	UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA			
	Documento	Código	Fecha	Revisión
	FORMATO HOJA DE RESUMEN PARA TRABAJO DE GRADO	F-AC-DBL-007	10-04-2012	A
Dependencia	Aprobado		Pág.	
DIVISIÓN DE BIBLIOTECA	SUBDIRECTOR ACADEMICO		i(115)	

RESUMEN – TRABAJO DE GRADO

AUTORES	ESTEFANIA GISELLE ALVAREZ CLARO
FACULTAD	INGENIERIAS
PLAN DE ESTUDIOS	INGENIERIA DE SISTEMAS
DIRECTOR	JESUS ALBERTO CAMARGO
TÍTULO DE LA TESIS	PLAN DE CONTINUIDAD DEL NEGOCIO PARA LA EMPRESA ASUCAP TV SAN JORGE

RESUMEN

EL RIESGO DE QUE UN INCIDENTE AFECTE LAS OPERACIONES NORMALES DE UNA EMPRESA SIEMPRE ESTA LATENTE. CON EL FIN DE MITIGAR EL IMPACTO DE INCIDENTES EN LA EMPRESA ASUCAP TV SAN JORGE SE DISEÑA E IMPLEMENTA UN PLAN DE CONTINUIDAD DEL NEGOCIO, YA QUE DICHO PLAN ESTA ORIENTADO A LA PROTECCION DE LAS PERSONAS, ASI COMO AL RESTABLECIMIENTO DE LOS PROCESOS, SERVICIOS CRITICOS E INFRAESTRUCTURA, FRENTE A EVENTOS DE INTERRUPCION.

CARACTERÍSTICAS

PÁGINAS: 115	PLANOS:	ILUSTRACIONES:	CD-ROM:
--------------	---------	----------------	---------



DISEÑO DE UN PLAN DE CONTINUIDAD DEL NEGOCIO PARA LA EMPRESA
ASUCAP TV SAN JORGE

Autor

ESTEFANÍA GISELLE ÁLVAREZ CLARO

Trabajo de grado presentado como requisito para optar por el título de ingeniero de
sistemas

Director

JESÚS ALBERTO CAMARGO

Esp. Ingeniero de Sistemas

UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA

FACULTADA DE INGENIERÍAS

INGENIERÍA DE SISTEMAS

Ocaña, Colombia

Octubre, 2020

Índice

	Pág.
Capítulo 1. Diseño de un plan de continuidad del negocio para la empresa ASUCAP TV SAN JORGE	1
1.1 Descripción de la empresa.....	1
1.1.1 Misión.	1
1.1.2 Visión..	1
1.1.3 Objetivos de la empresa.	2
1.1.4 Descripción de la estructura organizacional.....	3
1.1.5 Descripción de la dependencia y/o proyecto al que fue asignado.....	3
1.1.6 Diagnóstico inicial de la dependencia asignada.....	4
1.2 Planteamiento del problema	5
1.3 Objetivos de la pasantía.....	7
1.3.1 General..	7
1.3.2 Específicos..	7
1.4 Descripción de las actividades a desarrollar en la misma.....	8
 Capítulo 2. Enfoques referenciales	 9
2.1 Enfoque conceptual	9
2.2 Enfoque legal.....	9
 Capítulo 3. Presentación de resultados.....	 13
3.1 Realizar un diagnóstico de las tecnologías de información mediante una auditoría pasiva en la empresa ASUCAP TV SAN JORGE para la identificación de la situación actual de la organización	13
3.1.1 Misión, Visión y Objetivos de la empresa	15

3.1.2	Análisis de los procesos de apoyo de la empresa ASUCAP TV SAN JORGE.	15
3.1.3	Modelo de procesos.....	15
3.1.4	Proceso Gestión financiera.....	16
3.1.5	Proceso departamento de redes	17
3.1.6	Proceso departamento de programación	18
3.1.7	Proceso talento humano	19
3.1.8	Proceso mercadeo.....	20
3.2	Estudio los dominios de la norma ISO 27002:2013 Aplicado la empresa de ASUCAP TV San Jorge.....	20
3.3	Identificación de posibles riesgos asociados a la seguridad de la información de la empresa de ASUCAP TV SANJORGE	45
3.3.1	Controles para la seguridad de la información Gestión de activos	45
3.3.2	Seguridad física y del entorno Áreas Seguras.....	47
3.3.3	Equipos.....	48
3.3.4	Seguridad de las operaciones	49
3.3.5	Seguridad de las comunicaciones.....	50
3.4	Dictamen de auditoria.....	51
Capítulo 4. Presentación de resultados		53
4.1	Ejecución Norma ISO 31000:2018 Gestión de Riesgos.....	53
4.2	Ejecución Norma ISO 22301: Continuidad del Negocio	57
Capítulo 5. Conclusiones		87

Capítulo 6. Recomendaciones	88
Referencias	89
Apéndice	91

Lista de tablas

Tabla 1. Matriz DOFA (Debilidades, Oportunidades, Fortalezas y Amenazas	4
Tabla 2. Estrategias DOFA	5
Tabla 3. Descripción de las actividades a desarrollar.	8
Tabla 4. Roles y responsabilidades	15
Tabla 5. Dominios aplicados para la auditoria.....	21
Tabla 6 Lista de chequeo aplicada a la empresa ASUCAP TV SANJORGE	38

Lista de figuras

Figura 1. Estructura Organizacional de la empresa TV San Jorge	3
Figura 2. Modelo de procesos.....	16
Figura 3. Proceso Gestión financiera. Fuente: Autor del proyecto.....	16
Figura 4. Proceso departamento de redes. Fuente: Autor del proyecto	17
Figura 5. Proceso departamento de programación .Fuente: Autor del proyecto	18
Figura 6.Proceso talento humano. Autor del proyecto	19
Figura 7. Proceso mercadeo. Fuente: Autor del proyecto.....	20
Figura 8. Porcentaje pregunta 1	22
Figura 9.Porcentaje pregunta 2	23
Figura 10. Porcentaje pregunta 3	24
Figura 11. Porcentaje pregunta 4	24
Figura 12. Porcentaje pregunta 5	25
Figura 13.Porcentaje pregunta 6	26
Figura 14. Porcentaje pregunta 7	26
Figura 15. Porcentaje pregunta 8	27
Figura 16. Porcentaje pregunta 9	27
Figura 17. Porcentaje pregunta 10	28
Figura 18. Porcentaje pregunta 11	29
Figura 19. Porcentaje pregunta 12	29
Figura 20. Porcentaje pregunta 13	30
Figura 21. Porcentaje pregunta 14	30

Figura 22. Porcentaje pregunta 15	31
Figura 23. Porcentaje pregunta 16	31
Figura 24. Porcentaje pregunta 17	32
Figura 25. Porcentaje pregunta 18	32
Figura 26. Porcentaje pregunta 19	33
Figura 27. Porcentaje pregunta 20	33
Figura 28. Porcentaje pregunta 21	34
Figura 29. Porcentaje pregunta 22	34
Figura 30. Porcentaje pregunta 23	35
Figura 31. Porcentaje pregunta 24	35
Figura 32. Porcentaje pregunta 25	36
Figura 33. Porcentaje pregunta 26	36
Figura 34. Porcentaje pregunta 27	37
Figura 35. Presentación del plan.....	57
Figura 36. Plan de continuidad. Fuente. Ficohsa	58
Figura 37. Afectación.....	62
Figura 38. Incendio	65
Figura 39. Inundación/humedad	68
Figura 40. Interrupción de energía.....	69
Figura 41. Falla en el servicio de Red/Voz.....	71
Figura 42. Acceso no autorizado a la información lógica	73
Figura 43. Acceso físico no autorizado a las oficinas de T.I	75
Figura 44. Proceso de sanitario.....	83

Lista apéndice

Apéndice A. Programa para auditoria.....	92
Apéndice B. Instrumento de reelección de información.....	93
Apéndice C. Informe de auditoria.....	96
Apéndice D. Inventario Individual de Hardware.....	98
Apéndice E. Programa de auditoria.....	101
Apéndice F. Carta de culminación de los objetivos propuestos y compromiso por parte de la empresa para cumplir a cabalidad la debida implementación.....	102
Apéndice G. Evidencias fotográficas.....	103

Capítulo 1. Diseño de un plan de continuidad del negocio para la empresa

ASUCAP TV SAN JORGE

1.1 Descripción de la empresa

ASUCAP TV SAN JORGE, es una empresa constituida legalmente y netamente Ocañera, creada en el año 1991; se encuentra ubicada en el barrio Buenos Aires del municipio de Ocaña, perteneciente al departamento Norte de Santander. La función principal de esta empresa es la transmisión y producción de Televisión e Internet, con el fin de acercarse a la población de Ocaña por medio de los canales comunitarios y proporcionando la mejor calidad en el servicio de Internet utilizando los mecanismos, herramientas y dispositivos fundamentales, gracias a la gestión de arquitectura empresarial, lo que conlleva a la satisfacción Empresa-Usuario.

1.1.1 Misión. Somos una Asociación con miras a la excelencia, comprometida con la comunidad, ofreciendo producción propia a través de la señal de televisión e internet, contando con personal altamente competitivo.

1.1.2 Visión. En el 2022 Ser una Asociación líder, competitiva y comprometida con el desarrollo de la región, ofreciendo los mejores servicios de televisión e internet con tecnología de punta, programación y señal altamente calificada y certificada.

1.1.3 Objetivos de la empresa.

- ✓ Fomentar y estimular la participación de la comunidad en aspectos culturales, laborales, deportivos y recreativos, con el fin de ser medio eficaz de comunicación en el cual se puedan concentrar aspectos de interés común.
- ✓ Ser reconocida como la mejor empresa en Ocaña en cuanto a compromiso empresarial, responsabilidad social, apropiación de tecnología, eficiencia y eficacia en la prestación de sus servicios.
- ✓ Garantizar el crecimiento y sostenimiento de la empresa mediante el suministro de publicidad para el sector comercial de Ocaña.
- ✓ Incentivar el desarrollo económico, comercial y cultural a través de espacios para la industria y el comercio regional, mediante la difusión de sus estrategias comerciales y esfuerzos de mercadeo.
- ✓ Desarrollar contenidos y programación a partir de la opinión de los televidentes para alcanzar los niveles de raiting requeridos.
- ✓ Generar un clima laboral basado en el buen servicio donde el bienestar y el valor del talento humano que nos permita lograr las metas propuestas por la empresa.

1.1.4 Descripción de la estructura organizacional

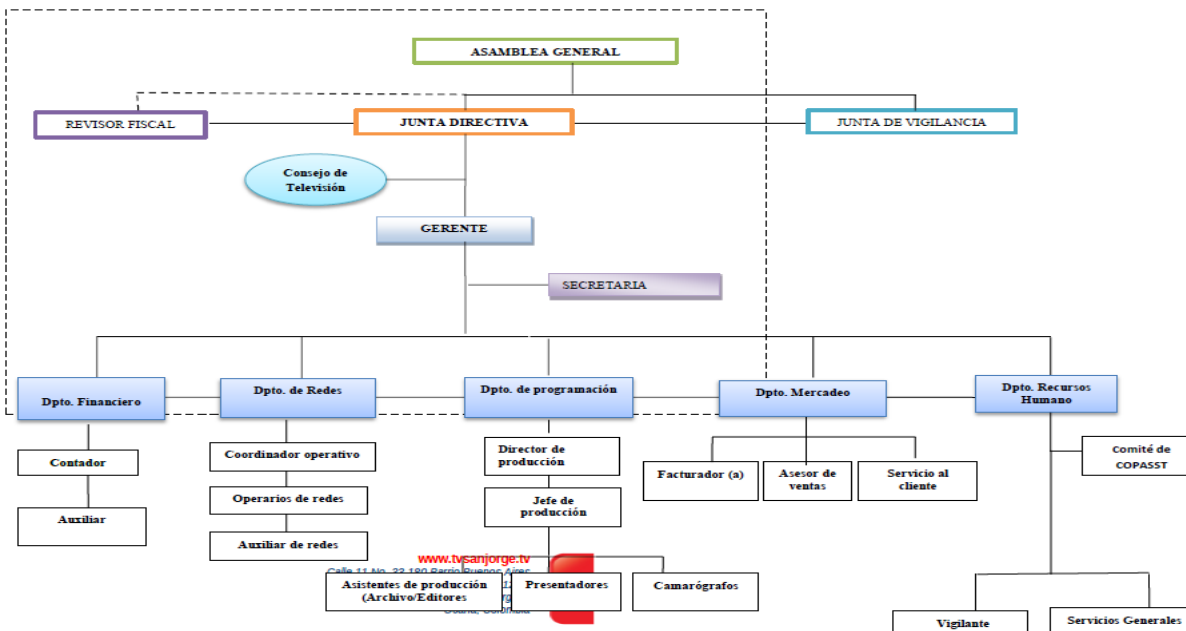


Figura 1. Estructura Organizacional de la empresa TV San Jorge

1.1.5 Descripción de la dependencia y/o proyecto al que fue asignado.

Actualmente el área Financiera, Telecomunicaciones y Televisión de la empresa ASUCAP TV SAN JORGE se encuentra en proceso de mejoramiento de las actividades que realizan, además, incluyendo crecimiento y expansión, deseando aumentar la calidad, eficacia y eficiencia del servicio prestado.

Debido a los deseos de la organización anteriormente mencionados, se debe contar con personal idóneo que apoye la ejecución de las tareas óptimas a realizar para el cumplimiento del objetivo.

1.1.6 Diagnóstico inicial de la dependencia asignada. Con el propósito de realizar un barrido inicial de la situación de la empresa a nivel del área en donde se plantea ejecutar las actividades en ASUCAP TV SAN JORGE, se plasma la matriz DOFA por medio de la cual se puede brindar soporte para la toma de decisiones empresariales.

Tabla 1

Matriz DOFA (Debilidades, Oportunidades, Fortalezas y Amenazas)

DEBILIDADES	OPORTUNIDADES
<ul style="list-style-type: none"> - Falta optimización de actividades en el sistema utilizado en el área financiera. - No cuenta con un plan estratégico que permita tomar las mejores decisiones frente a eventualidades presentadas. - Necesidad de mayor fuerza de venta. - No cuenta con un comité para la gestión de proyectos de crecimiento en la arquitectura empresarial. 	<ul style="list-style-type: none"> - Crear un plan estratégico de crecimiento empresarial para que permita mejorar el desempeño de la organización. - Determinar la viabilidad de los proyectos próximos a realizar. - Mayor afiliación de usuarios a la empresa. - Mejoramiento en los procesos que se llevan a cabo.
FORTALEZAS	AMENAZAS
<ul style="list-style-type: none"> - Personal idóneo de sistemas e informática. - Profesionalismo, compromiso y vocación de servicio por parte del personal. - Diversos planteamientos de ideas sobre proyectos para el crecimiento empresarial. - Disposición de recursos para implementar los mejoramientos y disposición del personal para mejorar el desempeño. 	<ul style="list-style-type: none"> - Utilización desmedida de recursos y esfuerzos en cuanto a la ejecución de actividades. - Proyectos en los que no se realice un estudio eficiente y no brinde el resultado esperado. - Competitividad de las diversas empresas que se encuentran en el municipio y prestan los mismos servicios.

Nota: la tabla muestra la matriz DOFA. Fuente. Autor del plan de trabajo.

Estrategias de la matriz DOFA aplicadas a la empresa ASUCAP TV SAN JORGE.

Tabla 2

Estrategias DOFA

ESTRATEGIAS (FO)	ESTRATEGIAS (DO)
<ul style="list-style-type: none"> - Realizar auditoria que permita obtener una visión de la situación actual de la organización. - Implementar metodologías que afiancen y aumenten el nivel de las ventas. - Estructurar un comité con personal idóneo en donde se promueva el monitoreo de cada uno de los procesos y proyectos en funcionamiento y próximos a funcionar. 	<ul style="list-style-type: none"> -Diseñar e implementar un plan estratégico de crecimiento empresarial en donde resalte los diversos mecanismos que promueven y consolidan la viabilidad de los proyectos. - Recolección de deficiencias en algunos procesos e implementar los ajustes necesarios. - Aumentar la confiabilidad de la población por medio de las nuevas medidas que se tomen con el fin de sumar más afiliaciones.
ESTRATEGIAS (FA)	ESTRATEGIAS (DA)
<ul style="list-style-type: none"> - Realizar capacitaciones sobre gestión de proyectos al personal involucrado. - Consolidar el compromiso de la empresa para mejorar la calidad de los servicios prestados. - Tener conocimiento adecuado sobre el manejo de los recursos. - Recaudar y organizar todas las ideas sobre ejecución de nuevos proyectos. 	<ul style="list-style-type: none"> - Evaluación eficaz y eficiente de los proyectos a ejecutar. - Mejorar la calidad del servicio prestado para contrarrestar la competencia que se genere con las demás empresas. - Implementar la tecnología y el sistema adecuado con el fin de lograr el objetivo y no malgastar recursos.

Nota: Estrategias planteadas. Fuente. Autor del plan de trabajo.

1.2 Planteamiento del problema

En la actualidad existen numerosos cambios en los mercados, competencias, organizaciones, tecnologías, sociedades y culturas, entre otros, razón por la cual se considera poco pertinente seguir maniobrando bajo el mismo enfoque tradicional. Para lograr ser competitivo dentro de este entorno tan cargado de dinamismo y turbulencia, es indispensable buscar ventajas competitivas y por ende un desarrollo económico a largo plazo, así como también desarrollar capacidad para producir, circular y utilizar

correctamente la información, la comunicación y el conocimiento, por cuanto ellos constituyen la materia prima de esta nueva sociedad. (Galo, 2018)

La empresa ASUCAP TV SAN JORGE es la encargada de la transmisión y producción de los servicios de Televisión e Internet; esta empresa se ha enfocado en ejecutar cada actividad de la mejor manera, realizando un gran esfuerzo con el fin de cumplir con el objetivo y la satisfacción de los clientes. Sin embargo, no se cuenta con un plan de continuidad en donde estén establecidas estrategias de negocio que permitan tomar decisiones óptimas para aumentar en un nivel considerable el crecimiento empresarial.

Los proyectos a ejecutar no cuentan con una adecuada planeación de las actividades y distribución de los recursos que garantice el cumplimiento de los requerimientos de las partes interesadas. (Cataño Turián & Pérez Monsalve, 2015). Al no contar con un plan de continuidad del negocio, se ve reflejado la falta de información sobre las fortalezas y oportunidades de mejora que se pueden implementar, de la misma manera, el descuido presentado frente a las debilidades y amenazas externas como lo es la competencia de las demás empresas que brindan los mismos servicios, desastres naturales, robo de información etc. Los planes de continuidad no son prioridad para la gran mayoría de empresas a nivel mundial, por lo que es necesario crear conciencia de la importancia de contar con este tipo de elementos para ser utilizados en caso se suscite algún siniestro. (Gustavo Adolfo, 2017)

1.3 Objetivos de la pasantía

1.3.1 General. Diseñar un plan de continuidad del negocio para la empresa ASUCAP TV San Jorge.

1.3.2 Específicos. Realizar un diagnóstico de las tecnologías de información mediante una auditoría pasiva en la empresa ASUCAP TV SAN JORGE para la identificación de la situación actual de la organización.

