RESUMEN – TRABAJO DE GRADO

AUTORES	**KAREN LORENA LEÒN PÈREZ** **DANNY JHOAN RIOS BARONA**
FACULTAD	**FACULTAD DE INGENIERIAS**
PLAN DE ESTUDIOS	**ESPECIALIZACION EN AUDITORIA DE SISTEMAS**
DIRECTOR	**ANDRES MAURICIO PUENTES VELASQUEZ**
TÍTULO DE LA TESIS	**PLAN DE CONTINUIDAD DEL NEGOCIO PARA EL AREA DE TECNOLOGÍAS DE LA INFORMACIÓN DEL PROYECTO RUTA DEL SOL - SECTOR 2.**

RESUMEN
(70 palabras aproximadamente)

En el presente trabajo se plantea la necesidad de diseñar el Plan de Continuidad del Negocio en el área de Tecnologías de la Información del proyecto Ruta del Sol - Sector 2.

Se realizó un análisis de los posibles riesgos y las vulnerabilidades a las cuales están expuestos con el fin de elaborar un diagnóstico que permita valorarlos para la toma de decisiones y/o estrategias técnicas y sistemáticas que ayude a mitigarlos.

CARACTERÍSTICAS

PÁGINAS:	PLANOS:	ILUSTRACIONES:	CD-ROM:

PLAN DE CONTINUIDAD DEL NEGOCIO PARA EL AREA DE TECNOLOGÍAS DE LA INFORMACIÓN DEL PROYECTO RUTA DEL SOL - SECTOR 2.

KAREN LORENA LEÓN PÉREZ

DANNY JHOAN RIOS BARONA

Trabajo presentado para obtener el título de Especialistas en Auditoria de Sistemas

Director

ING. ANDRÉS MAURICIO PUENTES VELÁSQUEZ

UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA

FACULTAD DE INGENIERÍAS

ESPECIALIZACIÓN EN AUDITORIA DE SISTEMAS

Ocaña, Colombia Mayo de 2017

CONTENIDO

LISTAS DE FIGURAS

pág.

LISTAS DE TABLAS

pág.

INTRODUCCIÓN

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

En el presente trabajo se plantea de forma clara y precisa la necesidad de diseñar el Plan de Continuidad del Negocio en el área de Tecnologías de la Información del proyecto Ruta del Sol - Sector 2, siendo este, el objeto a investigar en este proyecto.

Se realizó un análisis de los posibles riesgos potenciales y las vulnerabilidades a las cuales están expuestos los equipos de cómputo y sistemas de información, con el fin de elaborar un diagnóstico que permita evaluar y valorarlos para la toma de decisiones y/o estrategias técnicas y sistemáticas que ayude a mitigarlos.

Para el desarrollo del Plan de Continuidad del Negocio se tomó como referencia el análisis y la comparación de las normativas existentes conocidas como ISO/IEC 27001:2005, ISO/IEC 27002:2007, NTC 5722, NIST 800-34, NFPA1600:2010 Y ASIS SPC.1:2009 que permitirá a la empresa establecerlo como un instrumento en la continuidad de las actividades y operaciones tecnológicas,, garantizando las posibilidades de supervivencia y disminuyendo el impacto en las pérdidas que podría afectar la credibilidad de la empresa.

1. PLAN DE CONTINUIDAD DEL NEGOCIO PARA EL AREA DE TECNOLOGÍAS DE LA INFORMACIÓN DEL PROYECTO RUTA DEL SOL - SECTOR 2.

1.1 Planteamiento del problema

La rapidez con la cual las compañías pueden reiniciar sus operaciones comerciales luego de un desastre natural o acción humana, depende de los planes o estrategias que ella labore, FEMA (2014) afirma "si las empresas están listas para sobrevivir y recuperarse, la nación y su economía estarán más seguras" (p.2).

La empresa que tiene como objeto contractual el diseño, mejoramiento, rehabilitación y construcción del proyecto Ruta del Sol-Sector 2 y del proyecto Rio de Oro-Aguaclara-Gamarra, es la contratista Consol (Consorcio Constructor Ruta del Sol) de la Concesionaria Ruta del Sol sector 2, su oficina principal se encuentra ubicada en Aguachica cesar, donde ha sufrido de atentados con artefactos explosivos dejando solo daños materiales, (Lora, 2012, p.1).

