UNIVERSIDAD NACIONAL DE INGENIERÍA
Facultad De Electrotecnia y Computación

TRABAJO MONOGRÁFICO

Análisis de Incidentes de Ciberseguridad de la Empresa Casavisión

Para optar al título de

Ingeniero en computación

Elaborado por:

Br. Michell Victoria Gutiérrez Ríos

Br. Wilberth Antonio Montiel Hernández

Tutor:

MSc. Gabriel Rafael Lacayo Saballos

Managua, Nicaragua

Junio 2022

Dedicatoria

Dedicamos este trabajo primeramente a Dios por darnos la sabiduría, inteligencia y las fuerzas necesarias para poder sacar adelante este proyecto y alcanzar la meta de obtener nuestro título profesional.

A nuestras familias porque con su esfuerzo logramos ser los profesionales que somos, principalmente a nuestros padres por ser nuestro pilar en este mundo, a mi madre Boni Ríos García (Q.D.E.P) por su amor y apoyo incondicional.

A Francisco Javier Rodríguez Gaitán por ser siempre el motor para lograr cada proyecto de nuestras vidas.

A todas las personas que nos han apoyado y han hecho que el trabajo se realice con éxito en especial a aquellos que nos abrieron las puertas y compartieron sus conocimientos

Agradecimiento

Agradecemos primeramente a Dios ser maravilloso que nos dio fuerzas y ánimo para creer y lograr esta meta.

A nuestros padres por ayudarnos mientras realizábamos las investigaciones y por estar a nuestro lado en cada momento de nuestra vida. Por todo el apoyo incondicional que nos han brindado y toda la confianza que han puesto sobre nosotros a lo largo de nuestros estudios.

A las personas de la empresa Casavisión por abrirnos las puertas y facilitarnos toda la información requerida para el desarrollo de nuestro proyecto.

A nuestro tutor Ing. Gabriel Lacayo por colaborar como maestro y tutor, por tomarse la labor de revisar y corregir cada detalle realizado durante todo el trayecto de este trabajo monográfico.

Índice

1. Introducción 1

2. Antecedentes 2

3. Justificación 3

4. Objetivos 4

a. Objetivo General 4

b. Objetivos Específicos 4

5. Marco Teórico 5

5.1 Incidente 5

5.2 Ciberseguridad 5

5.3 Incidentes de Ciberseguridad 5

5.4 Norma ISO/IEC 27002 6

5.5 Dominios de la norma ISO 27002 6

5.6 Objetivos de la norma ISO 27002 7

5.7 Objetivos de control 7

6. Diseño Metodológico 7

6.1 Enfoque Metodológico 7

6.2 Tipo de Investigación 8

6.3 Universo, Población y Muestra 8

6.4 Diseño de Instrumentos 8

a. Entrevistas 9

b. Observación 9

c. Inspección 9

7. Análisis y presentación de resultados 9

7.1 Situación actual de la empresa 9

7.2 Reseña histórica de la empresa 11

7.3 Estructura Organizacional 11

7.4 Descripción de los Procesos de Negocio 13

7.5 Incidentes de Ciberseguridad en los Procesos Claves 15

7.5.1 Análisis de Riesgo 15

7.5.2 Identificación de Activos 17

7.5.3 Dimensiones de Valoración 19

7.5.4 Identificación de Amenazas 26

7.5.5 Criterios de evaluación 40
7.6 Procesos Claves y sus Incidencias 43
a. Controles de la Norma ISO 27002:2013 orientado a los procesos de la empresa 47
b. Implementación de la norma ISO 27002 48
8. Conclusiones y recomendaciones 92
8.1 Conclusiones 92
8.2 Recomendaciones 93
9. Bibliografía 95
10. Anexos 97

Índice de figuras

Figura 1. Proceso ante un incidente. 10
Figura 2. Organigrama 11
Figura 3. Mapa de Procesos..... 13
Figura 4. Análisis de riesgo 16
Figura 5. Estado de la Seguridad 91

Índice de tablas

Tabla 1. Puestos de trabajo 8
Tabla 2. Descripción funciones jefe de planta Externa 11
Tabla 3. Descripción de funciones de jefe de Datos 12
Tabla 4. Descripción de las funciones de soporte técnico y TV datos 12
Tabla 5. Activos de información 19
Tabla 6. Criterios de valoración de acuerdo al Impacto 20
Tabla 7. Valoración de activos de acuerdo al impacto 22
Tabla 8. Criterios de valoración de acuerdo a las dimensiones de seguridad 23
Tabla 9. Valoración de activos de acuerdo a la dimensión 25
Tabla 10. Catálogo de amenazas posibles 26
Tabla 11. Fuego 27
Tabla 12. Daños por agua 27
Tabla 13. Desastres naturales 28
Tabla 14. Fuego 28
Tabla 15. Daños por agua 29
Tabla 16. Desastres Industriales 29
Tabla 17. Contaminación mecánica 29
Tabla 18. Contaminación electromagnética 30
Tabla 19. Avería de origen físico o lógico 30
Tabla 20. Corte del suministro eléctrico 31
Tabla 21. Condiciones inadecuadas de temperatura 31
Tabla 22. Interrupción de otros servicios 31
Tabla 23. Degradación de los soportes 32
Tabla 24. Errores de los usuarios 32
Tabla 25. Errores del administrador 33
Tabla 26. Errores de configuración 33
Tabla 27. Deficiencias de la organización 33
Tabla 28. Difusión de software dañino 34
Tabla 29. Alteración accidental de la información 34
Tabla 30. Destrucción de la información 35
Tabla 31. Fuga de información 35
Tabla 32. Vulnerabilidades de los programas 35

Tabla 33. Errores de mantenimiento 36
Tabla 34. Caída del sistema 36
Tabla 35. Pérdida de equipos 37
Tabla 36. Indisponibilidad del personal 37
Tabla 37. Manipulación de configuración 37
Tabla 38. Suplantación de la identidad 38
Tabla 39. Abuso de privilegios 38
Tabla 40. Uso no previsto 39
Tabla 41. Difusión de software dañino 39
Tabla 42. Acceso no autorizado 40
Tabla 43. Probabilidad de ocurrencia 40
Tabla 44. Amenaza de los activos 43
Tabla 45. Incidencias de procesos 46
Tabla 46. Análisis Dominio Política de Seguridad de la Información. 49
Tabla 47. Análisis Dominio Aspectos Organizativos de la Seguridad de la Información. 49
Tabla 48. Análisis Dominio Gestión de Activos. 50
Tabla 49. Análisis Dominio Seguridad Física y Ambiental. 53
Tabla 50. Análisis Dominio Seguridad de las Operaciones 54
Tabla 51. Análisis Dominio Seguridad de las Comunicaciones. 56
Tabla 52. Análisis Dominio Adquisición, Desarrollo y Mantenimiento de los Sistemas de Información. 57
Tabla 53. Análisis Dominio Gestión de Incidentes de Seguridad de la Información. 59
Tabla 54. Análisis Dominio Gestión de Incidentes de Seguridad de la Información - Proceso Avería y Mantenimiento. 62
Tabla 55. Análisis Dominio Gestión de Incidentes de la Seguridad de la Información - Procesos Proyecto / Ingeniería 69
Tabla 56. Análisis Dominio Gestión de Incidentes de la Seguridad de la Información - Proceso Instalación. 74
Tabla 57. Análisis Dominio Gestión de Incidentes de la Seguridad de la Información - Proceso Soporte TI. 87
Tabla 58. Análisis Dominio Gestión de Incidentes de la Seguridad de la Información - Proceso Gestión de cobranza y ventas. 88

Tabla 59. Análisis Dominio Aspecto de Seguridad de la Información para la Gestión de Continuidad del Negocio. 90

Resumen

En el presente trabajo monográfico llamado “Análisis de Incidentes de Ciberseguridad de la Empresa Casavisión” tiene como propósito analizar los incidentes de la empresa con el fin de brindar recomendaciones para responder a las necesidades de la misma, utilizando la norma ISO 27002:2013.

Actualmente la empresa realiza estudios de incidencias de ciberseguridad de una forma no ordenada, centralizándose únicamente en resolver dicho incidente sin tomar en cuenta normas o protocolos dentro de la política de la ciberseguridad, lo que requiere mayor esfuerzo, tiempo y recursos al momento de posibles riesgos. Por esta razón se describe los procesos del negocio de la empresa, para lograr examinar los incidentes de ciberseguridad que han ocurrido en cada proceso clave.

En el marco teórico se define toda la teoría necesaria para llevar a cabo el desarrollo de dicho análisis. Seguido de ello se encuentra cada fase que contiene la metodología a utilizar, cada paso para la recolección de información, tipos de instrumentos a utilizar, análisis y presentación de resultados, descripción de los procesos del negocio, incidencias de los procesos claves y análisis de riesgo.

Cabe mencionar que para el análisis de riesgo se utilizó MAGERIT, metodología de análisis y gestión de riesgo que está directamente relacionada con la generalización del uso de tecnologías de la información.

Haciendo uso de la metodología de análisis y gestión de riesgos, MAGERIT y basados en la información suministrada por la empresa, se determinan los activos con los que cuenta.

Finalmente se identifican los controles de la Norma ISO 27002:2013 aplicados a los procesos clave de la empresa que nos permitieron evaluar como la empresa afronta los eventos e incidencias de ciberseguridad, con el fin de emitir recomendaciones que sean utilizadas como referencia para la toma de decisiones.

1. Introducción

A medida que los ciberataques continúan creciendo en volumen, diversidad y sofisticación, además de ser más disruptivos y dañinos, las organizaciones deben estar preparadas para manejarlos de manera efectiva. Además de implementar prácticas y soluciones de seguridad efectivas, necesitan la capacidad de identificar y abordar rápidamente ataques. (Kingatua, 2020)

Casavisión es una compañía privada de telecomunicaciones, 100% nicaragüense con sucursales en Managua (Rocargo y Miraflores) y Ciudad Sandino.

Casavisión como parte de su crecimiento hace uso de las Tic's (Tecnologías de la Información y la Comunicación) para sistematizar las áreas del negocio y así ofrecer servicios de calidad a sus clientes.

Por esa razón se pretende, tomando como base la norma ISO/IEC 27002:2013, analizar la situación actual de la empresa, proporcionando procesos, procedimientos y recomendaciones de las mejores prácticas en incidentes de ciberseguridad.

El documento está dividido de la siguiente manera:

La primera parte está enfocada en los antecedentes, justificación, objetivo general de la investigación y los objetivos específicos.

La segunda parte se aborda los aspectos conceptuales, teóricos de la gestión de incidentes de ciberseguridad y la metodología aplicada a la investigación.

2. Antecedentes

Internet es la red de redes que está cada día en evolución y que es actualmente indispensable para cualquier hogar, lugar de trabajo o algún medio que maneje información de forma masiva y haga uso de multimedia. (Sites, 2020)

El departamento de informática de Casavisión es encargado de las modulaciones de frecuencia por canal de transmisión, proveer internet a los departamentos, garantizar el tráfico internacional, garantizar el servicio de internet a los clientes, monitorear la saturación de los CMTS (Cable Modem Termination System), entre otros.

Casavisión tiene el propósito de implementar un plan de contingencia el cual trata de tener un Centro de Datos alterno o una réplica de los equipos que permita siempre mantener la fluidez del servicio ante cualquier eventualidad como falla eléctrica, daño de un equipo, corte de fibra, etc. El fin de dicha replica es garantizar la continuidad del servicio, evitando la caída del mismo y causando así solamente una degradación del servicio cuando se enrute al sitio de contingencia.

De igual manera tienen el propósito de realizar una lista de posibles incidentes de ciberseguridad que les ayudará a prever el problema y ser proactivo y no reactivo, ayudando así a diagnosticar de una manera más fácil la falla a ocurrir, sin embargo, la empresa no cuenta con una documentación que soporte dichas propuestas.

Con la existencia del departamento de informática se ha logrado un crecimiento importante en la empresa sin embargo aún no se ha hecho un análisis de incidentes de ciberseguridad, que permita verificar las debilidades y así aplicar las acciones correctivas en el tiempo oportuno para asegurar la información que posee.

3. Justificación

Todas las empresas, independientemente de su tamaño, organización y volumen de negocio, deben de ser conscientes de la importancia de tener implantadas una serie de medidas de seguridad para garantizar la continuidad de los procesos en caso de que se produzcan incidencias de ciberseguridad, fallos, actuaciones malintencionadas por parte de terceros, perdidas accidentales o desastres que afecten los datos e información almacenada.

La empresa Casavisión realizan estudio de incidentes de ciberseguridad de una manera no ordenada, solucionando únicamente cada incidente al momento ocurrido sin llevar un proceso y documentación de cada falla ocurrida y como fue solucionada para tener un soporte y contar con un listado de posibles fallas y su soluciones antes incidentes futuros, esto significa que redundan en esfuerzo, tiempo y recursos para solventar posibles riesgos que puedan ocurrir, sin embargo, la gerencia de dicha empresa está considerando mejorar la respuesta a estas situaciones y es por eso que requieren un análisis de incidentes de ciberseguridad.

Con el análisis de incidentes de ciberseguridad de la información en base a la norma ISO/IEC 27002:2013, se evaluará la eficacia y coherencia con que la empresa afronta los eventos e incidentes de ciberseguridad, con el fin de emitir recomendaciones que sirvan de referencia para la toma de decisiones.

4. Objetivos

4.1 Objetivo General

Analizar los incidentes de ciberseguridad de la empresa Casavisión para responder a las necesidades de la gerencia de dicha empresa, utilizando la norma ISO 27002:2013.

4.2 Objetivos Específicos

- Describir los procesos de negocio de la empresa Casavisión.
- Examinar los incidentes de ciberseguridad que han ocurrido en los procesos claves de la empresa Casavisión.
- Identificar los controles de la norma ISO 27002:2013 que se relacionen con los procesos de la empresa.

5. Marco Teórico

En esta parte se hará el análisis teórico sobre los incidentes de ciberseguridad, tomando como base la norma ISO/IEC 27002:2013, analizar la situación actual de la empresa, la cual se encarga de implementar un conjunto amplio de controles de seguridad bajo el marco de referencia global de un sistema de gestión coherente.

5.1 Incidente

Un incidente es un suceso repentino no deseado que ocurre por las mismas causas que se presentan los accidentes, sólo que por cuestiones del azar no desencadena lesiones en las personas, daños a la propiedad, al proceso o al ambiente. Un incidente es una alerta que es necesario atender. Es la oportunidad para identificar y controlar las causas básicas que lo generaron, antes de que ocurra un accidente. (Sura, s.f.)

5.2 Ciberseguridad

Según los profesionales en seguridad de ISACA (Information Systems Audit and Control Association) la ciberseguridad se define como una capa de protección para los archivos de información, a partir de ella, se trabaja para evitar todo tipo de amenazas, las cuales ponen en riesgo la información que es procesada, transportada y almacenada en cualquier dispositivo.

La ciberseguridad trata de trabajar en robustos sistemas que sean capaces de actuar antes, durante y después, no sirve solo para prevenir, sino también dar confianza a los clientes y al mercado, pudiendo así reducir el riesgo de exposición del usuario y de los sistemas. (lanz, 2018)

5.3 Incidentes de Ciberseguridad

Un incidente de Ciberseguridad es un evento singular o serie de eventos de seguridad de la información, inesperados o no deseados, que tienen una probabilidad significativa de comprometer las operaciones del negocio y de amenazar la seguridad de la información. (EVALUANDOCLOUD, 2020)

Se diferencian dos tipos de incidentes de ciberseguridad:

Incidentes de Ciberseguridad relacionados con la información, que provocan una pérdida o un uso indebido de la información, espionaje, fraude o robo de identidad.

Incidentes de Ciberseguridad relacionados con las infraestructuras TI, que producen la interrupción parcial o total de los Sistemas de Información, siendo los más comunes, la infección por malware, los ataques contra redes, etc. (EVALUANDOCLOUD, 2020)

5.4 Norma ISO/IEC 27002

En 1995, las organizaciones Internacionales ISO (The International Organization for Standardization) e IEC (International Electrotechnical Commission) dieron origen a un grupo de normas que consolidan las directrices relacionadas al alcance de la Seguridad de la Información, siendo representada por la serie 27000. En este grupo se encuentra la ISO/IEC 27002 (anteriormente denominada estándar 17799:2005), norma internacional que establece el código de mejores prácticas para apoyar la Gestión de Seguridad de la Información en las organizaciones. (Ostec, 2020)

ISO/IEC 27002 es una norma popular de buenas prácticas reconocida internacionalmente para la seguridad de la información. Su linaje se remonta más de 30 años a los precursores de BS 7799. (ISO/IEC 27002, 2020)

La norma ISO 27002:2013, contiene 14 dominios, los cuales se mencionan a continuación:

5.5 Dominios de la norma ISO 27002

1. Políticas de Seguridad.
2. Aspectos Organizativos de la seguridad de la información.
3. Seguridad Ligada a los Recursos Humanos.
4. Gestión de Activos.
5. Control de Accesos.
6. Cifrado.
7. Seguridad Física y Ambiental.
8. Seguridad en las Operaciones.

9. Seguridad en las comunicaciones.
10. Adquisición, Desarrollo y Mantenimiento de los Sistemas de Información.
11. Relaciones con Suministradores.
12. Gestión de Incidentes en la Seguridad de la Información.
13. Aspectos de Seguridad de la Información en la Gestión de la Continuidad del Negocio.
14. Cumplimiento.

5.6 Objetivos de la norma ISO 27002

El principal objetivo de la ISO 27002 es establecer directrices y principios generales para iniciar, implementar, mantener y mejorar la gestión de ciberseguridad en una organización. Esto también incluye la selección, implementación y administración de controles, teniendo en cuenta los entornos de riesgo encontrados en la empresa. (Ostec, 2020)

5.7 Objetivos de control

ISO/IEC 27002 especifica 35 objetivos de control con respecto a la necesidad de proteger la confidencialidad, integridad y disponibilidad de información.

Los objetivos de control están en un nivel bastante alto y, en efecto, comprenden una especificación genérica de requisitos funcionales para la arquitectura de gestión de seguridad de la información de una organización. (ISO/IEC 27002, 2020)

6. Diseño Metodológico

6.1 Enfoque Metodológico

La presente investigación se realizó desde un enfoque metodológico cualitativo. Este pretende enfocar los problemas o fenómenos a estudiar, a través de los datos descriptivos. Por eso los resultados se presentan en base a una descripción de características del objeto de estudio. (Becerra Meza & Weinborn De la Calle, 2005)

6.2 Tipo de Investigación

El enfoque propuesto para desarrollo del tema: Análisis de Incidentes de Ciberseguridad en la Empresa Casavisión, es de tipo analítico descriptivo que trabaja con la metodología cualitativa, se pretende analizar la problemática a los incidentes de ciberseguridad que ocurren en la empresa Casavisión.

Para esto se utilizó la Norma ISO/IEC 27002:2013 específicamente el Dominio de Gestión de Incidentes de Ciberseguridad de la Información y así determinar las fases necesarias para describir los procesos actuales, examinar los incidentes de ciberseguridad e identificar los controles según la norma a utilizar.

6.3 Universo, Población y Muestra

La investigación se realizó en la empresa Casavisión, la cual se tomó en cuenta 12 trabajadores. El total de los trabajadores representa el universo y la población objetivo de nuestra investigación.

Para la recolección de la información, se trabajó con 2 trabajadores los cuales son parte de Centro de datos ISP () y TV Datos y Soporte Técnico, los puestos que ocupan son:

Áreas	Puestos seleccionados para la muestra
Centro de Datos ISP Tv Datos y Soporte Técnico	• Jefe de Planta Externa
Centro de Datos ISP	• Jefe de Datos

Tabla 1. Puestos de trabajo

6.4 Diseño de Instrumentos

Para la ejecución de las etapas antes mencionadas, utilizó los siguientes instrumentos elaborados para obtener la mayor cantidad de información posible por parte de los involucrados en los procesos que analizados.

6.4.1 Entrevistas

Se usó entrevistas como instrumento para obtener información específica sobre los incidentes de ciberseguridad de la empresa Casavisión y el estado de su seguridad.

Dichas entrevistas estuvieron dirigidas a la gerencia, al supervisor y el responsable de gestión de incidentes. (Ver Anexo12, Anexo13)

6.4.2 Observación

Se ha dispuesto del tiempo, el lugar de trabajo y los medios oportunos para desarrollar el proceso de recopilación de información a través de métodos tan concretos como la observación directa.

El propósito de esta técnica es observar todas aquellas situaciones que se presentan en la empresa Casavisión.

6.4.3 Inspección

Consiste en examinar físicamente bienes, documentos y/o valores con el objeto de demostrar su autenticidad. (Técnicas de Auditoria, 2008)

7. Análisis y presentación de resultados

7.1 Situación actual de la empresa

Hoy en día la amenaza más importante contra la información, la encontramos dentro de la misma empresa donde laboramos. Ya sea por accesos indebidos o no autorizados a la información corporativa, son realizados principalmente por los empleados de la misma empresa.

La empresa Casavisión actualmente no ha realizado análisis de incidentes en los procesos claves, para poder tener conocimiento de la importancia que tienen estos riesgos.

Casavisión al momento de que ocurre un incidente en los procesos claves informan al responsable del área, el cual resuelve el incidente sin llevar un orden o documentación de lo ocurrido y su solución. En el siguiente flujograma

se observa el proceso general que realiza la empresa ante un incidente ocurrido.

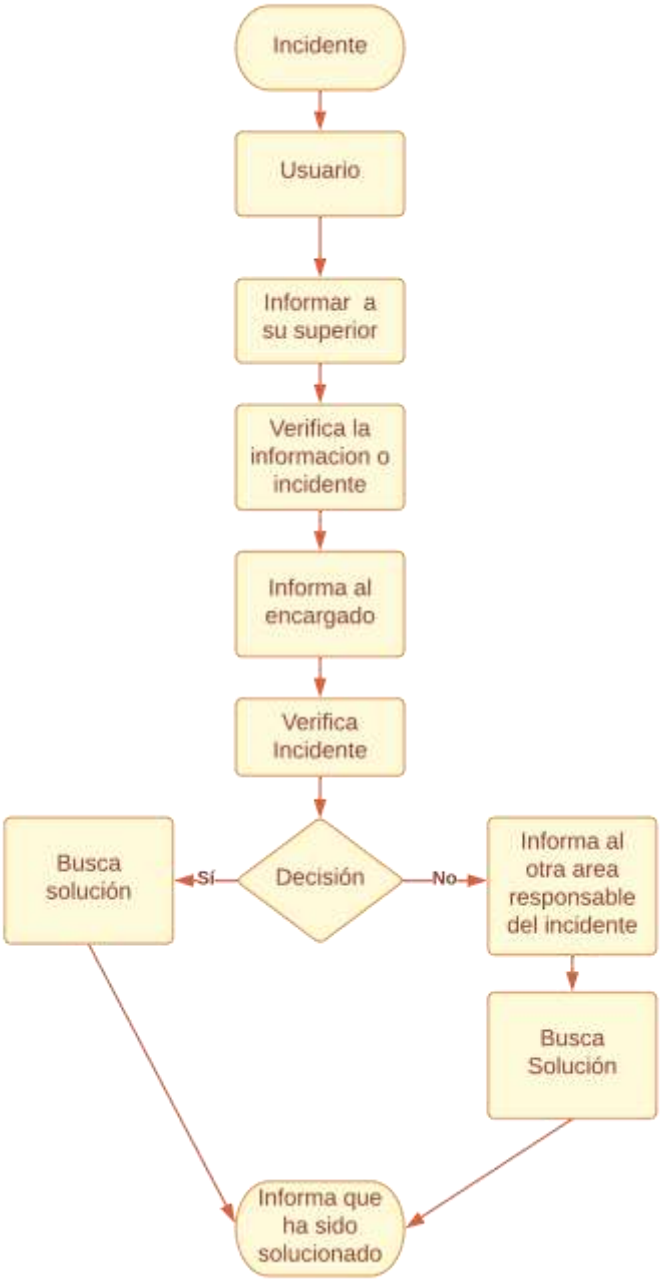


Figura 1. Proceso ante un incidente.