Definir estrategias que permitan la continuidad de los procesos en la empresa ASUCAP TV SAN JORGE para consignarlas en un plan de gestión de la continuidad.

Implementación del Plan de Continuidad del Negocio en la empresa ASCUPA TV SAN JORGE.

1.4 Descripción de las actividades a desarrollar en la misma.

Tabla 3

Descripción de las actividades a desarrollar.

Objetivo	General	Objetivos Específicos	Actividades a desarrollar en la empresa para hacer posible el cumplimiento de los Obj. Específicos
<p>PLAN DE CONTINUIDAD DEL NEGOCIO PARA LA EMPRESA ASUCAP TV SAN JORGE</p>		<p>Realizar un diagnóstico de las tecnologías de información mediante una auditoría pasiva en la empresa ASUCAP TV SAN JORGE para la identificación de la situación actual de la organización.</p>	<ul style="list-style-type: none"> -Recopilación de la información organizacional: Estructura orgánica, misión y visión de la empresa. -Entrevista con el jefe y los funcionarios de la empresa -Inventario de Hardware, Inventario de Software. -Aplicación de listas de chequeo (Seguridad de la información). -Revisión de la información obtenida del desarrollo de la auditoría. -Elaboración del borrador del Diagnóstico. - Presentación del borrador al Jefe de la empresa. -Elaboración y presentación del diagnóstico final.
		<p>Definir estrategias que permitan la continuidad de los procesos en la empresa ASUCAP TV SAN JORGE para consignarlas en un plan de gestión de la continuidad. Implementación del Plan de Continuidad del Negocio en la empresa ASUCAP TV SAN JORGE.</p>	<ul style="list-style-type: none"> Analizar las metodologías para la Gestión de la Continuidad del Negocio. - Presentación del plan de continuidad. -Seguimiento del plan de continuidad.

Nota: la tabla describe las actividades a desarrollar. Fuente. Autor del plan de trabajo

Capítulo 2. Enfoques referenciales

2.1 Enfoque conceptual

Seguridad de la información la definición de la seguridad de la información según Figueroa (2018) tributa a una disciplina "que se encarga de la implementación técnica de la protección de la información, el despliegue de las tecnologías que establecen de forma que se aseguran las situaciones de fallas parciales o totales, cuando la información es el activo que se encuentra en riesgo.

Continuidad del negocio. La continuidad del negocio es una colección de procedimientos e información que es desarrollada, compilada y mantenida en preparación para el uso en el evento de una emergencia o desastre (searchdatacenter, 2013).

Plan de continuidad del negocio. El plan de continuidad de negocio o BCP está orientado a la protección de las personas, así como al restablecimiento oportuno de los procesos, servicios críticos e infraestructura, frente a eventos de interrupción o desastre (searchdatacenter, 2013).

2.2 Enfoque legal

Siempre que se desea implementar un Sistema de Gestión, toda organización debe obligatoriamente cumplir con todas las leyes, normas, decretos, etc. que sean aplicables en el desarrollo de sus actividades. De manera general se puede mencionar el tema de seguridad

social, cumplir con la biblioteca, permisos, licencias de construcción, etc. pero en lo que se refiere específicamente a seguridad de la información, estas son las Leyes vigentes al día de hoy:

ISO 27001. La norma ISO 27001 fue publicada en octubre de 2005, esencialmente la sustitución de la antigua norma BS7799-2. Es la especificación para un SGSI, un Sistema de Gestión de Seguridad de la Información. Sí BS7799 era un estándar de larga data, publicado por primera vez en los años noventa como un código de prácticas. Como este maduró, una segunda parte surgió para cubrir los sistemas de gestión. Es esto en contra de la cual se concede la certificación. Hoy en día más de mil certificados están en su lugar, en todo el mundo. (Castro & Ciacedo, 2013). Certificación del Sistema de Gestión de Seguridad de la Información con ISO/IEC 27001 – ICONTEC. El Instituto Colombiano de Normas Técnicas y Certificación (ICONTEC), es el Organismo Nacional de Normalización de Colombia. Entre sus labores se destaca la creación de normas técnicas y la certificación de normas de calidad para empresas y actividades profesionales. ICONTEC es el representante de la Organización Internacional para la Estandarización (ISO), en Colombia. (NTC-ISO/IEC, 2006).

El estándar para la seguridad de la información ISO/IEC 27001 especifica los requisitos necesarios para establecer, implantar, mantener y mejorar un Sistema de Gestión de la Seguridad de la Información (NTC-ISO/IEC, 2006) Abarca: - Organización de la seguridad de la información. - Política de seguridad. - Gestión de activos. - Control de acceso. - Seguridad de los recursos humanos. - Cumplimiento. - Seguridad física y del entorno. - Adquisición, desarrollo y mantenimiento de los sistemas de información. - Gestión de las comunicaciones y operaciones. - Gestión de la continuidad del negocio. - Gestión de incidentes de seguridad de la información.

(ICONTEC, 2014). Ley 23 De 1982 Sobre derechos de autor. Los autores de obras literarias, científicas y artísticas gozarán de protección para sus obras en la forma prescrita por la presente Ley y en cuanto fuere compatible con ella, por el derecho común. También protege esta Ley a los intérpretes o ejecutantes, a los productores de programas y a los organismos de radiodifusión, en sus derechos conexos a los del autor.

Ley 527 De 1999. Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones. (Archivo General, 1999). Ámbito de aplicación. La presente ley será aplicable a todo tipo de información en forma de mensaje de datos, salvo en los siguientes casos:

- En las obligaciones contraídas por el Estado colombiano en virtud de convenios o tratados internacionales; en las advertencias escritas que por disposición legal deban ir necesariamente impresas en cierto tipo de productos en razón al riesgo que implica su comercialización, uso o consumo (Ley 527 De 1999, 2014) (secretaria senado, 2020).

Ley Estatutaria 1266 Del 31 De diciembre De 2008. Decreto N° 2952 de 2010 por el cual se reglamentan los artículos 12 y 13 de la Ley 1266 de 2008, EL PRESIDENTE DE LA REPÚBLICA DE COLOMBIA. En ejercicio de sus facultades constitucionales y legales, en especial, las conferidas por el numeral 11 del artículo 189 de la Constitución Política y en desarrollo de lo previsto en los artículos 12 y 13 de la Ley 1266 de 2008. 37 Que el 31 de diciembre de 2008 se expidió la Ley Estatutaria N° 1266 por la cual se dictan las disposiciones

generales del Hábeas Data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones (secretaria senado, 2020).

Ley 1273 Del 5 De enero De 2009. "Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones" (secretaria senado, 2020).

(Ley 1273 5 de enero de 2009). El 5 de enero de 2009 se decretó la Ley 1273 de 2009, la cual añade dos nuevos capítulos al Código Penal Colombiano: Capítulo Primero: De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos; Capítulo Segundo: De los atentados informáticos y otras infracciones. Como se puede ver, esta Ley está muy ligada a la ISO 27000, lo cual coloca al País a l vanguardia en legislación de seguridad de la información, abriendo así la posibilidad de nuevas entradas con este tema (secretaria senado, 2020).

Ley estatutaria 1581 de 2012. Por la cual se dictan disposiciones generales para la protección de datos personales. La presente ley tiene por objeto desarrollar el 38 derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos, y los demás derechos, libertades y garantías constitucionales a que se refiere el artículo 15 de la Constitución Política; así como el derecho a la información consagrado en el artículo 20 de la misma (Secretaria Senado, 2012).

Capítulo 3. Presentación de resultados

3.1 Realizar un diagnóstico de las tecnologías de información mediante una auditoria pasiva en la empresa ASUCAP TV SAN JORGE para la identificación de la situación actual de la organización

Descripción de la empresa: El sistema parabólico San Jorge nace en el año 1989 como producto de un proyecto de grado, cuya iniciativa fue de los ingenieros eléctricos Ciro Rodríguez y Raúl Rochel, quienes dos años más tarde lo entregan a la comunidad. Fue así como el 31 de agosto de 1991 nace la Asociación de Usuarios Comunitarios de la Antena Parabólica ASUCAP San Jorge en Ocaña, Norte de Santander, Colombia, con cerca de 700 usuarios ASUCAP SAN JORGE fue creciendo de manera rápida tanto en Asociados como en servicio de televisión.

La Junta Directiva del año 1998, vio la necesidad de tener producción propia de televisión, de tal forma que le hicieron el llamado a César Numa, Productor de Televisión, y le presentaron la propuesta. El señor Numa asumió con responsabilidad el reto y luego de varios meses de trabajo, el 31 de Agosto 1998 inicia la Televisión Comunitaria en Ocaña con la emisión de un informativo llamado **EL NOTICIERO**, cuyo slogan era *Informar para Educar* donde se daba a conocer los hechos relevantes de la ciudad, contando con la participación de un selecto equipo de trabajo como el reconocido periodista Geovanny Alfonso Torres Jácome, el productor de Televisión Yesid Antonio Navarro Areniz, el docente y periodista Rubén Helí Santisteban Carrascal, la joven presentadora Hayfa Numa Marchena, el periodista deportivo Jairo Alonso Rizo y el Productor de Televisión César Numa.

En el 2000 la comisión nacional de televisión (CNTV) da la licencia para que pueda funcionar de manera legal. El Canal Comunitario TV San Jorge empieza a brindarles a todos los usuarios una televisión con el fin educativo, cultural e informativo; después de que le fue otorgada la licencia, la programación tenía una durabilidad de una hora.

El sistema de televisión fue creciendo y así mismo la demanda de producción de televisión. A partir del año 2004 el canal comienza a brindar tres horas de programación propia agregando además del informativo programa de salud, cultura, ambientales, de opinión y un espacio directo para la comunidad. Gracias al fortalecimiento de la producción de televisión todos los programas que se hacen con un objetivo comunitario, dándole grandes satisfacciones al sistema con los premios y nominaciones que ha recibido el canal. Entre ellos cabe mencionar el Premio Nacional al Periodismo Agropecuario (SAC), Segundo lugar en el Premio Nacional Ambiental, Nominación a los Premios India Catalina e innumerables premios y nominaciones en la cooperativa multiactiva de televisión comunitaria (COMUTV), y en el año 2017 le otorgan el **Premio India Catalina como Mejor Producción de Televisión Comunitaria de Colombia** y cuyo programa ganador fue *Sequía en el Catatumbo*, presentado y dirigido por el periodista Geovanny Mejía Cantor.

A la fecha el canal Comunitario Tv San Jorge cuenta con un posicionamiento y reconocimiento en el país, gracias a su excelente producción comunitaria que ha logrado identificar a los Ocañeros.

ASUCAP SAN JORGE, empresa líder a nivel nacional cuenta con una nómina de cerca de 50 empleados que están muy comprometidos con el crecimiento de esta empresa comunitaria

3.1.1 Misión, Visión y Objetivos de la empresa

Tabla 4

Roles y responsabilidades

Talento humano	Rol
Geovanny Alfonso Torres Jácome	Presidente Junta Directiva
Oswaldo Augusto Jácome Suarez	Gerente
Yurbey Hernández	Jefe de personal
Yesid Antonio Navarro Areniz	Director Canal Comunitario
Iván Navarro Portillo	Coordinador informativo
Orlando Santiago Pérez	Coordinador Magazin Sala 20
Danuil Alexander Navarro Pérez	Coordinador Mercadeo y Publicidad
Ing. Edwin Ascanio	/ Director Telecomunicaciones
Hugo Marcell Bacca	Jefe Internet
Adrián Ricardo Lobo	Jefe Operativo
Dolly Rocío Arévalo	Contadora Publica
Nohemí Galvis	Jefe de Facturación

Nota: Se describen los roles de los empleados. Fuente: información de la empresa.

3.1.2 Análisis de los procesos de apoyo de la empresa ASUCAP TV SAN JORGE.

La empresa ASUCAP TV SAN JORGE cuenta con diversos procesos de apoyo que permiten el crecimiento y fortalecen la continuidad del negocio por medio de las actividades estipuladas y de actividades que surgen dependiendo de las necesidades que se presenten.

Dentro de estos procesos de apoyo se encuentran: Área Internet, Área Televisión, Área producción de televisión, Área presupuestal, Área financiera.

3.1.3 Modelo de procesos. Para llevar a cabo la realización de modelado de procesos se consultó información suministrada por el personal de la empresa