El 26 de septiembre del 2013 se registró un bloqueo en la vereda conocida como Cerro de los Chivos en el Sur del Cesar, la cual queda a 1 Km de las instalaciones de Consol, Cincuenta hombres encapuchados que se identificaron como mineros de Bolívar paralizaron el tráfico y pincharon llantas. Media hora después del inicio de los disturbios llegó el ESMAD, quien tuvo enfrentamiento por más de dos horas con los

manifestantes. (Bernal, 2013, pag.1), en otra fecha se presentó bloqueo en la vía durante 24 horas obligando a los empleados a evacuar las instalaciones y reanudar actividades luego de día y medio de disturbios, en este punto los campesinos impidieron el paso vehicular y quemaron 3 (tres) tractomulas, este disturbio dejo por lo menos 50 personas heridas, la mayoría campesinos y mineros. (Murillo, 2013, pag.1).

La empresa ha sufrido también de quema de maquinaria, los hechos se registraron hacia las 12:40 am del día 13 de Septiembre del 2015 en la vía entre Pelaya y San Roque más exactamente en el Kilómetro 20+900 Metros, donde fue quemado un tractor perteneciente a la contratista CONSOL. (Angarita, 2015, pag.1), Según investigaciones realizadas por la policía "Fue capturado el presunto responsable de la quema de maquinaria de CONSOL y segundo cabecilla de la comisión "Francisco Bossio" SAT-ELN" (Angarita, 2016, p.1)

En el área de T.I se evidencio una falla tecnológica que afecto toda la información del área de Ingeniería y Planeamiento del proyecto Rio de Oro-Aguaclara-Gamarra, se reportó una falla física en el disco duro donde almacenaban la información, el personal de T.I asumió que al almacenar la información automáticamente realizaba la copia de seguridad de tipo espejo, es decir, tomaba la mitad de la capacidad del disco para la información y la otra mitad para el backup, los responsables de T.I nunca verificaron el cumplimiento de este proceso de almacenamiento, realizaron todo de tipo de procedimiento para recuperar la información vital del área pero no fue posible, además por el área de T.I no se llevó a cabo la clasificación de la información esencial o critica de las áreas con el fin de dar a conocer a ellas el procedimiento y lugar adecuado de almacenamiento lógico que evite estos tipos de

incidentes, por lo tanto se evidencia la necesidad de implementar una estrategia que proporcione mecanismos más útiles y adecuados para reaccionar y responder con claridad y fundamento ante un desastre.

1.2. Formulación del problema

¿Con la elaboración de un Plan de Continuidad del Negocio se establecería para el área de T.I del proyecto Ruta del sol, un instrumento que garantice que las funciones esenciales puedan continuar durante y después de un desastre evitando la interrupción de los servicios y restablecer el pleno funcionamiento en el menor tiempo posible?

1.3.Objetivos

1.3.1 Objetivo general

Diseñar un Plan de Continuidad del Negocio para el área de Tecnologías de la Información del proyecto Ruta del Sol – Sector 2

1.3.2. Objetivos específicos

- Analizar los riesgos potenciales y vulnerabilidades a las cuales están expuestas las operaciones de la empresa.

- Elaborar el Plan de Continuidad del Negocio de acuerdo a los resultados obtenidos del análisis de vulnerabilidad.

- Socializar el Plan de Continuidad del Negocio con el personal del área de T.I

1.4. Justificación

La pérdida de reputación y la interrupción del negocio encabezan la lista de los mayores riesgos para las organizaciones. Hoy en día, la continuidad del negocio no sólo se asocia con fenómenos físicos como incendios o fallos tecnológicos, sino que se extiende a un nivel estratégico en el que la reputación y el valor del accionista son elementos clave.

