser avalados por el director del proyecto en el marco del cual se desarrolló el trabajo, y a criterio del Comité Editorial, podrá ser objeto de evaluación académica.

Aquellos artículos provenientes de actividades de capacitación formal universitaria, o tipos de trabajos provenientes de actividades no curriculares, quedarán a criterio del Comité Editorial quien determinará la necesidad de una evaluación académica.

En todos los casos, se realizará una revisión de formato y estructura del contenido, de modo que el trabajo se ajuste a los requerimientos que en tal sentido formule la revista.

Integridad ético-académica

El equipo editorial de ConCiencia Joven se compromete con la comunidad educativa a garantizar la ética y la calidad de los artículos que publica. La revista adhiere al Código de conducta y buenas prácticas establecido por el Committee on Publication Ethics o COPE, *Code of Conduct and Best Practice Guidelines for Journal Editors y Code of Conduct for Journals Publishers.*

En cumplimiento de este código, la revista asegurará la calidad técnica y académica de las publicaciones y la adecuada respuesta a las necesidades de los lectores y los autores. El código

alcanza a todas las partes implicadas en el proceso editorial de la revista. El Comité Editorial se compromete a publicar las correcciones, aclaraciones, retracciones y disculpas cuando sea preciso.

Cargos por publicación

ConCiencia Joven es digitalmente distribuida sin fines de lucro, garantizando el acceso abierto a la publicación. Asimismo, la revista no retribuye económicamente a sus colaboradores por su participación, independientemente de si actúan como evaluadores o escritores.

La revista no aplica costos de ningún tipo, ya sea para el acceso al texto completo de todos los números y artículos, como para el envío de originales, evaluación, procesamiento de artículos aprobados y su respectiva publicación.

Política de privacidad
Compromisos generales del comité editorial

El Comité Editorial de *ConCiencia Joven* se compromete a velar por el cumplimiento del debido proceso editorial establecido.

Entrega de información relativa a una publicación

Toda la información brindada por aquellos que colaboran en el proceso editorial de la revista es archivada en bases de datos propias. Los mismos podrán ejercer sus derechos a conocer, actualizar, rectificar y suprimir sus datos personales en el caso que así lo consideren.

Interacción con los autores

El equipo editorial de *ConCiencia Joven* se compromete a mantener la confidencialidad de los artículos recibidos y a no usar en sus propias investigaciones datos, argumentos o interpretaciones hasta que el artículo sea publicado con expresa referencia de su origen. Asimismo, el equipo editorial garantiza imparcialidad y gestión adecuada de los artículos recibidos.

Los nombres y las direcciones de correo electrónico introducidos en esta revista se usarán exclusivamente para los fines establecidos en ella y no se proporcionarán a terceros o para su uso con otros fines.

Derechos del Autor

El Autor retiene los Derechos sobre su Obra, contemplando todos los objetos digitales que pueden resultar de la publicación electrónica posterior y/o distribución.

Una vez aceptada la Obra, el Autor concede a la Editorial el derecho exclusivo de su primera publicación , como también el derecho permanente a incluirla en todos los servicios y productos documentales que desarrolle la casa editora y constituyan un sistema de acceso al texto completo.

El Autor puede establecer acuerdos contractuales adicionales para la distribución no exclusiva de la versión publicada en la revista. Se debe proporcionar en el documento una mención de la publicación inicial en esta revista.

REVISTA

ConCiencia Joven

Número 1 - 2022

INGENIERÍA
UNIVERSIDAD CATÓLICA DE SALTA