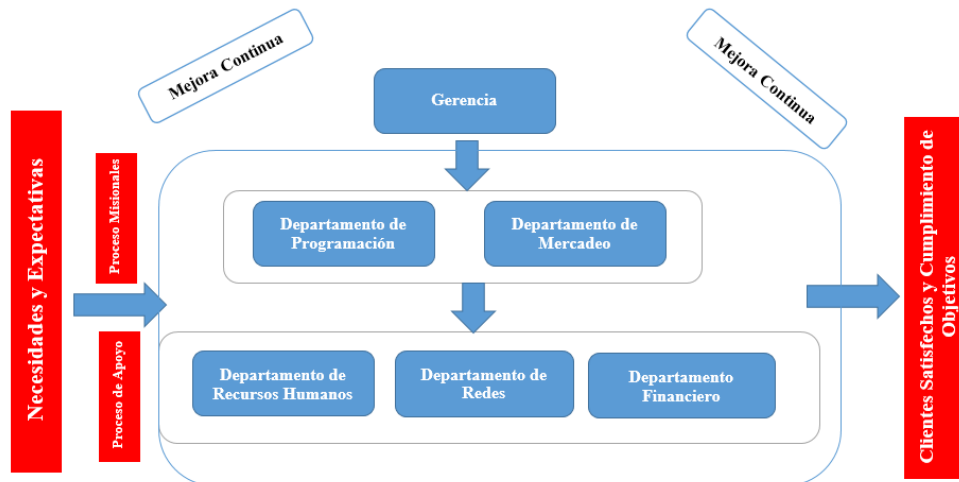


Figura 2. Modelo de procesos

3.1.4 Proceso Gestión financiera

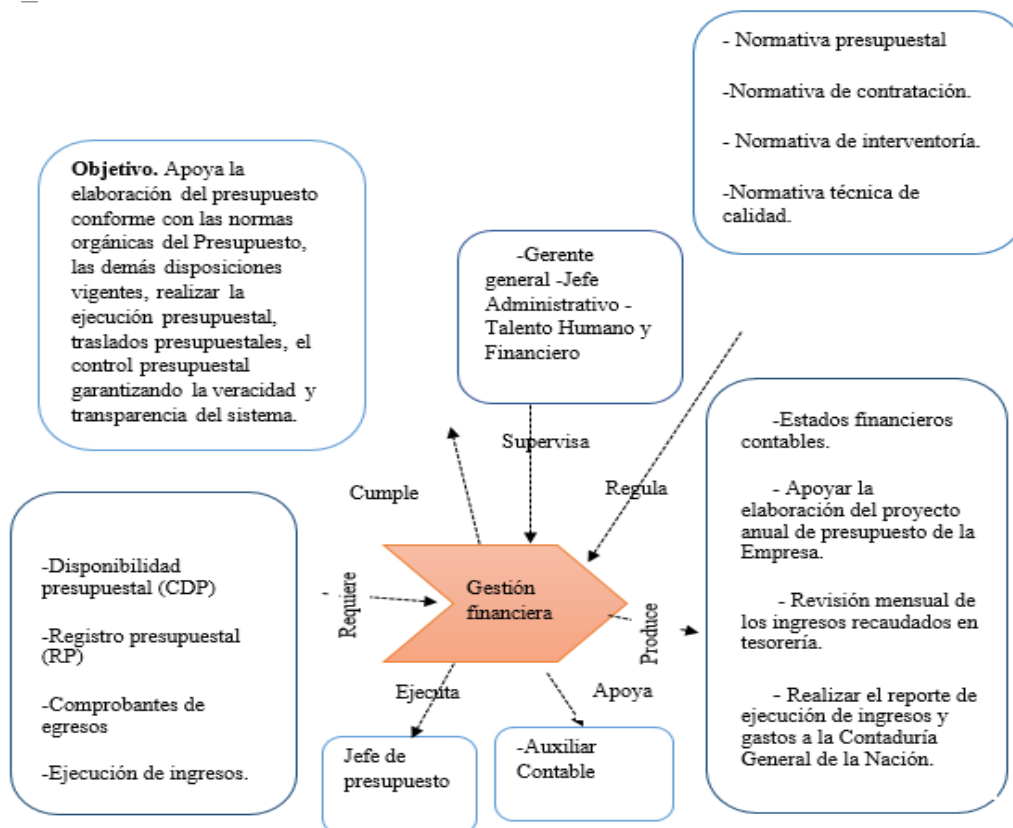


Figura 3. Proceso Gestión financiera. Fuente: Autor del proyecto

3.1.5 Proceso departamento de redes

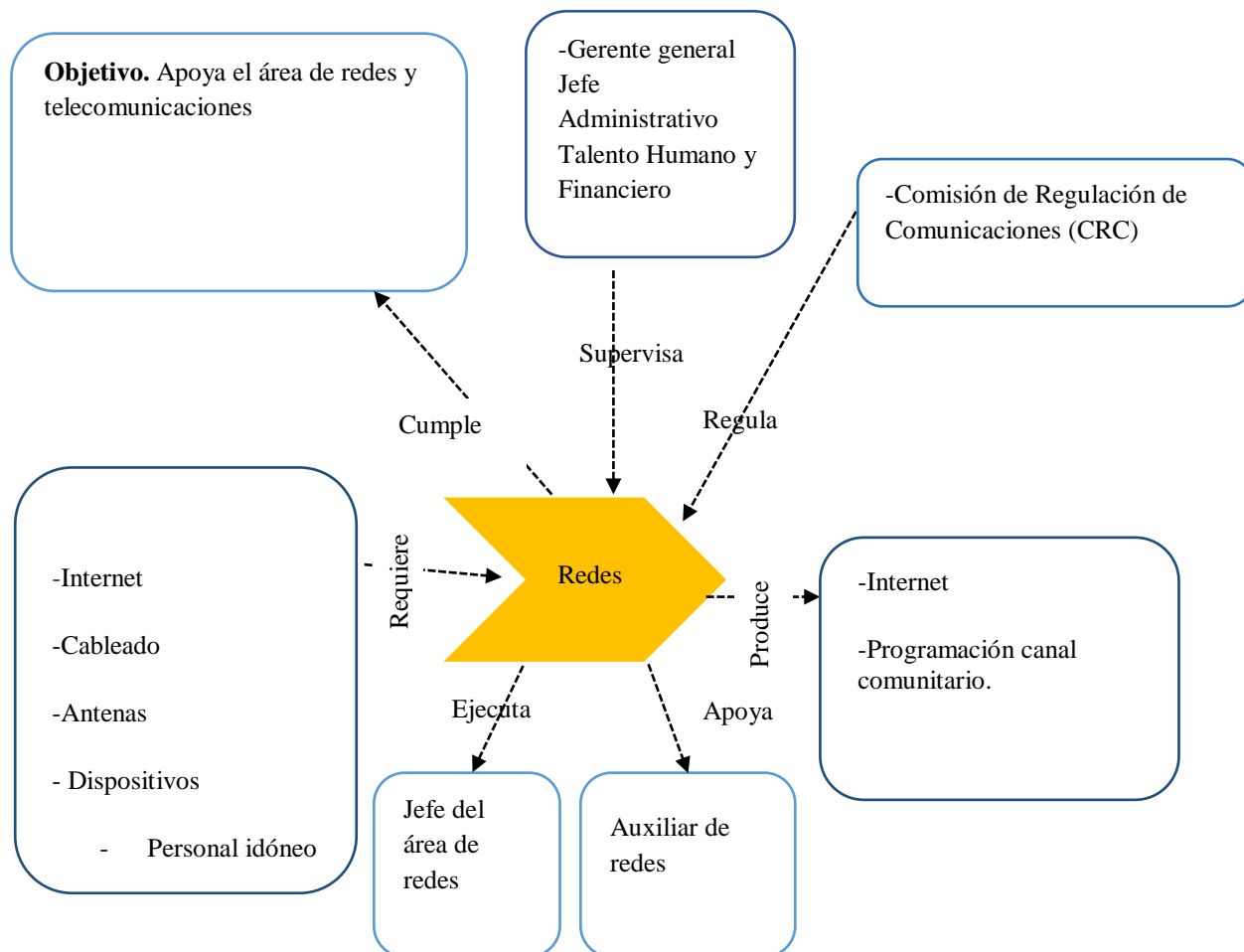


Figura 4. Proceso departamento de redes. Fuente: Autor del proyecto

3.1.6 Proceso departamento de programación

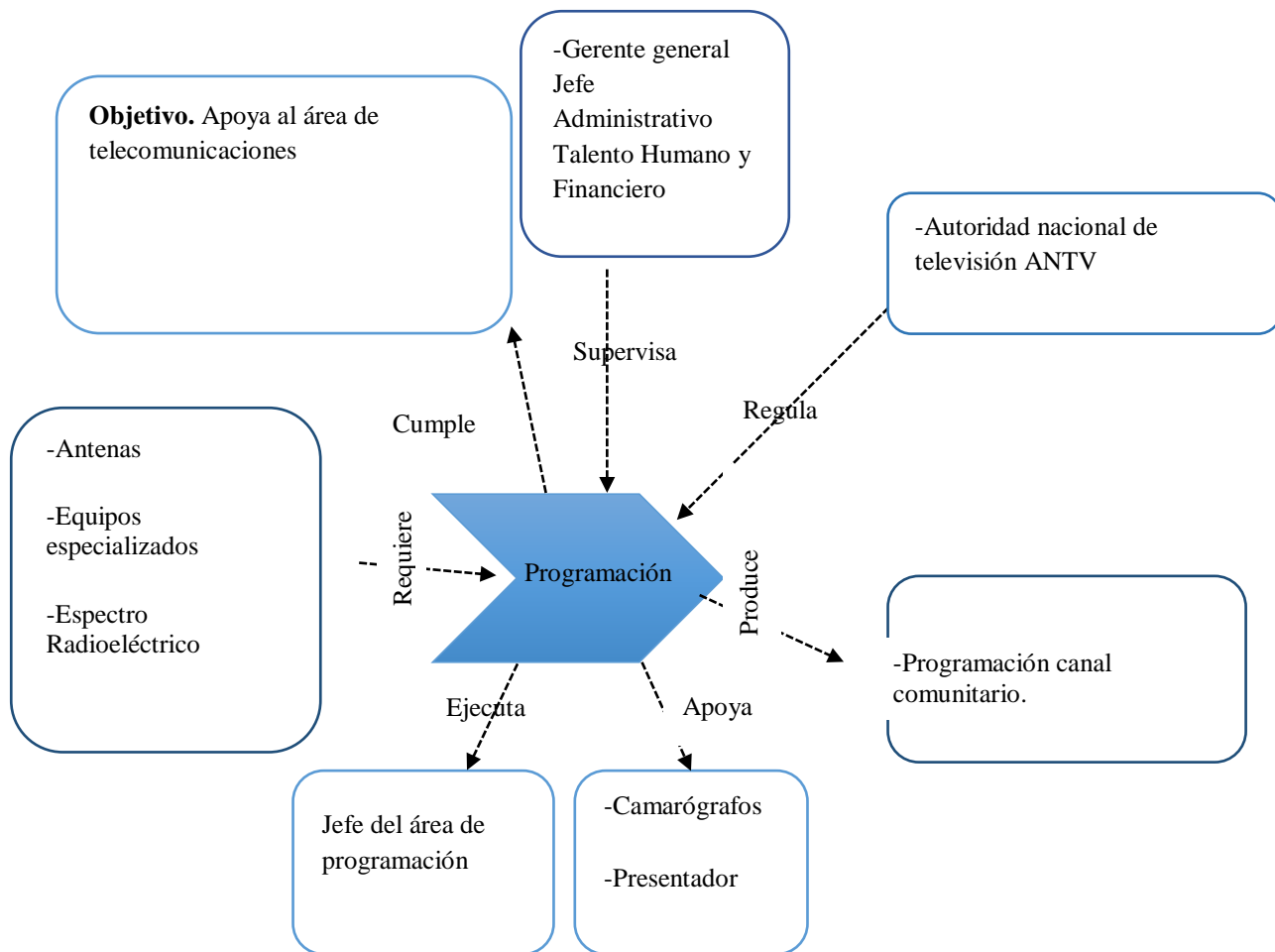


Figura 5. Proceso departamento de programación .Fuente: Autor del proyecto

3.1.7 Proceso talento humano

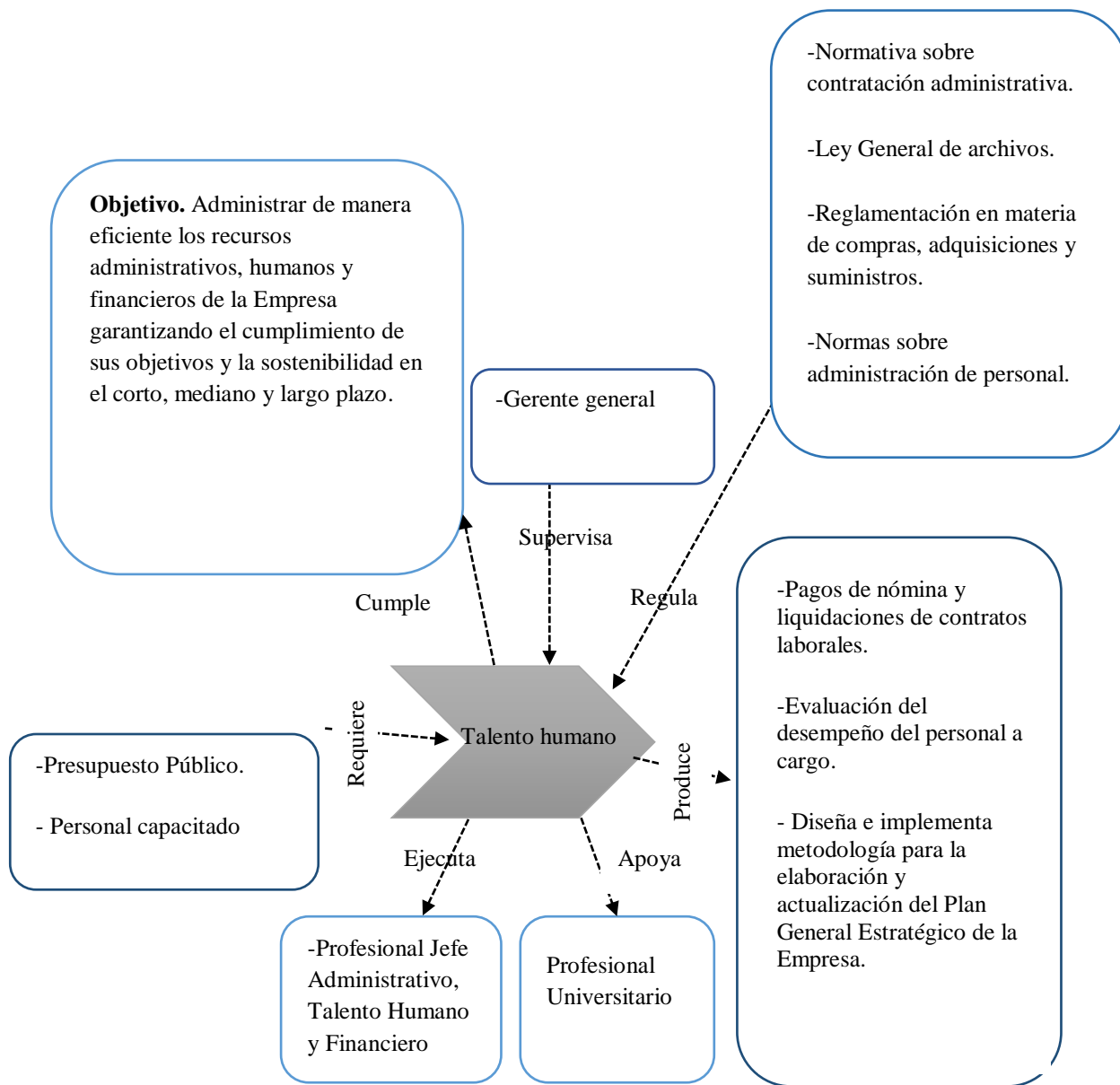


Figura 6. Proceso talento humano. Autor del proyecto

3.1.8 Proceso mercadeo

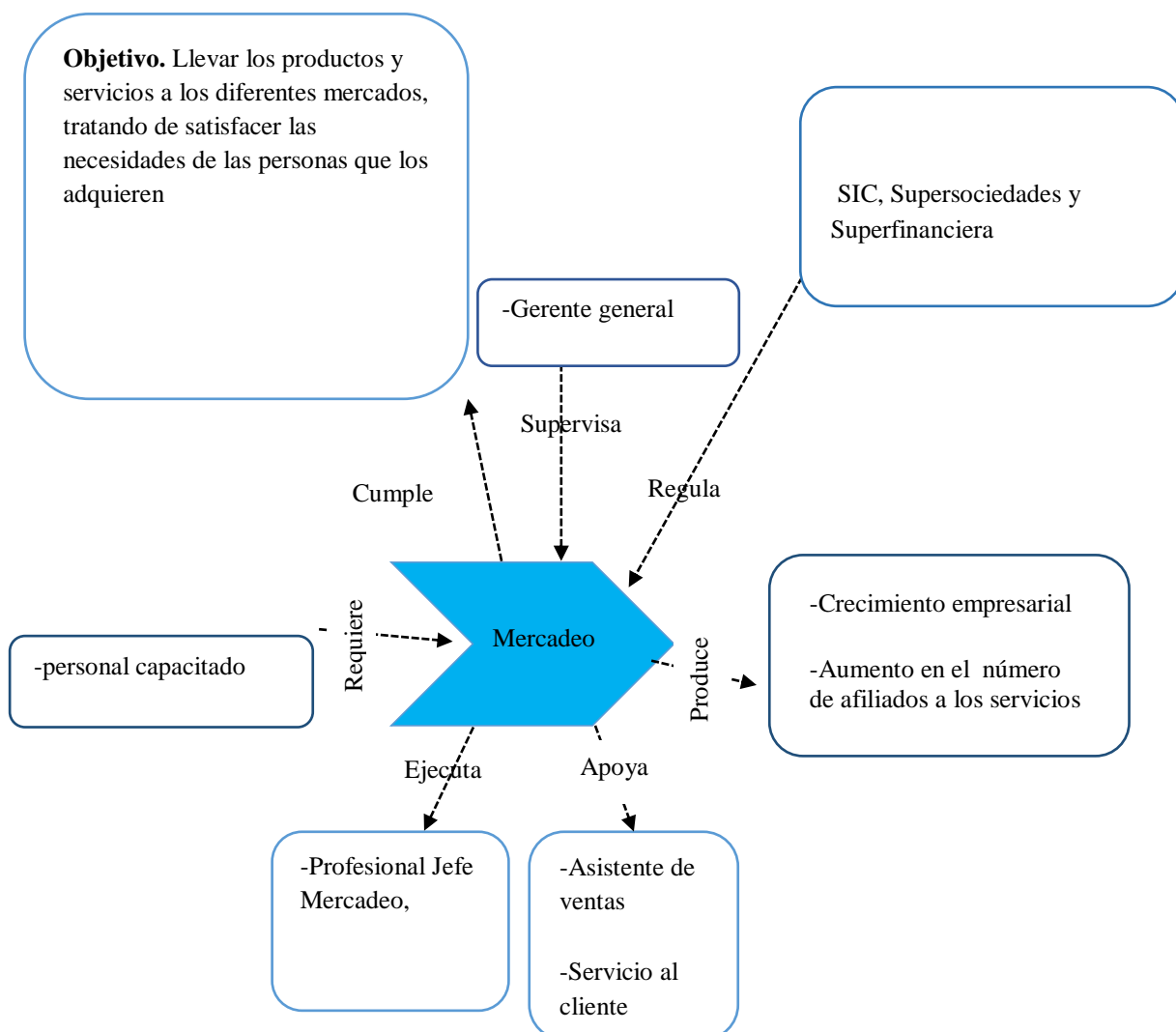


Figura 7. Proceso mercadeo. Fuente: Autor del proyecto

3.2 Estudio los dominios de la norma ISO 27002:2013 Aplicado la empresa de ASUCAP TV San Jorge

Para la realización de la auditoria se llevó la acabo el estudio previo de los dominios de la norma ISO 27002:2013 con la finalidad de establecer cuáles de los dominios de la norma que se

ajustan la actividad de negocios de la empresa **ASUCAP TV San Jorge** con el fin de diagnosticar la situación actual en la que se encuentra la empresa, además de identificar los riesgos, las vulnerabilidades a las que se encuentra expuesta la empresa y dar las respectivas recomendaciones.

En la siguiente tabla se presentarán los dominios que aplicarán para la auditoría. A5, A8, A9, A10, A11, A12, A16, A17.

Tabla 5

Dominios aplicados para la auditoría

Dominio	Descripción
A5	Políticas de seguridad de la información.
A8	Gestión de activos.
A9	Control de acceso
A10	Criptografía
A11	Seguridad física y del entorno
A12	Seguridad de las operaciones
A16	Gestión de incidentes de seguridad de la información.
A17	Aspectos de seguridad de la información de la gestión de continuidad de negocio.

Nota: La tabla describe los dominios para la auditoría. Fuente: autor del proyecto. Autor del proyecto

Diagnóstico de la situación actual de la empresa ASUCAP TV San Jorge. Para llevar a cabo la identificación de los riesgos a los que se encuentra expuesta la empresa **ASUCAP TV San Jorge** en cuanto a infraestructura tecnológica, hardware, software y seguridad de la información se realizaron una serie de entrevistas y encuestas al personal administrativos de la empresa la cual nos permitió evidenciar los siguientes resultados.

Conforme con los parámetros establecidos para el desarrollo del análisis se realizó una auditoría con el objetivo de realizar un estudio de los procesos que se llevan a cabo en la organización, para de esta manera identificar la situación actual de la empresa **ASUCAP TV San Jorge**. La encuesta fue dirigida al Jefe de telecomunicaciones y el ooperario de redes e internet.

La auditoría permitió la evaluación de los criterios establecidos dentro de los siguientes dominios y subdominios de la norma ISO27002:2013

1. ¿La empresa ASUCAP TV San Jorge cuenta con políticas de seguridad de información?

4 respuestas

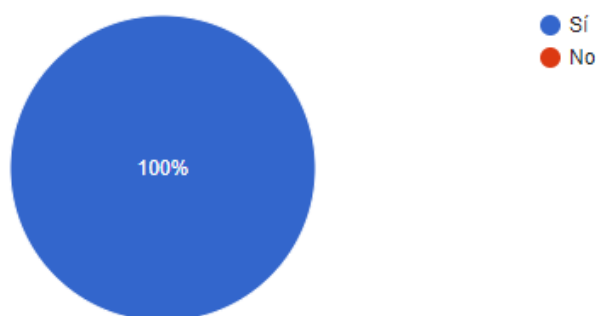


Figura 8. Porcentaje pregunta 1

El 100% de los encuestados manifestó que la empresa ASUCAP TV San Jorge cuenta con las políticas de seguridad de la información, lo que evidencia en gran medida la seriedad con la que se toma la seguridad de la información en la empresa

2. ¿La empresa cuenta con un inventario de activos de la información actualizados?

4 respuestas

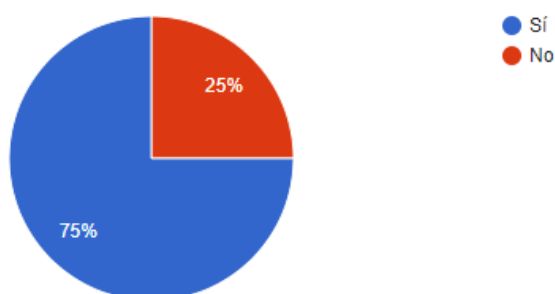


Figura 9. Porcentaje pregunta 2

Se evidencia que entre el total de encuestados el 75% afirmó que la empresa cuenta con activos de la información debidamente actualizados, frente a un 25% el cual mencionó que no cuentan con esos inventarios. Esto da a entender que no se tiene información completa y certera sobre los activos de la empresa, por lo cual se brinda como recomendación el estudio y actualización de esta con el fin elaborar un inventario que proporcione toda la información necesaria y se puedan tomar decisiones en caso tal que se presenten incidentes con los activos.

3. ¿La empresa ASUCAP TV San Jorge cuenta con manual de políticas de control de acceso?
Sí la respuesta es si conteste la pregunta No 4.

4 respuestas

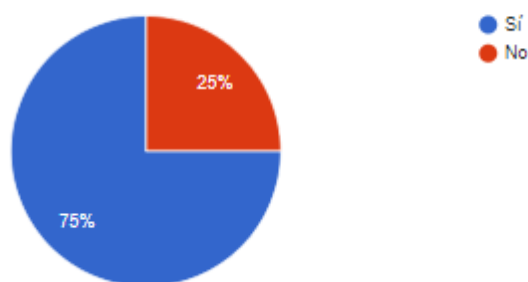


Figura 10. Porcentaje pregunta 3

Se evidencia que el 75% manifestó que la empresa cuenta con un manual de políticas de control de acceso frente a un 25%. Se infiere que no todo el personal conoce sobre estas políticas, es importante que todos estén informados de cualquier situación, ya sea en el caso de que el personal sea nuevo con el objetivo de mantener la comunicación o con el personal antiguo con el fin de salvaguardar y ser responsable de los activos o herramientas a cargo.

4. ¿Las políticas de control de acceso son aplicadas?