A través de una entrevista (VER ANEXO 1) realizada a T.I (Tecnología de la Información) donde se verificaba el cumplimiento de los dominios según ISO 27002:2013 y se identificaba el nivel de seguridad de la información dentro del área, se evidencio que el dominio de Gestión de los aspectos de la seguridad de la información para la continuidad del negocio obtuvo un 0% del cumplimiento, indicando que dentro de la empresa no se tiene establecido, documentado e implementado algún procedimiento y control para garantizar el nivel requerido de continuidad de la seguridad de la información durante una

situación adversa, también se observó que el dominio de Gestión de los incidentes de seguridad de la información se cumple en un 50%, según indicaciones de la Responsable del área no se cumple con: "la organización cuenta con un plan para la continuidad de la gestión de la seguridad durante una crisis o desastre", con esta herramienta de recolección de información se logró observar la necesidad de brindar a la organización un Plan de Continuidad del Negocio, debido a que no existe una estrategia que brinde una respuesta clara e inmediata ante un desastre natural o por causa de terceras personas que permita mitigar y contrarrestar las interrupciones en las actividades propias y proteger sus procesos críticos contra los efectos de fallas importantes en los sistemas y a su vez asegurar su recuperación oportuna.

Es importante que la empresa cuente con una estrategia que le indique como debe recuperar de forma parcial o total sus procedimientos esenciales dentro de un tiempo predeterminado luego de cualquier interrupción no deseada, o como prepararse para futuros incidentes aplicando medidas preventivas y correctivas para mantener la funcionalidad de la organización a un nivel mínimo aceptable durante una contingencia, ayudando a prevenir o identificar los posibles escenarios que generan estas interrupciones.

Al no tener una estrategia, la empresa asumiría el riesgo de contar con incidentes imprevistos, que en el peor de los casos pueda detener los procesos, viéndose afectada y por consiguiente incumpliendo los objetivos organizacionales, provocando pérdidas económicas y de información, teniendo en cuenta que es más económico prevenir o mitigar desastres que financiar la recuperación.

Un Plan de Continuidad del Negocio está enfocado en la prevención y manejo de cualquier tipo de desastre ya sea de origen natural o humano, con el fin de garantizar la disminución en el impacto de pérdidas de tipo financiero, de información crítica del negocio, credibilidad y productividad, que permiten la posibilidad de reaccionar y responder con rapidez en caso de sufrir un incidente que afecte la continuidad, este plan proporciona fortalezas a la vulnerabilidad que presente, identifica los diversos eventos que puedan impactar sobre la continuidad de las operaciones, aporta una ventaja competitiva frente a las otras organizaciones, identifica aquellos puntos más débiles de la infraestructura que son susceptibles de sufrir un incidente y promueve la seguridad de los empleados protegiendo su salud y bienestar.

1.5. Delimitaciones

1.5.1. Operativas

Este Plan de Continuidad del Negocio ha sido diseñado con el fin de orientar a los profesionales que desempeñan algún tipo de servicio, proceso o actividad a que conozcan cómo mantener la funcionalidad de la empresa a un nivel mínimo aceptable durante una contingencia.

1.5.2. Temporal

El proyecto se ejecutó en un periodo de 5 meses (Desde Diciembre del 2016 hasta Abril del 2017) a partir de su fecha de aprobación.

1.5.3. Espacial

Este proyecto se realizó en el municipio de Aguachica Departamento del Cesar, en el área de Tecnologías de la Información del Consorcio Constructor Ruta del Sol, sector 2 ubicada en la Carrera 40 Nº 5N-126 Barrio Nueva Colombia.

1.5.4. Contextual

Aguachica está ubicado al sur del Departamento del Cesar, en el País de Colombia, Demográfica y económicamente es la segunda ciudad más importante del departamento después de la capital, Valledupar.

Está ubicada a los 08º 18´ 45" de latitud norte y 73° 37´ 37" de longitud oeste del meridiano de Greenwich a 190 metros sobre el nivel del mar (msnm), y una temperatura media 28 °C; tiene una extensión total de 876,26 Km2 Km^2, limita al norte con los municipios de La Gloria (Cesar) y El Carmen (Norte de Santander), por el Este con el municipio de Río de Oro (Cesar), por el sur con San Martín (Cesar) y Puerto Wilches (Santander), por el Oeste con el municipio de Gamarra (Cesar) y Morales (Bolívar). Fue fundada oficialmente el 16 de agosto de 1748 por José Lázaro de Rivera.