Fuente: Elaboración propia.

La clave está en que existan políticas de ciberseguridad de la información y que sean puestas en práctica por los empleados de la empresa para que estén concientizados de la importancia de la información.

7.2 Reseña histórica de la empresa

Casavisión es una compañía privada de telecomunicaciones, 100% Nicaragüense, que se enfoca en brindar los mejores servicios de televisión por cable e internet. Inició operaciones en diciembre del 2013 en Granada, en diciembre del 2015 inicia operaciones en Managua, cuenta con su propio canal de TV Casa36 TV.

Actualmente cuenta con dos sucursales en Managua y una en ciudad Sandino.

7.3 Estructura Organizacional

a. Organigrama

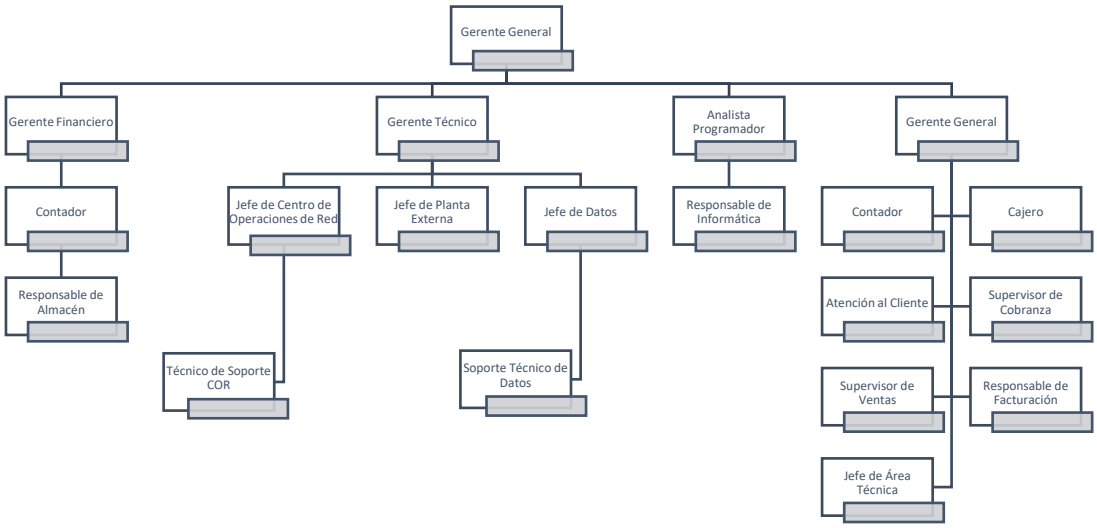


Figura 2. Organigrama

Fuente: Empresa Casavisión

b. Descripción de las principales funciones del departamento de Tecnología de la Información.

Jefe de Planta Externa	Objetivo: Responsable de TV análoga y Digital.
Responsabilidades: • Encargado de las modulaciones de frecuencias por canal de transmisión.	

Tabla 2. Descripción funciones jefe de planta Externa

Fuente: Elaboración Propia

Jefe de Datos	Objetivo: Responsable de Centro de Datos ISP
Responsabilidades: • Proveer internet a los departamentos. • Garantizar el tráfico Internacional. • Seguridad en la red. • Garantizar el servicio de internet a los clientes. • Monitorear la saturación de los CMTS.	

Tabla 3. Descripción de funciones de jefe de Datos

Fuente: Elaboración Propia

Soporte Técnico y TV Datos	Objetivo: Brindar soporte a los clientes y técnicos de la empresa.
Responsabilidades: • Soporte técnico al momento que el cliente solicita cambio de contraseña. • Reporte de problemas con el internet, problemas de velocidad e inconvenientes don la señal de cable. • Generación de órdenes de trabajo cuando el problema no puede ser resuelto desde el área de soporte. • Realizar activación de cable modem desde el sistema de internet. • Reactivar el servicio de internet a clientes suspendidos. • Monitorear constantemente la programación de TV para garantizar buenas señal y correcta programación.	

Tabla 4. Descripción de las funciones de soporte técnico y TV datos

Fuente: Elaboración Propia

c. Misión

Somos la empresa de telecomunicaciones con mayor nivel y calidad de servicio en Nicaragua, líder por excelencia en atención al cliente y reconocida por su integridad y cumplimiento de palabra. Estamos dedicados a brindar el mejor servicio de televisión por cable e internet y nuestro compromiso es ofrecer los mejores servicios a nuestros clientes.

d. Visión

Convertirnos en la compañía nicaragüense líder en telecomunicaciones, enfocada en brindar los mejores servicios de televisión por cable e internet y excelencia en atención al cliente, pioneros en innovación y tecnología.

7.4 Descripción de los Procesos de Negocio

Para elaborar el análisis de incidentes de ciberseguridad en la empresa Casavisión fue necesario recopilar información para conocer la situación actual de los procesos de negocio, la cual se realiza por medio de entrevistas a personas encargadas.

La empresa Casavisión cuenta con los siguientes procesos de negocio que le permite brindar un servicio de calidad y confianza para todos sus clientes.

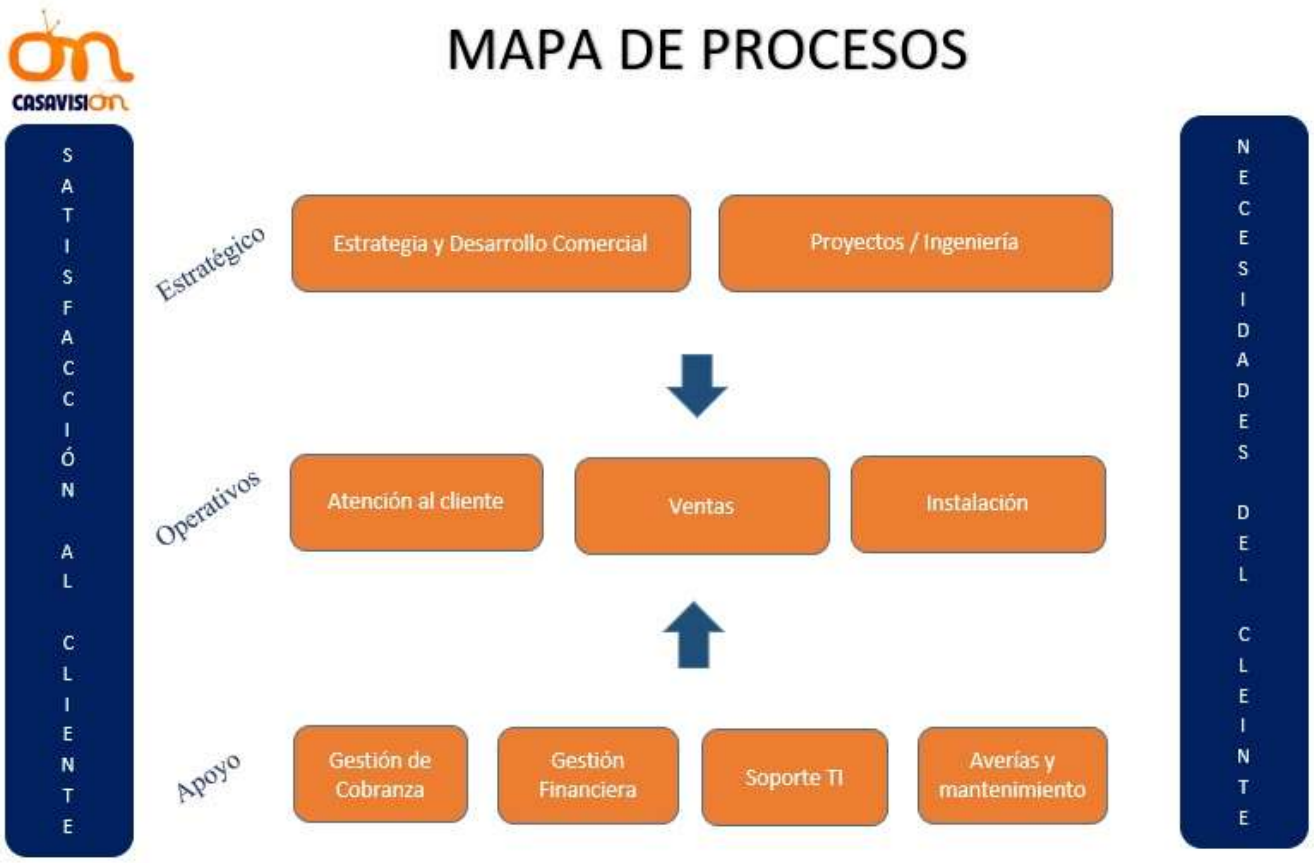


Figura 3. Mapa de Procesos

Fuente: Empresa Casavisión

Procesos estratégicos: Son procesos destinados a definir y controlar las metas de la organización, sus políticas y estrategias. Permiten llevar adelante la organización. Están en relación muy directa con la misión/visión de la organización. Involucran personal de primer nivel de la organización.

Casavisión cuenta con los siguientes procesos estratégicos:

1. Estrategia y desarrollo comercial: son las estrategias de marketing digital, posicionamiento de la marca, publicidad, verificación de competencia.

2. Proyecto / Ingeniería: realización de cartografía, levantamiento local con odómetro y GPS, levantamiento de información en las zonas de apertura (clientes aproximados, distancia entre postes), diseño de red, aprobación del diseño y construcción.

Procesos operativos: Son procesos que permiten generar el producto/servicio que se entrega al cliente, por lo que inciden directamente en la satisfacción del cliente final.

Casavisión cuenta con los siguientes procesos operativos:

1. Atención al cliente: se trata de conocer y ayudar a los clientes en sus necesidades, una comunicación fluida, respuestas rápidas y efectivas a sus solicitudes; hasta detectar sus necesidades para proponer acciones de mejora.

2. Ventas: es la sucesión de pasos que una empresa realiza desde el momento en que intenta captar la atención de un potencial cliente hasta que la transacción final se lleva a cabo, es decir, hasta que se consigue una venta efectiva del producto o servicio de la compañía.

3. Instalación: es el conjunto de medios o recursos necesarios para entregar el producto o servicio al cliente.

Procesos de Apoyo: Apoyan los procesos operativos. Sus clientes son internos. Ejemplos: Control de calidad, Selección de personal, Formación del personal, Compras, Sistemas de información, etc.

Casavisión cuenta con los siguientes procesos de apoyo:

1. Gestión de cobranza: se focaliza en contactar a los clientes morosos por distintos canales (avisos de cobros) para informarles el estado de sus facturas, la obligación de pago y ofrecerles opciones de normalización. Se encarga de generación de facturas, envío de facturas vía correo electrónico, verificación de pago, suspensión de servicio en caso de facturas vencidas, etc.

2. Gestión Financiera: es el proceso encargado de realizar estrategia para reducción de costo, estrategia de inversiones.

3. Soporte TI: se encarga de resolver los problemas técnicos de la empresa y de apoyar a los clientes a través de diferentes canales.

4. Averías y Mantenimiento: es la resolución de un problema en particular o falla en algún sector para ofrecerle al cliente un servicio de calidad.

7.5 Incidentes de Ciberseguridad en los Procesos Claves

Para empezar, se realizó un análisis de riesgo que nos permitió obtener las principales amenazas que se pueden presentar en la empresa, seguido a esto se examinaron amenazas materializadas o los incidentes ocurridos en los procesos claves de la empresa Casavisión.

7.5.1 Análisis de Riesgo

Se identificó todos los riesgos potenciales que afecten los procesos claves en el buen funcionamiento de la empresa, para dicho análisis se utilizó MAGERIT, metodología de análisis y gestión de riesgos que está directamente relacionada con la generalización del uso de las tecnologías de la información. MAGERIT implementa el proceso de gestión de riesgos dentro de un marco de

trabajo para que los órganos de gobierno tomen decisiones teniendo en cuenta los riesgos derivados del uso de tecnologías de la información.

El análisis de riesgo permite determinar cómo es, cuánto vale y como de protegidos se encuentran los activos evaluando de manera metódica para llegar a conclusiones con fundamento.

Elementos del Análisis de Riesgo:

- Activos: es todo aquel recurso que genere valor a la empresa y que sienta la necesidad de proteger.
- Amenazas: son eventos que les puede pasar a los activos provocando daños a la empresa.
- Salvaguardas: son mecanismos de defensa utilizados para aquellas amenazas no causen tanto daño.

Con los elementos anteriores se puede identificar:

- El impacto: lo que podría pasar.
- El riesgo: lo que probablemente pase.

La siguiente imagen recoge lo anteriormente mencionado:

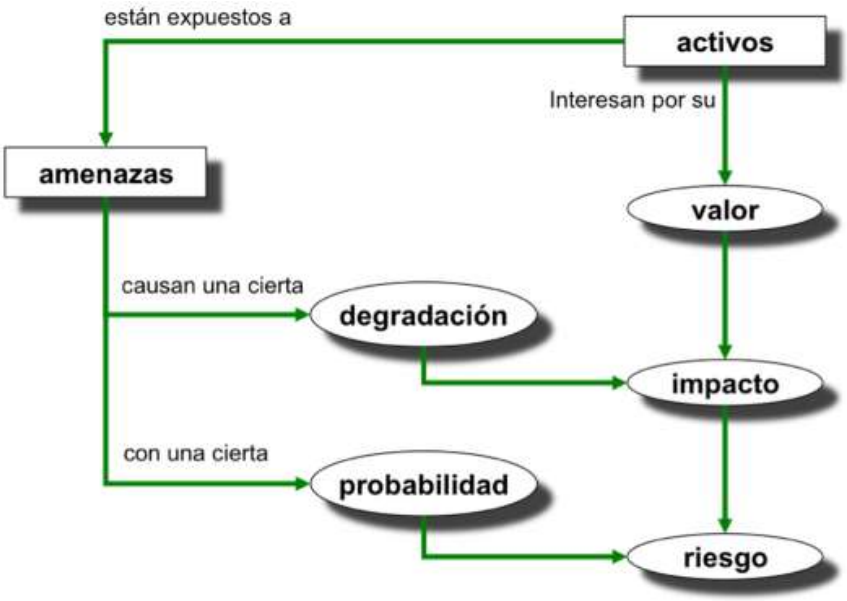


Figura 4. Análisis de riesgo

Fuente: Magerit

7.5.2 Identificación de Activos

El activo esencial es la información que se maneja, es el eslabón de información determinable e identificable, MAGERIT los clasifica y agrupa de la siguiente manera:

- [D] Datos: Los datos son el corazón que permite a una organización prestar sus servicios. La información es un activo abstracto que será almacenado en equipos o soportes de información.

- [S] Servicios: Función que satisface una necesidad de los usuarios (del servicio).

- [SW] Software: Con múltiples denominaciones (programas, aplicativos, desarrollos, etc.) se refiere a tareas que han sido automatizadas para su desempeño por un equipo informático. Las aplicaciones gestionan, analizan y transforman los datos permitiendo la explotación de la información para la prestación de los servicios.

- [HW] Hardware: Materiales físicos, destinados a soportar directa o indirectamente los servicios que presta la organización, siendo pues depositarios temporales o permanentes de los datos.

- [COM] Comunicaciones: Incluyendo tanto instalaciones dedicadas como servicios de comunicaciones contratados a terceros; pero siempre centrándose en que son medios de transporte que llevan datos de un sitio a otro.

- [MEDIA] Soportes de Información: Se consideran dispositivos físicos que permiten almacenar información de forma permanente o, al menos, durante largos periodos de tiempo.

- [AUX] Equipamiento Auxiliar: Se consideran otros equipos que sirven de soporte a los sistemas de información, sin estar directamente relacionados con datos.

- [P] Personal: aparecen las personas relacionadas con los sistemas de información.

Tipo de Activo	Código de Activo	Activos más relevantes en la empresa
[S] Servicios:	[ext] usuarios externos	Página Web Externa
		Soporte Técnico Externo
	[int] Usuario Internos	Página Web Interno (Intranet)
[SW] Software	SUB	Sistema de Cable (Facturación)
	HELPDESK	osTicket
		HESK
	ERP	Softland ERP
	EMAIL_CLIENT	CLIENTE CORREO
	EMAIL_SERVER	Correo Electrónico
	CORTAFUEGO	Fortinet
	STD	FortiClient (VPN)
	DBMS	Base de datos producción MS SQL SERVER 2014
		Base de datos pruebas y desarrollo MS SQL Server 2014
	BACKUP	Cobian Backup
	MONITOREO	Orion
		Cacti
	BROWSER	MS Edge
		Google Chrome
	PBX	Issabel
		FOP2
	AV	ESET Nod32 AV (Antivirus)
	HYPERVISOR	VMWare vSphere

	DESARROLLO	MS Visual Studio 2017
[HW] Hardware:	HOST	Servidores
		Unidades de Precisión
	NETWORK	Switch
		Equipos de la red cableada (router)
	PC	Portátiles Dell Inspiron 3583, Dell Inspiron 3501, Lenovo Ideapad S340-15IWL
		Computadoras Desktop HP core5
	FIREWALL	Firewall. Corta Fuegos
	PRINT	Servicio de Impresión
[COM] Comunicaciones	WIFI	Equipos de Red inalámbricos (Router, Cable Modem)
[MEDIA] Soportes de Información	NAS	NAS Corporativa
	DISK	Duro externo
[AUX] Equipamiento Auxiliar:	POWER	UPS
		Planta Eléctrica

Tabla 5. Activos de información

7.5.3 Dimensiones de Valoración

Son las características o atributos que hacen valioso un proceso, las dimensiones se utilizan para valorar las consecuencias de la materialización de una amenaza. La valoración que recibe un proceso en una cierta dimensión es la medida del perjuicio para la organización si el proceso se ve dañado en dicha dimensión. (MAGERIT)

La metodología MAGERIT clasifican los activos de acuerdo a su valoración por dimensiones

a) [D] Disponibilidad:

¿Qué importancia tendría que el activo no estuviera disponible?

b) [I] Integridad:

¿Qué importancia tendría que los datos fueran modificados fuera de control?

c) [C] Confidencialidad:

¿Qué importancia tendría que el dato fuera conocido por personas no autorizadas?

d) [T] Trazabilidad:

¿Qué importancia tendría que no quedara constancia fehaciente del uso del servicio?

7.5.3.1.1 Criterios de Valoración de Acuerdo al Impacto

Se presentan criterios de daños ocasionado, estos criterios son escalas cualitativas de valoración empleadas para la estimulación.

ESCALA	IMPACTO	VALOR	DESCRIPCIÓN
MA	Muy Alto	10	Daño muy grave
A	Alto	7-9	Daño grave
M	Medio	4-6	Daño importante
B	Bajo	1-3	Daño menor
MB	Muy Bajo	0	Irrelevante a efectos prácticos

Tabla 6. Criterios de valoración de acuerdo al Impacto

Tipo de Activo	Código de Activo	Activos más relevantes en la empresa	Impacto
[S] Servicios:	[ext] usuarios externos	Página Web Externa	M

		Soporte Técnico Externo	
	[int] Usuario Internos	Página Web Interno (Intranet)	M
[SW] Software	SUB	Sistema de Cable (Facturación)	A
	HELPDESK	osTicket	M
		HESK	M
	ERP	Softland ERP	M
	EMAIL_CLIENT	Cliente Correo	B
	EMAIL_SERVER	Correo Electrónico	M
	CORTAFUEGO	Fortinet	A
	STD	FortiClient (VPN)	A
	DBMS	Base de datos producción MS SQL SERVER 2014	MA
		Base de datos pruebas y desarrollo MS SQL Server 2014	M
	BACKUP	Cobian Backup	MA
	MONITOREO	Orion	M
		Cacti	M
	BROWSER	MS Edge	M
		Google Chrome	M
	PBX	Issabel	A
		FOP2	A
	AV	ESET Nod32 AV	A
	HYPERVIDOR	VMWare vSphere	A
	DESARROLLO	MS Visual Studio 2017	A
		Servidores	MA

[HW] Hardware:	HOST	Unidades de precisión	MA
	NETWORK	Switch	A
		Equipos de la red cableada (router)	A
	PC	Portátiles Dell Inspiron 3583, Dell Inspiron 3501, Lenovo Ideapad S340-15IWL	A
		Computadoras Desktop HP core5	A
	FIREWALL	Firewall. Corta Fuegos	A
	PRINT	Servicio de Impresión	B
[COM] Comunicaciones	WIFI	Equipos de Red inalámbricos (Router, Cable Modem)	M
[MEDIA] Soportes de Información	NAS	NAS Corporativa	A
	DISK	Duro externo	A
[AUX] Equipamiento Auxiliar:	POWER	UPS	A
		Planta Eléctrica	A

Tabla 7. Valoración de activos de acuerdo al impacto

7.5.3.1.2 Criterios de Valoración de Acuerdo a las Dimensiones de seguridad

"Las dimensiones se utilizan para dar un valor a las consecuencias de la materialización de una amenaza. La valoración que recibe un activo en una cierta dimensión es la medida del perjuicio para la organización si el activo se ve dañado en dicha dimensión".

1. [D] Disponibilidad: Propiedad o característica de los activos consistente en que las entidades o procesos autorizados tienen acceso a los mismos cuando lo requieren.

2. [I] Integridad: Propiedad o característica consistente en que el activo de información no ha sido alterado de manera no autorizada.

3. [C] Confidencialidad: Propiedad o característica consistente en que la información ni se pone a disposición, ni se revela a individuos, entidades o procesos no autorizados.

4. [A] Autenticidad: Propiedad o característica consistente en que una entidad es quien dice ser o bien que garantiza la fuente de la que proceden los datos.

5. [T] Trazabilidad: Propiedad o característica consistente en que las actuaciones de una entidad pueden ser imputadas exclusivamente a dicha entidad. (MAGERIT)

Mediante una tabla comprendida por una escala de 10 valores iniciando en 0 como el valor despreciable a nivel de riesgo, hasta llegar a 10 que sería el valor que se le puede dar a un activo con un daño extremo.

VALOR			CRITERIO
MA	Muy Alto	10	Daño muy grave
A	Alto	7-9	Daño grave
M	Medio	4-6	Daño importante
B	Bajo	1-3	Daño menor
D	Despreciable	0	Irrelevante a efectos prácticos

Tabla 8. Criterios de valoración de acuerdo a las dimensiones de seguridad

Tipo de Activo	Activos más relevantes en la empresa	Valoración de Activos				
		[D]	[C]	[I]	[A]	[T]
[S] Servicios:	Página Web Externa Soporte Técnico Externo	A	A	A	M	A

	Página Web Interno (Intranet)	A	A	A	A	A
[SW] Software	Sistema de Cable	M	M	M	B	A
	osTicket	M	M	M	M	M
	HESK	M	M	M	M	M
	Softland ERP	M	M	M	M	M
	MS Outlook	M	M	M	M	M
	Fortinet	MA	MA	MA	MA	MA
	FortiClient	MA	M	M	M	M
	Base de datos producción MS SQL SERVER 2014	MA	MA	MA	MA	MA
	Base de datos pruebas y desarrollo MS SQL Server 2014	M	MA	M	M	M
	Cobian Backup	M	M	M	M	M
	Orion	M	M	M	M	M
	Cacti	M	M	M	M	M
	MS Edge	M	M	M	M	M
	Google Chrome	M	M	M	M	M
	Issabel	M	MA	M	M	M
	FOP2	M	A	A	A	A
	Flowdat	MA	MA	MA	MA	MA
	ESET Nod32 AV	A	A	A	A	A
	VMWare vSphere	MA	MA	MA	A	A

	MS Visual Studio 2017	A	A	A	A	A
[HW] Hardware:	Servidores	MA	MA	MA	MA	MA
	Unidades de precisión	MA	MA	MA	MA	MA
	Switch	A	A	A	A	A
	Equipos de la red cableada (router)	MA	A	A	A	A
	Portátiles Dell Inspiron 3583, Dell Inspiron 3501, Lenovo Ideapad S340-15IWL	M	M	M	M	M
	Computadoras Desktop HP core5	M	M	M	M	M
	Firewall. Corta Fuegos	MA	MA	MA	MA	MA
	Servicio de Impresión	M	M	M	M	M
[COM] Comunicaciones	Equipos de Red inalámbricos (Router, Cable Modem)	A	A	A	A	A
[MEDIA] Soportes de Información	NAS Corporativa	A	A	A	A	A
	Duro externo	A	A	A	A	A
[AUX] Equipamiento Auxiliar:	UPS	MA	A	A	M	MA
	Planta Eléctrica	A	M	M	M	M

Tabla 9. Valoración de activos de acuerdo a la dimensión

7.5.4 Identificación de Amenazas

Para valorar el nivel o frecuencia de la amenaza en cada activo, es necesario valorar también el impacto que sería en realidad el daño causado al activo en caso de materialización de una amenaza; Así mismo se podrá estimar en qué grado el activo es afectado sobre las dimensiones de seguridad que la metodología MAGERIT ha considerado como la Autenticidad (A), confidencialidad (C), integridad (I), disponibilidad (D) y la trazabilidad del servicio (T). Se efectuará la valoración del impacto que tendrían las amenazas para los activos de la entidad en las cinco dimensiones de seguridad (Disponibilidad, I: Integridad, C: Confiabilidad, A: Autenticidad y T: Trazabilidad), teniendo en cuenta su frecuencia.