4 respuestas

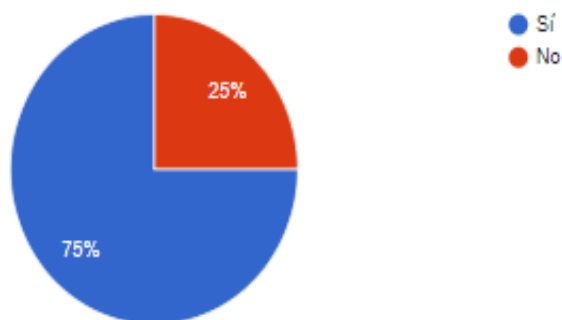


Figura 11. Porcentaje pregunta 4

Se evidencia que el 75% de los encuestado manifesto que las politicas de control de acceso son aplicadas frente a un 25% el cual manifesto que no son aplicadas. Se puede inferir que el 25% de los encuestados quienes manifestaron que las politicas de control de acceso no son aplicadas sean el mismo 25% que manifestó que no se contaban con esas politicas.

5. ¿Todas las aplicaciones cuentan con una contraseña para permitir el acceso a los usuarios?
4 respuestas

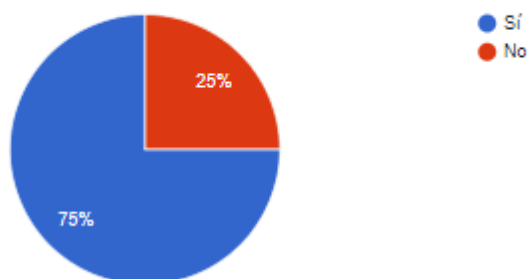


Figura 12. Porcentaje pregunta 5

El 75% de los encuestados manifestó que las aplicaciones que usan tienen contraseñas para permitir el acceso, frente a un 25% quien manifestó que no tienen esas contraseñas. Existe un porcentaje de empleados que han manifestado el no contar con ciertos elementos, es repetitivo en varias preguntas, por lo que resulta muy importante capacitar e informar a ese porcentaje de personal para mantener una buena comunicación.

6. ¿las credenciales de acceso del personal (usuarios y contraseñas) tienen una combinación de mayúsculas, minúsculas y números?

4 respuestas

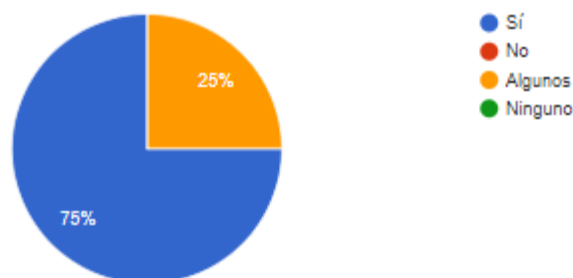


Figura 13. Porcentaje pregunta 6

Del total de encuestados se evidencia que el 75% tiene contraseñas que cumplen con los protocolos establecidos en cuanto a seguridad, manteniendo las combinaciones necesarias, frente a un 25% que no hace uso de contraseñas seguras. Aquí es notable observar según la gráfica que se hace evidente la necesidad de una reunión con el personal para colocarlos al tanto de los procesos que se están manejando en lo que hace referencia a la seguridad de la información con el fin de prevenir robos o mal uso del activo que se encuentra procesando.

7. ¿El personal realiza periódicamente cambios de dichas contraseñas?

4 respuestas

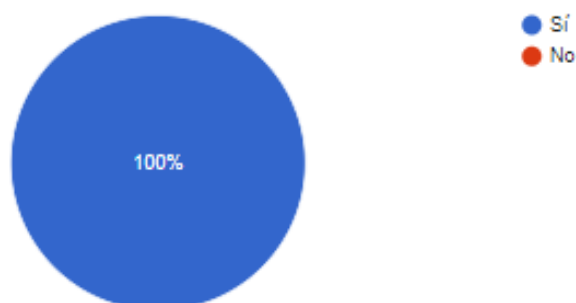


Figura 14. Porcentaje pregunta 7

El 100% manifestó que realiza cambios de las contraseñas periódicamente, es importante que los empleados actualicen sus contraseñas constantemente para mantener ciertos niveles de seguridad. En la empresa se tiene establecido el cambio de contraseña cada 3 meses.

8. ¿las aplicaciones cuentan con restricción de acceso a páginas web (redes sociales, instagram, twitter etc.)?

4 respuestas

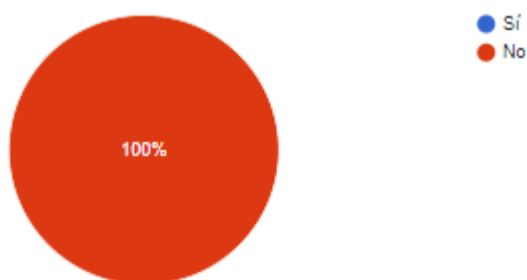


Figura 15. Porcentaje pregunta 8

El 100% de los encuestados manifestó que las páginas web no tienen un control de acceso con las redes sociales, resulta fundamental que a los empleados se les restrinja ciertas páginas por las cuales se podrían presentar casos de ingeniería social u otro problema de cualquier índole.

9. ¿Los empleados de la empresa cuentan con un acuerdo de confidencialidad de la información?

4 respuestas

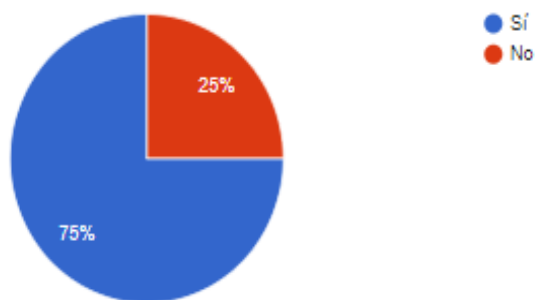


Figura 16. Porcentaje pregunta 9

El 75% de los encuestados menciono que la empresa cuenta con un acuerdo de confidencialidad frente a un 25% los cuales afirmaron que la organización no las tenía, como se ha mencionado anteriormente en otras preguntas en donde existe un porcentaje de empleados en los que se evidencia no estar al día con cierta información de la empresa, por lo que resulta fundamental capacitarlos e indicarles con que se cuenta y con que no. Además, se da oportunidad para la inclusión de una cláusula contractual donde se haga compromiso con éste parámetro.

10. ¿El personal Realiza Backup (Copias de Seguridad de la Información) de la información que gestiona?

4 respuestas

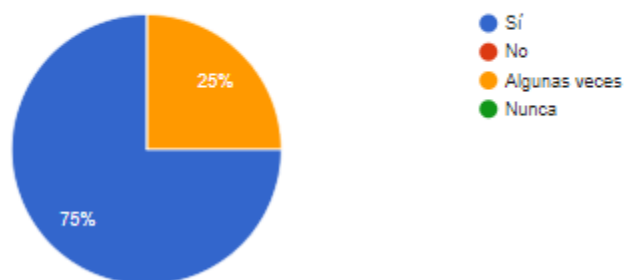


Figura 17. Porcentaje pregunta 10

El 75% de los encuestados manifestó que realizan Backups frente a un 25 % que no lo hace. Se da a conocer que no todo el personal realiza las copias de seguridad, exponiendo a riesgos latentes la pérdida de dicha información importante, por lo cual si no es manejada adecuadamente puede caer a manos de terceros o interrumpir los procesos que se estén llevando a cabo en la empresa.

11. ¿Se realizan copias de seguridad a los sistemas información?

4 respuestas

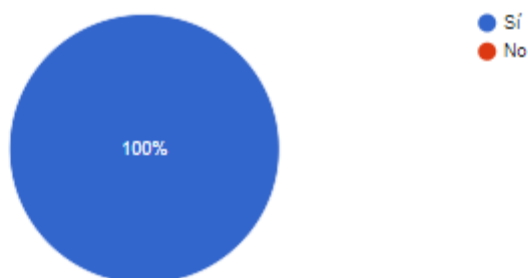


Figura 18. Porcentaje pregunta 11

El 100% de los encuestados manifestó que si se realizan copias de seguridad, esto resulta importante ante cualquier caso de emergencia que pudiese presentar porque permite tener un respaldo ante cualquier eventualidad.

12. ¿En qué medios se almacenan las copias de seguridad ?

4 respuestas



Figura 19. Porcentaje pregunta 12

13. ¿Cómo se permite el acceso a las copias de seguridad?

4 respuestas

Contraseña
Un encargado tiene las contraseña para recuperar las copias de seguridad
SOLICITANDOLO AL JEFE INMEDIATO DE CADA AREA
Por contraseñas

Figura 20. Porcentaje pregunta 13

14. ¿Los equipos de la dependencia están ubicados en lugares estratégicos para evitar amenazas o peligro al entorno, además de manipulación externa?

4 respuestas

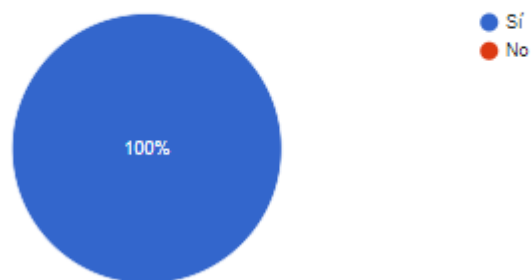


Figura 21. Porcentaje pregunta 14

El 100% de los encuestados manifestó que los equipos en la empresa se encuentran en un lugar estratégico, lo que resulta importante por los procesos que maneja la información en cuanto al uso de y edición de noticias o primicias, además, el resguardo y protección de los mismos frente a eventualidades no esperadas.

15. ¿Los equipos están protegidos contra fallas en el suministro de energía y otras anomalías?

4 respuestas



Figura 22. Porcentaje pregunta 15

El 100% de los encuestados manifestó que la empresa cuenta con las herramientas necesarias para evitar fallas en el suministro de energía ya que se cuenta con UPS dentro de la empresa y en las diferentes estaciones de trabajo como lo son las torres; es fundamental que se cuenten con ciertas medidas de contingencia frente a las nuevas medidas de expansión tecnológica tomadas por la empresa.

16. ¿La empresa cuenta con un procedimiento formal de reportes de incidentes?

4 respuestas

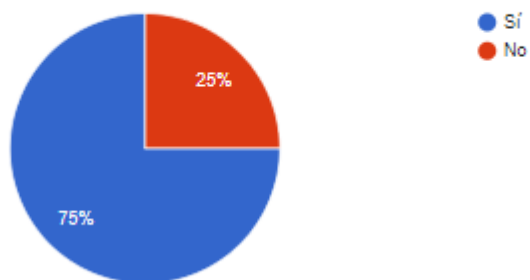


Figura 23. Porcentaje pregunta 16

El 75% de los encuestados manifestó que la empresa cuenta con el procedimiento de

reporte de incidentes frente a un 25 % que menciono que no cuenta con los procedimientos, es fundamental tener al personal informado y capacitado para dar paso una solución oportuna.

17. ¿Son capacitados para que el manejo de la información se suministre de una forma segura?

4 respuestas

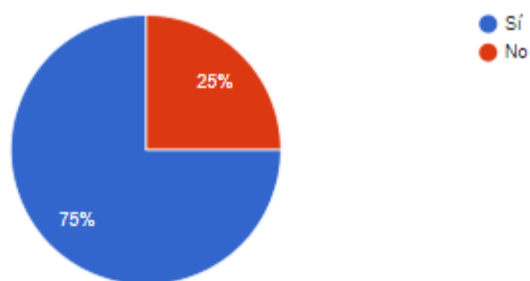


Figura 24. Porcentaje pregunta 17

El 75% de los encuestados manifestó que son capacitados frente a un 25 % que afirmo que no es capacitado. Esto pone en constancia lo que anteriormente se evidenciaba en cuanto a la capacitación y la transmisión de información, surgiendo la necesidad de aplicar medidas con respecto a la seguridad de la información.

18. ¿Se identifican los activos organizacionales y se definen las responsabilidades de protección adecuadas?

4 respuestas

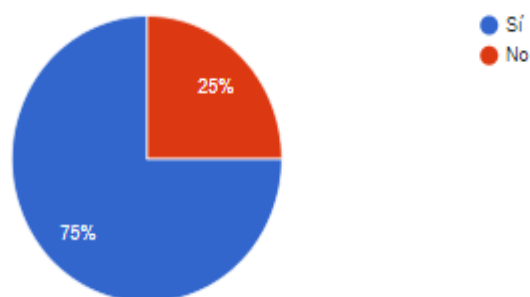


Figura 25. Porcentaje pregunta 18

El 75% de los encuestados manifestó que si se identifican los activos frente a un 25 % que afirmo que no lo hace. Se deben tomar medidas en cuanto las responsabilidades para la protección adecuada, esto evitara ciertos problemas a futuro

19. ¿Los usuarios sólo tienen acceso a los servicios para cuyo uso están específicamente autorizados?

4 respuestas

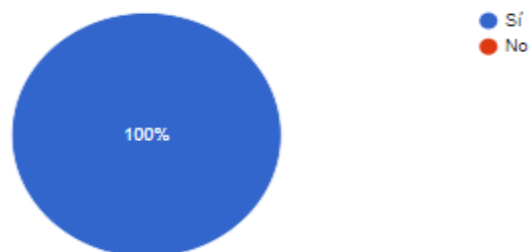


Figura 26. Porcentaje pregunta 19

El 100% de los encuestados manifestó que los usuarios tienen acceso a los servicios específicamente autorizados, por lo cual se evitan problemas dentro de la empresa con el personal presente.

20. ¿Cada funcionario de la dependencia cuenta con un usuario único con su respectiva contraseña?

4 respuestas

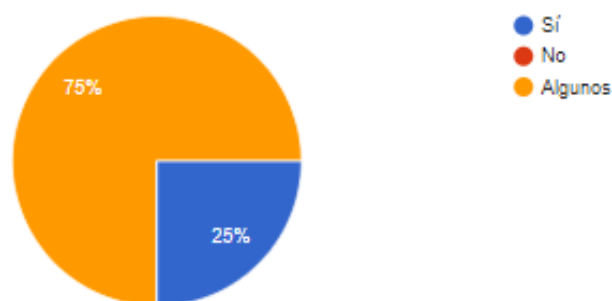


Figura 27. Porcentaje pregunta 20

El 75% de los encuestados manifestó que cuenta con un usuario único con su respectiva contraseña frente a un 25 % que afirmó que no cuenta con esas contraseñas. Aquí se evidencia que algunos funcionarios pueden tener acceso compartido a ciertos dispositivos por lo cual se debe manejar de mejor manera el acceso y la información que esté en uso.

21. ¿Los computadores cuentan con software para la prevención de código malicioso (Virus, Malware, etc.)?

4 respuestas

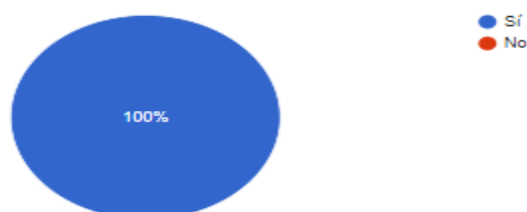


Figura 28. Porcentaje pregunta 21

El 100% de los encuestados manifestó los equipos cuentan con software para la prevención de código malicioso, es importante mantener a los equipos con su debido software para evitar cualquier tipo de código malicioso, amenazas o ataques.

22. ¿Las redes cuentan con las medidas de seguridad para garantizar el buen uso de los servicios de red y la seguridad de la información?

4 respuestas



Figura 29. Porcentaje pregunta 22

El 100% de los encuestados manifestó que las redes cuentan con las medidas de seguridad para garantizar el buen uso de los servicios de red, para la organización este es un pilar fundamental ya que uno de sus objetivos comerciales es el de servir como proveedor de internet.

23. ¿El cableado eléctrico y de datos se encuentra establecidos según la norma?

4 respuestas



Figura 30. Porcentaje pregunta 23

El 100% de los encuestados manifestó que el cableado utilizado está conforme a las normas establecidas.

24. ¿Los equipos están ubicados en lugares estratégicos para evitar amenazas o peligro al entorno, además de manipulación externa?

4 respuestas

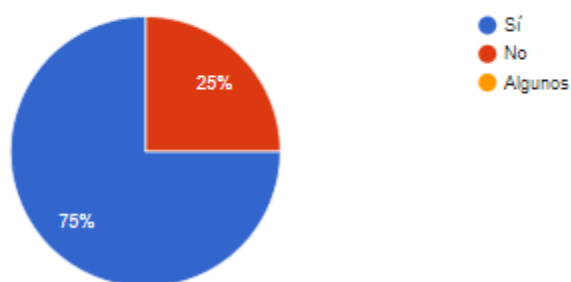


Figura 31. Porcentaje pregunta 24

El 75% de los encuestados manifestó que los equipos son ubicados en lugares estratégicos frente a un 25 % que afirmo que no están ubicado en lugares estratégicos, este punto es importante porque permitirá evitar amenazas de seguridad a futuro.

25. ¿Cuentan con área de acceso única para carga y despacho para evitar el ingreso de personal no autorizado?

4 respuestas

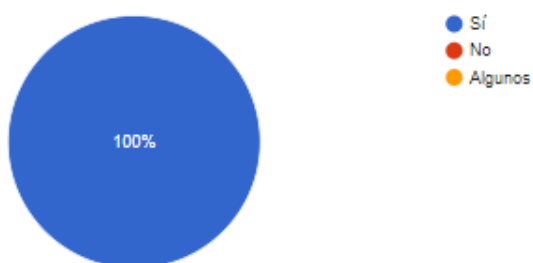


Figura 32. Porcentaje pregunta 25

El 100% de los encuestados manifestó que cuentan con un área de acceso única para la carga lo cual resulta muy importante para evitar cualquier problema de infiltración en un futuro o daños con dispositivos importantes que se encuentran en la empresa.

26. ¿Cada oficina cuenta con sus controles de acceso apropiados?

4 respuestas

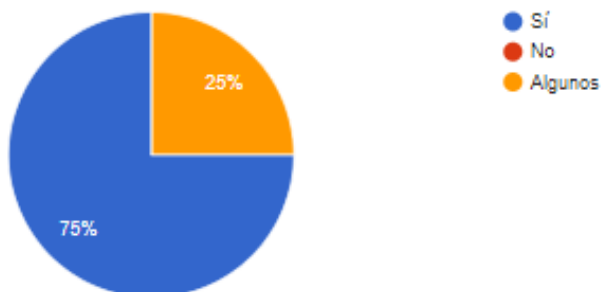


Figura 33. Porcentaje pregunta 26

El 75% de los encuestados manifestó que cuentan con controles de acceso rápido frente a un 25 % que afirmo que no tienen esos controles. Se debe manejar este punto en un 100% ya que la empresa maneja información sensible, y al no implementar estos controles pueden quedar expuestos a terceros perjudicando procesos normales que se manejan. El lugar seguro del área de Telecomunicaciones es llamado Cabecera, en donde se encuentran ubicados gran cantidad de dispositivos tecnológicos para el funcionamiento óptimo de la empresa.