El actual territorio de Aguachica se empezó a consolidar en los primeros veinte años del siglo XVIII a partir de la hacienda de San Roque de propiedad de Don Antón García de Bonilla, localizada al oriente de la actual vía cuarenta, hacia la planta del acueducto municipal. Por razones asociadas a una los primeros pobladores de éste asentamiento debieron trasladarse más abajo, alrededor del actual Parque San Roque. El primer núcleo poblacional era un incipiente núcleo de habitación en propiedades que hacia 1722 pertenecía a Don Casimiro ramos de Barahoja, articulado al flujo de mercancías y población de Gamarra a Ocaña. Unas décadas después, el 16 de agosto de 1748, mediante concesión Realenga de los terrenos de Aguachica viejo y San Francisco hecho a favor de Don José Lázaro de Rivera se realizó un acto de fundación o reconocimiento de la parroquia. Sus fundaciones o refundaciones fueron reconfirmadas por la administración del Virrey José Alfonso Pizarro, entre 1749 y 1753. Tanto en la fundación de Aguachica como la de san Francisco, hacia 1753 se inició la construcción de algunas casas. Se acepta como fecha de fundación, el 16 de agosto de 1748, habiendo sido elevado a la categoría municipal en virtud de la ordenanza número 40 de 1914. (Montes, 2016, pag.1)

"Según resultados y proyecciones del último censo realizado se reporta que la ciudad cuenta aproximadamente con 106.957 habitantes en total. Departamento Administrativo Nacional de Estadística. (2005) Proyecciones de población municipal por área" (DANE, 2015).

1.5.5. Conceptual

Los conceptos manejados en este proyecto fueron enmarcados dentro de los lineamientos y conceptos establecidos con la Gestión y Continuidad del Negocio según las normas ISO/IEC 27001:2005, ISO/IEC 27002:2007, NTC 5722, NIST 800-34, NFPA1600:2010 Y ASIS SPC.1:2009.

2. Marco referencial

2.1 Antecedentes históricos

- PLAN DE CONTINUIDAD DE NEGOCIOS EN EL ÁMBITO EDUCATIVO. Fabián Patricio Martínez Bermúdez. Universidad Técnica Particular de Loja. Loja, Ecuador. 2010.

Este proyecto está orientado a establecer planes de aseguramiento en continuidad de procesos como una manera de estrategia que mantendrá la buena reputación de la Obra Educativa "Nuestra Señora del Rosario", Así mismo, acogiendo a la institución a la Norma ISO 9001:2008 es por ello que consideran básico generar reportes, para que los equipos de auditoria tomen en cuenta estos temas para el buen funcionamiento de las salas. Esto se añaden, en el desarrollo de la presente tesis, los criterios de tecnología de la información que constan en el COBIT y que son parte de la Norma ISO 27002:2005, como un modo de contribución para alcanzar el objetivo propuesto por la Obra Educativa.

- DESARROLLO DE UN PLAN DE CONTINUIDAD DE NEGOCIO PARA EL DEPARTAMENTO DE TI DE EMPRESAS. Sandra Milena Nazamues Quenguan, Santiago Alejandro Sandoval Hinojosa. Escuela Politécnica Nacional. Quito, Ecuador. 2016.

Este documento se encuentra estructurado para realizar el reconocimiento organizacional teniendo como objetivo principal conocer la situación actual tanto de la organización como del Departamento de TI, toman como base la Norma ISO 22301:2012 desarrollan el Plan de Continuidad enfocándose en las cláusulas que presenta la norma, describen los escenarios donde toma lugar la aplicabilidad del Plan de Continuidad a través de los procedimientos detallados para posteriormente obtener el análisis de resultados, describen las conclusiones y recomendaciones obtenidas una vez culminado el desarrollo y aplicación del Plan de Continuidad del Negocio.

- PLAN DE CONTINUIDAD DEL NEGOCIO DE UNA TIC. Javier García Fort. Universidad Pontificia Comillas. Madrid, España 2010.

Este proyecto consiste en la elaboración de un Plan de Continuidad del Negocio para una empresa del sector de las Tecnologías de la Información. El objetivo que se pretende conseguir es preparar a la empresa, mediante una serie de protocolos de actuación, procedimientos y políticas de seguridad, para afrontar cualquier situación de contingencia en los sistemas de información de la empresa. De esta manera, aplicando las medidas aprobadas en el BCP de la empresa en caso de desastre, se podrán recuperar todos y cada uno de los procesos de negocio afectados en unos tiempos que se consideren como tolerables para la organización.