Se presenta a continuación un catálogo de amenazas posibles sobre los activos de un sistema de información. Para cada amenaza se presenta un cuadro como el siguiente:

[código] descripción sucinta de lo que puede pasar	
• Tipos de activos: que se pueden ver afectados por este tipo de amenazas	**Dimensiones:** 1. de seguridad que se pueden ver afectadas por este tipo de amenaza, ordenadas de más a menos relevante
Descripción: complementaria o más detallada de la amenaza: lo que le puede ocurrir a activos del tipo indicado con las consecuencias indicadas	

Tabla 10. Catálogo de amenazas posibles

- **[N] Desastres Naturales**

Sucesos que pueden ocurrir sin intervención de los seres humanos como causa directa o indirecta.

Origen: Natural (accidental)

[N.1] Fuego

[N.1] Fuego	
Tipos de activos: • [HW] equipos informáticos (hardware) • [Media] soportes de información • [AUX] equipamiento auxiliar • [L] instalaciones	**Dimensiones:** 1. [D] disponibilidad
Descripción: Incendios: posibilidad de que el fuego acabe con recursos del sistema.	

Tabla 11. Fuego

[N.2] Daños por agua

[N.2] Daños por agua	
Tipos de activos: • [HW] equipos informáticos (hardware) • [Media] soportes de información • [AUX] equipamiento auxiliar • [L] instalaciones	**Dimensiones:** 1. [D] disponibilidad
Descripción: Inundaciones: posibilidad de que el agua acabe con recursos del sistema.	

Tabla 12. Daños por agua

[N.*] Desastres naturales

[N.*] Desastre naturales	
Tipos de activos: • [HW] equipos informáticos (hardware) • [Media] soportes de información • [AUX] equipamiento auxiliar • [L] instalaciones	**Dimensiones:** 1. [D] disponibilidad
Descripción: Otros incidentes que se producen sin intervención humana: rayo, tormenta eléctrica, terremoto, ciclones, avalancha, corrimiento de tierras,... Se excluyen desastres específicos tales como incendios (ver [N.1]) e	

inundaciones (ver [N.2]). Se excluye al personal por cuanto se ha previsto una amenaza específica [E.31] para cubrir la indisponibilidad involuntaria del personal sin entrar en sus causas.

Tabla 13. Desastres naturales

- **[I] De origen industrial**

Sucesos que pueden ocurrir de forma accidental, derivados de la actividad humana de tipo industrial. Estas amenazas pueden darse de forma accidental o deliberada.

[I.1] Fuego

[I.1] Fuego	
Tipos de activos: • [HW] equipos informáticos (hardware) • [Media] soportes de información • [AUX] equipamiento auxiliar • [L] instalaciones	**Dimensiones:** 1. [D] disponibilidad
Descripción: Incendio: posibilidad de que el fuego acabe con los recursos del sistema. Origen: Entorno (accidental) Humano (accidental o deliberado)	

Tabla 14. Fuego

[I.2] Daños por agua

[I.2] Daños por agua	
Tipos de activos: • [HW] equipos informáticos (hardware) • [Media] soportes de información • [AUX] equipamiento auxiliar • [L] instalaciones	**Dimensiones:** 1. [D] disponibilidad
Descripción:	

Escapes, fugas, inundaciones: posibilidad de que el agua acabe con los recursos del sistema. Origen: Entorno (accidental) Humano (accidental o deliberado)

Tabla 15. Daños por agua

[I.*] Desastres industriales

[I.*] Desastres industriales	
Tipos de activos: • [HW] equipos informáticos (hardware) • [Media] soportes de información • [AUX] equipamiento auxiliar • [L] instalaciones	**Dimensiones:** 1. [D] disponibilidad
Descripción: Otros desastres debidos a la actividad humana: explosiones, derrumbes, ... contaminación química, ... sobrecarga eléctrica, fluctuaciones eléctricas, ... accidentes de tráfico, ... Se excluyen amenazas específicas como incendio (ver [I.1]) e inundación (ver [I.2]). Se excluye al personal por cuanto se ha previsto una amenaza específica, [E.31], para cubrir la indisponibilidad involuntaria del personal sin entrar en sus causas. Origen: Entorno (accidental) Humano (accidental o deliberado)	

Tabla 16. Desastres Industriales

[I.3] Contaminación mecánica

[I.3] Contaminación mecánica	
Tipos de activos: • [HW] equipos informáticos (hardware) • [Media] soportes de información • [AUX] equipamiento auxiliar	**Dimensiones:** 1. [D] disponibilidad
Descripción: vibraciones, polvo, suciedad, ... Origen: Entorno (accidental) Humano (accidental o deliberado)	

Tabla 17. Contaminación mecánica

[I.4] Contaminación electromagnética

[I.4] Contaminación electromagnética	
Tipos de activos: • [HW] equipos informáticos (hardware) • [Media] soportes de información • [AUX] equipamiento auxiliar	**Dimensiones:** 1. [D] disponibilidad
Descripción: interferencias de radio, campos magnéticos, luz ultravioleta, ... Origen: Entorno (accidental) Humano (accidental o deliberado)	

Tabla 18. Contaminación electromagnética

[I.5] Avería de origen físico o lógico

[I.5] Avería de origen físico o lógico	
Tipos de activos: • [SW] aplicaciones (software) • [HW] equipos informáticos (hardware) • [Media] soportes de información • [AUX] equipamiento auxiliar	**Dimensiones:** 1. [D] disponibilidad
Descripción: Fallos en los equipos y/o fallos en los programas. Puede ser debida a un defecto de origen o sobrevenida durante el funcionamiento del sistema. En sistemas de propósito específico, a veces es difícil saber si el origen del fallo es físico o lógico; pero para las consecuencias que se derivan, esta distinción no suele ser relevante. Origen: Entorno (accidental) Humano (accidental o deliberado)	

Tabla 19. Avería de origen físico o lógico

[I.6] Corte del suministro eléctrico

[I.6] Corte del suministro eléctrico	
Tipos de activos: • [HW] equipos informáticos (hardware) • [Media] soportes de información	**Dimensiones:** 1. [D] disponibilidad

• [AUX] equipamiento auxiliar	
Descripción: cese de la alimentación de potencia Origen: Entorno (accidental) Humano (accidental o deliberado)	

Tabla 20. Corte del suministro eléctrico

[I.7] Condiciones inadecuada de temperatura o humedad

[I.7] Condiciones inadecuada de temperatura o humedad	
Tipos de activos: • [HW] equipos informáticos (hardware) • [Media] soportes de información • [AUX] equipamiento auxiliar	**Dimensiones:** 1. [D] disponibilidad
Descripción: Deficiencias en la aclimatación de los locales, excediendo los márgenes de trabajo de los equipos: excesivo calor, excesivo frío, exceso de humedad... Origen: Entorno (accidental) Humano (accidental o deliberado)	

Tabla 21. Condiciones inadecuadas de temperatura

[I.9] Interrupción de otros servicios y suministros esenciales

[I.9] Interrupción de otros servicios y suministros esenciales	
Tipos de activos: • [AUX] equipamiento auxiliar	**Dimensiones:** 1. [D] disponibilidad
Descripción: otros servicios o recursos de los que depende la operación de los equipos; por ejemplo, papel para las impresoras, toner, refrigerante, ... Origen: Entorno (accidental) Humano (accidental o deliberado)	

Tabla 22. Interrupción de otros servicios

[I.10] Degradación de los soportes de almacenamiento de información

[I.10] Degradación de los soportes de almacenamiento de información	
Tipos de activos: • [Media] soportes de información	**Dimensiones:** 1. [D] disponibilidad

Descripción: como consecuencia del paso del tiempo Origen: Entorno (accidental) Humano (accidental o deliberado)

Tabla 23. Degradación de los soportes

- **[E] Errores y fallos no intencionados**

Fallos no intencionales causados por las personas. La numeración no es consecutiva, sino que está alineada con los ataques deliberados, muchas veces de naturaleza similar a los errores no intencionados, difiriendo únicamente en el propósito del sujeto.

Origen: Humano (accidental)

[E.1] Errores de los usuarios

[E.1] Errores de los usuarios	
Tipos de activos: • [D] datos / información • [keys] claves criptográficas • [S] servicios [SW] aplicaciones (software) • [Media] soportes de información	**Dimensiones:** 1. [I] integridad 2. [C] confidencialidad 3. [D] disponibilidad
Descripción: equivocaciones de las personas cuando usan los servicios, datos, etc.	

Tabla 24. Errores de los usuarios

[E.2] Errores del administrador

[E.2] Errores del administrador	
Tipos de activos: • [D] datos / información • [keys] claves criptográficas • [S] servicios • [SW] aplicaciones (software) • [HW] equipos informáticos (hardware) • [COM] redes de comunicaciones • [Media] soportes de información	**Dimensiones:** 1. [I] integridad 2. [C] confidencialidad 3. [D] disponibilidad

Descripción:
equivocaciones de personas con responsabilidades de instalación y operación

Tabla 25. Errores del administrador

[E.4] Errores de configuración

[E.4] Errores de configuración	
Tipos de activos: • [D.conf] datos de configuración	**Dimensiones:** 1. [I] integridad
Descripción: Introducción de datos de configuración erróneos. Prácticamente todos los activos dependen de su configuración y ésta de la diligencia del administrador: privilegios de acceso, flujos de actividades, registro de actividad, encaminamiento, etc.	

Tabla 26. Errores de configuración

[E.7] Deficiencias de la organización

[E.7] Deficiencias de la organización	
Tipos de activos: • [P] personal	**Dimensiones:** 1. [D] disponibilidad
Descripción: Cuando no está claro quién tiene que hacer exactamente qué y cuándo, incluyendo tomar medidas sobre los activos o informar a la jerarquía de gestión. Acciones descoordinadas, errores por omisión, etc.	

Tabla 27. Deficiencias de la organización

[E.8] Difusión de software dañino

[E.8] Difusión de software dañino	
Tipos de activos: • [SW] aplicaciones (software)	**Dimensiones:** 1. [I] integridad 2. [C] confidencialidad

	3. [D] disponibilidad
Descripción: propagación inocente de virus, espías (spyware), gusanos, troyanos, bombas lógicas, etc.	

Tabla 28. Difusión de software dañino

[E.15] Alteración accidental de la información

[E.15] Alteración accidental de la información	
Tipos de activos: • [D] datos / información • [keys] claves criptográficas • [S] servicios • [SW] aplicaciones (SW) • [COM] comunicaciones (tránsito) • [Media] soportes de información • [L] instalaciones	**Dimensiones:** 1. [I] integridad
Descripción: Alteración accidental de la información. Esta amenaza sólo se identifica sobre datos en general, pues cuando la información está en algún soporte informático, hay amenazas específicas.	

Tabla 29. Alteración accidental de la información

[E.18] Destrucción de la información

[E.18] Destrucción de la información	
Tipos de activos: • [D] datos / información • [keys] claves criptográficas • [S] servicios • [SW] aplicaciones (SW) • [COM] comunicaciones (tránsito) • [Media] soportes de información • [L] instalaciones	**Dimensiones:** 1. [D] disponibilidad
Descripción:	

Pérdida accidental de información. Esta amenaza sólo se identifica sobre datos en general, pues cuando la información está en algún soporte informático, hay amenazas específicas.

Tabla 30. Destrucción de la información

[E.19] Fuga de información

[E.19] Fuga de información	
Tipos de activos: • [D] datos / información • [keys] claves criptográficas • [S] servicios • [SW] aplicaciones (SW) • [COM] comunicaciones (tránsito) • [Media] soportes de información • [L] instalaciones • [P] personal (revelación)	**Dimensiones:** 1. [C] confidencialidad
Descripción: Revelación por indiscreción. Incontinencia verbal, medios electrónicos, soporte papel, etc.	

Tabla 31. Fuga de información

[E.20] Vulnerabilidades de los programas (Software)

[E.20] Vulnerabilidades de los programas (Software)	
Tipos de activos: • [SW] aplicaciones (SW)	**Dimensiones:** 1. [I] integridad 2. [C] confidencialidad 3. [D] disponibilidad
Descripción: Defectos en el código que dan pie a una operación defectuosa sin intención por parte del usuario, pero con consecuencias sobre la integridad de los datos o la capacidad misma de operar.	

Tabla 32. Vulnerabilidades de los programas

[E.23] Errores de mantenimiento / Actualización de equipo (hardware)

[E.23] Errores de mantenimiento / Actualización de equipo (hardware)	
Tipos de activos: • [HW] equipos informáticos (hardware) • [Media] soportes electrónicos • [AUX] equipamiento auxiliar	**Dimensiones:** 1. [D] disponibilidad
Descripción: Defectos en los procedimientos o controles de actualización de los equipos que permiten que sigan utilizándose más allá del tiempo nominal de uso.	

Tabla 33. Errores de mantenimiento

[E.24] Caída del sistema por agotamiento de recursos

[E.24] Caída del sistema por agotamiento de recursos	
Tipos de activos: • [S] servicios • [HW] equipos informáticos (hardware) • [COM] redes de comunicaciones	**Dimensiones:** 1. [D] disponibilidad
Descripción: La carencia de recursos suficientes provoca la caída del sistema cuando la carga de trabajo es desmesurada.	

Tabla 34. Caída del sistema

[E.25] Pérdida de equipos

[E.25] Robo	
Tipos de activos: • [HW] equipos informáticos (hardware) • [Media] soportes electrónicos • [AUX] equipamiento auxiliar	**Dimensiones:** 1. [D] disponibilidad 2. [C] confidencialidad
Descripción: La pérdida de equipos provoca directamente la carencia de un medio para prestar los servicios, es decir una indisponibilidad. Se puede perder todo tipo de equipamiento, siendo la pérdida de equipos y soportes de información los	

más habituales. En el caso de equipos que hospedan datos, además se puede sufrir una fuga de información.

Tabla 35. Pérdida de equipos

[E.28] Indisponibilidad del personal

[E.28] Indisponibilidad del personal	
Tipos de activos: • [P] personal interno	**Dimensiones:** 1. [D] disponibilidad
Descripción: Ausencia accidental del puesto de trabajo: enfermedad, alteraciones del orden público, guerra bacteriológica,...	

Tabla 36. Indisponibilidad del personal

- **[A] Ataques intencionados**

Fallos deliberados causados por las personas.

La numeración no es consecutiva para coordinarla con los errores no intencionados, muchas veces de naturaleza similar a los ataques deliberados, difiriendo únicamente en el propósito del sujeto.

Origen:
Humano (deliberado)

[A.4] Manipulación de configuración

[A.4] Manipulación de configuración	
Tipos de activos: • [D.log] registros de actividad	**Dimensiones:** 1. [I] integridad 2. [C] confidencialidad 3. [D] disponibilidad
Descripción: prácticamente todos los activos dependen de su configuración y ésta de la diligencia del administrador: privilegios de acceso, flujos de actividades, registro de actividad, encaminamiento, etc.	

Tabla 37. Manipulación de configuración

[A.5] Suplantación de la identidad del usuario

[A.5] Suplantación de la identidad del usuario	
Tipos de activos: • [D] datos / información • [keys] claves criptográficas • [S] servicios • [SW] aplicaciones (SW) • [COM] comunicaciones (tránsito)	**Dimensiones:** 1. [C] confiabilidad 2. [A] autenticidad 3. [I] integridad
Descripción: Cuando un atacante consigue hacerse pasar por un usuario autorizado, disfruta de los privilegios de este para sus fines propios. Esta amenaza puede ser perpetrada por personal interno, por personas ajenas a la Organización o por personal contratado temporalmente.	

Tabla 38. Suplantación de la identidad

[A.6] Abuso de privilegios de acceso

[A.6] Abuso de privilegios de acceso	
Tipos de activos: • [D] datos / información • [keys] claves criptográficas • [S] servicios • [SW] aplicaciones (SW) • [HW] equipos informáticos (hardware) • [COM] comunicaciones (tránsito)	**Dimensiones:** 1. [C] confiabilidad 2. [D] disponibilidad 3. [I] integridad
Descripción: Cada usuario disfruta de un nivel de privilegios para un determinado propósito; cuando un usuario abusa de su nivel de privilegios para realizar tareas que no son de su competencia, hay problemas.	

Tabla 39. Abuso de privilegios

[A.7] Uso no previsto

[A.7] Uso no previsto	
Tipos de activos: • [S] servicios	**Dimensiones:**

• [SW] aplicaciones (SW) • [HW] equipos informáticos (hardware) • [COM] comunicaciones (tránsito) • [Media] soportes de información • [L] instalaciones	1. [C] confiabilidad 2. [D] disponibilidad 3. [I] integridad
Descripción: utilización de los recursos del sistema para fines no previstos, típicamente de interés personal: juegos, consultas personales en Internet, bases de datos personales, programas personales, almacenamiento de datos personales, etc.	

Tabla 40. Uso no previsto

[A.8] Difusión de software dañino

[A.8] Difusión de software dañino	
Tipos de activos: • [SW] aplicaciones (SW)	**Dimensiones:** 1. [I] integridad 2. [C] confidencialidad 3. [D] disponibilidad
Descripción: propagación intencionada de virus, espías (spyware), gusanos, troyanos, bombas lógicas, etc.	

Tabla 41. Difusión de software dañino

[A.11] Acceso no autorizado

[A.11] Acceso no autorizado	
Tipos de activos: • [D] datos / información • [keys] claves criptográficas • [S] servicios • [SW] aplicaciones (SW) • [HW] equipos informáticos (hardware) • [COM] comunicaciones (tránsito) • [Media] soportes de información • [AUX] equipamiento auxiliar • [L] instalaciones	**Dimensiones:** 1. [C] confidencialidad 2. [I] integridad

Descripción:
El atacante consigue acceder a los recursos del sistema sin tener autorización para ello, típicamente aprovechando un fallo del sistema de identificación y autorización.

Tabla 42. Acceso no autorizado

7.5.5 Criterios de evaluación

Con el fin de medir el nivel de frecuencia de una amenaza en los activos de la organización se hace necesario tener el valor del impacto el cual es el equivalente al daño generado al activo, esto en el caso de que se materialice una amenaza, permitiendo de esta forma determinar el grado de afectación en cada una de las dimensiones de seguridad.

Nomenclatura	**Valor**	**Criterio**	
		Frecuencia	**Rango de Frecuencia**
MF	100	Muy frecuente	A diario
F	10	Frecuente	Mensual
FN	1	Normal	Una vez al año
PF	1/10	Poco frecuente	Cada varios años
MB	1/100	Muy poco frecuente	Siglos

Tabla 43. Probabilidad de ocurrencia

1. Evaluación de las amenazas a los activos

Tipo de Activo	**Nombre de activos**	**Amenazas**	**Frecuencia**	**[D]**	**[C]**	**[I]**	**[A]**	**[T]**
[S] Servicios:	Página Web Externa Soporte Técnico Externo	[E.15]	PF	A	A	A	M	A
	Página Web Interno (Intranet)	[E.24]	PF	A	A	A	A	A
[SW] Software	Sistema de Cable	[E.2]	MF	M	M	M	B	A
	osTicket	[E.1]	MB	M	M	M	M	M

	HESK	[E.1]	MB	M	M	M	M	M
	Softland ERP	[E.1]	MB	M	M	M	M	M
	MS Outlook	[E.1]	MB	M	M	M	M	M
	Fortinet	[E.1]	MB	MA	MA	MA	MA	MA
	FortiClient	[E.1]	MB	MA	M	M	M	M
	Base de datos producción MS SQL SERVER 2014	[A.8]	FN	MA	MA	MA	MA	MA
	Base de datos pruebas y desarrollo MS SQL Server 2014	[E.18]	FN	M	MA	M	M	M
	Cobian Backup	[E.19]	PF	M	M	M	M	M
	Orion	[E.20]	PF	M	M	M	M	M
	Cacti	[E.20]	PF	M	M	M	M	M
	MS Edge	[A.7]	PF	M	M	M	M	M
	Google Chrome	[A.7]	MB	M	M	M	M	M
	Issabel	[E.20]	PF	M	MA	M	M	M
	FOP2	[E.20]	PF	M	A	A	A	A
	Flowdat	[E.20]	PF	MA	MA	MA	MA	MA
	ESET Nod32 AV	[E.23]	FN	A	A	A	A	A
	VMWare vSphere	[E.23]	FN	MA	MA	MA	A	A

	MS Visual Studio 2017	[E.23]	FN	A	A	A	A	A
[HW] Hardware:	Servidores	[E.23]	FN	MA	MA	MA	MA	MA
	Unidades de precisión	[E.23]	FN	MA	MA	MA	MA	MA
	Switch	[I.5]	FN	A	A	A	A	A
	Equipos de la red cableada (router)	[I.5]	FN	MA	A	A	A	A
	Portátiles Dell Inspiron 3583, Dell Inspiron 3501, Lenovo Ideapad S340-15IWL	[A.7]	PF	M	M	M	M	M
	Computadoras Desktop HP core5	[A.7]	PF	M	M	M	M	M
	Firewall. Corta Fuegos	[E.23]	FN	MA	MA	MA	MA	MA
	Servicio de Impresión	[I.5]	MB	M	M	M	M	M
[COM] Comunicaciones	Equipos de Red inalámbricos (Router, Cable Modem)	[A.7]	FN	A	A	A	A	A
[MEDIA] Soportes de Información	NAS Corporativa	[E.15]	PF	A	A	A	A	A
	Duro externo	E.19]	PF	A	A	A	A	A
	UPS	[I.6]	MB	MA	A	A	M	MA

[AUX] Equipamiento Auxiliar:	Planta Eléctrica	[I.9]	MB	A	M	M	M	M

Tabla 44. Amenaza de los activos

7.6 Procesos Claves y sus Incidencias

Con ayuda del análisis de riesgo se pudo determinar cuáles son los procesos claves de la empresa Casavisión, así también se ha podido determinar que incidentes de ciberseguridad han ocurrido en dichos procesos y con qué frecuencia se han presentado. A continuación se enumera los procesos claves de la empresa identificados que tienen mayor impacto para su funcionamiento:

1- Avería y Mantenimiento.
2- Proyecto / ingeniería.
3- Instalación.
4- Soporte TI.
5- Gestión de Cobranza.
6- Venta.