27. ¿La empresa cuenta con un procedimiento formal de reportes de incidentes?
4 respuestas

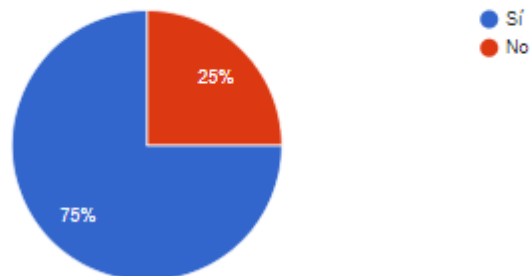


Figura 34. Porcentaje pregunta 27

El 75% de los encuestados manifestó que la empresa cuenta con un procedimiento para el reporte formal de incidente frente a un 25 % que afirmo que no cuentan con esos procedimientos lo que evidencia que gran parte de los empleados no conocen esos procedimientos.

Se evidencia que la empresa ASUCAP TV SANJORGE no cuenta con un documento formal sobre la continuidad del negocio lo que a futuro podría perjudicarlos generando pérdidas dentro de la organización.

Tabla 6

Lista de chequeo aplicada a la empresa ASUCAP TV SANJORGE.

ANEXO	
A5	POLÍTICAS DE LA SEGURIDAD DE LA INFORMACION
A5.1	Orientación de la dirección para la gestión de la seguridad de la información
	Objetivo: Brindar orientación y soporte, por parte de la dirección, para la seguridad de la información de acuerdo con los requisitos del negocio y con las leyes y reglamentos pertinentes
A5.1.1	Políticas para la seguridad de la información
A5.1.2	Revisión de las políticas para la seguridad de la información.
A6	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACION
A6.1	Organización interna
	Objetivo: Establecer un marco de referencia de gestión para iniciar y controlar la implementación y operación de la seguridad de la información dentro de la organización.
A6.1.1	Roles y responsabilidades para la seguridad de la información
A6.1.2	Separación de deberes
A6.1.3	Contacto con las autoridades
A6.1.4	Contacto con grupos de interés especial
A6.1.5	Seguridad de la información en la gestión de proyectos.
A6.2	Dispositivos móviles y teletrabajo
	Objetivo: Garantizar la seguridad del teletrabajo y el uso de dispositivos móviles
A6.2.1	Política para dispositivos móviles
A6.2.2	Teletrabajo
A7	SEGURIDAD DE LOS RECURSOS HUMANOS
A7.1	Antes de asumir el empleo
	Objetivo: Asegurar que los empleados y contratistas comprenden sus responsabilidades y son idóneos en los roles para los que se consideran.
A7.1.1	Selección
A7.1.2	Términos y condiciones del empleo
A7.2	Durante la ejecución del empleo

Objetivo: Asegurarse de que los empleados y contratistas tomen conciencia de sus responsabilidades de seguridad de la información y las cumplan.

- A7.2.1 **Responsabilidades de la dirección**
- A7.2.2 **Toma de conciencia, educación y formación en la seguridad de la información.**
- A7.2.3 **Proceso disciplinario**

A7.3 Terminación y cambio de empleo

Objetivo: Proteger los intereses de la organización como parte del proceso de cambio o terminación de empleo

- A7.3.1 **Terminación o cambio de responsabilidades de empleo**

A8 GESTION DE ACTIVOS

A8.1 Responsabilidad por los activos

Objetivo: Identificar los activos organizacionales y definir las responsabilidades de protección adecuadas.

- A8.1.1 **Inventario de activos**
- A8.1.2 **Propiedad de los activos**
- A8.1.3 **Uso aceptable de los activos**
- A8.1.4 **Devolución de activos**
- A8.2 **Clasificación de la información**

Objetivo: Asegurar que la información recibe un nivel apropiado de protección, de acuerdo con su importancia para la organización.

- A8.2.1 **Clasificación de la información**
- A8.2.2 **Etiquetado de la información**
- A8.2.3 **Manejo de activos**
- A8.3 **Manejo de medios**

Objetivo: Evitar la divulgación, la modificación, el retiro o la destrucción no autorizados de información almacenada en los medios

- A8.3.1 **Gestión de medio removibles**
- A8.3.2 **Disposición de los medios**
- A8.3.3 **Transferencia de medios físicos**

A9 CONTROL DE ACCESO

A9.1 Requisitos del negocio para el control de acceso

Objetivo: Limitar el acceso a información y a instalaciones de procesamiento de información.

- A9.1.1 **Política de control de acceso**
- A9.1.2 **Acceso a redes y a servicios en red**
- A9.2 **Gestión de acceso de usuarios**

Objetivo: Asegurar el acceso de los usuarios autorizados y evitar el acceso no autorizado a sistemas y servicios.

- A9.2.1** Registro y cancelación del registro de usuarios
- A9.2.2** Suministro de acceso de usuarios
- A9.2.3** Gestión de derechos de acceso privilegiado
- A9.2.4** Gestión de información de autenticación secreta de usuarios
- A9.2.5** Revisión de los derechos de acceso de usuarios
- A9.2.6** Retiro o ajuste de los derechos de acceso

A9.3 Responsabilidades de los usuarios

Objetivo: Hacer que los usuarios rindan cuentas por la salvaguarda de su información de autenticación.

- A9.3.1** Uso de información de autenticación secreta
- A9.4** Control de acceso a sistemas y aplicaciones

Objetivo: Evitar el acceso no autorizado a sistemas y aplicaciones.

- A9.4.1** Restricción de acceso a la información
- A9.4.2** Procedimiento de ingreso seguro
- A9.4.3** Sistema de gestión de contraseñas
- A9.4.4** Uso de programas utilitarios privilegiados
- A9.4.5** Control de acceso a códigos fuente de programas

A10 CRIPTOGRAFIA

A10.1 Controles criptográficos

Objetivo: Asegurar el uso apropiado y eficaz de la criptografía para proteger la confidencialidad, autenticidad y/o la integridad de la información

- A10.1.1** Política sobre el uso de controles criptográficos
- A10.1.2** Gestión de llaves

A11 SEGURIDAD FISICA Y DEL ENTORNO

A11.1 Áreas seguras

Objetivo: Prevenir el acceso físico no autorizado, el daño e la interferencia a la información y a las instalaciones de procesamiento de información de la organización.

- A11.1.1** Perímetro de seguridad física
- A11.1.2** Controles de acceso físicos
- A11.1.3** Seguridad de oficinas, recintos e instalaciones.
- A11.1.4** Protección contra amenazas externas y ambientales.
- A11.1.5** Trabajo en áreas seguras.
- A11.1.6** Áreas de carga, despacho y acceso público
- A11.2** Equipos

Objetivo: Prevenir la pérdida, daño, robo o compromiso de activos, y la interrupción de las operaciones de la organización.

- A11.2.1 Ubicación y protección de los equipos
- A11.2.2 Servicios de suministro
- A11.2.3 Seguridad en el cableado.
- A11.2.4 Mantenimiento de los equipos.
- A11.2.5 Retiro de activos
- A11.2.6 Seguridad de equipos y activos fuera de las instalaciones
- A11.2.7 Disposición segura o reutilización de equipos
- A11.2.8 Equipos de usuario desatendido
- A11.2.9 Política de escritorio limpio y pantalla limpia
- A12 **SEGURIDAD DE LAS OPERACIONES**
- A12.1 Procedimientos operacionales y responsabilidades

Objetivo: Asegurar las operaciones correctas y seguras de las instalaciones de procesamiento de información.

- A12.1.1 Procedimientos de operación documentados
- A12.1.2 Gestión de cambios
- A12.1.3 Gestión de capacidad
- A12.1.4 Separación de los ambientes de desarrollo, pruebas y operación
- A12.2 Protección contra códigos maliciosos

Objetivo: Asegurarse de que la información y las instalaciones de procesamiento de información estén protegidas contra códigos maliciosos.

- A12.2.1 Controles contra códigos maliciosos
- A12.3 Copias de respaldo

Objetivo: Proteger contra la pérdida de datos

- A12.3.1 Respaldo de la información
- A12.4 Registro y seguimiento

Objetivo: Registrar eventos y generar evidencia

- A12.4.1 Registro de eventos
- A12.4.2 Protección de la información de registro
- A12.4.3 Registros del administrador y del operador
- A12.4.4 Sincronización de relojes

- A12.5 Control de software operacional

Objetivo: Asegurarse de la integridad de los sistemas operacionales

- A12.5.1 Instalación de software en sistemas operativos
- A12.6 Gestión de la vulnerabilidad técnica

Objetivo: Prevenir el aprovechamiento de las vulnerabilidades técnicas

- A12.6.1 Gestión de las vulnerabilidades técnicas

- A12.6.2 Restricciones sobre la instalación de software
- A12.7 Consideraciones sobre auditorías de sistemas de información

Objetivo: Minimizar el impacto de las actividades de auditoría sobre los sistemas operativos

- A12.7.1 Controles de auditorías de sistemas de información

A13 SEGURIDAD DE LAS COMUNICACIONES

- A13.1 Gestión de la seguridad de las redes

Objetivo: Asegurar la protección de la información en las redes, y sus instalaciones de procesamiento de información de soporte.

- A13.1.1 Controles de redes
- A13.1.2 Seguridad de los servicios de red
- A13.1.3 Separación en las redes

- A13.2 Transferencia de información

Objetivo: Mantener la seguridad de la información transferida dentro de una organización y con cualquier entidad externa.

- A13.2.1 Políticas y procedimientos de transferencia de información
- A13.2.2 Acuerdos sobre transferencia de información
- A13.2.3 Mensajería Electrónica
- A13.2.4 Acuerdos de confidencialidad o de no divulgación

- A14 Adquisición, desarrollo y mantenimiento de sistemas

- A14.1 Requisitos de seguridad de los sistemas de información

Objetivo: Asegurar que la seguridad de la información sea una parte integral de los sistemas de información durante todo el ciclo de vida. Esto incluye también los requisitos para sistemas de información que prestan servicios sobre redes.

- A.14.1.1 Análisis y especificación de requisitos de seguridad de la información
- A.14.1.2 Seguridad de servicios de las aplicaciones en redes públicas
- A.14.1.3 Protección de transacciones de los servicios de las aplicaciones.

- A14.2 Seguridad en los procesos de Desarrollo y de Soporte

Objetivo: Asegurar que la seguridad de la información este diseñada e implementada dentro del ciclo de vida de desarrollo de los sistemas de información.

- A.14.2.1 Política de desarrollo seguro
- A.14.2.2 Procedimientos de control de cambios en sistemas

- A.14.2.3 **Revisión técnica de las aplicaciones después de cambios en la plataforma de operación**
- A.14.2.4 **Restricciones en los cambios a los paquetes de software**
- A.14.2.5 **Principio de Construcción de los Sistemas Seguros.**
- A.14.2.6 **Ambiente de desarrollo seguro**
- A.14.2.7 **Desarrollo contratado externamente**
- A.14.2.8 **Pruebas de seguridad de sistemas**
- A.14.2.9 **Prueba de aceptación de sistemas**
- A14.3 **Datos de prueba**
Objetivo: Asegurar la protección de los datos usados para pruebas.
- A.14.3.1 **Protección de datos de prueba**
- A15 **RELACIONES CON LOS PROVEEDORES**
- A15.1 **Seguridad de la información en las relaciones con los proveedores.**
Objetivo: Asegurar la protección de los activos de la organización que sean accesibles a los proveedores.
- A15.1.1 **Política de seguridad de la información para las relaciones con proveedores**
- A15.1.2 **Tratamiento de la seguridad dentro de los acuerdos con proveedores**
- A15.1.3 **Cadena de suministro de tecnología de información y comunicación**
- A15.2 **Gestión de la prestación de servicios de proveedores**
Objetivo: Mantener el nivel acordado de seguridad de la información y de prestación del servicio en línea con los acuerdos con los proveedores
- A15.2.1 **Seguimiento y revisión de los servicios de los proveedores**
- A15.2.2 **Gestión del cambio en los servicios de los proveedores**
- A16 **GESTION DE INCIDENTES DE SEGURIDAD DE LA INFORMACION**
- A16.1 **Gestión de incidentes y mejoras en la seguridad de la información**
Objetivo: Asegurar un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información, incluida la comunicación sobre eventos de seguridad y debilidades.
- A16.1.1 **Responsabilidades y procedimientos**
- A16.1.2 **Reporte de eventos de seguridad de la información**
- A16.1.3 **Reporte de debilidades de seguridad de la información**

- A16.1.4** Evaluación de eventos de seguridad de la información y decisiones sobre ellos
- A16.1.5** Respuesta a incidentes de seguridad de la información
- A16.1.6** Aprendizaje obtenido de los incidentes de seguridad de la información
- A16.1.7** Recolección de evidencia
- A17** **ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE CONTINUIDAD DE NEGOCIO**
- A17.1** Continuidad de Seguridad de la información
Objetivo: La continuidad de seguridad de la información se debe incluir en los sistemas de gestión de la continuidad de negocio de la organización.
- A17.1.1** Planificación de la continuidad de la seguridad de la información
- A17.1.2** Implementación de la continuidad de la seguridad de la información
- A17.1.3** Verificación, revisión y evaluación de la continuidad de la seguridad de la información
- A17.2** Redundancias
Objetivo: Asegurar la disponibilidad de instalaciones de procesamiento de información.
- A17.2.1** Disponibilidad de instalaciones de procesamiento de información
- A18** **CUMPLIMIENTO**
- A18.1** Cumplimiento de requisitos legales y contractuales
Objetivo: Evitar el incumplimiento de las obligaciones legales, estatutarias, de reglamentación o contractuales relacionadas con seguridad de la información y de cualquier requisito de seguridad.
- A18.1.1** Identificación de la legislación aplicable.
- A18.1.2** Derechos propiedad intelectual (DPI)
- A18.1.3** Protección de registros
- A18.1.4** Privacidad y protección de información de datos personales
- A18.1.5** Reglamentación de controles criptográficos.
- A18.2** Revisiones de seguridad de la información
Objetivo: Asegurar que la seguridad de la información se implemente y opere de acuerdo con las políticas y procedimientos organizacionales.
- A18.2.1** Revisión independiente de la seguridad de la información
- A18.2.2** Cumplimiento con las políticas y normas de seguridad
- A18.2.3** Revisión del cumplimiento técnico

Nota: Descripción lista de chequeo. Fuente: NTC-ISO-IEC 27001:2013

3.3 Identificación de posibles riesgos asociados a la seguridad de la información de la empresa de ASUCAP TV SANJORGE

De acuerdo con los parámetros establecidos en el desarrollo de la investigación se llevó a cabo un análisis metódico y exhaustivo del funcionamiento de los procesos organizativos de esta manera diagnosticar la situación actual. El análisis ha permitido que se evalúen los siguientes aspectos dentro de la empresa determinando consigo los siguientes hallazgos o riesgos.

La auditoría permitió la evaluación de los criterios establecidos dentro de los siguientes dominios y subdominios de la norma ISO27002:2013.

De acuerdo a los parámetros establecidos para el desarrollo del análisis, se realizó una auditoría con el objetivo de realizar un estudio de los procesos que se llevan a cabo en la organización, para de esta manera identificar la situación actual de la empresa y establecer los controles pertinentes ASUCAP TV SANJORGE.

3.3.1 Controles para la seguridad de la información Gestión de activos

- Se deben identificar los activos asociados con información e instalaciones de procesamiento de información, y se debe elaborar y mantener un inventario de estos activos.
- Los activos mantenidos en el inventario deben tener un propietario.
- Se deben identificar, documentar e implementar reglas para el uso aceptable de información y de activos asociados con información e instalaciones de procesamiento de información.

- Todos los empleados y usuarios de partes externas deben devolver todos los activos de la organización que se encuentren a su cargo, al terminar su empleo, contrato o acuerdo.
- La información se debe clasificar en función de los requisitos legales, valor, criticidad y susceptibilidad a divulgación o a modificación no autorizada.
- Se debe desarrollar e implementar un conjunto adecuado de procedimientos para el etiquetado de la información, de acuerdo con el esquema de clasificación de información adoptado por la organización.
- Se deben desarrollar e implementar procedimientos para el manejo de activos, de acuerdo con el esquema de clasificación de información adoptado por la organización.
- Se debe establecer, documentar y revisar una política de control de acceso con base en los requisitos del negocio y de la seguridad de la información.
- Se debe implementar un proceso de suministro de acceso formal de usuarios para asignar o revocar los derechos de acceso para todo tipo de usuarios para todos los sistemas y servicios.
- Se debe restringir y controlar la asignación y uso de derechos de acceso privilegiado
- La asignación de información de autenticación secreta se debe controlar por medio de un proceso de gestión formal.
- Los propietarios de los activos deben revisar los derechos de acceso de los usuarios, a intervalos regulares.

- Los derechos de acceso de todos los empleados y de usuarios externos a la información y a las instalaciones de procesamiento de información se deben retirar al terminar su empleo, contrato o acuerdo, o se deben ajustar cuando se hagan cambios.

- Se debe exigir a los usuarios que cumplan las prácticas de la organización para el uso de información de autenticación secreta.

- El acceso a la información y a las funciones de los sistemas de las aplicaciones se debe restringir de acuerdo con la política de control de acceso.

- Cuando lo requiere la política de control de acceso, el acceso a sistemas y aplicaciones se debe controlar mediante un proceso de ingreso seguro.

- Los sistemas de gestión de contraseñas deben ser interactivos y deben asegurar la calidad de las contraseñas.

- Se debe restringir y controlar estrictamente el uso de programas utilitarios que podrían tener capacidad de anular el sistema y los controles de las aplicaciones.

3.3.2 Seguridad física y del entorno Áreas Seguras

- Se deben definir y usar perímetros de seguridad, y usarlos para proteger áreas que contengan información confidencial o crítica, e instalaciones de manejo de información.

- Las áreas seguras deben estar protegidas con controles de acceso apropiados para asegurar que sólo se permite el acceso a personal autorizado.

- Se debe diseñar y aplicar la seguridad física para oficinas, recintos e instalaciones.

- Se deben diseñar y aplicar protección física contra desastres naturales, ataques maliciosos o accidentes.
- Se deben diseñar y aplicar procedimientos para trabajo en áreas seguras.
- Se deben controlar los puntos de acceso tales como las áreas de despacho y carga y otros puntos por donde pueden entrar personas no autorizadas y, si es posible, aislarlos de las instalaciones de procesamiento de información para evitar el acceso no autorizado.

3.3.3 Equipos

- Los equipos deben de estar ubicados y protegidos para reducir los riesgos de amenazas y peligros del entorno, y las posibilidades de acceso no autorizado.
- Los equipos se deben proteger contra fallas de energía y otras interrupciones causadas por fallas en los servicios de suministro.
- El cableado de energía eléctrica y de telecomunicaciones que porta datos o brinda soporte a los servicios de información se debe proteger contra interceptación, interferencia o daño.
- Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.
- Los equipos, información o software no se deben retirar de su sitio sin autorización previa

- Se deben aplicar medidas de seguridad a los activos que se encuentran fuera de las instalaciones de la organización, teniendo en cuenta los diferentes riesgos de trabajar fuera de dichas instalaciones.

- Se deben verificar todos los elementos de equipos que contengan medios de almacenamiento para asegurar que cualquier dato confidencial o software licenciado haya sido retirado o sobrescrito en forma segura antes de su disposición 67 o reúso.