- PLAN DE CONTINUIDAD DEL NEGOCIO UNA PERSPECTIVA PREVENTIVA PARA EVITAR IMPACTOS POTENCIALES CASO PREBEL, S. A. Andrés Mauricio Osorio Montoya. Universidad EAFIT Escuela de Administración – MBA. Medellín, Colombia 2011.

Prebel S. A., busca ser capaz de reaccionar rápidamente ante una crisis, asegurar la continuidad de su negocio y restaurar el flujo normal de su cadena productiva y logística ante cualquier suspensión, mediante el desarrollo de un plan de continuidad. El Plan de Continuidad de Negocios (*Business Continuity Plan*, BCP) de Prebel se centra en su operación productiva de cosméticos, analizando, según metodologías de gestión del riesgo avaladas internacionalmente, sus equipos, servicios y recurso humano clave; reduciendo sus riesgos, con base en los hallazgos; generando planes de acción; y desarrollando planes de recuperación ante catástrofes mayores. Para estos efectos, la compañía realizó importantes inversiones en servicios tales como sistemas de tratamiento de agua desionizada, equipos para análisis de laboratorio y equipos críticos para el envasado de sus productos. Asimismo, la compañía formalizó alianzas estratégicas con otros maquiladores que, en caso de ser necesario, pudieran prestar sus servicios, garantizando el abastecimiento de producto terminado ante una interrupción temporal de su actividad productiva. El enfoque del BCP permite a la organización determinar el nivel de inversión/esfuerzo que debe realizar, y concentrarse en las necesidades vitales del negocio.

- DISEÑAR UN PLAN DE CONTINUIDAD DEL NEGOCIO EN EL PROCESO DE ADMINISTRACIÓN DE RECURSOS DE TI DE LA OFICINA DE INFORMATICA Y TELEMATICA DE LA ALCALDIA DE SANTIAGO DE CALI. Carlos Andrés Téllez Mondragón. Universidad Autónoma de Occidente. Cali, Colombia. 2015.

Se aplica la norma ISO 22301 para el diseño del sistema de gestión de continuidad del negocio en la oficina de informática y telemática de la alcaldía de Cali con el fin de lograr y mejorar la disponibilidad de los servicios que esta presenta hacia otras dependencias y la ciudadanía.

- DISEÑO DEL PLAN DE CONTINUIDAD DEL NEGOCIO PARA LA E.S.E HOSPITAL EMIRO QUINTERO CAÑIZARES DE OCAÑA MEDIANTE EL ESTÁNDAR ISO 27001:2013. Karen Paola Sánchez Jaime. Universidad Francisco De Paula Santander Ocaña. Ocaña, Colombia 2015.

El principal objetivo de este trabajo es la realización del Plan de Continuidad del Negocio para la E.S.E Hospital Emiro Quintero Cañizares, determinándose la necesidad de evaluar los riesgos tecnológicos, Con el propósito de darle un buen manejo de las tecnologías de la información y de las comunicaciones, se vio la necesidad de elaborar un Plan de Contingencia completo, instrumento que servirá para evitar la posible pérdida,

destrucción, robo y otras amenazas de la información para definir las tareas orientadas a reducir dichos riesgos.

- PLAN DE CONTINUIDAD PARA EL CENTRO DE DESARROLLO E INNOVACCIÓN TECNOLOGIA DE LA UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA. Javier Alexander Blanco Lindarte, Lina Fernanda Martínez Vega, Claudia Del Pilar Quintero Prado, Jorge Francisco Rincón Angarita. Universidad Francisco de Paula Santander Ocaña. Ocaña Norte de Santander, Colombia. 2012.

El Centro de Desarrollo e Innovación Tecnológica de la Universidad Francisco de Paula Santander Ocaña, por su ubicación geográfica requiere establecer acciones preventivas y correctivas que garanticen que los procedimientos están debidamente custodiados para dar continuidad a su quehacer institucional, por lo que es preciso estructurar planes adecuados para que la misión, la visión, los objetivos y los requisitos del cliente se cumplan.