Procesos	**Descripción**	**Activo afectado (AA)**	**Incidentes (Inc)**	**Frecuencia**
Averías y Mantenimiento	Es la resolución de un problema en particular o falla en algún sector para ofrecerle al cliente un servicio de calidad.	AA.1.Servidores.	Inc.1. Saturación de servidores	FN
		AA.2.UPS.	Inc.2. UPS dañada	FN
		A.A.3.Unidades de Precisión.	Inc.3. Unidad de Precisión dañada	FN
		A.A.4.Serivicio de Internet.	Inc.4. Caída del servicio por parte de los proveedores.	PF

Proyecto / Ingeniería	Es el encargado de realización de cartografía, levantamiento local, diseño de red.	A.A.5.Equipos de red (Tap, Mufa, Caja metálica para empalme, etc.)	Inc.5. Falta de equipo.	MB
			Inc.6. Fibra dañada al momento de la instalación.	FN
			Inc.7. Alcaldía no da permiso de cablear	MB
			Inc.8. Nap falladas.	PF
Instalación	Es el conjunto de medios o recursos necesarios para entregar el producto o servicio al cliente.	A.A.6.Equipos de red inalámbricos (Modem, full domus, cable utp)	Inc.9. Falta de equipos.	PF
			Inc.10. Saturación de órdenes de instalación.	F
			Inc.11. Sin acceso al lugar de instalación.	MB
Soporte TI	Se encarga de resolver los problemas técnicos de la empresa y de apoyar a los clientes a través de diferentes canales.	A.A.7.Sistema Issabel (software de código abierto de telefonía IP y comunicaciones unificadas).	Inc.12. Caída del sistema	FN
		A.A.8.FOP2 (permite ver el estado de los anexos de Asterisk, hacer	Inc.13. Caída del sistema	FN

		llamadas, transferirlas, etc.)		
		A.A.9.Flowdat (Software de gestión y monitoreo para redes de internet)	Inc.14. Licencia Vencida.	PF
		A.A.10.3CXPhone (permite hacer llamadas desde Windows, Mac OS, Android y iPhone, a cualquier destino nacional, móviles y llamadas)	Inc.15. Desconfiguración del 3CXPhone	PF
		A.A.11.Sistema de Servicio.	Inc.16. Errores de actualización del sistema.	MF
			Inc.17. Introducción incorrecta de la información solicitada.	FN
			Inc.18. Mala interpretación del Web Service al realizar una activación.	PF

			Inc.19. Proceso incorrecto de activaciones de equipo (Modem o full domus)	PF
		A.A.12.Forticlient (Cliente VPN)	Inc.20. VNP se desconecta por inestabilidad de internet	F
Gestión de Cobranza	Se focaliza en contactar a los clientes morosos por distintos canales (avisos de cobros) para informarles el estado de sus facturas, la obligación de pago y ofrecerles opciones de normalización.	A.A.13.Sistema de facturación.	Inc.21. Errores de actualización del sistema.	MF
		A.A.14.Servicio de impresión.	Inc.22. Falta de tinta.	MB
			Inc.23. Daño de componente de impresora.	MB
Venta	Captar un prospecto o un posible cliente para llevar a cabo una transacción final.	A.A.15.Servicio de impresión	Inc.24. No cuentan con contratos impresos	MB

Tabla 45. Incidencias de procesos

a. Controles de la Norma ISO 27002:2013 orientado a los procesos de la empresa

La identificación de los controles de la norma ISO 27002:2013 que se relacionen con los procesos de la empresa, proviene de la recopilación de información, hallazgo y análisis de la situación actual de la empresa Casavisión correspondiente a los 14 dominios de la norma, de los cuales se tomaron los siguientes para el análisis de incidentes de ciberseguridad los siguientes controles:

- Políticas de Seguridad.
- Aspectos Organizativos de la seguridad de la información.
- Gestión de Activos.
- Seguridad Física y Ambiental.
- Seguridad en las Operaciones.
- Seguridad en las Comunicaciones.
- Adquisición, Desarrollo y Mantenimiento de los Sistemas de Información.
- Gestión de Incidentes en la Seguridad de la Información.
- Aspectos de Seguridad de la Información en la Gestión de la Continuidad del Negocio.

b. Implementación de la norma ISO 27002

Para la implementación de los controles de la norma ISO que se relacionen con los procesos claves de la empresa, se realizó el análisis correspondiente. Para ello se estructura una tabla que nos permita una mayor comprensión de la información. En la cual se establece el dominio aplicado con su respectivo objetivo de control y control, los procesos clave de la empresa, activos afectados (A.A), incidente (Inc.) ocurrido en los activos afectados, la actividad de control del dominio aplicado, el hallazgo encontrado y su recomendación. Se realiza una lista de chequeo que permite analizar de una manera efectiva el cumplimiento de los requisitos que indica el control. Como se observa a continuación:

Dominio: POLITICA DE SEGURIDAD DE LA INFORMACIÓN							
Directrices de la gestión de la seguridad de la información							
Objetivo: Proporcionar orientación y apoyo a la gestión de la información de acuerdo con los requisitos del negocio, las leyes y normas pertinentes.							
Procesos	**A.A**	**Inc.**	**Actividad de control**	**Control**	**Lista de Chequeo**	**Hallazgo**	**Recomendaciones**
• Averías y Mantenimiento • Proyecto / Ingeniería • Instalación • Soporte TI • Gestión de Cobranza • Venta	A.A.1 A.A.2 A.A.3 A.A.4 A.A.5 A.A.6 A.A.7 A.A.8 A.A.9 A.A.10 A.A.11 A.A.12 A.A.13 A.A.14	Inc.1 Inc.2 Inc.3 Inc.4 Inc.5 Inc.6 Inc.7 . . . Inc.25	**Políticas de seguridad de la información.**	Se debe definir un conjunto de políticas para la seguridad de la información, aprobada por la dirección, publicada y comunicada a los empleados y a las partes externas pertinentes	Verificar que para todos los cargos concernientes a Seguridad de la Información, existan roles y responsabilidades.	La empresa Casavisión no cuenta con un documento formal que detalle los roles y responsabilidades, según el organigrama la empresa no cuenta con un departamento de seguridad informática.	Se debe definir en conjunto de las políticas de seguridad de la información de acuerdo a las necesidades identificadas en el análisis de riesgos, aprobada por la dirección, publicada y comunicada a los empleados y partes externas pertinentes.
			Revisión de las políticas para la	Las políticas para la seguridad de la información deben revisarse a intervalos planificados o siempre	Realizar la revisión de las políticas de seguridad de la información para mantener un	La empresa no cuenta con políticas de seguridad de la información.	Una vez definidas las políticas de seguridad, se debe revisar de forma periódica para mantenerlas

	A.A.15		**seguridad de la información.**	que se produzcan cambios significativos, a fin de asegurar que se mantenga su idoneidad, adecuación y eficacia.	seguimiento adecuado de la misma.		actualizadas, o si ocurren cambios significativos, asegurar su conveniencia, adecuación y eficacia continuas.

Tabla 46. Análisis Dominio Política de Seguridad de la Información.

Dominio: ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACION							
Organización Interna							
Objetivo: Establecer un marco de gestión para iniciar y controlar la implementación y operación de la seguridad de la información dentro de la organización.							
Procesos	**A.A**	**Inc.**	**Actividad de control**	**Control**	**Lista de Chequeo**	**Hallazgo**	**Recomendaciones**
• Averías y Mantenimiento • Proyecto / Ingeniería • Instalación • Soporte TI • Gestión de Cobranza • Venta	A.A.1 A.A.2 A.A.3 A.A.4 A.A.5 A.A.6 A.A.7 A.A.8 A.A.9 A.A.10 A.A.11 A.A.12 A.A.13 A.A.14 A.A.15	Inc.1 Inc.2 Inc.3 Inc.4 Inc.5 Inc.6 Inc.7 . . . Inc.25	**Roles y responsabilidades en la seguridad de la información**	Todas las responsabilidades en seguridad de la información deben ser definidas y asignadas.	Revisar en los manuales de políticas y procedimientos que no existan inconsistencia en la asignación de responsabilidades.	No se encontró documento en cuanto a la asignación de roles y funciones. Actualmente no existe personal dedicado a la seguridad de la información.	Se debe mantener una organización de seguridad, donde los roles y responsabilidades estén definidas y asignadas a los participantes en el modelo de seguridad establecido por la Entidad.

Tabla 47. Análisis Dominio Aspectos Organizativos de la Seguridad de la Información.

Dominio: GESTION DE ACTIVOS							
Responsabilidad sobre los Activos							
Objetivo: Identificar los activos de la organización y definir responsabilidades de protección adecuada.							
Procesos	**A.A**	**Inc.**	**Actividad de control**	**Control**	**Lista de Chequeo**	**Hallazgo**	**Recomendaciones**
• Averías y Mantenimiento • Proyecto / Ingeniería • Instalación • Soporte TI • Gestión de Cobranza • Venta	A.A.1 A.A.2 A.A.3 A.A.4 A.A.5 A.A.6 A.A.7 A.A.8 A.A.9 A.A.10 A.A.11 A.A.12 A.A.13 A.A.14 A.A.15	Inc.1 Inc.2 Inc.3 Inc.4 Inc.5 Inc.6 Inc.7 . . . Inc.25	**Inventario de Activos**	Los activos asociados a la información y a los recursos para el tratamiento de la información deben estar claramente identificados y debe elaborarse y mantenerse un inventario.	Verificar la existencia de inventarios de activos de la información.	La empresa no cuenta con una política de inventario donde se pueda verificar los activos que posee la misma.	Casavisión debe mantener un inventario de activos de información. Los responsables de la información deben clasificar la información basados en su valor, sensibilidad y riesgo de pérdida.
			Propiedad de los Activos	Los activos mantenidos en el inventario deben tener un propietario.	Verificar que se cuente con un propietario de inventario de activos.	Al no contar con un inventario de activos en la empresa, no se cuenta de igual manera con un propietario de inventario de activos.	Establecer un propietario que permita a la empresa tener identificado, clasificados y actualizado los activos de la misma.
			Devolución de los Activos	Todos los empleados y terceras partes deben devolver todos los activos de la organización que estén a su poder al finalizar su empleo, contrato o acuerdo.	Los empleados deben de firma un acta de entrega de los equipos asignados.	En la actualidad para un retiro de personal se realiza un acta de entrega de cargo donde se garantiza que los activos que estaban bajo responsabilidad de esta persona, se entreguen en perfecto estado.	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. Debe quedar un acta de dicha devolución, firmada por ambas partes.

Tabla 48. Análisis Dominio Gestión de Activos.

Dominio: SEGURIDAD FISICA Y AMBIENTAL							
Seguridad de los equipos							
Objetivo: Evitar la pérdida, daño, robo o el compromiso de los activos y la interrupción de las operaciones de la organización							
Procesos	**A.A**	**Inc.**	**Actividad de control**	**Control**	**Lista de Chequeo**	**Hallazgo**	**Recomendaciones**
• Averías y Mantenimiento • Proyecto / Ingeniería • Instalación	A.A.2 A.A.5 A.A.6	Inc.2 Inc.3 Inc.5 Inc.6 Inc.8 Inc.9	**Emplazamiento y Protección de equipos**	Los equipos deben situarse o protegerse de forma que se reduzcan los riesgos de las amenazas y los riesgos ambientales así como las oportunidades de que se produzcan accesos no autorizados.	Protección de los equipos.	Actualmente se cumple con la normatividad necesaria para cumplir con la seguridad de los recursos físicos, en caso de temas ambientales, sin embargo en algunas no se cumple con las normativas.	Los recursos informáticos de la Entidad deben estar físicamente protegidos contra amenazas de acceso no autorizado y amenazas ambientales para prevenir exposición, daño o pérdida de los activos e interrupción de las actividades.
					Verificar si existen políticas de seguridad industrial sobre comer, beber y fumar en las instalaciones críticas de la empresa.	No existe política referente al tema.	Establecer políticas de seguridad referente a ingerir alimentos en instalaciones críticas de la empresa para evitar riesgos en daño de equipos.
• Averías y Mantenimiento • Proyecto / Ingeniería • Instalación	A.A.2 A.A.5 A.A.6	Inc.2 Inc.3 Inc.5 Inc.6 Inc.8 Inc.9	**Instalaciones de suministro**	Los equipos deben de estar protegidos contra fallos de alimentación y otras alteraciones causadas por fallos en las instalaciones de suministro.	Verificar políticas de seguridad de la información donde indique los mantenimientos tales como: electricidad, agua o aire acondicionado.	Actualmente no existen políticas de seguridad referente a instalación o mantenimiento de suministro.	La empresa debe asegurar que las labores de mantenimiento de suministros, sean realizadas por personal idóneo y apropiadamente autorizado e identificado; así mismo, se debe llevar control de la programación de los mantenimientos preventivos.

Dominio: SEGURIDAD FISICA Y AMBIENTAL							
Seguridad de los equipos							
Objetivo: Evitar la pérdida, daño, robo o el compromiso de los activos y la interrupción de las operaciones de la organización							
Procesos	**A.A**	**Inc.**	**Actividad de control**	**Control**	**Lista de Chequeo**	**Hallazgo**	**Recomendaciones**
			Seguridad del cableado	El cableado eléctrico y de telecomunicaciones que transmiten datos o sirve de soporte a los servicios de información deben estar protegidos frente a interceptaciones, interferencias o daños.	Verificar que exista la protección adecuada para evitar que el cable sufra algún daño en su operativo o protección alterna.	No se cuenta con una protección o ubicación adecuada del cableado lo que ocasiona que muchas veces sean desconectados por tercera personas. (Ver anexo)	Realizar una correcta organización del cableado para evitar daños o interrupción en el servicio.
• Averías y Mantenimiento • Proyecto / Ingeniería • Instalación	A.A.2 A.A.5 A.A.6	Inc.2 Inc.3 Inc.5 Inc.6 Inc.8 Inc.9	**Mantenimiento de los equipos**	Los equipos deben de recibir un mantenimiento correcto que asegure su disponibilidad y su integridad continuas.	Verificar que tipo de acuerdo hay con los proveedores con respecto a los mantenimientos.	Se realizan mantenimientos a los equipos periódicamente sin embargo eso depende del tipo de equipo y su importancia.	Los medios y equipos donde se almacena, procesa o comunica la información, deben mantenerse con las medidas de protección físicas y lógicas, que permitan su monitoreo y correcto estado de funcionamiento; para ello se debe realizar los mantenimientos preventivos periódicamente.
			Retirada de materiales propiedad de la empresa	Sin autorización previa, los equipos, la información o el software no deben sacarse de las instalaciones.	Verificar que se cuente con políticas que eviten sacar los equipos sin previo aviso o autorización.	No se cuenta con políticas referente al tema.	Establecer políticas que permitan la seguridad de los equipos, información o software de la empresa.

Dominio: SEGURIDAD FISICA Y AMBIENTAL							
Seguridad de los equipos							
Objetivo: Evitar la pérdida, daño, robo o el compromiso de los activos y la interrupción de las operaciones de la organización							
Procesos	**A.A**	**Inc.**	**Actividad de control**	**Control**	**Lista de Chequeo**	**Hallazgo**	**Recomendaciones**
			Seguridad de los equipos fuera de las instalaciones	Deben de aplicarse medidas de seguridad a los equipos situados fuera de las instalaciones de la empresa, teniendo en cuenta los diferentes riesgos que conlleva trabajar fuera de dichas instalaciones.	¿Existen seguros de los equipos al momento de trasladarlo de un lugar a otro?	No se cuenta con ningún seguro de los equipos, al momento de ser trasladados fuera de las instalaciones corre sobre la responsabilidad del empleado.	Los recursos físicos deben velar porque los equipos que se encuentran sujetos a traslados físicos fuera de la empresa, posean pólizas de seguro que cubran los diferentes riesgos que puedan presentar.
• Averías y Mantenimiento • Proyecto / Ingeniería • Instalación	A.A.2 A.A.5 A.A.6	Inc.2 Inc.3 Inc.5 Inc.6 Inc.8 Inc.9	**Reutilización o eliminación segura de equipos**	Todos los soportes de almacenamiento deben ser comprobados para confirmar que todo dato sensible y software bajo licencia se ha eliminado de manera segura, antes deshacerse de ellos.	Verificar que exista procedimiento establecido para la reutilización o eliminación de equipos de manera segura.	No existe un procedimiento ni política de seguridad del mismo, solamente se lleva un registro por parte del área de bodega de los equipos reutilizados y dañados.	El área de Tecnología debe efectuar la reutilización o retirada segura de los dispositivos de almacenamiento que tienen información de la empresa, a través de los mecanismos necesarios en la plataforma tecnológica, ya sea cuando son dados de baja o cambian de usuario.

Tabla 49. Análisis Dominio Seguridad Física y Ambiental.

Dominio: SEGURIDAD DE LAS OPERACIONES							
Registro y Supervisión							
Objetivo: Registrar eventos y generar evidencias							
Procesos	**A.A**	**Inc.**	**Actividad de control**	**Control**	**Lista de Chequeo**	**Hallazgo**	**Recomendaciones**
• Averías y Mantenimiento • Proyecto / Ingeniería • Instalación • Soporte TI • Gestión de Cobranza • Venta	A.A.1 A.A.2 A.A.3 A.A.4 A.A.5 A.A.6 A.A.7 A.A.8 A.A.9 A.A.10 A.A.11 A.A.12 A.A.13 A.A.14 A.A.15	Inc.1 Inc.2 Inc.3 Inc.4 Inc.5 Inc.6 Inc.7 . . . Inc.25	**Registro de Eventos**	Se deben registrar, proteger y revisar periódicamente las actividades de los usuarios, excepciones, fallos y eventos de seguridad de la información.	Verificar que se cuente con un registro de las actividades realizadas en referencia a la seguridad de la información.	No se lleva registro alguno de las actividades de los usuarios, fallos o eventos donde se vea expuesta la seguridad de la información.	La empresa debe de monitorear permanente el uso que dan los usuarios a los recursos de la plataforma tecnológica y los sistemas de información.
			Protección de la información de registro	Los dispositivos de registro y la información del registro deben estar protegidos contra manipulaciones indebidas y accesos no autorizados.	Revisar que se cuente con la protección adecuada ante manipulaciones.	Se cuenta con seguridad necesaria en los sistemas más críticos como el acceso a servidores.	Integrar métodos de protección a los sistemas de la empresa que permita asegurar la información ante cualquier manipulación.

Tabla 50. Análisis Dominio Seguridad de las Operaciones

Dominio: SEGURIDAD DE LAS COMUNICACIONES							
Intercambio de información							
Objetivo: Mantener la seguridad en la información que se transfiere dentro de una organización y con cualquier entidad externa.							
Procesos	**A.A**	**Inc.**	**Actividad de control**	**Control**	**Lista de Chequeo**	**Hallazgo**	**Recomendaciones**
• Averías y Mantenimiento • Proyecto / Ingeniería • Instalación	A.A.1 A.A.2 A.A.3 A.A.4	Inc.1 Inc.2 Inc.3 Inc.4	**Políticas y procedimientos de**	Deben establecer políticas, procedimientos y controles formales que	Verificar si la empresa cuenta con políticas, procedimientos	Actualmente no cuentan con políticas, procedimientos y controles que protejan la información	La empresa debe contar con la protección de la información en el momento de ser transferida o intercambiada con otras

Dominio: SEGURIDAD DE LAS COMUNICACIONES							
Intercambio de información							
Objetivo: Mantener la seguridad en la información que se transfiere dentro de una organización y con cualquier entidad externa.							
Procesos	**A.A**	**Inc.**	**Actividad de control**	**Control**	**Lista de Chequeo**	**Hallazgo**	**Recomendaciones**
• Soporte TI • Gestión de Cobranza • Venta	A.A.5 A.A.6 A.A.7 A.A.8 A.A.9 A.A.10 A.A.11 A.A.12 A.A.13 A.A.14 A.A.15	Inc.5 Inc.6 Inc.7 . . . Inc.25	**intercambio de información.**	protejan el intercambio de información mediante el uso de todo tipo de recursos de comunicación.	y controles referentes al intercambio de información.	en los distintos canales que utiliza la empresa.	entidades u otro destino externo y establecer procedimientos y controles necesarios para el intercambio de información
			Acuerdos de intercambio de información.	Deben establecer acuerdos para el intercambio seguro de la información del negocio y software entre la organización y terceros.	Verificar si se cuenta con políticas que establezcan acuerdos de intercambio de información.	No cuentan con política para realizar intercambios de información. Realizan el intercambio de información sin ninguna medida de seguridad ya sea por correo electrónico, WhatsApp o llamada telefónica.	Deben definir los modelos de Acuerdos de Confidencialidad y/o de Intercambio de Información entre la empresa y terceras partes incluyendo los compromisos adquiridos y las penalidades civiles o penales por el incumplimiento de dichos acuerdos.
			Mensajería electrónica.	La información que sea objeto de mensajería electrónica debe estar adecuadamente protegida.	¿Existen políticas que correspondan a mensajería electrónica?	No se tienen políticas referentes al tema, al usuario únicamente se le indica su correo y contraseña configurada.	Establecer políticas de seguridad de la información en mensajería electrónica que respete los principios de confiabilidad, integridad, disponibilidad y autenticidad.
			Acuerdo de confiabilidad o no revelación	Deben identificarse, documentarse y revisarse regularmente los requisitos de acuerdos de confiabilidad o no revelación.	Verificar que se cuenten con acuerdos de confiabilidad o no revelación de la información.	La empresa no tiene acuerdos establecidos de confiabilidad o no revelación de la información. El usuario no tiene conocimiento de la importancia de la confiabilidad de la	Establecer acuerdos de confiabilidad, dejando explicitas las responsabilidades por la divulgación de información.

Dominio: SEGURIDAD DE LAS COMUNICACIONES							
Intercambio de información							
Objetivo: Mantener la seguridad en la información que se transfiere dentro de una organización y con cualquier entidad externa.							
Procesos	**A.A**	**Inc.**	**Actividad de control**	**Control**	**Lista de Chequeo**	**Hallazgo**	**Recomendaciones**
						información con la que cuenta la empresa.	

Tabla 51. Análisis Dominio Seguridad de las Comunicaciones.

Dominio: ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN							
Requisitos de seguridad en sistemas de información.							
Objetivo: Garantizar que la seguridad de la información sea parte integral de los sistemas de información a través de todo el ciclo de vida. Esto también incluye los requisitos para los sistemas de información que proporcionan los servicios a través de redes públicas.							
Procesos	**A.A**	**Inc.**	**Actividad de control**	**Control**	**Lista de Chequeo**	**Hallazgo**	**Recomendaciones**
• Soporte TI • Gestión de Cobranza	A.A.7 A.A.8 A.A.9 A.A.10 A.A.11 A.A.12 A.A.14	Inc.12 Inc.13 Inc.14 Inc.15 Inc.16 . . . Inc.23	**Análisis de requisitos y especificaciones de seguridad de la información.**	Los requisitos relacionados con la seguridad de la información deben incluirse en los requisitos para los nuevos sistemas de información o mejoras a los sistemas de información existentes.	Detallar si existen políticas de adquisición o desarrollo de SW según las necesidades de la empresa.	De acuerdo a las necesidades de la empresa se especifican requisitos de seguridad en funcionamiento a la seguridad de la información, sin embargo en algunas ocasiones no es de total conocimiento para los diferentes funcionarios.	Establecer requerimientos de seguridad de la información, los cuales deben ser identificados previos al diseño de los sistemas de tecnología de la información.
• Soporte TI • Gestión de Cobranza	A.A.7 A.A.8 A.A.9 A.A.10	Inc.12 Inc.13 Inc.14 Inc.15	**Asegurar los servicios de aplicaciones en redes públicas.**	La información involucrada en aplicaciones que pasan a través de redes públicas debe ser protegida de cualquier	Verificar que las aplicaciones expuesta a redes públicas se cuente con la protección adecuada	La empresa cuenta con seguridad adecuada para evitar revelación y modificación no autorizada.	Asegurar que los sistemas de información o aplicativos informáticos que pasan a través de redes públicas, incluyen controles de seguridad y cumplen con las políticas de seguridad de la

Dominio: ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN							
Requisitos de seguridad en sistemas de información.							
Objetivo: Garantizar que la seguridad de la información sea parte integral de los sistemas de información a través de todo el ciclo de vida. Esto también incluye los requisitos para los sistemas de información que proporcionan los servicios a través de redes públicas.							
Procesos	**A.A**	**Inc.**	**Actividad de control**	**Control**	**Lista de Chequeo**	**Hallazgo**	**Recomendaciones**
	A.A.11 A.A.12 A.A.14	Inc.16 . . . Inc.23		actividad fraudulenta, disputa de contrato, revelación y modificación no autorizados.			información, con el fin de proteger la información de la Entidad de posibles ataques.
			Protección de las transacciones de servicios de aplicaciones.	La información involucrada en las transacciones de servicios de aplicaciones debe ser protegida para prevenir la transmisión incompleta, errores de enrutamiento, alteración no autorizada del mensaje, revelación, duplicación o reproducción de mensaje no autorizado.	Verificar que las transacciones de servicios de aplicaciones se cuenten con la protección adecuada.	Los servicios de aplicaciones con los que cuentan la empresa, presentan debilidad en la protección de la información ya que constantemente se dan errores de enrutamiento, duplicación de información y transmisión incompleta.	Los desarrolladores de las aplicaciones, deben certificar la transmisión de información relacionada con pagos o transacciones en línea a los operadores encargados, por medio de canales seguros.