- Los usuarios deben asegurarse de que a los equipos desatendidos se les da protección apropiada.

- Se debe adoptar una política de escritorio limpio para los papeles y medios de almacenamiento removibles, y una política de pantalla limpia en las instalaciones de procesamiento de información.

3.3.4 Seguridad de las operaciones

- Los procedimientos de operación se deben documentar y poner a disposición de todos los usuarios que los necesitan.

- Se deben controlar los cambios en la organización, en los procesos de negocio, en las instalaciones y en los sistemas de procesamiento de información que afectan la seguridad de la información.

- Se deben elaborar, conservar y revisar regularmente los registros acerca de actividades del usuario, excepciones, fallas y eventos de seguridad de la información.

- Las instalaciones y la información de registro se deben proteger contra alteración y acceso no autorizado.

3.3.5 Seguridad de las comunicaciones

- Se debe contar con políticas, procedimientos y controles de transferencia información formales para proteger la transferencia de información mediante el uso de • todo tipo de instalaciones de comunicaciones.

- Los acuerdos deben tratar la transferencia segura de información del negocio entre la organización y las partes externas.

- Se debe proteger adecuadamente la información incluida en la mensajería electrónica.

Gestión de incidentes de seguridad de la información

- Se deben establecer las responsabilidades y procedimientos de gestión para asegurar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información.

- Los eventos de seguridad de la información se deben informar a través de los canales de gestión apropiados, tan pronto como sea posible.

- Se debe exigir a todos los empleados y contratistas que usan los servicios y sistemas de información de la organización, que observen y reporten cualquier debilidad de seguridad de la información observada o sospechada en los sistemas o servicios.

- Los eventos de seguridad de la información se deben evaluar y se debe decidir si se van a clasificar como incidentes de seguridad de la información.

- Se debe dar respuesta a los incidentes de seguridad de la información de acuerdo con procedimientos documentados.

- El conocimiento adquirido al analizar y resolver incidentes de seguridad de la información se debe usar para reducir la posibilidad o impacto de incidentes futuros.

- La organización debe definir y aplicar procedimientos para la identificación, recolección, adquisición y preservación de información que pueda servir como evidencia

3.4 Dictamen de auditoría

De acuerdo con los resultados obtenidos de la evaluación, se encontraron las siguientes situaciones:

Se determinó que algunos equipos no cuentan con claves de acceso a los computadores, lo que podría originar acceso indebido de personas ajenas a la empresa, como también de manipulación y robo de información. En las medidas internas de control algunos equipos no tienen un plan de respaldo de copias de seguridad para los documentos manejados internamente, lo que ocasiona que, en caso de daño del equipo, daño del disco local C y robo de información, los documentos se pierdan y no se tenga una manera de poder recuperar esta información, trayendo problemas. En medidas de seguridad en caso de presentarse un problema con los sistemas de información o módulos usados por los funcionarios, algunos funcionarios no son capacitados. Por último, la empresa no cuenta con un plan de continuidad del negocio, lo que podría ocasionar demoras o agilidad en los procesos que se trabajan a diario y se tienen programados de manera semestral. De antemano estaré atento a cualquier inquietud que tenga con respecto al presente dictamen. Atentamente,

ESTEFANÍA ÁLVAREZ

Auditor Líder

Capítulo 4. Presentación de resultados

4.1 Ejecución Norma ISO 31000:2018 Gestión de Riesgos

La norma se centra de forma exhaustiva en la atención de la gestión del riesgo, como una herramienta para minimizar de forma anticipada las posibles inseguridades que pudieran producirse. Por tanto, **ISO 31000:2018** se aplica en este proyecto para dar respuesta con eficacia y seguridad a los riesgos y peligros actuales a los que se enfrentan las organizaciones y empresas.

En el conocimiento y comprensión del contexto, se deberá definir las amenazas que lo aquejan para prever acciones que le ayuden a mitigar sus posibles impactos adversos; es precisamente aquí en donde se genera una incertidumbre sobre los riesgos que representan esas amenazas; para ello debe adoptar una gestión de riesgos que le aporte los insumos suficientes para administrar de forma más acertada la incertidumbre y tomar las decisiones más adecuadas.

Los incidentes encontrados a los que la empresa ASUCAP TV SAN JORGE se encuentra expuesta son: Movimiento Telúrico, Incendio, Inundación/Humedad, Interrupción de energía, Falla en el servicio Red/Voz, Acceso no autorizado a la información lógica, Acceso físico no autorizado y Covid-19. Por lo tanto, con el objeto de elaborar un **Plan para Tratamiento del Riesgo** que resulte adecuado a lo especificado por la **Norma ISO 31000:2018**, se deberían tomar en consideración los siguientes aspectos:

- **Definición del alcance del plan de riesgos.** Los riesgos a tratar se circunscriben a un proyecto, a un proceso, o abarcan a toda la compañía.
- **Recopilación de información sobre riesgos.** Se debe obtener información sobre los riesgos a tratar.
- **Identificación de los controles de cada riesgo.** Los controles son actividades, procedimientos o mecanismos que, una vez implementados, pueden actuar sobre un riesgo, alterando su probabilidad o su impacto.
- **Análisis de probabilidad.** Para cada riesgo de la lista, se debe determinar la probabilidad de que este riesgo se materialice.
- **Análisis del impacto.** Para cada riesgo de la lista, se debe determinar la magnitud de las consecuencias de que este riesgo se materialice.
- **Determinación del nivel del riesgo,** en base a la probabilidad y al impacto de cada riesgo.
- **Definición de prioridades,** en función del nivel de riesgo.
- **Planificación de estrategias de mitigación** (reducir la probabilidad de que un riesgo se materialice) y **contingencia** (reducir el impacto de un riesgo si se materializa)
- **Análisis de eficacia** de las estrategias implementadas.
- **Monitoreo de los riesgos.** Se debería disponer de herramientas cuantitativas que permitan monitorear, realizar seguimiento y establecer cuándo tomar acciones para mitigar riesgos. Dichos indicadores cuantitativos son comúnmente conocidos como o **KRI (key risk indicator)**, y se trata de métricas creadas para poder sintetizar objetivamente aquellos riesgos considerados como significativos y que necesitan un tratamiento diferenciado. Estas métricas

permiten llevar un registro de incidencias, monitorear su comportamiento, informar sobre su evolución, reportarlos y establecer planes de acción cuando salen de la tendencia esperada.

Por consiguiente, esta información se encuentra plasmada y gestionada en el Plan de Continuidad del Negocio, donde se establecen diversas estrategias y se da paso a la obtención de beneficios muy significativos.

Beneficios:

Beneficios para las partes interesadas:

- Ofrece seguridad a sus partes interesadas, al tratar con una organización comprometida con la adecuada gestión de sus amenazas y riesgos.
- Aumenta la eficacia en la respuesta ante situaciones de emergencia.
- Permite contar con planes adecuados para enfrentar posibles amenazas o riesgos.

Beneficios en el mercado:

- Imagen de credibilidad y prestigio.
- Brinda seguridad y confianza a sus partes interesadas.
- Competitividad, fortaleza y adecuada gestión de riesgos, evitando afectar a sus partes interesadas.

Beneficios para la organización:

- Imagen de credibilidad y prestigio del organismo.
- Brinda seguridad y confianza a sus colaboradores y clientes.

- Con la norma **ISO 31000:2018** permite a las partes interesadas destacar en la toma de decisiones, el logro de objetivos y la mejora del desempeño ante amenazas y riesgos que se presenten en la organización.

- Cualquier organización está expuesta a factores externos, internos e influencias que hacen que sea incierto si lograrán sus objetivos, sin embargo, con las buenas prácticas y los conocimientos obtenidos en gestión de riesgos, se pueden mejorar los procesos de implementación.

- La gestión del riesgo es dinámica y ayuda a las organizaciones a establecer estrategias, alcanzar objetivos y tomar decisiones informadas.

- Contribuye a la mejora de los sistemas de gestión de riesgos.

4.2 Ejecución Norma ISO 22301: Continuidad del Negocio



PLAN DE CONTINUIDAD DEL NEGOCIO

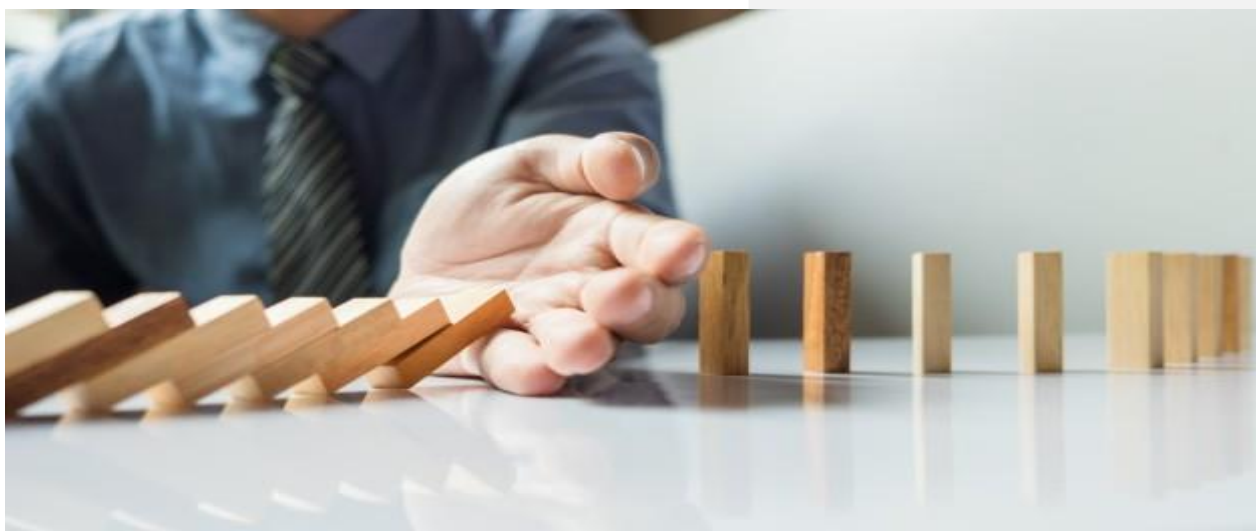


Figura 35. Presentación del plan

La continuidad del negocio (conocida en inglés como Business Continuity) es un conjunto de estrategias, procedimientos preventivos y reactivos que una organización pone en marcha para garantizar que las funciones esenciales puedan continuar durante y después de un desastre. La Planificación de la Continuidad del Negocio (BCP) trata de evitar la interrupción de los servicios

de misión crítica y restablecer el pleno funcionamiento de la forma más rápida y fácil que sea posible (searchdatacenter, 2013).

Para evitar los diversos tipo de amenazas, en la actualidad, las organizaciones están implementando el Sistema de Gestión de Continuidad de Negocio basado en la normativa **ISO 22301**, por lo cual, según todos los parámetros establecidos en ésta norma se consideró pertinente su debida aplicación en la empresa ASUCAP TV SAN JORGE.



Figura 36. Plan de continuidad. Fuente. Ficohsa

Fases del Plan de Continuidad del Negocio según la ISO 22301

- **Determinación del alcance**

El diseño de este plan solo contempla el área de Tecnologías e información de la empresa ASUCAP TV SANJORGE.

- **Análisis de la empresa**

Se recolectó toda la información de la organización con el fin de identificar **cuáles son los procesos de negocios críticos (activos)**, cómo se les dará soporte y cuáles son las necesidades que se presentan.

- **Determinación de la estrategia**

Una vez definidos **los** activos establecer que si en caso de que se llegue a presentar una amenaza se está en la capacidad de recuperar estos activos en corto plazo, si por el contrario requiere de un tiempo mayor se deben establecer estrategias.

Respuesta a la contingencia

Elegir las estrategias necesarias que se podrán en marcha en caso de presentarse un desastre y se creará un plan de crisis en donde se documentará toda la información.

- **Pruebas, mantenimiento y revisión**

En este punto **es** demasiado importante contar con recursos tecnológicos que permitirán crear planes de prueba y con el personal idóneo para poder realizar el respectivo mantenimiento y revisión, para identificar cuáles son las buenas prácticas y en qué se debe mejorar.

- **Concienciación**

Se debe crear una cultura dentro de **la** organización para que todos los empleados conozcan el plan de acción y se apropien de la situación, al igual que entiendan cuál será su rol dentro de este plan.

Objetivo.

-Proporcionar una respuesta rápida y apropiada para cualquier imprevisto, reduciendo los impactos resultantes.

-Mantener la funcionalidad de la empresa a un nivel mínimo aceptable durante su estado de contingencia.

-Reducir el tiempo de recuperación y las probables pérdidas económicas, directas e indirectas, como resultado de una interrupción.

Activación y desactivación del Plan.

Para activar el Plan de Continuidad del Negocio es necesario detectar una situación que represente riesgo, como las indicadas en el capítulo informar al personal involucrado el estado activo de contingencia y ejecutar el Plan, de igual manera, informar cuando a su juicio esa circunstancia que provocaron activar el estado de contingencia desaparezca y se esté en condiciones de continuar con las actividades normalmente, el responsable de la ejecución del Plan de Continuidad del Negocio deberá decidir si se desactiva o se continua en estado activo el Plan luego de realizar una evaluación de la situación.

-Estrategias de Recuperación para situación que se considere crítica o con tiempo de recuperación larga al presentarse una situación que se considere crítica, con tiempo de recuperación larga y/o afecte de manera directa las funciones principales se tomará como referencia la alternativa del Warm Site y/o Hot Site; este lugar alternativo no tendría ningún costo de suscripción, cuotas mensuales, cargos por uso, etc., ya que estos puntos serían propios de la empresa.

Protocolo para situación de contingencia con tiempo corto de recuperación

Proceso general: Como prioridad debemos salvaguardar la vida propia y de los empleados, luego, dentro de lo posible es necesario identificar el lugar que origina la emergencia con el fin de ser controlado (si se está en capacidad de hacerlo y no afecte la vida propia o de alguien más) e informar al área de seguridad física la situación presentada, ellos, según su procedimiento se encargarán de solicitar apoyo a las personas o entidades correspondientes.

Siempre contar con botiquín de primeros auxilios dentro de las oficinas o en las áreas que se consideren estratégicas para la empresa, consultar en la página de la Cruz Roja Colombiana cuales son los elementos primordiales y ejecutar cronograma de revisión de caducidad de dichos elementos.

Reforzar las capacitaciones y repasar periódicamente el grupo de brigadista dentro del T.I estipulado por el área de Salud y Seguridad del Trabajo.

Con el fin de conocer el procedimiento a seguir para cada caso específico, se definieron las siguientes situaciones de emergencia que se pueden presentar en especial en el área de T.I:

Movimiento telúrico (temblor), Incendio, inundación y/o humedad, interrupción de energía, falla en el servicio de internet, acceso no autorizado a la información lógica, acceso físico no autorizado a las oficinas de T.I.

Movimiento telúrico (temblor)**Probabilidad:** Posible**Impacto:** Muy Alto**Escenario:**

Un terremoto puede provocar la destrucción total no solo de la oficina sino del edificio; dependiendo de la magnitud puede destruir apenas solo parte de la oficina o completamente las edificaciones

Afectación:

Dependiendo el grado de magnitud el terremoto puede causar que se cuarteen o caigan paredes con bajo nivel de destrucción o puede ser una destrucción completa



Figura 37. Afectación.

Instituciones internacionales como la Agencia Federal para el Manejo de Emergencias de Estados Unidos (FEMA), Agencia Meteorológica de Japón, la Campaña “Bogotá, con los pies en la tierra”, la Agencia para el Manejo de Emergencias de California y otras aconsejan las siguientes medidas para prevenir y disminuir los daños causados por un sismo (herson, 2020).

Medidas preventivas:

-Con el fin de minimizar los riesgos al presentarse un temblor, es necesario inspeccionar la ubicación de los equipos de cómputo y tecnológicos con el fin de no dejarlos en una posición tal que ante un movimiento pueda generar mediante su caída una falla o destrucción.

-Verificar que los equipos de cómputo y tecnológicos se encuentren fuera de sufrir algún accidente de caída libre de objeto pesado que genere interrupción del proceso de operación normal.

-Practicar simulacros para identificar los pasos a seguir y la ubicación más pertinente para evitar accidente durante el movimiento.

-Conocer dónde y cómo cerrar el paso de la electricidad, el gas y el agua en los interruptores y tomas principales.

-Mantener en la oficina un Kit de emergencia que contenga elementos de ayuda como linterna con pilas, botiquín de primeros auxilios, agua embotellada, pito, etc.

Durante la situación:

-Es importante que en lo posible se mantenga tranquilo y permanezca en un lugar seguro mientras dure el temblor.

-Dé solo los pasos que le permitan colocarse debajo de un lugar seguro, como un escritorio o mesa resistente -Manténgase alejado de ventanas de vidrio, espejos, puertas o paredes y de todo lo que pueda caerle como lámparas y muebles

- Alejarse de objetos que puedan caer.

Después de la situación:

-Realizar el proceso de evacuación y desplazamiento a un sitio seguro indicados por el área de SST - Salud y Seguridad del Trabajo.

-Cuando la situación lo permita y se den las indicaciones por parte del área de SST volver a los lugares de trabajo.

-Realizar una inspección física en los puntos donde se encuentran ubicados los Switch Oficina de T.I, para verificar si físicamente los Switch sufrieron algún daño o tiene la probabilidad que ocurra por elementos a su alrededor, con el fin de garantizar la integridad de los activos materiales

Por lo general un sismo afecta únicamente parte de la estructura del edificio, por lo tanto, no se verían afectados los datos, sin embargo, es importante verificar que las conexiones a estos dispositivos de comunicación no se hayan afectado. Usualmente, luego de un movimiento telúrico el sistema de telefonía celular colapsa, por ende, es importante implementar algún sistema de comunicación ante alguna situación de emergencia, se recomienda utilizar los siguientes medios de comunicación: mensajes cortos de texto (SMS), y/o Comunicación vía internet a través de la cuenta de correo electrónico corporativo.

Incendio



Figura 38. Incendio

Probabilidad: Posible

Impacto: Alto

Escenario:

Un incendio puede provocar la devastación total de las oficinas perdiendo no solo los equipos de cómputo, sino las vidas que en ese momento estén presentes

Afectación: El grado de afectación es severo al tener pérdidas humanas que es el recurso más valioso de la organización y en adición los equipos que ofrecen el servicio para cumplir con las labores.

Medidas preventivas

-Realizar entrenamiento y simulacros al personal de T.I sobre la utilización de los extintores, y al personal de las oficinas donde se encuentran puntos de comunicación como Switch y Router.

-Realizar periódicamente revisión de las instalaciones eléctricas existentes, teniendo en cuenta que son fuente que puede provocar un incendio.

-Gestionar la instalación de detección de humo en los lugares estratégicos con punto de comunicación.

-No permitir el ingreso de personal fumando y/o con fósforos dentro de las oficinas.

-Cambiar de ubicación las copias de seguridad, ya que estas se encuentran dentro de la oficina en los mismos servidores, al ocurrir una situación como incendio se correría un gran riesgo de perder la información vital y sus copias de seguridad, estableciendo una pérdida total del activo más importante que es la Información.