2.2. Marco teórico

En la década del 2000 y con el rápido crecimiento de la Internet, las organizaciones, cualquiera sea su tamaño se volvieron más dependientes de los sistemas informáticos, pero

también con ello la toma de conciencia de posibles desastres a gran escala, como lo fue el ataque terrorista en los Estados unidos el 11 de septiembre de 2001, la cual contribuyo al crecimiento de la relación entre las industrias y la recuperación ante desastres, un factor clave fueron las regulaciones gubernamentales, que comenzaron a exigir que las organizaciones de cualquier sector de la economía contaran con un plan de sistema de gestión de la continuidad del negocio (SGCN). Lo ocurrido el 11 de septiembre demostró que, a pesar del alto impacto, podría ocurrir eventos de baja probabilidad y que a pesar de la afectación en los edificios y bloques de Manhattan las empresas e instituciones con buenos planes de continuidad sobrevivieron. (Sánchez, 2002).

Según Jorge Burgos Salazar y Pedro G. Campos, para la correcta administración del plan de continuidad se deben establecer y mantener acciones que busquen cumplir con los tres requerimientos de mayor importancia para la información, son los siguientes:

- Confidencialidad. Busca prevenir el acceso no autorizado ya sea en forma intencional o no intencional a la información. La pérdida de la confidencialidad puede ocurrir de muchas maneras, como por ejemplo con la publicación intencional de información confidencial de la organización (Burgos Salazar & Campos, 2008).

- Integridad. Busca asegurar que no se realicen modificaciones por personas no autorizadas a los datos o procesos y que los datos sean consistentes tanto interna como externamente.

- Disponibilidad. Busca asegurar acceso confiable y oportuno a los datos o recursos para el personal apropiado.

Un Plan de Continuidad del Negocio es un proceso diseñado para prevenir interrupciones que afecten el desempeño de las actividades normales de un negocio. En caso de que un evento de riesgo no pueda ser evitado, este plan debe minimizar su impacto (económico y duración). El Plan de Continuidad del Negocio tiene un alcance operativo y tecnológico.

Antecedentes: En la última década, los riesgos de desastres naturales, fallas técnicas con carácter accidental, y actividades maliciosas han incrementado las posibilidades de interrupciones en las organizaciones. Las empresas que sufren una interrupción por espacio de diez días consecutivos, nunca se recuperan y desaparecen del mercado. Lamentablemente, muy pocas son las empresas que invierten en planificación de actividades para minimizar posibles desastres y asegurarse de continuar operando después de una posible calamidad.

Objetivos de Un Plan de Continuidad del Negocio:

-Obtener una imagen clara y detallada de los procesos de negocio de la entidad, determinando sus criticidades, interdependencias y riesgos.
-Lograr un conocimiento profundo de la plataforma tecnológica.
-Determinar las necesidades críticas para permitir un grado de operatividad en línea con la estrategia definida.

-Desarrollar una solución cuya relación costo – beneficio cumpla los requisitos y las expectativas de la entidad.

-Prever y documentar las acciones necesarias para restaurar la actividad.

-Lograr una situación que garantice la continuidad del negocio.

Importancia del Plan de Continuidad del Negocio: Un Plan de Continuidad del Negocio debe ser considerado parte integral de la estrategia del negocio. Un buen plan revisa los procesos críticos de las operaciones en las empresas, los clasifica, prioriza y determina cuáles son los más sensibles y cuáles no pueden dejar de operar para que el negocio continúe su funcionamiento. Si las empresas no cuidan ni manejan correctamente su información, en el momento en que padezcan una eventualidad no podrán atender asuntos prioritarios como: a quién le deben pagar, quién les debe, a quién le venden, a quién le deben otorgar un descuento, quién es meritorio de un crédito, entre otras variables vitales del negocio. El hecho de no poder acceder a estos datos puede ocasionar importantes pérdidas al negocio, (como no saber cómo operan, cuántas piezas producen, cuál era el pedido urgente, cuando llega la materia prima para correr la programación de producción, entre otros).

Alcance del Plan de Continuidad del Negocio: Desarrollar un Plan para la Continuidad del Negocio, que tenga como objetivo el mantenimiento de la actividad de la empresa, mediante la recuperación de los procesos de soporte o mediante la aplicación de procesos de emergencia. El proyecto debe involucrar a todos los procesos y áreas críticas del departamento de producción.