Tabla 52. Análisis Dominio Adquisición, Desarrollo y Mantenimiento de los Sistemas de Información.

Dominio: GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACION.							
Gestión de incidentes de la seguridad de la información y mejoras.							
Objetivo: Asegurar un enfoque coherente y eficaz para la gestión de incidentes de la seguridad de la información, incluida la comunicación de eventos de seguridad y debilidades.							
Procesos	**A.A**	**Inc.**	**Actividad de control**	**Control**	**Lista de Chequeo**	**Hallazgo**	**Recomendaciones**
• Averías y Mantenimiento • Proyecto / Ingeniería • Instalación • Soporte TI • Gestión de cobranza y ventas	A.A.1 A.A.2 A.A.3 A.A.4 A.A.5 A.A.6 A.A.7 A.A.8 A.A.9 A.A.10 A.A.11 A.A.12 A.A.13 A.A.14 A.A.15	Inc.1 Inc.2 Inc.3 Inc.4 Inc.5 Inc.6 Inc.7 . . . Inc.25	**Responsabilidades y procedimientos**	Se deben establecer responsabilidades y procedimientos de gestión para garantizar una respuesta rápida, efectiva y adecuada de los incidentes de la ciberseguridad de la información.	Documentar, de existir un procedimiento formal en el cual deben estar establecido las responsabilidades ante un incidente de ciberseguridad.	La empresa no cuenta con un documento formal donde establezca las responsabilidades y procedimientos a seguir en cualquiera de los incidentes ocurrido en los procesos clave de la empresa.	Establecer responsabilidades y procedimientos formarles para actuar con rapidez y eficiencia ante cualquier incidente de la seguridad de la información.
					Verificar en los actuales manuales las responsabilidades de los empleados ante un incidente de ciberseguridad.	Si bien existe un manual de funciones en la empresa, no se evidencian autoridades, roles y responsabilidades en materia de ciberseguridad y riesgos relacionados.	Agregar en los actuales manuales los roles y responsabilidades en materia de ciberseguridad.
	A.A.1 A.A.2 A.A.3 A.A.4 A.A.5 A.A.6 A.A.7 A.A.8 A.A.9 A.A.10 A.A.11 A.A.12 A.A.13 A.A.14	Inc.1 Inc.2 Inc.3 Inc.4 Inc.5 Inc.6 Inc.7 . . . Inc.25	**Notificación de los eventos de ciberseguridad.**	Los eventos de ciberseguridad de la información se deben notificar por los canales de gestión adecuados lo antes posible.	Revisar los canales de comunicación establecidos para los incidentes o eventos.	Al momento de que ocurre un incidente por falta de equipo los canales de comunicación utilizados por la empresa son vía telefónica o mensajes (Texto/WhatsApp).	Establecer canales de comunicación de manera formal.
					Verificar que los usuarios estén informados y familiarizados con los mecanismos de notificación.	Los empleados tienen conocimiento sobre los mecanismos de notificación, pero no así de los responsables de atender la incidencia, al no existir un plan con las responsabilidades y	Realizar capacitaciones constantes a los empleados para dar a conocer los mecanismos de notificación a emplear al presentarse un incidente.

Dominio: GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACION.							
Gestión de incidentes de la seguridad de la información y mejoras.							
Objetivo: Asegurar un enfoque coherente y eficaz para la gestión de incidentes de la seguridad de la información, incluida la comunicación de eventos de seguridad y debilidades.							
Procesos	**A.A**	**Inc.**	**Actividad de control**	**Control**	**Lista de Chequeo**	**Hallazgo**	**Recomendaciones**
	A.A.15					procedimientos ante los incidentes.	

Tabla 53. Análisis Dominio Gestión de Incidentes de Seguridad de la Información.

Dominio: GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN.							
Gestión de incidentes de la seguridad de la información y mejoras							
Objetivo: Asegurar un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información, incluida la comunicación de eventos de seguridad y debilidades.							
Procesos	**A.A**	**Inc.**	**Objetivo de Control**	**Control**	**Lista de Chequeo**	**Hallazgo**	**Recomendaciones**
• Averías y Mantenimiento	A.A.1. A.A.2. A.A.3. A.A.4.	Inc.1. Inc.2. Inc.3. Inc.4.	**Notificación de puntos débiles de la seguridad**	Se requiere anotar e informar sobre cualquier debilidad sospechosa en la ciberseguridad de los sistemas o servicios.	Los usuarios deben conocer la exigencia de observar y reportar cualquier debilidad de la información vista o sospechada en los sistemas o servicios.	Conocen que deben informar ante cualquier debilidad encontrada, pero no se les ha informado de manera formal la exigencia de no pasar por alto cualquier sospecha que pueda perjudicar los sistemas o servicios.	Dar a conocer la importancia que tiene un incidente en los activos de la empresa para poder reportar cualquier debilidad observada.
			Valoración de eventos de seguridad de la información y toma de decisiones	Deben ser evaluados los eventos de ciberseguridad y decidir su clasificación como incidentes.	La existencia de un criterio de priorización dependiendo del sistema o servicio afectado.	Realizan estudios de los eventos de ciberseguridad de una manera no ordenada o documentada.	Realizar lista de priorización de los posibles incidentes para actuar de manera correcta al momento que un activo presente un riesgo evitando que causa mayor impacto.
					Verificar que exista el registro de evaluación de incidentes donde se analice los parámetros de calidad	No se cuenta con registro de evaluación de incidentes que permita analizar su resolución y tampoco que los clasifique.	Mantener el registro de los eventos e incidentes de ciberseguridad que permita analizar la clasificación e impacto para la empresa.

Dominio: GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN.							
Gestión de incidentes de la seguridad de la información y mejoras							
Objetivo: Asegurar un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información, incluida la comunicación de eventos de seguridad y debilidades.							
Procesos	**A.A**	**Inc.**	**Objetivo de Control**	**Control**	**Lista de Chequeo**	**Hallazgo**	**Recomendaciones**
					tanto en la resolución como en la clasificación.		
• Averías y Mantenimiento • Averías y Mantenimiento	A.A.1. A.A.2. A.A.3. A.A.4. A.A.1. A.A.2. A.A.3. A.A.4.	Inc.1. Inc.2. Inc.3. Inc.4. Inc.1. Inc.2. Inc.3. Inc.4.	**Respuesta a los incidentes**	Se debería de responder ante los incidentes de ciberseguridad en atención a los procedimientos documentados	La empresa tiene la capacidad para resolver el incidente por sí misma o necesita ayuda de terceros	La empresa resuelve cada incidente en el menor tiempo posible, sin un plan de procedimientos, esto no significa que están actuando de manera correcta, porque con una debida planificación ahorrarían tiempo y recursos en resolverlos.	Realizar un plan de procedimientos a seguir tomando en cuenta la necesidad de ayuda de terceros para los diversos incidentes.
					Sistema de comunicación necesaria entre usuarios y el equipo de gestión de incidencias sobre las actuaciones y situación del proceso de resolución de la incidencia.	La notificación de un incidente se realiza vía telefónica o a través de mensaje.	Establecer un sistema de comunicación confiable para la gestión de incidentes.
					Registro de acciones llevadas a cabo y los resultados de las mismas.	El responsable del área cuenta con una bitácora donde se debe realizar el registro de los incidentes sin embargo hay registro solamente a partir del 2021 a la fecha.	El responsable de seguridad debe integrar los eventos e incidentes a la matriz de riesgos.

Dominio: GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN.							
Gestión de incidentes de la seguridad de la información y mejoras							
Objetivo: Asegurar un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información, incluida la comunicación de eventos de seguridad y debilidades.							
Procesos	**A.A**	**Inc.**	**Objetivo de Control**	**Control**	**Lista de Chequeo**	**Hallazgo**	**Recomendaciones**
					Deberá existir un análisis que determine la causa de cada incidente.	Se realiza análisis momentáneo de la causa que dio origen al incidente, plasma la causa y solución de la falla.	Realizar un análisis, documentar y dar seguimientos a los incidentes ocurridos.
• Averías y Mantenimiento	A.A.1. A.A.2. A.A.3. A.A.4.	Inc.1. Inc.2. Inc.3. Inc.4.	**Aprendizaje de los incidentes de ciberseguridad**	Deberán utilizar el conocimiento obtenido del análisis y resolución de incidentes de ciberseguridad para reducir la probabilidad y/o impacto de incidentes futuros.	Verificar que exista documentación de registro de ciberseguridad con su respectivo informe. El informe debería incluir: • Detalle del incidente • En que afecto el incidente, cual fue el impacto que causo. • Como resolvieron el incidente.	Existe la idea de realizar un listado de los posibles riesgos que se pueden presentar en la empresa, pero no ha sido plasmado.	Realizar un informe detallado de los incidentes ocurrido que permita el análisis correcto para determinar la posible existencia de nuevos incidentes de ciberseguridad.
					Después del incidente, se realiza alguna evaluación para identificar incidentes de ciberseguridad y poder neutralizarlos antes que ocurran.	Los distintos incidentes de ciberseguridad ocurridos en la empresa no son evaluados de manera organizada o formal, ya que únicamente al momento de ocurrir una falla se centran en poder solucionarla sin tomar en cuenta fallas a futuro.	Evaluar de forma correcta los incidentes de ciberseguridad para lograr neutralizarlos antes de que ocurran.

Dominio: GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN.							
Gestión de incidentes de la seguridad de la información y mejoras							
Objetivo: Asegurar un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información, incluida la comunicación de eventos de seguridad y debilidades.							
Procesos	**A.A**	**Inc.**	**Objetivo de Control**	**Control**	**Lista de Chequeo**	**Hallazgo**	**Recomendaciones**
			Recopilación de evidencias	Deberían definir y aplicar los procedimientos necesarios para la identificación que puede servir de evidencia.	Documentar donde se custodia y trata las evidencias de incidentes de ciberseguridad	Con base al análisis efectuado se puede determinar que el estado actual de la gestión de ciberseguridad es inicial.	Gestionar una adecuada implementación de las salvaguardas de la seguridad de la información sobre los activos más importantes para la entidad.

Tabla 54. Análisis Dominio Gestión de Incidentes de Seguridad de la Información - Proceso Avería y Mantenimiento.

Dominio: GESTIÓN DE INCIDENTES DE LA SEGURIDAD DE LA INFORMACIÓN							
Gestión de incidentes de la seguridad de la información y mejoras							
Objetivo: Asegurar un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información, incluida la comunicación de eventos de seguridad y debilidades.							
Procesos	**A.A**	**Inc.**	**Actividad del Control**	**Control**	**Lista de Chequeo**	**Hallazgo**	**Recomendaciones**
• Proyecto / Ingeniería	A.A.5	Inc.5	**Respuesta a los incidentes**	Se debería de responder ante los incidentes de ciberseguridad en atención a los procedimientos documentados	La empresa tiene la capacidad para resolver el incidente por sí misma o necesita ayuda de terceros	La empresa resuelve cada incidente en el menor tiempo posible, sin un plan de procedimientos, esto no significa que están actuando de manera correcta, porque con una debida planificación ahorrarían tiempo y recursos en resolverlos.	Realizar un plan de procedimientos a seguir tomando en cuenta la necesidad de ayuda de terceros para los diversos incidentes.
					Sistema de comunicación necesaria entre usuarios y el equipo de gestión de incidencias sobre	La notificación de un incidente se realiza vía telefónica o a través de mensaje.	Establecer un sistema de comunicación confiable para la gestión de incidentes.

Dominio: GESTIÓN DE INCIDENTES DE LA SEGURIDAD DE LA INFORMACIÓN							
Gestión de incidentes de la seguridad de la información y mejoras							
Objetivo: Asegurar un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información, incluida la comunicación de eventos de seguridad y debilidades.							
Procesos	**A.A**	**Inc.**	**Actividad del Control**	**Control**	**Lista de Chequeo**	**Hallazgo**	**Recomendaciones**
					las actuaciones y situación del proceso de resolución de la incidencia.		
					Registro de acciones llevadas a cabo y los resultados de las mismas.	No se lleva registro de las acciones que se realizan al momento de un incidente ni de los resultados obtenidos.	El responsable de seguridad debe integrar los eventos e incidentes a la matriz de riesgos.
					Deberá existir un análisis que determine la causa de cada incidente.	Se realiza análisis momentáneo de la causa que dio origen al incidente, pero no se tiene documentado para futuros fallos.	Realizar un análisis, documentar y dar seguimientos a los incidentes ocurridos.
• Proyecto / Ingeniería	A.A.5	Inc.5	**Aprendizaje de los incidentes de ciberseguridad**	Deberán utilizar el conocimiento obtenido del análisis y resolución de incidentes de ciberseguridad para reducir la probabilidad y/o impacto de incidentes futuros.	Verificar que exista documentación de registro de ciberseguridad con su respectivo informe. El informe debería incluir: • Detalle del incidente • En que afecto el incidente, cual fue el impacto que causo.	No se realiza informe que detalle la falta de equipos	Realizar informe de manera formal siguiendo un esquema o prototipo que le permita informar la falta de equipo antes de que ocurra el incidente.

Dominio: GESTIÓN DE INCIDENTES DE LA SEGURIDAD DE LA INFORMACIÓN							
Gestión de incidentes de la seguridad de la información y mejoras							
Objetivo: Asegurar un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información, incluida la comunicación de eventos de seguridad y debilidades.							
Procesos	**A.A**	**Inc.**	**Actividad del Control**	**Control**	**Lista de Chequeo**	**Hallazgo**	**Recomendaciones**
					• Como resolvieron el incidente.		
					Después del incidente, se realiza alguna evaluación para identificar incidentes de ciberseguridad y poder neutralizarlos antes que ocurran.	Los distintos incidentes de ciberseguridad ocurridos en la empresa no son evaluados de manera organizada o formal, ya que únicamente al momento de ocurrir una falla se centran en poder solucionarla sin tomar en cuenta fallas a futuro.	Evaluar de forma correcta los incidentes de ciberseguridad para lograr neutralizarlos antes de que ocurran.
			Recopilación de evidencias	Deberían definir y aplicar los procedimientos necesarios para la identificación que puede servir de evidencia.	Documentar donde se custodia y trata las evidencias de incidentes de ciberseguridad	No se realiza documentación al momento de falta de equipos.	Documentar la falta de equipo como incidente y la causa del mismo para poder identificar el momento oportuno de actuar antes que ocurra el incidente.
• Proyecto / Ingeniería	A.A.5	Inc.6	**Valoración de eventos de seguridad de la información y toma de decisiones**	Deben ser evaluados los eventos de ciberseguridad y decidir su clasificación como incidentes.	La existencia de un criterio de priorización dependiendo del sistema o servicio afectado.	Se evalúa la posibilidad de ocurrir nuevamente dicho incidente por esta razón se cuenta con una reserva de fibra en cada sector.	Realizar lista de priorización para seguir implementando acciones adecuadas ante cualquier incidente.
					Verificar que exista el registro de evaluación de incidentes donde se analice los parámetros de	Se realiza un informe de medición de la fibra quebrada y los metros obtenidos de la reserva.	Continuar con la realización del informe al momento de presentar el incidente como soporte y evidencia del análisis realizado.

Dominio: GESTIÓN DE INCIDENTES DE LA SEGURIDAD DE LA INFORMACIÓN							
Gestión de incidentes de la seguridad de la información y mejoras							
Objetivo: Asegurar un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información, incluida la comunicación de eventos de seguridad y debilidades.							
Procesos	**A.A**	**Inc.**	**Actividad del Control**	**Control**	**Lista de Chequeo**	**Hallazgo**	**Recomendaciones**
					calidad tanto en la resolución como en la clasificación.		
• Proyecto / Ingeniería	A.A.5	Inc.6	**Respuesta a los incidentes**	Se debería de responder ante los incidentes de ciberseguridad en atención a los procedimientos documentados	La empresa tiene la capacidad para resolver el incidente por sí misma o necesita ayuda de terceros	La empresa tiene la capacidad de afrentar por sí misma ya que cuenta con un plan establecido ante este tipo de incidente.	Realizar un plan de procedimientos a seguir tomando en cuenta la necesidad de ayuda de terceros para los diversos incidentes.
					Registro de acciones llevadas a cabo y los resultados de las mismas.	Se lleva registro de la reserva tomada para poder superar dicho incidente.	Continuar realizando el registro de la reserva tomada.
					Deberá existir un análisis que determine la causa de cada incidente.	Se realiza análisis momentáneo de la causa que dio origen al incidente, pero no se tiene documentado para futuros fallos.	Documentar análisis que se realice de la causa que hace posible dicha falla para tratar de evitar que vuelva a ocurrir.
			Aprendizaje de los incidentes de ciberseguridad	Deberán utilizar el conocimiento obtenido del análisis y resolución de incidentes de ciberseguridad para reducir la probabilidad y/o impacto de incidentes futuros.	Verificar que exista documentación de registro de ciberseguridad con su respectivo informe. El informe debería incluir: • Detalle del incidente	No se realiza informe que detalle el incidente, más que el material utilizado y la cantidad para solucionar el incidente.	Realizar mas a detalle un informe que permita identificar la causa y como evitar el incidente.

Dominio: GESTIÓN DE INCIDENTES DE LA SEGURIDAD DE LA INFORMACIÓN							
Gestión de incidentes de la seguridad de la información y mejoras							
Objetivo: Asegurar un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información, incluida la comunicación de eventos de seguridad y debilidades.							
Procesos	**A.A**	**Inc.**	**Actividad del Control**	**Control**	**Lista de Chequeo**	**Hallazgo**	**Recomendaciones**
					• En que afecto el incidente, cual fue el impacto que causo. • Como resolvieron el incidente.		
					Después del incidente, se realiza alguna evaluación para identificar incidentes de ciberseguridad y poder neutralizarlos antes que ocurran.	No se cuenta con un informe formal donde se identifique el incidente ni cómo evitarlo.	Evaluar las causas que ocasionan dicho incidente.
• Proyecto / Ingeniería	A.A.5	Inc.6	**Recopilación de evidencias**	Deberían definir y aplicar los procedimientos necesarios para la identificación que puede servir de evidencia.	Documentar donde se custodia y trata las evidencias de incidentes de ciberseguridad	Solo se presenta un documento donde se especifica la cantidad dañada y reemplazada.	Documentar de manera correcta el incidente ocurrido.
• Proyecto / Ingeniería	A.A.5	Inc.7	**Respuesta a los incidentes**		La empresa tiene la capacidad para resolver el incidente por sí misma o necesita ayuda de terceros	La empresa resuelve cada incidente en el menor tiempo posible, sin un plan de procedimientos, esto no significa que están actuando de manera correcta, porque con una debida planificación	Realizar un plan de procedimientos a seguir tomando en cuenta la necesidad de ayuda de terceros para los diversos incidentes.

Dominio: GESTIÓN DE INCIDENTES DE LA SEGURIDAD DE LA INFORMACIÓN							
Gestión de incidentes de la seguridad de la información y mejoras							
Objetivo: Asegurar un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información, incluida la comunicación de eventos de seguridad y debilidades.							
Procesos	**A.A**	**Inc.**	**Actividad del Control**	**Control**	**Lista de Chequeo**	**Hallazgo**	**Recomendaciones**
						ahorrarían tiempo y recursos en resolverlos.	
				Se debería de responder ante los incidentes de ciberseguridad en atención a los procedimientos documentados	Sistema de comunicación necesaria entre usuarios y el equipo de gestión de incidencias sobre las actuaciones y situación del proceso de resolución de la incidencia.	La notificación de un incidente se realiza vía telefónica o a través de mensaje.	Establecer un sistema de comunicación confiable para la gestión de incidentes.
					Registro de acciones llevadas a cabo y los resultados de las mismas.	No se lleva registro de las acciones que se realizan al momento de un incidente ni de los resultados obtenidos.	El responsable de seguridad debe integrar los eventos e incidentes a la matriz de riesgos.
					Deberá existir un análisis que determine la causa de cada incidente.	Se realiza análisis momentáneo de la causa que dio origen al incidente, pero no se tiene documentado para futuros fallos.	Realizar un análisis, documentar y dar seguimientos a los incidentes ocurridos.
			Aprendizaje de los incidentes de ciberseguridad		Verificar que exista documentación de registro de ciberseguridad con su respectivo informe.	Existe la idea de realizar un listado de los posibles riesgos	Realizar un informe detallado de los incidentes ocurrido que permita el análisis correcto para determinar la posible existencia de nuevos incidentes de ciberseguridad.

Dominio: GESTIÓN DE INCIDENTES DE LA SEGURIDAD DE LA INFORMACIÓN							
Gestión de incidentes de la seguridad de la información y mejoras							
Objetivo: Asegurar un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información, incluida la comunicación de eventos de seguridad y debilidades.							
Procesos	**A.A**	**Inc.**	**Actividad del Control**	**Control**	**Lista de Chequeo**	**Hallazgo**	**Recomendaciones**
				Deberán utilizar el conocimiento obtenido del análisis y resolución de incidentes de ciberseguridad para reducir la probabilidad y/o impacto de incidentes futuros.	El informe debería incluir: • Detalle del incidente • En que afecto el incidente, cual fue el impacto que causo. • Como resolvieron el incidente.	que se pueden presentar en la empresa, pero no ha sido plasmado.	
					Después del incidente, se realiza alguna evaluación para identificar incidentes de ciberseguridad y poder neutralizarlos antes que ocurran.	Los distintos incidentes de ciberseguridad ocurridos en la empresa no son evaluados de manera organizada o formal, ya que únicamente al momento de ocurrir una falla se centran en poder solucionarla sin tomar en cuenta fallas a futuro.	Evaluar de forma correcta los incidentes de ciberseguridad para lograr neutralizarlos antes de que ocurran.
• Proyecto / Ingeniería	A.A.5	Inc.8	**Valoración de eventos de seguridad de la información y toma de decisiones**	Deben ser evaluados los eventos de ciberseguridad y decidir su clasificación como incidentes.	Verificar que exista el registro de evaluación de incidentes donde se analice los parámetros de calidad tanto en la resolución como en la clasificación.	Se realiza un informe de la Nap afectada, si dicho incidente es en todo el equipo o bien en algún componente del mismo.	Realizar un informe detallado de la causa del incidente.

Dominio: GESTIÓN DE INCIDENTES DE LA SEGURIDAD DE LA INFORMACIÓN							
Gestión de incidentes de la seguridad de la información y mejoras							
Objetivo: Asegurar un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información, incluida la comunicación de eventos de seguridad y debilidades.							
Procesos	**A.A**	**Inc.**	**Actividad del Control**	**Control**	**Lista de Chequeo**	**Hallazgo**	**Recomendaciones**
			Recopilación de evidencias	Deberían definir y aplicar los procedimientos necesarios para la identificación que puede servir de evidencia.	Documentar donde se custodia y trata las evidencias de incidentes de ciberseguridad	Se realiza un reporte de la Nap, la potencia que tiene, y cada una de sus salidas.	Documentar el incidente y posibles causas que pueden ocasionarlo.