-Conocer la salida, ruta de evacuación y salida de emergencia si durante la situación estas se encuentran obstruidas.

Durante la situación:

-Conservar la calma.

-Comprobar el punto donde se genera el incendio.

-Verificar si entra calor o humo por las rendijas de la puerta para saber si hay fuego al otro lado, de ser así no abras la puerta e identifica otra salida.

-Si el incendio es de poca magnitud y sabes utilizar el extintor, intenta apagarlo.

-Si el humo es excesivo desaloja e informa al área de Seguridad Física y al área de Salud y Seguridad del Trabajo.

-Apagar y desconectar los equipos de cómputo, servidores, salir de la red.

-Utilizar los extintores

-Si hay humo utilizar un pañuelo o prenda húmeda para cubrirse la boca y la nariz.

-Si se encuentra en pisos superiores abrir las ventanas para que el humo salga

Después de la situación:

-Verificar que la situación no haya afectado las estaciones de trabajo y dispositivos de comunicación, de ser así, identificar si su daño es físico o lógico para ejecutar el procedimiento establecido.

-Solicitar a un electricista de la oficina de Servicios Generales inspección del cableado. - Realizar una lista de inventario de los daños y pérdidas, de ser posible tome fotografías, no deseche ninguno de los artículos dañados hasta realizarse el inventario oficial, la compañía de seguro toma en consideraciones todos los daños.

-Revisar posibles nuevos focos de incendio.

Inundación/Humedad



Figura 39. Inundación/humedad

Medidas preventivas

- Practicar simulacros para identificar los pasos a seguir durante la situación.
- Solicitar la revisión cada cierto tiempo del estado de los desagües y sumideros.
- Verificar situaciones de humedad que pueden desencadenar el crecimiento del moho.

Durante la Situación:

- Evite caminar por aguas en movimiento.
- Suba a un lugar alto y permanezca allí.
- Si el tiempo lo permite, mueva a un lugar seguro los elementos que soportan los procesos críticos o que ayude a restablecerlo para cuando la situación de contingencia se desactive. -Si la situación lo permite suspenda el servicio de luz, agua y gas y evacue.

Después de la situación.

-Realizar la inspección siempre que la situación lo permita y sea seguro, de la situación de la infraestructura de la oficina, haga los arreglos temporales mínimos necesarios.

-Realizar una lista de inventario de los daños y pérdidas, de ser posible tome fotografías, no deseche ninguno de los artículos dañados hasta realizarse el inventario oficial, la compañía de seguro toma en consideraciones todos los daños.

-Verificar que la situación no haya afectado las estaciones de trabajo y dispositivos de comunicación, de ser así, identificar si su daño es físico o lógico para ejecutar el procedimiento establecido.

Interrupción de energía

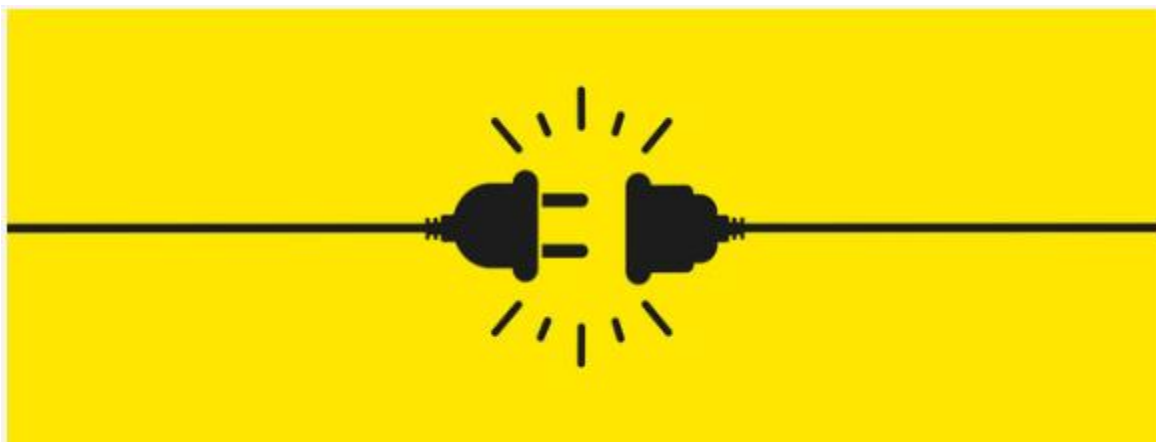


Figura 40. Interrupción de energía

Probabilidad: Posible

Impacto: Alto

Escenario:

Las edificaciones pueden presentar fallas eléctricas por lo general una tormenta eléctrica lo cual puede producir un cortocircuito que origine 2 posibles escenarios:

1-Apagon total de energía

2-Incendio

Afectación: La afectación puede ser severa o severa dependiendo del escenario, en el caso de un apagón puede quedar solamente la discontinuidad de los servicios, por otro lado, también pueden quemarse los equipos no los UPS sino los servidores en sí. En caso de que se produzca un incendio la afectación pasa a ser más severa y se caería a un riesgo de incendio.

Medidas preventivas:

-Identificar cuanto es el tiempo que brindaría la UPS de soporte para la empresa teniendo en cuenta el tiempo de deterioro y los usuarios conectados a la corriente. -Social izar al personal de la empresa la clasificación de conexión donde se especifica que dispositivos deben ir conectados a los tipos de corriente con los que cuenta la empresa (Regulada/No Regulada).

-Solicitar al área de Servicios Generales informes del estado y las revisiones periódicas de las instalaciones eléctricas.

Durante la situación:

-Verificar si la falla de energía es solo en un punto, en la empresa, o en toda la ciudad con el fin de informar a los empleados y tomar las medidas necesarias en cuanto al almacenamiento de información para evitar perdida de datos por apagarse los dispositivos.

-Desconectar los equipos electrónicos que puedan verse afectados al retorno de la energía.

Después de la situación:

-Verificar que el flujo de energía este en las óptimas condiciones, esperar el tiempo que se considere necesario para estar seguros que el flujo de energía está controlado y no se tengan alteraciones del flujo.

Falla en el servicio de Red/Voz

Figura 41. *Falla en el servicio de Red/Voz*

Probabilidad: Posible

Impacto: Medio

Escenario:

Existen varios tipos de causas por las cuales puede producirse fallas en la red, como son:

- 1-Mala conexión
- 2-Ruptura en los cables
- 3-Exceso de ruido y/o estática

Afectación: el efecto que causan las fallas en la red es netamente con los sistemas de información, ya que si los servidores están haciendo rutinas automáticas de respaldo o incluso el personal está haciendo sus propios respaldos puede generar conflicto o fallas al generar la información respaldada, además de errores en la comunicación

Medidas preventivas:

-Informar en las oficinas donde están ubicados los puntos de comunicación que ante un fallo deben reportarlo y no manipular el Rack, Solo el personal autorizado podrá manipular estos puntos de comunicación.

-Planificar rutas de comunicación alternativas ante las diversas situaciones de fallo.

Durante la situación:

-De no ser posible restaurar la comunicación a través de los ingenieros de la empresa, comunicar al personal de soporte de las empresas que brindan dichos servicios.

-Informar al personal de la empresa el tiempo estimado de recuperación del servicio.

Después de la situación

-Verificar que el servicio este completamente activo y funcional.

Acceso no autorizado a la información lógica



Figura 42. Acceso no autorizado a la información lógica

Probabilidad: Posible

Impacto: Alto

Escenario:

Al contar con información crítica de los clientes es necesario que la resguardemos de manera confidencia, aunque los piratas informáticos contratados por otras empresas atacarían la red organización para obtener información.

Afectación: Sí la información sensible queda expuesta ante terceros, la organización inmediatamente pierde confianza y credibilidad, lo cual afectaría mucho a la empresa en el desempeño de sus procesos.

Medidas preventivas:

-Socializar medidas preventivas del buen uso de las herramientas informáticas y el manejo correcto para la seguridad de la información.

-Realizar pruebas del cumplimiento de las políticas de seguridad sobre la seguridad de la información.

-Seguimiento de actualización y funcionamiento del anti-virus y firewall.

-Continuar con el control de autenticación de usuario para el uso del computador y su cambio de contraseña en el periodo determinado por la empresa.

-Anexar una cláusula contractual en la cual los empleados se comprometen a hacer buen uso de los materiales y tecnologías de la empresa.

Durante la situación:

-Realizar cambios de contraseña.

-Bloquear el acceso a la información lógica.

-Realizar un escaneo a las redes

Después de la situación:

-Identificar los datos que pueden estar expuestos y verificar su estado de integridad.

-Realizar cambios de contraseña si se considera necesario.

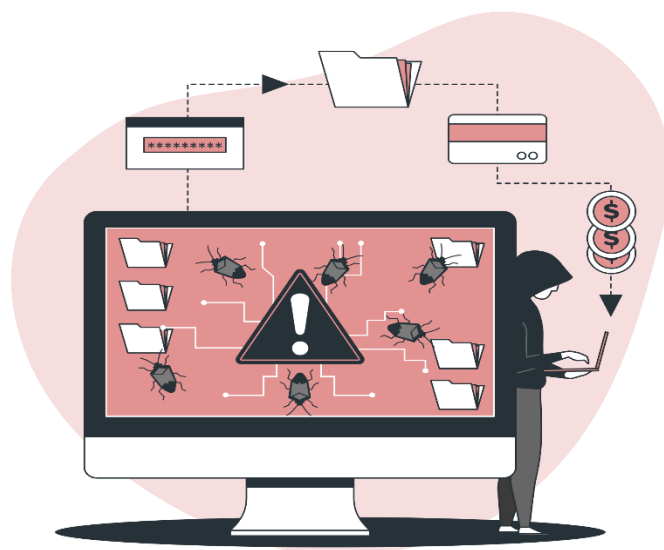
Acceso físico no autorizado a las oficinas de T.I

Figura 43. Acceso físico no autorizado a las oficinas de T.I

Medidas preventivas:

-Solicitar al área de Seguridad Física informar cuando la cámara de seguridad falle para estar alerta.

-Realizar cambios periódicos de la cerradura que permite el acceso a la oficina y por lo tanto al punto principal de comunicación de la empresa.

Durante la situación:

-Abandonar el lugar donde se encuentra el intruso

-Informar inmediatamente al área de Seguridad Física.

Después de la situación:

-Una vez la situación está bajo control y se autorice el ingreso por parte del área de Seguridad Física verificar con el inventario que elementos hacen falta e informar al área de Seguridad para tomar las medidas pertinentes.

Para el años 2020 el día 6 de marzo en Colombia es detectado el primer caso de coronavirus, inmediatamente el gobierno emprende acción para contrarrestar de en cierta medida los niveles de contagios, por ellos decreta la cuarentena con estrictos lineamientos y protocolos (Minsalud, 2020).

Ahora bien, muchas organizaciones no estaban preparadas para hacer frente a esta situación, con el pasar de los meses muchas empresas de diferentes sectores tuvieron que cerrar sus puertas definitivamente, muy pocas contaban con planes de continuidad del negocio que les permitiría responder de manera adecuada ante esta pandemia.

El Plan de Continuidad de Negocio es un plan operativo que implica garantizar que las funciones críticas de una empresa pueden recuperarse y restaurarse ante un desastre natural, fallos tecnológicos, errores humanos o cualquier interrupción súbita de los procesos. Deberá cuantificar el personal y las actividades imprescindibles para la continuidad del negocio, considerando las ausencias de trabajadores en todos los niveles de la organización, dado que el virus tiene un alto grado de contagio que deja poco tiempo para ejecutar acciones de contención y protección hacia el personal

Para la empresa ASCUAP TV SAN JORGE al no contar con un plan de continuidad del negocio definido y al no contemplar los posibles escenarios frente al Covid 19 se formula un aparte o un ítem especial donde se dan las pautas de manera general como una estrategia para el plan de continuidad.

1. Asignación económica extraordinaria para proteger al personal y a los clientes durante la pandemia

- Poner a disposición de los empleados suficiente material para el control del virus: productos para la higiene de las manos, pañuelos desechables...
- Asegurarse de que los empleados tengan acceso a consultas y consejos médicos durante una emergencia.
- Contemplar posibles necesidades de apoyo psicológico que les ayude a superar la situación generada, gestionar la cuarentena, posible duelo.

2. Preparación para el impacto de una pandemia en la organización

- Designar a un coordinador y a un equipo con responsabilidades y funciones bien definidas para elaborar y mantener actualizado el plan de actividades específicas para hacer frente a la pandemia en la organización.
- Determinar áreas y empleados esenciales y/o críticos, así como productos y servicios fundamentales necesarios para no interrumpir la continuidad de negocio.

- Estipular los impactos que tendrían las medidas de control emitidas por organismos de salud y por las decisiones tomadas por el gobierno (por ejemplo, el teletrabajo, cierre de fronteras, aislamiento...).
- Elaborar y actualizar periódicamente un plan de comunicación para casos de emergencia. Debe indicar el nombre de las personas a contactar, incluyendo proveedores y clientes.
- Implementar procedimientos de desinfección en las instalaciones.

3. **Preparación para el impacto de una pandemia en los empleados, clientes y proveedores**

- Prepararse para la ausencia prolongada de empleados por enfermedad personal o en la familia, por la aplicación de medidas de contención o por la interrupción del transporte público.
- Mantener estrechos canales de comunicación con empleados y colaboradores garantizando que conozcan de primera mano la estrategia, decisiones y ayudas que se vayan poniendo a su disposición.

4. **Establecimiento de medidas de contingencia para la pandemia**

- Contar con un Equipo de Respuesta a Contingencias que establezca la estrategia y marque los objetivos del plan de emergencia.
- Implementar políticas con respecto a compensación por enfermedad.
- Activar protocolos que permitan prevenir la propagación del virus en el lugar de trabajo.
- Habilitar procedimientos para que los empleados puedan trabajar desde casa o tener un horario flexible.

5. Culturización y/o educación de los empleados y esquemas de comunicación con ellos

- Establecer y difundir programas y materiales con información básica sobre la pandemia, así como estrategias de protección y el cuidado en casa.
- Prever situaciones de temor y ansiedad, rumores e información errónea.

6. Coordinar actividades con otras empresas y/u organizaciones

- Colaborar con los organismos de salud pública y protección civil para darles a conocer los planes de preparación que tiene la empresa.
- Informar a los organismos públicos sobre los recursos y los servicios con los que podría contribuir.

7. **Vuelta a la normalidad**

- Siguiendo las recomendaciones e indicaciones de las autoridades y organismos de salud pública, vuelta progresiva de los empleados a sus centros de trabajo.
- Establecer protocolos y canales de comunicación y ayuda que garanticen la atención a empleados y familiares ante posibles secuelas postpandemia.
- Hacer balance de daños para la superación del impacto económico.
- Obtención de lecciones aprendidas y actualización de las actividades del plan de continuidad donde proceda

8. **Medidas preventivas para el manejo de documentos físicos**

- Antes de tomar los documentos, se deben aplicar las medidas de higiene de manos y luego ponerse los guantes. En caso de no tener la posibilidad de lavarse las manos con agua y jabón, use un desinfectante para manos a base de alcohol glicerinado.
- Se establece el uso de medios virtuales para el envío de documentos o información escrita, según se requiera.
- Al entregar los documentos en físico, se debe evitar el ingreso al lugar donde se encuentra el receptor, evitando al máximo el contacto físico.
- Utilice guantes y tapabocas desechables mientras se trabaja en el manejo de archivo. Se debe evitar el contacto de los guantes sucios con cualquier parte del cuerpo. Si las actividades se deben desarrollar en cuartos de archivo, adicionalmente es necesario el uso de bata de trabajo, la cual debe usarse cerrada y limpia. La bata se utilizará solo en el área de trabajo y mientras se

ejecuten las labores. No olvide quitársela si va a realizar otras acciones, como consumir alimentos o ir al baño.

9. Orden, limpieza y desinfección en los sitios de trabajo

- Los baños deben limpiarse y desinfectarse, incluyendo paredes y puertas, según la frecuencia de uso, desde las partes más altas a las más bajas y por último el piso.
- Mantén limpios y desinfectados los recipientes de recolección de residuos.
- Desinfectar los equipos y herramientas utilizadas, estas deben ser de uso personal.
- Para limpiar y desinfectar utilizar los elementos de protección personal: guantes largos (no quirúrgicos) puestos debajo de las mangas, protección de mucosas (respiratoria y visual).
- En lo posible, utiliza paños impregnados con el agente desinfectante o tapabocas para todo el personal.
- No utilices cepillos o herramientas que salpiquen.
- Retirar el polvo en húmedo.
- Evitar levantar nubes de polvo que favorezcan la propagación del virus.
- La aspersion solo debe realizarse sobre superficies que no se deban tocar posteriormente, como residuos biosanitarios o superficies que se presuman o no contaminadas.

Al finalizar las actividades:

- Realizar limpieza y desinfección de herramientas, máquinas, equipos de trabajo, elementos de protección personal y calzado.

- Antes de salir de la obra realizar el cambio de ropa, guardar en una bolsa plástica y realizar el lavado diario de la misma.
- Implementar lavado de manos antes de la salida de la obra.
- Fomentar en los trabajadores al regreso a casa el lavado de manos, el cambio de ropa y baño antes de tener contacto con los miembros del grupo familiar.

De acuerdo a la organización mundial de la salud en la siguiente imagen demuestran como es el proceso adecuado para lavarse las manos, por lo que se sugiere que los empleados de la empresa ASUCAP TV SAN JORGE deban obligatoriamente estas recomendaciones.

¿Cómo lavarse las manos?

¡Lávese las manos solo cuando estén visiblemente sucias! Si no, utilice la solución alcohólica

0 Duración de todo el procedimiento: 40-60 segundos



0 Mójese las manos con agua;



1 Deposite en la palma de la mano una cantidad de jabón suficiente para cubrir todas las superficies de las manos;



2 Frótese las palmas de las manos entre sí;



3 Frótese la palma de la mano derecha contra el dorso de la mano izquierda entrelazando los dedos y viceversa;



4 Frótese las palmas de las manos entre sí, con los dedos entrelazados;



5 Frótese el dorso de los dedos de una mano con la palma de la mano opuesta, agarrándose los dedos;



6 Frótese con un movimiento de rotación el pulgar izquierdo, atrapándolo con la palma de la mano derecha y viceversa;



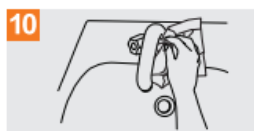
7 Frótese la punta de los dedos de la mano derecha contra la palma de la mano izquierda, haciendo un movimiento de rotación y viceversa;



8 Enjuáguese las manos con agua;



9 Séquese con una toalla desechable;



10 Sirvase de la toalla para cerrar el grifo;



11 Sus manos son seguras.



Organización
Mundial de la Salud

Seguridad del Paciente

UNA ALIANZA MUNDIAL PARA UNA ATENCIÓN MÁS SEGURA

SAVE LIVES

Clean Your Hands

La Organización Mundial de la Salud no garantiza todas las recomendaciones expuestas para promover la información contenida en este documento. Sin embargo, el material publicado se elabora con garantía de rigor científico, se basa en evidencia científica y respalda la importancia de la higiene y el uso del alcohol. La Organización Mundial de la Salud no asume ninguna responsabilidad por los daños que pudieran ocasionar su utilización. La OMS se adhiere a la Resolución Universitaria de Ginebra (2005) en relación a los miembros del Programa de Cambio de Comportamiento, su participación activa en la reducción de este material.