Tabla 55. Análisis Dominio Gestión de Incidentes de la Seguridad de la Información - Procesos Proyecto / Ingeniería

Dominio: GESTIÓN DE INCIDENTES DE LA CIBERSEGURIDAD DE LA INFORMACIÓN							
Gestión de incidentes de la seguridad de la información y mejoras							
Objetivo: Asegurar un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información, incluida la comunicación de eventos de seguridad y debilidades.							
Procesos	**A.A**	**Inc.**	**Actividad del Control**	**Control**	**Lista de Chequeo**	**Hallazgo**	**Recomendaciones**
• Instalación	A.A.6	Inc.9	**Valoración de eventos de seguridad de la información y toma de decisiones**	Deben ser evaluados los eventos de ciberseguridad y decidir su clasificación como incidentes.	La existencia de un criterio de priorización dependiendo del sistema o servicio afectado.	Se realiza la notificación de forma verbal al gerente cuando ya quedan pocos equipos.	Realizar lista de priorización de los posibles incidentes para actuar de manera correcta al momento que un activo presente un riesgo evitando que causa mayor impacto.
					Verificar que exista el registro de evaluación de incidentes donde se analice los parámetros de calidad tanto en la resolución como en la clasificación.	No se realiza ninguna evaluación para este incidente.	Mantener el registro de los eventos e incidentes de ciberseguridad que permita analizar la clasificación e impacto para la empresa.

Dominio: GESTIÓN DE INCIDENTES DE LA CIBERSEGURIDAD DE LA INFORMACIÓN							
Gestión de incidentes de la seguridad de la información y mejoras							
Objetivo: Asegurar un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información, incluida la comunicación de eventos de seguridad y debilidades.							
Procesos	**A.A**	**Inc.**	**Actividad del Control**	**Control**	**Lista de Chequeo**	**Hallazgo**	**Recomendaciones**
• Instalación	A.A.6	Inc.9	**Respuesta a los incidentes**	Se debería de responder ante los incidentes de ciberseguridad en atención a los procedimientos documentados	La empresa tiene la capacidad para resolver el incidente por sí misma o necesita ayuda de terceros	La empresa resuelve el incidente sin ayuda de terceros.	Realizar un plan de procedimientos a seguir tomando en cuenta la necesidad de ayuda de terceros para los diversos incidentes.
					Sistema de comunicación necesaria entre usuarios y el equipo de gestión de incidencias sobre las actuaciones y situación del proceso de resolución de la incidencia.	Se notifica de la falta de equipo de forma verbal.	Establecer un sistema de comunicación confiable para la gestión de incidentes.
					Registro de acciones llevadas a cabo y los resultados de las mismas.	No se lleva registro de las acciones que se realizan al momento falta de equipos ni de los resultados obtenidos.	El responsable de seguridad debe integrar los eventos e incidentes a la matriz de riesgos.
			Aprendizaje de los incidentes de ciberseguridad	Deberán utilizar el conocimiento obtenido del análisis y resolución de incidentes de ciberseguridad para reducir la probabilidad	Verificar que exista documentación de registro de ciberseguridad con su respectivo informe. El informe debería incluir:	No se cuenta con documentación, la falta de equipo solo se realiza de forma visual.	Realizar un informe del incidente ocurrido detallando la causa del mismo.

Dominio: GESTIÓN DE INCIDENTES DE LA CIBERSEGURIDAD DE LA INFORMACIÓN							
Gestión de incidentes de la seguridad de la información y mejoras							
Objetivo: Asegurar un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información, incluida la comunicación de eventos de seguridad y debilidades.							
Procesos	**A.A**	**Inc.**	**Actividad del Control**	**Control**	**Lista de Chequeo**	**Hallazgo**	**Recomendaciones**
				y/o impacto de incidentes futuros.	• Detalle del incidente • En que afecto el incidente, cual fue el impacto que causo. • Como resolvieron el incidente.		
					Después del incidente, se realiza alguna evaluación para identificar incidentes de ciberseguridad y poder neutralizarlos antes que ocurran.	Se procura notificar a gerencia la falta de equipo antes de que ocurra dicho incidente.	Evaluar de forma correcta las posibles causas de la falta de equipo para prevenir dicho incidente.
• Instalación	A.A.6	Inc.10	**Valoración de eventos de seguridad de la información y toma de decisiones**	Deben ser evaluados los eventos de ciberseguridad y decidir su clasificación como incidentes.	La existencia de un criterio de priorización dependiendo del sistema o servicio afectado.	Se realiza un criterio de priorización en dependencia a la queja del cliente.	Organizar de manera adecuada la cantidad de órdenes de acuerdo a la fecha generada.
					Verificar que exista el registro de evaluación de incidentes donde se analice los parámetros de calidad tanto en la	El sistema de servicio realiza un reporte que evalúa la priorización de las ordenes no atendidas sin embargo no es utilizado.	Utilizar el informe que realiza el sistema de servicio para poder minimizar el incidente.

Dominio: GESTIÓN DE INCIDENTES DE LA CIBERSEGURIDAD DE LA INFORMACIÓN							
Gestión de incidentes de la seguridad de la información y mejoras							
Objetivo: Asegurar un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información, incluida la comunicación de eventos de seguridad y debilidades.							
Procesos	**A.A**	**Inc.**	**Actividad del Control**	**Control**	**Lista de Chequeo**	**Hallazgo**	**Recomendaciones**
					resolución como en la clasificación.		
• Instalación	A.A.6	Inc.10	**Respuesta a los incidentes**	Se debería de responder ante los incidentes de ciberseguridad en atención a los procedimientos documentados	La empresa tiene la capacidad para resolver el incidente por sí misma o necesita ayuda de terceros	La empresa realiza contratos temporales de técnicos para dar a basto cuando hay saturación de órdenes.	Realizar contratos fijos, permitiendo contar con personal que abarque la demanda de visita técnica.
					Sistema de comunicación necesaria entre usuarios y el equipo de gestión de incidencias sobre las actuaciones y situación del proceso de resolución de la incidencia.	Se notifica al área técnica los clientes que llaman por su orden atrasada y se le da prioridad si la requiere.	Cumplir con el lapso establecido de atención de orden para evitar que ocurrida dicho incidente.
					Registro de acciones llevadas a cabo y los resultados de las mismas.	Se realiza el cierre de las órdenes atendidas.	Atender órdenes en tiempo y forma para evitar tener lapso de tiempo fuera de lo establecido al momento de cerrar las órdenes.
					Deberá existir un análisis que determine la causa de cada incidente.	No se realiza análisis de dicho incidente.	Realizar un análisis que permita determinar la causa de saturación de órdenes para poder implementar acciones correctivas.

Dominio: GESTIÓN DE INCIDENTES DE LA CIBERSEGURIDAD DE LA INFORMACIÓN							
Gestión de incidentes de la seguridad de la información y mejoras							
Objetivo: Asegurar un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información, incluida la comunicación de eventos de seguridad y debilidades.							
Procesos	**A.A**	**Inc.**	**Actividad del Control**	**Control**	**Lista de Chequeo**	**Hallazgo**	**Recomendaciones**
• Instalación	A.A.6	Inc.10	**Aprendizaje de los incidentes de ciberseguridad**	Deberán utilizar el conocimiento obtenido del análisis y resolución de incidentes de ciberseguridad para reducir la probabilidad y/o impacto de incidentes futuros.	Verificar que exista documentación de registro de ciberseguridad con su respectivo informe. El informe debería incluir: • Detalle del incidente • En que afecto el incidente, cual fue el impacto que causo. • Como resolvieron el incidente.	No se realiza documentación para verificar el incidente ocurrido.	Documentar detalladamente el incidente, causas y soluciones para evitar futuras fallas.
			Recopilación de evidencias	Deberían definir y aplicar los procedimientos necesarios para la identificación que puede servir de evidencia.	Documentar donde se custodia y trata las evidencias de incidentes de ciberseguridad.	No se realiza ninguna documentación que soporte la causa del incidente.	Evaluar de forma correcta los incidentes de ciberseguridad para lograr neutralizarlos antes de que ocurran.
• Instalación	A.A.6	Inc.11	**Notificación de puntos débiles de la seguridad**	Se requiere anotar e informar sobre cualquier debilidad sospechosa en la ciberseguridad de los sistemas o servicios.	Los usuarios deben conocer la exigencia de observar y reportar cualquier debilidad de la información vista o	Se fotografía el sector donde se ve afectado para poderlo reportar al área técnica.	Informar al cliente de la falla para aclarar a que se debe la demora de atender alguna falla.

Dominio: GESTIÓN DE INCIDENTES DE LA CIBERSEGURIDAD DE LA INFORMACIÓN							
Gestión de incidentes de la seguridad de la información y mejoras							
Objetivo: Asegurar un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información, incluida la comunicación de eventos de seguridad y debilidades.							
Procesos	**A.A**	**Inc.**	**Actividad del Control**	**Control**	**Lista de Chequeo**	**Hallazgo**	**Recomendaciones**
					sospechada en los sistemas o servicios.		
			Respuesta a los incidentes		Registro de acciones llevadas a cabo y los resultados de las mismas.	Se informa al cliente afectado y se deja observación en sistema de incidente.	Informar al cliente del incidente para poder acordar la fecha en que se pueda visitar.
			Recopilación de evidencias	Deberían definir y aplicar los procedimientos necesarios para la identificación que puede servir de evidencia.	Documentar donde se custodia y trata las evidencias de incidentes de ciberseguridad	No se realiza documentación, sin embargo, se realiza fotográfica a manera de evidencia.	Gestionar una adecuada implementación de las salvaguardas de la seguridad de la información sobre los activos más importantes para la entidad.

Tabla 56. Análisis Dominio Gestión de Incidentes de la Seguridad de la Información - Proceso Instalación.

Dominio: GESTIÓN DE INCIDENTES DE LA SEGURIDAD DE LA INFORMACIÓN							
Gestión de incidentes de la seguridad de la información y mejoras							
Objetivo: Asegurar un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información, incluida la comunicación de eventos de seguridad y debilidades.							
Procesos	**A.A**	**Inc.**	**Actividad del Control**	**Control**	**Lista de Chequeo**	**Hallazgo**	**Recomendaciones**
• Soporte TI	A.A.7 A.A.8	Inc.12 Inc.13	**Notificación de puntos débiles de la seguridad**	Se requiere anotar e informar sobre cualquier debilidad sospechosa en la ciberseguridad de los sistemas o servicios.	Los usuarios deben conocer la exigencia de observar y reportar cualquier debilidad de la información vista o	El área correspondiente que utiliza dicho sistema conoce la importancia de reportar cualquier debilidad observada en el sistema.	Realizar capacitaciones constantes para informar de cualquier debilidad observada.

Dominio: GESTIÓN DE INCIDENTES DE LA SEGURIDAD DE LA INFORMACIÓN							
Gestión de incidentes de la seguridad de la información y mejoras							
Objetivo: Asegurar un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información, incluida la comunicación de eventos de seguridad y debilidades.							
Procesos	**A.A**	**Inc.**	**Actividad del Control**	**Control**	**Lista de Chequeo**	**Hallazgo**	**Recomendaciones**
					sospechada en los sistemas o servicios.		
			Valoración de eventos de seguridad de la información y toma de decisiones	Deben ser evaluados los eventos de ciberseguridad y decidir su clasificación como incidentes.	La existencia de un criterio de priorización dependiendo del sistema o servicio afectado.	Se realiza un criterio de priorización ya que es el sistema que permite recibir llamadas de los clientes.	Utilizar el sistema de Ticket para dar prioridad a los incidentes con forme a su importancia e impacto.
					Verificar que exista el registro de evaluación de incidentes donde se analice los parámetros de calidad tanto en la resolución como en la clasificación.	Se realiza una evaluación momentánea del incidente, pero hay registro del mismo.	Realizar el registro de los incidentes y sus soluciones en el sistema de ticket existente.
• Soporte TI	A.A.7 A.A.8	Inc.12 Inc.13	**Respuesta a los incidentes**	Se debería de responder ante los incidentes de ciberseguridad en atención a los procedimientos documentados	La empresa tiene la capacidad para resolver el incidente por sí misma o necesita ayuda de terceros	La empresa resuelve cada incidente en el menor tiempo posible.	Realizar un plan de procedimientos a seguir tomando en cuenta la necesidad de ayuda de terceros para los diversos incidentes.
					Sistema de comunicación necesaria entre usuarios y el equipo de gestión de	La notificación de un incidente se realiza vía telefónica o a través de mensaje.	Establecer un sistema de comunicación confiable para la gestión de incidentes.

Dominio: GESTIÓN DE INCIDENTES DE LA SEGURIDAD DE LA INFORMACIÓN							
Gestión de incidentes de la seguridad de la información y mejoras							
Objetivo: Asegurar un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información, incluida la comunicación de eventos de seguridad y debilidades.							
Procesos	**A.A**	**Inc.**	**Actividad del Control**	**Control**	**Lista de Chequeo**	**Hallazgo**	**Recomendaciones**
					incidencias sobre las actuaciones y situación del proceso de resolución de la incidencia.		
					Registro de acciones llevadas a cabo y los resultados de las mismas.	No se lleva registro de las acciones que se realizan al momento de un incidente ni de los resultados obtenidos.	Utilizar el sistema establecido para llevar el registro de los incidentes ocurridos.
					Deberá existir un análisis que determine la causa de cada incidente.	Se realiza análisis momentáneo de la causa que dio origen al incidente, pero no se tiene documentado para futuros fallos.	Realizar un análisis, documentar y dar seguimientos a los incidentes ocurridos.
• Soporte TI	A.A.7 A.A.8	Inc.12 Inc.13	**Aprendizaje de los incidentes de ciberseguridad**	Deberán utilizar el conocimiento obtenido del análisis y resolución de incidentes de ciberseguridad para reducir la probabilidad y/o impacto de incidentes futuros.	Verificar que exista documentación de registro de ciberseguridad con su respectivo informe. El informe debería incluir: • Detalle del incidente • En que afecto el incidente, cual	Se cuenta con un sistema de ticket para reportar y documentar dicho incidente, pero no se utiliza al momento del incidente.	Realizar un informe detallado con los incidentes reportados a través del sistema de ticket.

Dominio: GESTIÓN DE INCIDENTES DE LA SEGURIDAD DE LA INFORMACIÓN							
Gestión de incidentes de la seguridad de la información y mejoras							
Objetivo: Asegurar un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información, incluida la comunicación de eventos de seguridad y debilidades.							
Procesos	**A.A**	**Inc.**	**Actividad del Control**	**Control**	**Lista de Chequeo**	**Hallazgo**	**Recomendaciones**
					fue el impacto que causo. • Como resolvieron el incidente.		
					Después del incidente, se realiza alguna evaluación para identificar incidentes de ciberseguridad y poder neutralizarlos antes que ocurran.	Se realiza una evaluación momentánea de lo que pudo ocasionar el incidente.	Evaluar de forma correcta los incidentes de ciberseguridad para lograr neutralizarlos antes de que ocurran.
			Recopilación de evidencias	Deberían definir y aplicar los procedimientos necesarios para la identificación que puede servir de evidencia.	Documentar donde se custodia y trata las evidencias de incidentes de ciberseguridad	No se documenta ni se evidencia este tipo de incidente.	Gestionar una adecuada implementación de las salvaguardas de la seguridad de la información sobre los activos más importantes para la entidad.
• Soporte TI	A.A.9	Ind.14	**Notificación de puntos débiles de la seguridad**	Se requiere anotar e informar sobre cualquier debilidad sospechosa en la ciberseguridad de los sistemas o servicios.	Los usuarios deben conocer la exigencia de observar y reportar cualquier debilidad de la información vista o sospechada en los sistemas o servicios.	El área correspondiente que utiliza dicho sistema conoce la importancia de reportar cualquier debilidad observada en el sistema.	Realizar capacitaciones constantes para informar de cualquier debilidad observada.

Dominio: GESTIÓN DE INCIDENTES DE LA SEGURIDAD DE LA INFORMACIÓN							
Gestión de incidentes de la seguridad de la información y mejoras							
Objetivo: Asegurar un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información, incluida la comunicación de eventos de seguridad y debilidades.							
Procesos	**A.A**	**Inc.**	**Actividad del Control**	**Control**	**Lista de Chequeo**	**Hallazgo**	**Recomendaciones**
			Valoración de eventos de seguridad de la información y toma de decisiones	Deben ser evaluados los eventos de ciberseguridad y decidir su clasificación como incidentes.	La existencia de un criterio de priorización dependiendo del sistema o servicio afectado.	Se realiza un criterio de priorización ya que es el sistema que permite ingresar clientes nuevos y brindarles el servicio.	Establecer otras alternativas de comunicación con el proveer del sistema.
					Verificar que exista el registro de evaluación de incidentes donde se analice los parámetros de calidad tanto en la resolución como en la clasificación.	Se realiza una evaluación momentánea del incidente, pero hay registro del mismo.	Realizar un registro de los incidentes y su respectiva evaluación.
• Soporte TI	A.A.9	Ind.14	**Respuesta a los incidentes**	Se debería de responder ante los incidentes de ciberseguridad en atención a los procedimientos documentados	La empresa tiene la capacidad para resolver el incidente por sí misma o necesita ayuda de terceros	Se contacta al proveedor del sistema para poder indicar el incidente.	Informar a los usuarios de dicho sistema de a quién debe contactar para evitar pérdida de tiempo.
					Sistema de comunicación necesaria entre usuarios y el equipo de gestión de incidencias sobre las actuaciones y situación del	La notificación de un incidente se realiza vía telefónica o a través de mensaje.	Establecer un sistema de comunicación confiable para la gestión de incidentes.

Dominio: GESTIÓN DE INCIDENTES DE LA SEGURIDAD DE LA INFORMACIÓN							
Gestión de incidentes de la seguridad de la información y mejoras							
Objetivo: Asegurar un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información, incluida la comunicación de eventos de seguridad y debilidades.							
Procesos	**A.A**	**Inc.**	**Actividad del Control**	**Control**	**Lista de Chequeo**	**Hallazgo**	**Recomendaciones**
					proceso de resolución de la incidencia.		
					Registro de acciones llevadas a cabo y los resultados de las mismas.	No se lleva registro de las acciones que se realizan al momento de un incidente ni de los resultados obtenidos.	Utilizar el sistema establecido para llevar el registro de los incidentes ocurridos.
					Deberá existir un análisis que determine la causa de cada incidente.	Se realiza análisis momentáneo de la causa que dio origen al incidente, pero no se tiene documentado para futuros fallos.	Realizar un análisis, documentar y dar seguimientos a los incidentes ocurridos.
• Soporte TI	A.A.9	Ind.14	**Aprendizaje de los incidentes de ciberseguridad**	Deberán utilizar el conocimiento obtenido del análisis y resolución de incidentes de ciberseguridad para reducir la probabilidad y/o impacto de incidentes futuros.	Verificar que exista documentación de registro de ciberseguridad con su respectivo informe. El informe debería incluir: • Detalle del incidente • En que afecto el incidente, cual fue el impacto que causo.	No se cuenta con informe que detalle dicho incidente.	Documentar cada incidente ocurrido en el sistema para contar con soporte para posibles fallas futuras.

Dominio: GESTIÓN DE INCIDENTES DE LA SEGURIDAD DE LA INFORMACIÓN							
Gestión de incidentes de la seguridad de la información y mejoras							
Objetivo: Asegurar un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información, incluida la comunicación de eventos de seguridad y debilidades.							
Procesos	**A.A**	**Inc.**	**Actividad del Control**	**Control**	**Lista de Chequeo**	**Hallazgo**	**Recomendaciones**
					• Como resolvieron el incidente.		
					Después del incidente, se realiza alguna evaluación para identificar incidentes de ciberseguridad y poder neutralizarlos antes que ocurran.	Se realiza una evaluación momentánea de lo que pudo ocasionar el incidente.	Evaluar de forma correcta los incidentes de ciberseguridad para lograr neutralizarlos antes de que ocurran.
			Recopilación de evidencias	Deberían definir y aplicar los procedimientos necesarios para la identificación que puede servir de evidencia.	Documentar donde se custodia y trata las evidencias de incidentes de ciberseguridad	No se documenta ni se evidencia este tipo de incidente.	Gestionar una adecuada implementación de las salvaguardas de la seguridad de la información sobre los activos más importantes para la entidad.
• Soporte TI	A.A.10	Ind.15	**Notificación de puntos débiles de la seguridad**	Se requiere anotar e informar sobre cualquier debilidad sospechosa en la ciberseguridad de los sistemas o servicios.	Los usuarios deben conocer la exigencia de observar y reportar cualquier debilidad de la información vista o sospechada en los sistemas o servicios.	El área correspondiente que utiliza dicho sistema conoce la importancia de reportar cualquier debilidad observada en el sistema.	Realizar capacitaciones constantes para informar de cualquier debilidad observada.

Dominio: GESTIÓN DE INCIDENTES DE LA SEGURIDAD DE LA INFORMACIÓN							
Gestión de incidentes de la seguridad de la información y mejoras							
Objetivo: Asegurar un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información, incluida la comunicación de eventos de seguridad y debilidades.							
Procesos	**A.A**	**Inc.**	**Actividad del Control**	**Control**	**Lista de Chequeo**	**Hallazgo**	**Recomendaciones**
			Valoración de eventos de seguridad de la información y toma de decisiones	Deben ser evaluados los eventos de ciberseguridad y decidir su clasificación como incidentes.	La existencia de un criterio de priorización dependiendo del sistema o servicio afectado.	Se realiza un criterio de priorización ya que es el sistema que permite atender las llamadas de clientes, técnicos y sucursales.	Capacitar al personal que utiliza el sistema para que pueda configurar sin ayuda de terceros al momento de presentar el incidente.
					Verificar que exista el registro de evaluación de incidentes donde se analice los parámetros de calidad tanto en la resolución como en la clasificación.	Se realiza una evaluación momentánea del incidente, pero hay registro del mismo.	Realizar un registro de los incidentes y su respectiva evaluación.
• Soporte TI	A.A.10	Ind.15	**Respuesta a los incidentes**	Se debería de responder ante los incidentes de ciberseguridad en atención a los procedimientos documentados	La empresa tiene la capacidad para resolver el incidente por sí misma o necesita ayuda de terceros	Se realiza un ticket para poder configurar el sistema de 3CXPhone y poder nuevamente realizar y recibir llamadas.	Realizar un informe detallado con los incidentes reportados a través del sistema de ticket.
					Sistema de comunicación necesaria entre usuarios y el equipo de gestión de incidencias sobre las actuaciones y situación del	La notificación de un incidente se realiza vía telefónica, a través de mensaje o ticket	Establecer un sistema de comunicación confiable para la gestión de incidentes.

Dominio: GESTIÓN DE INCIDENTES DE LA SEGURIDAD DE LA INFORMACIÓN							
Gestión de incidentes de la seguridad de la información y mejoras							
Objetivo: Asegurar un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información, incluida la comunicación de eventos de seguridad y debilidades.							
Procesos	**A.A**	**Inc.**	**Actividad del Control**	**Control**	**Lista de Chequeo**	**Hallazgo**	**Recomendaciones**
					proceso de resolución de la incidencia.		
					Registro de acciones llevadas a cabo y los resultados de las mismas.	No se lleva registro de las acciones que se realizan al momento de un incidente ni de los resultados obtenidos.	Utilizar el sistema establecido para llevar el registro de los incidentes ocurridos.
					Deberá existir un análisis que determine la causa de cada incidente.	Se realiza análisis momentáneo de la causa que dio origen al incidente, pero no se tiene documentado para futuros fallos.	Realizar un análisis, documentar y dar seguimientos a los incidentes ocurridos.
• Soporte TI	A.A.10	Ind.15	**Aprendizaje de los incidentes de ciberseguridad**	Deberán utilizar el conocimiento obtenido del análisis y resolución de incidentes de ciberseguridad para reducir la probabilidad y/o impacto de incidentes futuros.	Verificar que exista documentación de registro de ciberseguridad con su respectivo informe. El informe debería incluir: • Detalle del incidente • En que afecto el incidente, cual fue el impacto que causo.	Se cuenta con un sistema de ticket para reportar y documentar dicho incidente, pero no se realiza o utiliza al momento del incidente.	Realizar un informe detallado con los incidentes reportados a través del sistema de ticket.