Organización Mundial de la Salud, Octubre 2010

Figura 44. Proceso de sanitario.

PLAN DE PRUEBA

Permite evaluar la viabilidad de los procedimientos de recuperación descritos anteriormente.

Objetivos a cumplir:

- Medir capacidad del lugar respaldo

- Evaluar tiempo de respuesta o de recuperación de funciones críticas o afectadas.

- Evaluar cantidad de recursos y suministros para el lugar de respaldo.

- Evaluar costos de los posibles daños en la empresa

- Evaluar el desempeño de los empleados y personal involucrado en la ejecución de la prueba.

- Verificar el cubrimiento del Plan de Continuidad del Negocio.

- Evaluar la coordinación del personal del área de T.I

- Evaluar el correcto funcionamiento de los procedimientos indicados en Plan.

Se deben estipular los tiempos para ejecutar las pruebas y simulacros, tanto para situaciones menores como para una situación que implica la suspensión total o parcial de las actividades y sistemas, todo en comunicación y aprobación con los gerentes de las áreas.

La prueba consiste en un simulacro de diversas situaciones de desastre como las indicadas en procesos y estrategias de recuperación, se recomienda realizarlas de forma independiente con el fin de analizar su cumplimiento.

Al finalizar la prueba se creará un informe con el fin de evaluar para cada situación de desastre el tiempo empleado para restaurar las funciones afectadas, identificar problemas de aplicación de los procedimientos de recuperación, evaluación del personal encargado para realizar los procedimientos de recuperación y los recursos necesarios para su ejecución.

PLAN DE MANTENIMIENTO

Permite realizar seguimiento periódico de los resultados del Plan de Continuidad del Negocio a través de su proceso cíclico de mejora y revisión, este se debe llevar a cabo especialmente en dos circunstancias del ciclo de vida del Plan de Continuidad del Negocio que son:

- Identificación de fallos en la fase de prueba del Plan de Continuidad.
- Cambios en el entorno del Plan de Continuidad, como:
 - Renovaciones tecnológicas.
 - Cambios estructurales del área de T.I o puntos de trabajo indicados como alternativos de recuperación.

Si durante el proceso de prueba se identifican estas circunstancias se deben realizar las modificaciones correspondientes en el Plan de Continuidad del Negocio con el fin de mantener actualizado dicho plan, luego de realizar dichas modificaciones se debe seguir el proceso de aprobación y socialización de dichos cambios al personal involucrado.

CONCIENCIACIÓN

Teniendo en cuenta la Gestión de Riesgos ejecutada por medio de la norma ISO 31000:2018 y el Plan de Continuidad del Negocio ejecutado por medio de la norma ISO 22301, se procede a la socialización de las medidas y estrategias tomadas con el personal involucrado del área de Telecomunicaciones con el fin de afianzar su compromiso para la puesta en marcha de éste plan y las diversas ventajas que consigo lleva la debida implementación.

Capítulo 5. Conclusiones

- Con el diagnóstico realizado haciendo uso de la ISO 27001:2013 se logró detectar varias vulnerabilidades en cuanto a la seguridad de la información, con la aplicación de la ISO 27002:2013, por cada vulnerabilidad detectada se propusieron los controles respectivos dando cumplimiento con la implementación y de esa manera mitigar cualquier amenaza que pudiese surgir a futuro.
- En la empresa ASUCAP TV SAN JORGE se evidenció que no contaban con una Gestión de Riesgos y un Plan de Continuidad del Negocio. Partiendo de este barrido y analizando la situación actual, se procedió a hacer uso de las normas ISO 31000:2018 e ISO 22301 determinando parámetros y estrategias para realizar el Plan de Continuidad el cual permitiría como herramienta de apoyo seguir con los procesos críticos propios de la compañía.
- Con la implementación del Plan de Continuidad del Negocio se logra que la empresa pueda tener planes a futuro y hacer frente a las eventualidades que se pudieran presentar y de esta manera apuntar a la mejor continua con el restablecimiento oportuno de los procesos.
- Debido al corto tiempo de duración del trabajo de práctica y a los últimos eventos presentados, se dejan procesos iniciados, los cuales se llevarán a cabo durante el año 2020.

Capítulo 6. Recomendaciones

- Se recomienda que la empresa siga haciendo uso de los controles de seguridad de la información y del plan de continuidad del negocio para asegurar en cierta medida la mejora continua en la empresa.

- Se debe mantener actualizado el Plan de Continuidad del Negocio según las necesidades que se vayan presentando y los mejoramientos pertinentes por realizar.

Referencias

- Cataño Turián, L. M., & Pérez Monsalve, P. A. (2015). *Diseño de un plan de continuidad del negocio en una constructora de la ciudad de Medellín-Colombia bajo la norma ISO 22301:2012*. Obtenido de https://repository.uniminuto.edu/bitstream/handle/10656/5687/TEGP_Cata%C3%B1oTuri%C3%A1nLuzMarleny_2015.pdf?sequence=1&isAllowed=y
- Figuroa, J. (2017). La seguridad informática y la seguridad de la información. *Polo del Conocimiento*.
- Galo, C. (5 de Enero de 2018). *Las TIC en las empresas: evolución de la tecnología y cambio estructural en las organizaciones*. Obtenido de <file:///D:/Dialnet-LasTICsEnLasEmpresas-6313252.pdf>
- Gonzalez, I. H. (31 de Octubre de 2018). *ISO 31000:2018- Directrices para gestionar riesgos* . Obtenido de <https://calidadgestion.wordpress.com/2018/10/31/iso-31000-2018-directrices-para-gestion-de-riesgos/>
- Gustavo Adolfo, C. G. (2017). *Plan de continuidad del negocio basado en servicios en la nube para el área de tecnología*. Obtenido de <http://biblioteca.galileo.edu/tesario/bitstream/123456789/578/1/Tesis%20-%20Plan%20de%20continuidad%20del%20negocio%20basado%20en%20servicios%20en%20la%20nube%20para%20el%20area%20de%20tecnologia.pdf>

herson. (2020). Obtenido de <http://herson.com.co/como-prepararnos-para-un-sismo-content-72.html>

Minsalud. (6 de Marzo de 2020). Obtenido de <https://www.minsalud.gov.co/Paginas/Colombia-confirma-su-primer-caso-de-COVID-19.aspx>

searchdatacenter. (2013). *searchdatacenter*. Obtenido de <https://searchdatacenter.techtarget.com/es/definicion/Continuidad-de-negocios-BC>


secretaria senado. (2020). Obtenido de http://www.secretariasenado.gov.co/senado/basedoc/ley_0527_1999.html

Apéndice

Apéndice A. Programa para auditoria

	Programa de auditoria		
OBJETIVOS:	<ul style="list-style-type: none"> - Verificar el nivel de implementación de la Norma NTC ISO 27002:2013 - Realizar una evaluación real sobre los posibles riesgos que se pueden realizar en la empresa. - Identificar y analizar las vulnerabilidades que se pueden presentar en sistema de información que maneja la empresa. 		
ALCANCE:	Inicia con la elaboración y socialización del programa de auditoría y finaliza con la entrega de los informes por parte del equipo auditor.		
RECURSOS:	Humanos (Estefanía Giselle Álvarez Claro, estudiante de ingeniería de sistemas)		
CRITERIOS:	ISO 27002:2013		
RESPONSABLE:	Estefanía Álvarez		
MÉTODOS DE AUDITORIA:	Listas de verificación Entrevistas Observación		
PERIODO:	Febrero a Julio del 2020		
FECHA DE ELABORACIÓN:	20-03-2020	FECHA DE ACTUALIZACIÓN:	
EMPRESA A AUDITAR		FECHA Y HORA	EQUIPO AUDITOR
EMPRESA ASUCAP TV SANJORGE			Estefanía Álvarez
OBSERVACIÓN:			

Apéndice B. Instrumento de reelección de información

			
Objetivo	Diagnosticas el estado actual de la seguridad de la información en la empresa ASUCAP TV SANJORGE		
Dirigido a	Líder de TI		
PREGUNTAS	SI	NO	OBSERVACIONES
1. ¿La empresa ASUCAP TV San Jorge cuenta con políticas de seguridad de información?			
2. ¿La empresa cuenta con un inventario de activos de la información actualizados?			
3. ¿La empresa ASUCAP TV San Jorge cuentan con manual de políticas de control de acceso?			
4. Si la respuesta anterior es si entonces ¿Las políticas de control de acceso son aplicadas?			
5. ¿Todas las aplicaciones cuentan con una contraseña para permitir el acceso a los usuarios?			
6. ¿Su usuario y contraseña tiene una combinación de mayúsculas, minúsculas y números?			
7. ¿Realiza periódicamente cambios de dichas contraseñas?			

<p>8. ¿Las aplicaciones cuentan con restricción de acceso a páginas web (redes sociales, etc.)?</p> <p>9. ¿Los equipos de la dependencia están ubicados en lugares estratégicos para evitar amenazas o peligro al entorno, además de manipulación externa?</p>			
<p>10. ¿Los equipos están protegidos contra fallas en el suministro de energía y otras anomalías?</p>			
<p>11. ¿Los empleados de la empresa cuentan con un acuerdo de confidencialidad de la información?</p>			
<p>12. ¿Realiza Backup (Copias de Seguridad de la Información) de la información a su disposición?</p>			
<p>13. ¿Las copias de seguridad realizadas a los sistemas información, se llevan a cabo a una hora determinada para evitar pérdidas de la información?</p>			
<p>14. ¿La empresa cuenta con un procedimiento formal de reportes de incidentes?</p>			
<p>15. ¿Son capacitados para que manejo de la información se suministre de una forma segura?</p>			
<p>16. ¿Se identifican los activos organizacionales y se definen las responsabilidades de protección adecuadas?</p>			
<p>17. ¿Los usuarios sólo tienen acceso a los servicios para cuyo uso están específicamente autorizados?</p>			

18. ¿Cada funcionario de la dependencia cuenta con un usuario único con su respectiva contraseña?			
19. ¿Los computadores cuentan con software para la prevención de código malicioso (Virus, Malware, etc.)?			
20. ¿Las redes cuentan con las medidas de seguridad para garantizar el buen uso de los servicios de red y la seguridad de la información?			
21. ¿El cableado eléctrico y de datos se encuentra establecidos según la norma? 22. ¿Los equipos están ubicados en lugares estratégicos para evitar amenazas o peligro al entorno, además de manipulación externa?			
23. ¿Cuenta con área de acceso única para carga y despacho para evitar el ingreso de personal no autorizado? Si no algunos			
24. ¿Cada oficina cuenta con sus controles de acceso apropiados? Si no algunos			
25. ¿La empresa tiene establecidos planes para mantener la continuidad del negocio en caso de presentarse algún problema con las actividades que tienen programadas a diario?			

Apéndice C. Informe de auditoria

Empresa ASUCAP TV SAJN JORGE

1. Objetivo de la Auditoria

- Diagnosticar los niveles de seguridad de la información de acuerdo a la Norma NTC ISO 27002:2013
- Realizar una evaluación sobre los posibles riesgos que se pueden realizar en la empresa.
- Identificar las amenazas y vulnerabilidades que se puedan encontrar definiendo una serie de controles para cada uno de ellos

2. Alcance de la auditoria

La auditoría tiene la finalidad de verificar la de seguridad de la información de la empresa ASUCAP TV SAN JORGE

3. Hallazgos

- Falta de claves de accesos en algunos computadores de la empresa
- No se cuenta con procedimiento formal de incidentes
- Falta de capacitaciones la hora de reportar incidentes
- Falta de información de empleados sobre el uso de políticas de protección de datos y privacidad de la información de los colaboradores.
- Falta de elementos de seguridad en caso de presentarse una emergencia.
- Falta de un Plan de Contingencia basado en una evaluación de riesgos que permita identificar un conjunto de medidas y acciones básicas concretas de respuesta.

4. Recomendaciones

- Capacitar a los empleados sobre la importancia de tener claves de acceso a los equipos y sobre dispositivos externos que pueden afectar la seguridad de la información.
- Capacitar a los empleados para reporte de incidentes
- Capacitar a los empleados sobre el uso de políticas de protección de datos y privacidad de la información de los colaboradores
- Implementar manual de políticas de seguridad de la información
- Adquirir elementos de seguridad ante emergencias
- Mantener copias de seguridad resguardadas al exterior de la empresa
- Cláusula de compromiso en los contratos de los colaboradores con respecto a seguridad, confiabilidad e integridad de los datos.
- Implementación de un Plan de Contingencia en donde se consoliden estrategias frente incidentes

Apéndice D. Inventario Individual de Hardware

Computador Recepción

Núm.	Equipo	Marca	Núm. Inventario	Características	Observaciones
1	Computador de escritorio	Hp		Sistema operativo de 64 bits	Funcional
2	Procesador	Intel Core		Intel core i3 2.90GHz 500 DD	
3	Teclado	Genius			En buen estado
4	Mouse	Hp			En buen estado

Gerencia

Núm.	Equipo	Marca	Núm. Inventario	Características	Observaciones
1	Computador portátil	Hp		Sistema operativo 64 Bits	
2	Procesador	Core		Intel core i5 2.90GHz 1000GB DD	
3	Teclado	Genius			En buen estado
4	Mouse	Hp			En buen estado

Computador Jefe de programación

Núm.	Equipo	Marca	Núm. Inventario	Características	Observaciones
1	Computador de escritorio	Hp		Sistema operativo 64 Bits 1000GB DD	Funcional
2	Procesador	core		Intel core i5 2.90GHz	
3	Teclado	Genius			En buen estado
4	Mouse	Hp			En buen estado
5	Impresora	EPSON		L380	En buen estado

Computador área Mercadeo

Núm.	Equipo	Marca	Núm. Inventario	Características	Observaciones
1	Computador todo en uno	Hp		Sistema operativo de 64 bits 500 GB DD	Funcional
2	Procesador	Intel Core		Intel core i5 2.90GHz	
3	Teclado	Genius			En buen estado
4	Mouse	Hp			En buen estado

Computador área de redes

Núm.	Equipo	Marca	Núm. Inventario	Características	Observaciones
1	Computador de escritorio	Hp		8.00 GB, sistema operativo de 64 bits 1000 GB DD	Estado funcional
2	Procesador	Intel Core		Interl@core(MT) Core i7 CPU @	En buen estado
3	Teclado	Genius			En buen estado
4	Mouse	Hp			En buen estado

Computador área financiera

Núm.	Equipo	Marca	Núm. Inventario	Características	Observaciones
1	Computador de escritorio	Samsung		Sistema de 32 bits 2.00 GB	
2	Procesador	Intel Pentium		Intel(R)Pentium(R) Dual CPU E2180 @2.00GHz 2.00GHz	Funcional
3	Teclado	Genius			Funcional
4	Mouse	Genius			Funcional

Apéndice E. Programa de auditoria

PROGRAMA DE AUDITORIA				
Empresa: ASUCAP TV SAN JORGE				Fecha: 01-06-2020
Fase	Actividad	Horas Estimadas	Hora Total	Encargados
1	Visita Preliminar <ul style="list-style-type: none"> Recopilación de la información organizacional: Estructura orgánica, misión y visión de la dependencia, Recurso humano. Reunión con el gerente 	6 Hrs	8 Hrs	Estefanía Álvarez
		2 Hrs		
2	Desarrollo de la auditoria <ul style="list-style-type: none"> Entrevista con el jefe Encuesta a funcionarios de la dependencia Inventario de Hardware Aplicación de listas de chequeo (Seguridad de la información) 	2 Hrs	200 Hrs	Estefanía Álvarez
		16 Hrs		
		20 Hrs		
		20 Hrs		

Apéndice F. Carta de culminación de los objetivos propuestos y compromiso por parte de la empresa para cumplir a cabalidad la debida implementación.



ASOCIACIÓN DE USUARIOS DEL CANAL COMUNITARIO DE TELEVISIÓN DE OCAÑA
"ASUCAP TV SAN JORGE"
 "NO somos televisión por suscripción" Personería Jurídica Resolución No. 134/91
 Gobernación N. De S.N.T. 800.144.216-4, Resolución 1936/26 de diciembre de 2018 prórroga de
 licencia No. 0117/28 de febrero 2000 ANTV.

Ocaña, 17 de julio de 2020

Señorita
ESTEFANIA GISELLE ALVAREZ CLARO
 Estudiante UFPSO
 Ingeniería de Sistemas

Cordial saludo,

Para Asucap Tv San Jorge es grato contribuir en la formación profesional de las diferentes carreras que tiene nuestra Alma Mater. Según informe presentado, se certifica la culminación de los objetivos propuestos inicialmente de la mejor manera, brindando a nuestra empresa un Plan de Continuidad del Negocio aplicado siguiendo los reglamentos y políticas establecidas, de la misma manera, comprometiéndonos a su continua aplicación para nuestra mejora.

Por lo anterior, agradecemos su labor realizada.

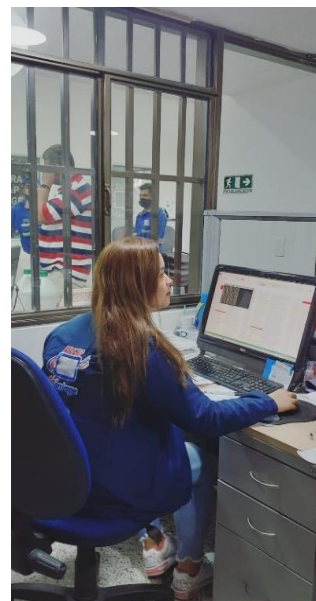
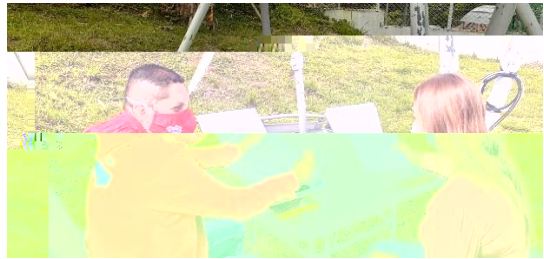
Cordialmente,


OSWALDO AUGUSTO JACOME SUAREZ
 Gerente y Representante Legal
ASUCAP TV SAN JORGE

www.tvsanjorg
 e.tv Calle 11 No. 33-180 Barrio
 Buenos Aires Tel.: (7561) 12 72
 - (7561) 12 77
 gerencia@tvсанjor
 ge.tv Ocaña,
 Colombia



Apéndice G. Evidencias fotográficas



Socialización por el medio comunitario de ASUCAP TV SAN JORGE el trabajo realizado en la empresa.



<https://www.facebook.com/tvsanjorge/videos/893530227799662/>