Dominio: GESTIÓN DE INCIDENTES DE LA SEGURIDAD DE LA INFORMACIÓN							
Gestión de incidentes de la seguridad de la información y mejoras							
Objetivo: Asegurar un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información, incluida la comunicación de eventos de seguridad y debilidades.							
Procesos	**A.A**	**Inc.**	**Actividad del Control**	**Control**	**Lista de Chequeo**	**Hallazgo**	**Recomendaciones**
					• Como resolvieron el incidente.		
					Después del incidente, se realiza alguna evaluación para identificar incidentes de ciberseguridad y poder neutralizarlos antes que ocurran.	Se realiza una evaluación momentánea de lo que pudo ocasionar el incidente.	Evaluar de forma correcta los incidentes de ciberseguridad para lograr neutralizarlos antes de que ocurran.
			Recopilación de evidencias	Deberían definir y aplicar los procedimientos necesarios para la identificación que puede servir de evidencia.	Documentar donde se custodia y trata las evidencias de incidentes de ciberseguridad	No se documenta ni se evidencia este tipo de incidente.	Gestionar una adecuada implementación de las salvaguardas de la seguridad de la información sobre los activos más importantes para la entidad.
• Soporte TI	A.A.11 A.A.13	Ind.16 Ind.17 Ind.18 Ind.19 Ind.21	**Notificación de puntos débiles de la seguridad**	Se requiere anotar e informar sobre cualquier debilidad sospechosa en la ciberseguridad de los sistemas o servicios.	Los usuarios deben conocer la exigencia de observar y reportar cualquier debilidad de la información vista o sospechada en los sistemas o servicios.	El área correspondiente que utiliza dicho sistema conoce la importancia de reportar cualquier debilidad observada en el sistema.	Realizar capacitaciones constantes para informar de cualquier debilidad observada.

Dominio: GESTIÓN DE INCIDENTES DE LA SEGURIDAD DE LA INFORMACIÓN							
Gestión de incidentes de la seguridad de la información y mejoras							
Objetivo: Asegurar un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información, incluida la comunicación de eventos de seguridad y debilidades.							
Procesos	**A.A**	**Inc.**	**Actividad del Control**	**Control**	**Lista de Chequeo**	**Hallazgo**	**Recomendaciones**
			Valoración de eventos de seguridad de la información y toma de decisiones	Deben ser evaluados los eventos de ciberseguridad y decidir su clasificación como incidentes.	La existencia de un criterio de priorización dependiendo del sistema o servicio afectado.	Se realiza un criterio de priorización ya que es el sistema que contiene información del cliente, se realizan activaciones de clientes nuevos, reconexiones, suspensiones, averías, mensualidad entre otras.	Utilizar el sistema de Ticket para dar prioridad a los incidentes con forme a su importancia e impacto.
• Soporte TI	A.A.11 A.A.13	Ind.16 Ind.17 Ind.18 Ind.19 Ind.21			Verificar que exista el registro de evaluación de incidentes donde se analice los parámetros de calidad tanto en la resolución como en la clasificación.	Se realiza una evaluación momentánea del incidente, pero hay registro del mismo.	Realizar el registro de los incidentes y sus soluciones en el sistema de ticket existente.
			Respuesta a los incidentes	Se debería de responder ante los incidentes de ciberseguridad en atención a los procedimientos documentados	La empresa tiene la capacidad para resolver el incidente por sí misma o necesita ayuda de terceros	La empresa cuenta con su área de programación encargada de verificar los incidentes en el sistema.	Procurar realizar las correcciones del sistema en el menor tiempo posible.
					Sistema de comunicación necesaria entre usuarios y el equipo de gestión de incidencias sobre	Se realiza un ticket o bien se informa por WhatsApp del incidente ocurrido en el sistema	Utilizar el sistema de ticket de manera correcta para dar prioridad a los incidentes y plasmar su solución.

Dominio: GESTIÓN DE INCIDENTES DE LA SEGURIDAD DE LA INFORMACIÓN							
Gestión de incidentes de la seguridad de la información y mejoras							
Objetivo: Asegurar un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información, incluida la comunicación de eventos de seguridad y debilidades.							
Procesos	**A.A**	**Inc.**	**Actividad del Control**	**Control**	**Lista de Chequeo**	**Hallazgo**	**Recomendaciones**
					las actuaciones y situación del proceso de resolución de la incidencia.		
					Registro de acciones llevadas a cabo y los resultados de las mismas.	No se lleva registro de las acciones que se realizan al momento de un incidente ni de los resultados obtenidos.	Utilizar el sistema establecido para llevar el registro de los incidentes ocurridos.
					Deberá existir un análisis que determine la causa de cada incidente.	Se realiza análisis momentáneo de la causa que dio origen al incidente, pero no se tiene documentado para futuros fallos.	Realizar un análisis, documentar y dar seguimientos a los incidentes ocurridos.
• Soporte TI	A.A.11 A.A.13	Ind.16 Ind.17 Ind.18 Ind.19 Ind.21	**Aprendizaje de los incidentes de ciberseguridad**	Deberán utilizar el conocimiento obtenido del análisis y resolución de incidentes de ciberseguridad para reducir la probabilidad	Verificar que exista documentación de registro de ciberseguridad con su respectivo informe. El informe debería incluir:	Se cuenta con un sistema de ticket para reportar y documentar dicho incidente, pocas veces se utiliza dicho sistema o se da seguimiento de los incidentes notificados por ese medio.	Documentar cada incidente ocurrido en el sistema para contar con soporte para posibles fallas futuras.

Dominio: GESTIÓN DE INCIDENTES DE LA SEGURIDAD DE LA INFORMACIÓN							
Gestión de incidentes de la seguridad de la información y mejoras							
Objetivo: Asegurar un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información, incluida la comunicación de eventos de seguridad y debilidades.							
Procesos	**A.A**	**Inc.**	**Actividad del Control**	**Control**	**Lista de Chequeo**	**Hallazgo**	**Recomendaciones**
• Soporte TI	A.A.11 A.A.13	Ind.16 Ind.17 Ind.18 Ind.19 Ind.21		y/o impacto de incidentes futuros.	• Detalle del incidente • En que afecto el incidente, cual fue el impacto que causo. • Como resolvieron el incidente.		
					Después del incidente, se realiza alguna evaluación para identificar incidentes de ciberseguridad y poder neutralizarlos antes que ocurran.	Se realiza una evaluación momentánea de lo que pudo ocasionar el incidente.	Evaluar de forma correcta los incidentes de ciberseguridad para lograr neutralizarlos antes de que ocurran.
			Recopilación de evidencias	Deberían definir y aplicar los procedimientos necesarios para la identificación que puede servir de evidencia.	Documentar donde se custodia y trata las evidencias de incidentes de ciberseguridad	No se documenta el incidente, sin embargo, se toman evidencia del incidente que ocurre para poder darle solución.	Gestionar una adecuada implementación de las salvaguardas de la seguridad de la información sobre los activos más importantes para la entidad.
• Soporte TI	A.A.12	Ind.20	**Notificación de los eventos de ciberseguridad**	Los eventos de ciberseguridad se deben informar lo más antes posible utilizando los canales de	Revisar los canales de comunicación establecidos para los incidentes o eventos.	Se realiza notificación vía telefónica o WhatsApp.	Establecer canales de comunicación de manera formal.

Dominio: GESTIÓN DE INCIDENTES DE LA SEGURIDAD DE LA INFORMACIÓN							
Gestión de incidentes de la seguridad de la información y mejoras							
Objetivo: Asegurar un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información, incluida la comunicación de eventos de seguridad y debilidades.							
Procesos	**A.A**	**Inc.**	**Actividad del Control**	**Control**	**Lista de Chequeo**	**Hallazgo**	**Recomendaciones**
				administración adecuados.	Verificar que los usuarios estén informados y familiarizados con los mecanismos de notificación.	El área de soporte técnico y atención al cliente conocen el mecanismo de notificación.	Informar del canal de comunicación una vez establecido para ser utilizado de manera correcta.
			Notificación de puntos débiles de la seguridad	Se requiere anotar e informar sobre cualquier debilidad sospechosa en la ciberseguridad de los sistemas o servicios.	Los usuarios deben conocer la exigencia de observar y reportar cualquier debilidad de la información vista o sospechada en los sistemas o servicios.	Al momento de presentar este tipo de incidente se procede a contactar al proveedor del servicio.	Monitorear e informar siempre el consumo del servicio para reportar a tiempo las debilidades observadas.
• Soporte TI	A.A.12	Ind.20	**Recopilación de evidencias**	Deberían definir y aplicar los procedimientos necesarios para la identificación que puede servir de evidencia.	Documentar donde se custodia y trata las evidencias de incidentes de ciberseguridad	No se realiza ninguna documentación más que informar al supervisor del área y de requerir orden de avería en el servicio se evidencia la orden de parte del proveedor.	Contar con una documentación donde se detalle el incidente ocurrido, la falla y solución del mismo.

Tabla 57. Análisis Dominio Gestión de Incidentes de la Seguridad de la Información - Proceso Soporte TI.

Dominio: GESTIÓN DE INCIDENTES DE LA SEGURIDAD DE LA INFORMACIÓN							
Gestión de incidentes de la seguridad de la información y mejoras							
Objetivo: Asegurar un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información, incluida la comunicación de eventos de seguridad y debilidades.							
Procesos	**A.A**	**Inc.**	**Actividad del Control**	**Control**	**Lista de Chequeo**	**Hallazgo**	**Recomendaciones**
• Gestión de cobranza y ventas	A.A.14 A.A.15	Inc.22 Inc.23 Inc.24	**Notificación de los eventos de ciberseguridad**	Los eventos de ciberseguridad se deben informar lo más antes posible utilizando los canales de administración adecuados.	Revisar los canales de comunicación establecidos para los incidentes o eventos.	La comunicación es de forma verbal.	Establecer canales de comunicación de manera formal.
• Gestión de cobranza y ventas	A.A.14 A.A.15	Inc.22 Inc.23 Inc.24			Verificar que los usuarios estén informados y familiarizados con los mecanismos de notificación.	Los encargados están ya familiarizados con el mecanismo de comunicación.	Realizar una notificación del incidente de manera detallada.
			Notificación de puntos débiles de la seguridad	Se requiere anotar e informar sobre cualquier debilidad sospechosa en la ciberseguridad de los sistemas o servicios.	Los usuarios deben conocer la exigencia de observar y reportar cualquier debilidad de la información vista o sospechada en los sistemas o servicios.	Los encargados conocen la importancia de que ocurran estos incidentes. Por esta razón se informa de cualquier anomalía lo antes posible.	Capacitar al personal encargado para que pueda determinar a tiempo las debilidades a ocurrir.
			Recopilación de evidencias	Deberían definir y aplicar los procedimientos necesarios para la identificación que puede servir de evidencia.	Documentar donde se custodia y trata las evidencias de incidentes de ciberseguridad	No se realiza ninguna documentación más que informar al supervisor del área para que se le brinde mantenimiento preventivo a dicho equipo.	Evaluar de forma correcta las posibles causas de la falta de equipo para prevenir dicho incidente.

Tabla 58. Análisis Dominio Gestión de Incidentes de la Seguridad de la Información - Proceso Gestión de cobranza y ventas.

Dominio: ASPECTO DE SEGURIDAD DE LA INFORMACION PARA LA GESTION DE CONTINUIDAD DEL NEGOCIO					
Continuidad de la seguridad de la información.					
Objetivo: La continuidad de la seguridad de la información debe de formar parte de los sistemas de gestión de la continuidad de negocio de la organización.					
Procesos	**Actividad de control**	**Control**	**Lista de Chequeo**	**Hallazgo**	**Recomendaciones**
• Averías y Mantenimiento • Proyecto / Ingeniería • Instalación • Soporte TI • Gestión de Cobranza • Venta	**Planificación de la continuidad de la seguridad de la información.**	La organización debe determinar sus necesidades de seguridad de la información y de continuidad para la gestión de seguridad de la información en situaciones adversas, por ejemplo, durante una crisis o desastre.	Verificar que la empresa cuente con una planificación adecuada para la continuidad de la seguridad de la información.	Casavisión no cuenta con una planificación de continuidad de la seguridad de la información que le permita resguardarla antes situaciones adversas.	Se debe desarrollar, documentar, implementar procedimientos para asegurar una recuperación razonable y a tiempo de la información crítica de la empresa.
	Implementar la continuidad de la seguridad de la información.	La organización debe establecer, documentar, implementar y mantener procesos, y controles para asegurar el nivel requerido de continuidad de la seguridad de la información durante una situación adversa.	Revisar los procesos y controles establecidos por la empresa para la continuidad del negoción.	La empresa no ha implementado o establecido procesos ni controles para la continuidad de la seguridad de la información.	Implementar procesos y controles que permita asegurar el nivel requerido de la continuidad de la seguridad de la información ante situaciones adversas que puedan presentarse.
	Verificación, revisión y evaluación de la continuidad de la seguridad de la información.	La organización debe comprobar los controles establecidos e implementados a intervalos regulares para asegurar que son válidos y eficaces	Revisar continuamente los controles establecidos e implementados para su respectiva validación y eficacia.	No se realizan verificación, ni evaluación de controles para la continuidad de la seguridad de la información.	Se debe asegurar la realización de pruebas periódicas del plan de recuperación ante desastres y/o continuidad de negocio, verificando la seguridad de la información durante su

Dominio: ASPECTO DE SEGURIDAD DE LA INFORMACION PARA LA GESTION DE CONTINUIDAD DEL NEGOCIO					
Continuidad de la seguridad de la información.					
Objetivo: La continuidad de la seguridad de la información debe de formar parte de los sistemas de gestión de la continuidad de negocio de la organización.					
Procesos	**Actividad de control**	**Control**	**Lista de Chequeo**	**Hallazgo**	**Recomendaciones**
		durante situaciones adversas.			realización y la documentación de dichas pruebas.

Tabla 59. Análisis Dominio Aspecto de Seguridad de la Información para la Gestión de Continuidad del Negocio.

Con base al análisis efectuado se puede determinar que el estado actual de la ciberseguridad de la información de la empresa Casavisión es inicial.

Figura 5. Estado de la Seguridad

Fuente: Elaboración propia

8. Conclusiones y recomendaciones

8.1 Conclusiones

Con el análisis de los incidentes de Ciberseguridad realizado en la empresa Casavisión, se pudo determinar que la empresa actualmente no cuenta con un enfoque coherente y eficaz para gestionar los incidentes de ciberseguridad, así como la comunicación de los eventos y sus debilidades.

Se verifica que la empresa realiza un control de incidentes en los procesos claves de una manera no ordenada. Actualmente no cuentan con un canal de comunicación oficial que le permita comunicar a los responsables de los incidentes que ocurren, no tienen documentados políticas de seguridad ni llevan registro de los incidentes que pasan. Al momento que suceden los incidentes únicamente se centran en informarlo y darle solución lo antes posible.

La descripción de los procesos del negocio de la empresa nos permitió conocer y examinar sus procesos claves, de igual manera las incidencias históricas que ocurren en ellos, identificando los controles necesarios que se relacionen con cada proceso según la norma ISO 27002:2013, con el fin de brindar recomendaciones que permitan afrontar los eventos e incidentes de ciberseguridad a dicha empresa.

Por esta razón es importante que la empresa cuente con un área encargada de gestionar la ciberseguridad de la información, así como la gestión de las políticas y documentos, que es una de las funciones que tiene que fortalecer a fin de que los procedimientos existentes sean alineados con un SGSI y las políticas y procedimientos.

8.2 Recomendaciones

- Mantener el registro de los eventos e incidentes de seguridad de la Información.
- El responsable de seguridad debe integrar los eventos e incidentes a la matriz de riesgos.
- Realizar capacitaciones a los funcionarios de la entidad en lo relacionado a eventos e incidentes de seguridad de la información.
- Implementar controles preventivos.
- Hacer una revisión trimestral del proceso de identificación de incidentes con el fin de determinar la posible existencia de nuevos tipos de eventos de seguridad de la información.
- Hacer un seguimiento, monitoreo y una revisión continúa de todo el proceso de gestión del riesgo.
- Destinar los recursos y esfuerzos que sean necesarios para hacer una identificación completa de los activos de la entidad en pro de lograr su adecuada gestión y administración.
- Gestionar una adecuada implementación de las salvaguardas de la seguridad de la información sobre los activos más importantes para la entidad.
- Verificar la correcta implementación y documentación de las buenas prácticas en seguridad para la incorporación de nuevas funcionalidades en las aplicaciones.
- Realizar evaluaciones periódicas de riesgo, usando las metodologías que permitan obtener un mapa de riesgos apropiados para diseñar y controlar los riesgos residuales, y que permita a Casavisión definir su apetito de riesgo de forma efectiva.

- Se recomienda realizar auditorías externas de evaluación y seguimiento, para asegurar el cumplimiento de objetivos y efectividad del SGSI.

9. Bibliografía

Becerra Meza, L., & Weinborn De la Calle, L. (11 de 2005). *https://www.sename.cl/wsename/otros/genero/2_estudio_descriptivo.pdf.* Obtenido de https://www.sename.cl/wsename/otros/genero/2_estudio_descriptivo.pdf

CEUPE. (21 de 01 de 2021). *CEUPE*. Obtenido de https://www.ceupe.com/blog/importancia-de-la-gestion-de-incidentes-en-ti.html

EVALUANDOCLOUD. (19 de 03 de 2020). Obtenido de https://evaluandocloud.com/tipos-incidentes-ciberseguridad/#:~:text=Un%20incidente%20de%20ciberseguridad%20es,la%20seguridad%20de%20la%20informaci%C3%B3n

INCIBE. (21 de 01 de 2021). Obtenido de https://www.incibe-cert.es/sites/default/files/contenidos/guias/doc/incibe-cert_gestion_ciberincidentes_sector_privado.pdf

ISO/IEC 27002. (31 de 07 de 2020). Obtenido de iso27001security.com/html/27002.html

ISO27000.ES. (2013). Obtenido de https://www.iso27000.es/iso27002_16.html

Kingatua, A. (02 de 04 de 2020). *GEEKFLARE.* Obtenido de https://geekflare.com/es/cyber-security-incident-response-management/

lanz, L. (22 de 05 de 2018). *OpenWebinars*. Obtenido de https://openwebinars.net/blog/que-es-la-ciberseguridad/

MAGERIT. (s.f.). Recuperado el 31 de 03 de 2021, de https://pilar.ccn-cert.cni.es/index.php/docman/documentos/2-magerit-v3-libro-ii-catalogo-de-elementos/file

Magerit. (s.f.). *Metodo de analisis de riesgo.*

OPTARIS. (2019). *OPTARIS*. Obtenido de https://www.optaris.com/guia-de-planificacion-de-respuesta-a-incidentes-para-2019/

Ostec. (31 de 07 de 2020). Obtenido de https://ostec.blog/es/generico/iso-27002-buenas-practicas-gsi

Rivas, G. (21 de 05 de 2019). *gb advisors*. Obtenido de https://www.gb-advisors.com/es/gestion-de-incidentes/

Rivas, G. (21 de 05 de 2019). *Gb Advisors*. Obtenido de https://www.gb-advisors.com/es/gestion-de-incidentes/

Sites. (2020). *Sites*. Obtenido de https://sites.google.com/site/introduccionredescomputadoras/5-internet-tecnologia-y-servicios

Sura. (s.f.). Obtenido de https://www.arlsura.com/index.php/326#:~:text=Un%20INCIDENTE%20es%20un%20suceso,al%20proceso%20o%20al%20ambiente.

Técnicas de Auditoria. (08 de 06 de 2008). Obtenido de Técnicas de Auditoria: http://tecnicasdeauditoriainvest.blogspot.com/

TECON. (31 de 07 de 2020). Recuperado el 31 de 07 de 2020, de https://www.tecon.es/la-seguridad-de-la-informacion/#:~:text=Por%20seguridad%20de%20la%20informaci%C3%B3n,se%20utilizan%20en%20una%20organizaci%C3%B3n.

Troncoso Pantoja, C., & Amaya Placencia, A. (2017). Obtenido de http://www.scielo.org.co/pdf/rfmun/v65n2/0120-0011-rfmun-65-02-329.pdf

10. Anexos

Anexo1: Principal medio de comunicación para reportar incidentes.

CASAVISION	Entidad afectada	Es entidad o empresa que ha sido afectada por el problema detectado
	Afectación	El problema que se está presentando o la incidencia en si
	Síntomas	cómo se logró percibir que habia un problema
	Responsable	Persona encargada de solucionar el problema

BITÁCORA DE INCIDENCIAS EN DATA CENTER

Fecha	Hora	Entidad afectada	Afectación	Causa	Persona que detectó
01/07/2021	10:15 AM	Caida total	Afectación todos los enlace de Casavisión	Se estaba realizando un cambio con proveedor y este no logro levantar el enlace provocando caida total del servicio	Jennyfer /Ernesto
02/07/2021	6:00 AM	Caida de algunos servicio	Afectación de energia eléctrica comercial	Circuito de energia daño en calle	Jennyfer
10/07/2021	9:17 AM	Enlace	Afectación por problema energético	Alto voltaje de energia que provocó que ups se pusiera en baipás	Jorge Rodriguez
12/08/2021	12:30 AM	data center	caida total de los servicios	ventana de mantenimiento realizada por los de fibra	Ernesto/Jennyfer
15/10/2021	3:10 PM	Aires data center	filtro de agua de uno de los aires	suciedad en los filtro de agua	Jennyfer López

Anexo2: Bitácora de incidentes de la empresa Casavisión.

```
CASAVISION-C3200-ROCARGO>show docsis downstream channel utilization
Downstream              Total BW    Utilization Online Secondary Channel
Slot/Port/Channel       (Mb/Sec)    Percentage  Modems Modems    Description
-------------------------------------------------------------------------------
0/0/0 (717000000 Hz)    42.9        73          58     156       DELICIAS, RECONCIL #1, RECONCIL #2, MERCEDES
0/0/1 (723000000 Hz)    42.9        71          24     189       DELICIAS, RECONCIL #1, RECONCIL #2, MERCEDES
0/0/2 (729000000 Hz)    42.9        72          23     191       DELICIAS, RECONCIL #1, RECONCIL #2, MERCEDES
0/0/3 (735000000 Hz)    42.9        75          25     189       DELICIAS, RECONCIL #1, RECONCIL #2, MERCEDES
0/1/0 (741000000 Hz)    42.9        71          20     193       DELICIAS, RECONCIL #1, RECONCIL #2, MERCEDES
0/1/1 (747000000 Hz)    42.9        71          26     188       DELICIAS, RECONCIL #1, RECONCIL #2, MERCEDES
0/1/2 (753000000 Hz)    42.9        72          22     191       DELICIAS, RECONCIL #1, RECONCIL #2, MERCEDES
0/1/3 (759000000 Hz)    42.9        71          19     194       DELICIAS, RECONCIL #1, RECONCIL #2, MERCEDES
0/2/0 (717000000 Hz)    42.9        94          56     301       LOMAS GUADALUPE #1, LOMAS GUADALUPE #2, MIRADOR LA SABANA, CDTE.
0/2/1 (723000000 Hz)    42.9        95          53     305       LOMAS GUADALUPE #1, LOMAS GUADALUPE #2, MIRADOR LA SABANA, CDTE.
0/2/2 (729000000 Hz)    42.9        94          45     312       LOMAS GUADALUPE #1, LOMAS GUADALUPE #2, MIRADOR LA SABANA, CDTE.
0/2/3 (735000000 Hz)    42.9        94          40     309       LOMAS GUADALUPE #1, LOMAS GUADALUPE #2, MIRADOR LA SABANA, CDTE.
0/3/0 (741000000 Hz)    42.9        94          34     323       LOMAS GUADALUPE #1, LOMAS GUADALUPE #2, MIRADOR LA SABANA, CDTE.
0/3/1 (747000000 Hz)    42.9        93          35     322       LOMAS GUADALUPE #1, LOMAS GUADALUPE #2, MIRADOR LA SABANA, CDTE.
0/3/2 (753000000 Hz)    42.9        93          44     313       LOMAS GUADALUPE #1, LOMAS GUADALUPE #2, MIRADOR LA SABANA, CDTE.
0/3/3 (759000000 Hz)    42.9        93          44     314       LOMAS GUADALUPE #1, LOMAS GUADALUPE #2, MIRADOR LA SABANA, CDTE.
1/0/0 (717000000 Hz)    42.9        39          106    30        31 DIC, CONCEPCION MARIA, RODEO #1, RODEO #2
1/0/1 (723000000 Hz)    42.9        40          5      139       31 DIC, CONCEPCION MARIA, RODEO #1, RODEO #2
1/0/2 (729000000 Hz)    42.9        41          1      146       31 DIC, CONCEPCION MARIA, RODEO #1, RODEO #2
```

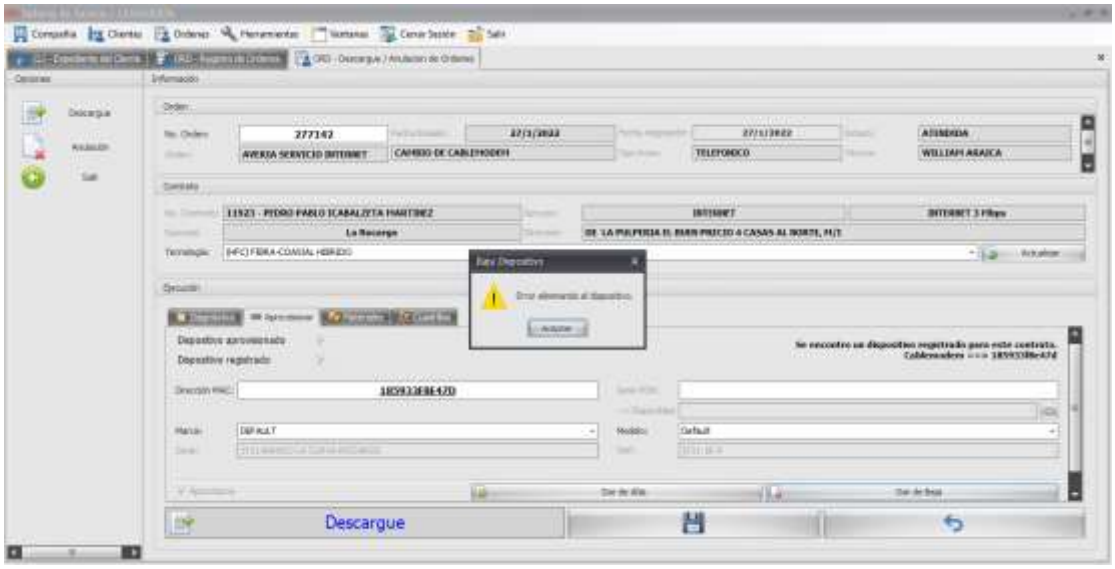
Anexo3: Ejemplo de incidente Ind.1. Saturación de servidores.

Anexo4: Ejemplo de incidente Ind.8. Nap falladas.

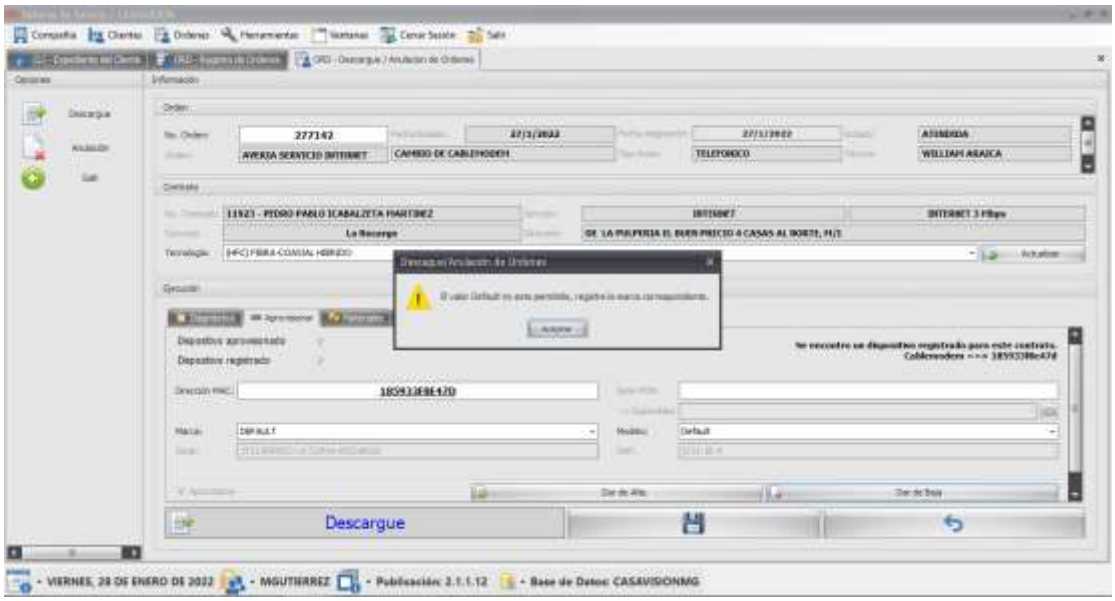
mTiempoEjecucion												
Sucursal / Clase / Tipo Orden	2021-03	2021-04	2021-05	2021-06	2021-07	2021-08	2021-09	2021-10	2021-11	2021-12	2022-01	2022-02
CSandino	8.0	8.2	11.3	6.8	10.8	8.4	12.1	11.8	8.2	9.3	14.4	12.3
AVERIA INTERNET	13.0	9.5	19.6	11.7	12.9	14.4	19.3	17.6	13.7	16.8	24.0	19.4
AVERIA TV	11.1	10.3	11.0	8.9	13.1	12.0	12.0	15.9	12.3	12.4	17.7	17.2
INSTALACION	6.3	7.9	8.6	5.3	11.7	6.9	11.3	9.3	5.6	8.2	10.8	7.4
RECONEXION	7.2	6.9	9.4	4.7	7.7	5.0	9.1	10.5	5.7	6.4	9.7	9.4
Miraflores	14.2	37.3	25.1	19.4	23.5	10.6	13.3	10.2	18.9	19.9	18.8	22.4
AVERIA INTERNET	22.3	23.4	28.1	29.0	31.8	16.6	18.8	14.2	16.2	21.0	18.9	22.0
AVERIA TV	23.9	23.4	24.9	25.5	14.9	10.4	11.8	8.7	11.8	18.8	18.7	17.6
INSTALACION	11.2	41.8	28.0	17.8	25.0	8.8	13.4	10.2	23.3	23.2	20.7	26.7
RECONEXION	18.0	17.1	14.3	13.8	25.6	7.7	11.3	9.5	17.1	15.0	15.2	17.8
Rocargo	21.0	24.4	20.8	24.7	11.3	2.8	3.4	3.7	9.1	16.2	14.8	17.3
AVERIA INTERNET	21.4	26.4	21.1	30.0	11.6	4.4	4.4	3.4	8.9	20.2	15.3	15.8
AVERIA TV	23.1	22.0	18.5	21.9	9.3	3.6	3.3	2.8	9.2	12.9	12.0	12.2
INSTALACION	18.0	23.2	15.3	20.2	8.8	1.8	3.0	3.7	9.9	13.5	15.0	18.1
RECONEXION	23.3	25.2	25.9	27.4	15.0	2.7	3.3	4.0	7.9	19.2	15.7	19.4
Promedio	14.8	24.7	19.1	18.3	13.4	6.0	8.2	8.2	10.7	14.9	15.6	16.8

OT Reales	Horas Meta
563.0	
109.0	24
66.0	24
232.0	72
156.0	48
504.0	
148.0	24
85.0	24
238.0	72
33.0	48
513.0	
4.0	24
12.0	24
17.0	72
480.0	48
1,273.0	

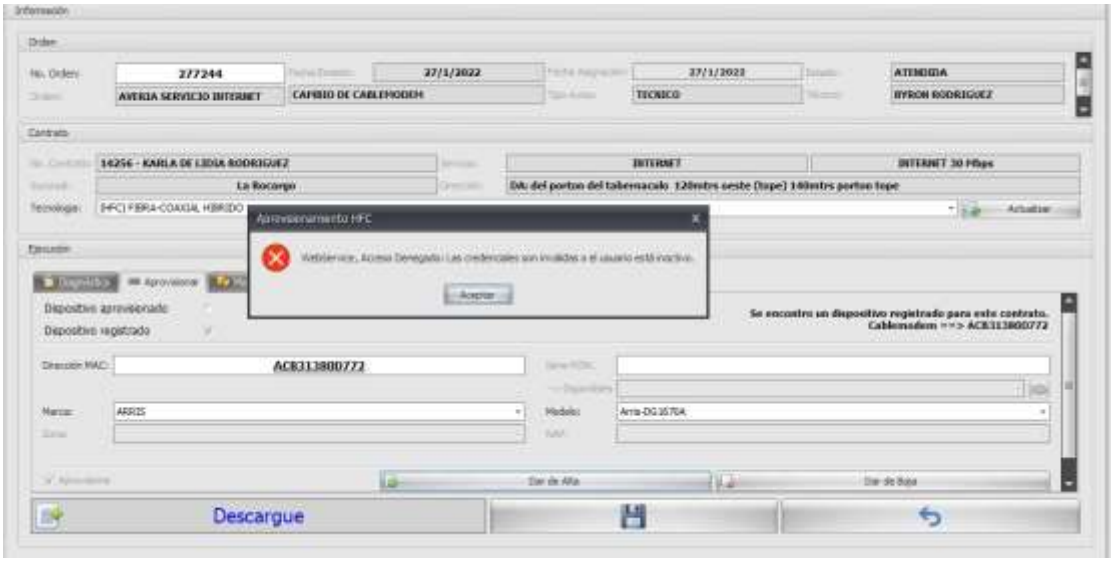
Anexo5: Cuadro de calor – Ejemplo de incidente de Ind.10. Saturación de órdenes de instalación.



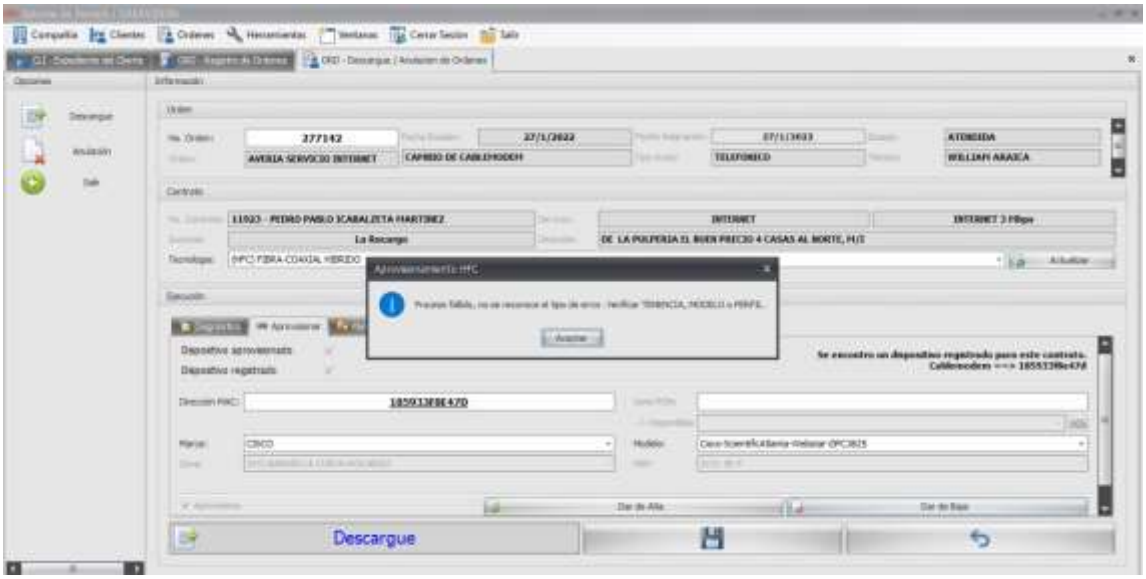
Anexo6: Ejemplo de incidente Ind.17. Introducción incorrecta de la información solicitada.



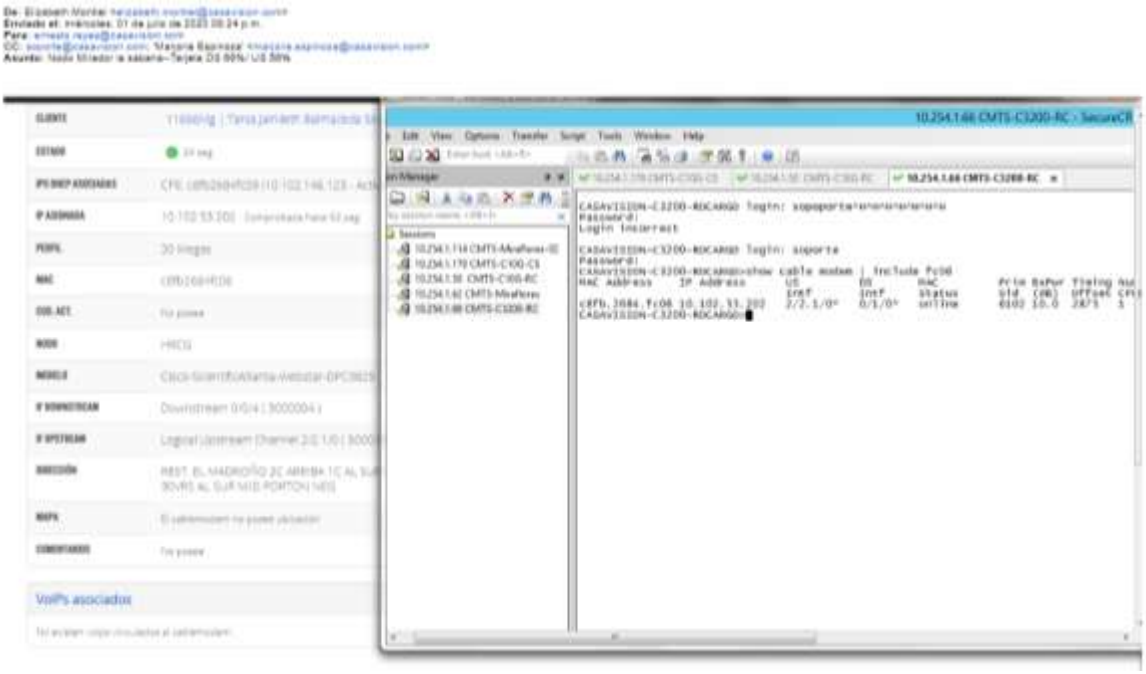
. Anexo7: Ejemplo de incidente Ind.17. Introducción incorrecta de la información solicitada.



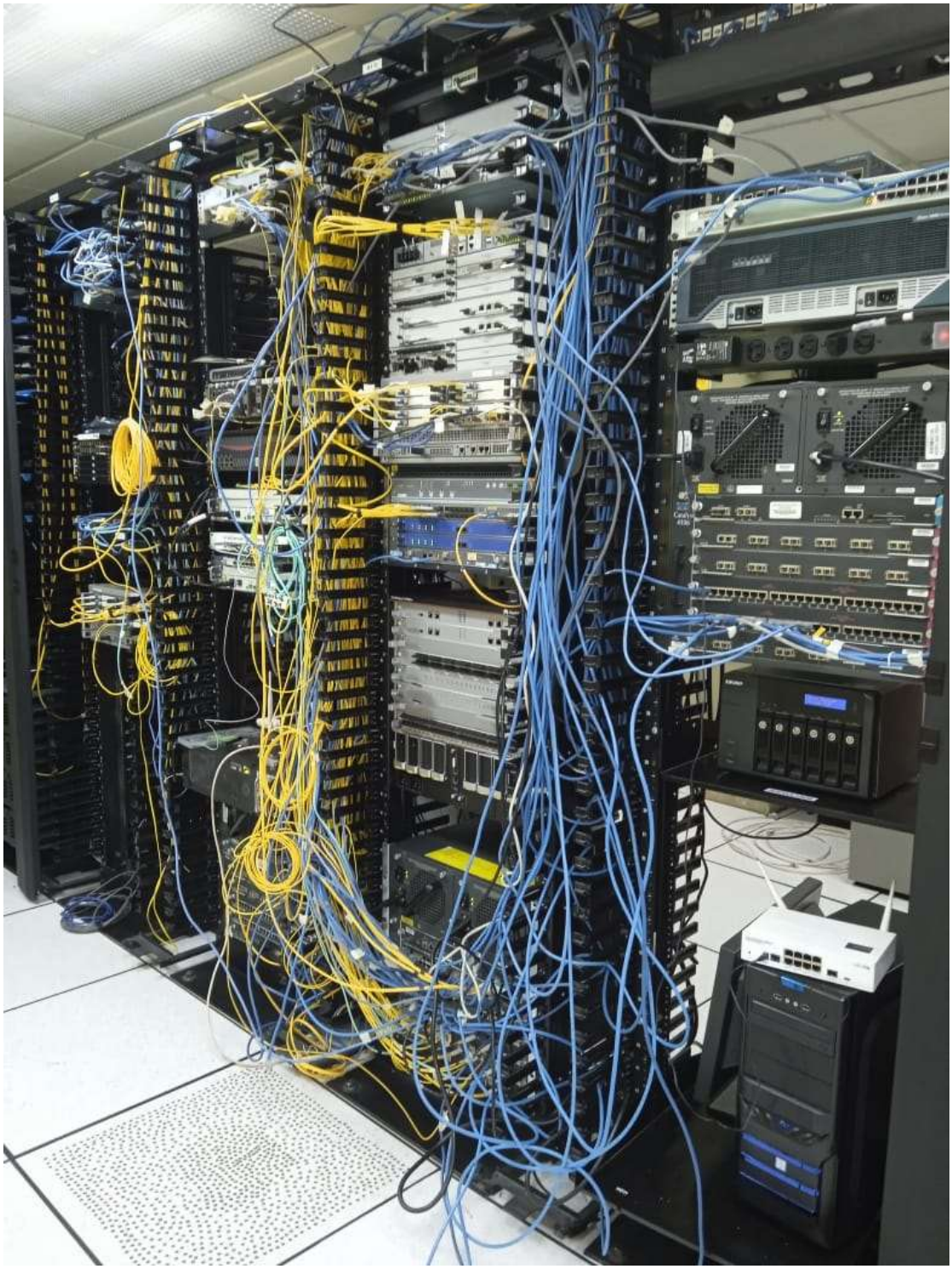
Anexo8: Ejemplo de incidente Ind.18. Mala interpretación del Web Service al realizar una activación.



Anexo9: Ejemplo de incidente Ind.21. Errores de actualización del sistema.



Anexo10: Notificación de saturación de servidor.



Anexo11: Cableado desorganizado.

Características de la entrevista	
Fecha de aplicación	
Tipo de entrevista	Entrevista a profundidad
Enfoque	Sujeto – Objeto

Objetivos	• Identificar los procesos involucrados en los incidentes de ciberseguridad de la empresa Casavisión. • Conocer las expectativas de la gerencia con relación a la gestión de incidentes.
Quien realiza la entrevista	Michell Victoria Gutiérrez Ríos
Nombre Entrevistado	
Edad	
Ocupación	
Nivel de educación	Profesional
Relación con el proyecto	Gerente

Cuestionario Preparado
A. Introducción.
La entrevista está enfocada en obtener la información desde el punto de vista de la gerencia de Casavisión, para ver el enfoque que desde la gerencia se tiene del proceso de gestión de incidentes.
B. Identificar Entrevistados y Participantes.
C. Preguntas Expectativas del sistema de gestión de seguridad de la información.
C.1. Indíquenos la cantidad de empleados de Casavisión. C.2. ¿Qué tipo de estructura organizacional tiene? C.3. ¿Las políticas corporativas son definidas por un área específica? C.4. ¿Cómo se controla el cumplimiento de las políticas corporativas? C.5. ¿Las políticas corporativas son comunicadas a los empleados de la empresa? ¿De qué manera? C.6. ¿Cómo se tramitan los requerimientos entre las áreas de la empresa? C.7. ¿Existe una política de adquisiciones para los activos de la empresa? C.8. ¿Se cuentan con manuales de operaciones? ¿Dónde se almacenan? C.9. ¿La infraestructura de la empresa (Servidores, equipos de cómputo, equipos de redes) es propia? C.10. ¿Cuenta la empresa con políticas para el control de activos? C.11. ¿Cuentan con políticas de continuidad de negocio? C.12. ¿La empresa cuenta con políticas de acceso a la información? C.13. ¿Cuenta la empresa con medios de respaldo para la infraestructura (UPS, Planta eléctrica)?

C.14. ¿Existen políticas para el envío de la información a clientes y proveedores? C.15. ¿Cuenta la empresa con políticas de acceso a redes Wifi? C.16. ¿Las políticas de seguridad esta alineadas con los objetivos de la empresa? ¿De qué manera? C.17. ¿Cuenta el personal con los perfiles requeridos para su cargo? C.18. ¿La empresa tiene contemplado operaciones a través de internet?
D. Preguntas procesos de gestión de incidentes en Casavisión
D.1. ¿Qué tipo de políticas tiene definidas? D.2. ¿Con relación a la seguridad, que políticas tiene la empresa dispuestas? D.3. ¿Existen políticas de contratación de personal de gestión de incidentes? D.4 ¿Cuántas personas realizan la gestión de incidentes?

Anexo12: Características de la entrevista a la gerencia

Características de la entrevista	
Fecha de aplicación	
Tipo de entrevista	Entrevista a profundidad
Enfoque	Sujeto – Objeto
Objetivos	• Identificar los recursos involucrados en el proceso de gestión de incidentes de ciberseguridad. • Conocer como es la estructura del sistema de seguridad de información de Casavisión. • Conocer cómo se realiza el control de los lineamientos y políticas definidos en la gestión de incidentes.
Quien realiza la entrevista	Michell Victoria Gutiérrez Ríos
Nombre Entrevistado	
Edad	
Ocupación	
Nivel de educación	Profesional
Relación con el proyecto	Responsable

Cuestionario Preparado
A. Introducción.

La entrevista está enfocada en obtener la información que el responsable de incidentes maneja y como desde las labores operativas es percibida y manejada la seguridad de la información.
B. Identificar Entrevistados y Participantes.
C. Preguntas identificación de recursos involucrados.
C.1. ¿El acceso al cuarto de equipos donde se encuentran los servidores se encuentra restringido? ¿Cómo se definen los procedimientos de acceso al Datacenter? C.2. ¿Se cuenta con medios de respaldo para la información de incidentes? C.3. ¿Los accesos a los sistemas cuentan con perfiles? C.4. ¿Cuenta la empresa con una política de manejo de respaldos de información (Discos duros, cintas)? C.5. ¿Qué tipo de contingencias se tiene contempladas y ante qué clase de eventos?
D. Preguntas de conocimiento de estructura del Sistema de gestión de seguridad de la información.
D.1. ¿Qué políticas están definidas dentro del proceso de gestión de incidentes? D.2. ¿Quién realiza el control de acceso a los equipos de red y seguridad? D.3. ¿Sabe si en los contratos laborales existen cláusulas contractuales para el manejo de información confidencial? D.4. ¿Quién es el encargado de asignar los accesos a los sistemas?
E. Preguntas identificación de control de los lineamientos y políticas dentro del proceso de gestión de incidentes.
E.1. ¿El personal de gestión de incidentes conoce las políticas de seguridad de la empresa? ¿Cómo son notificados de las mismas? E.2. ¿Realiza seguimiento al cumplimiento de las políticas establecidas por la empresa? ¿De qué manera lo hace? E.3. ¿Cuentan los dispositivos de red y seguridad con controles de acceso? E.4. ¿Qué tipo de controles se tienen para el acceso al Datacenter? E.5. ¿Hay definidos protocolos para la información que es enviada vía correo electrónico?

Anexo13 Características de la entrevista al responsable de incidentes