2.3. Marco legal

2.3.1 Constitución Política de 1991 En los artículos 209 y 269 se fundamenta el sistema de control interno en el Estado Colombiano, el primero establece: "La administración pública, en todos sus órdenes, tendrá un control interno que se ejercerá en los términos que señale la ley" y en el 269, se soporta el diseño del sistema: "En las entidades públicas, las autoridades correspondientes están obligadas a diseñar y aplicar, según la naturaleza de sus funciones, métodos y procedimientos de control interno, de conformidad con lo que disponga la ley, la cual podrá establecer excepciones y autorizar la contratación de dichos servicios con empresas privadas colombianas".

2.3.2 Leyes Informáticas Colombianas

***Ley estatutaria 1266 del 31 de diciembre de 2008*.** Por la cual se dictan las disposiciones generales del Hábeas Data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones.

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

***Ley 1341 del 30 de julio de 2009*.** Por la cual se definen los principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones -TIC-, se crea la Agencia Nacional del Espectro y se dictan otras disposiciones.

Ley estatutaria 1581 de 2012. Entró en vigencia la Ley 1581 del 17 de octubre 2012 de PROTECCIÓN DE DATOS PERSONALES, sancionada siguiendo los lineamientos establecidos por el Congreso de la República y la Sentencia C-748 de 2011 de la Corte Constitucional.

Como resultado de la sanción de la anunciada ley toda entidad pública o privada, cuenta con un plazo de seis meses para crear sus propias políticas internas de manejo de datos personales, establecer procedimientos adecuados para la atención de peticiones, quejas y reclamos, así como ajustar todos los procesos, contratos y autorizaciones a las disposiciones de la nueva norma.

Cualquier ciudadano tendrá la posibilidad de acceder a su información personal y solicitar la supresión o corrección de la misma frente a toda base de datos en que se encuentre registrado.

Establece los principios que deben ser obligatoriamente observados por quienes hagan uso, de alguna manera realicen el tratamiento o mantengan una base de datos con información personal, cualquiera que sea su finalidad.

Aclara la diferencia entre clases de datos personales construyendo las bases para la instauración de los diversos grados de protección que deben presentar si son públicos o privados, así como las finalidades permitidas para su utilización.

Crea una especial protección a los datos de menores de edad.

Establece los lineamientos para la cesión de datos entre entidades y los procesos de importación y exportación de información personal que se realicen en adelante.

Define las obligaciones y responsabilidades que empresas de servicios tercerizados tales como Call y Contact Center, entidades de cobranza y, en general, todos aquellos que manejen datos personales por cuenta de un tercero, deben cumplir en adelante.

Asigna la vigilancia y control de las bases de datos personales a la ya creada Superintendencia Delegada para la Protección de Datos Personales, de la Superintendencia de Industria y Comercio.

Crea el Registro Nacional de Bases de Datos.

Establece una serie de sanciones de carácter personal e institucional dirigidas a entidades y funcionarios responsables del cumplimiento de sus lineamientos.

Ley 603 de 2000. Esta ley se refiere a la protección de los derechos de autor en Colombia. Recuerde: el software es un activo, además está protegido por el Derecho de

Autor y la Ley 603 de 2000 obliga a las empresas a declarar si los problemas de software son o no legales.

Constitución Política de 1991. En su artículo 61, que expresa: "El Estado protegerá la propiedad intelectual por el tiempo y mediante las formalidades que establezca la ley".

Decisión 351 de 1993, o Régimen Común Andino sobre Derecho de Autor y Derechos Conexos, es de aplicación directa y preferente a las leyes internas de cada país miembro del Grupo Andino.

Ley 23 de 1982, contiene las disposiciones generales y especiales que regulan la protección del derecho de autor en Colombia.

Ley 44 de 1993 (febrero 15), modifica y adiciona la Ley 23 de 1982 y se modifica la Ley 29 de 1944.

DECRETO 1474 DE 2002 (Julio 15). "Por el cual se promulga el "Tratado de la OMPI, Organización Mundial de la Propiedad Intelectual, sobre Derechos de Autor (WCT)", adoptado en Ginebra, el veinte (20) de diciembre de mil novecientos noventa y seis (1996)".

Ley 734 de 2002, Numeral 21 y 22 del Art. 34, son deberes de los servidores Públicos "vigilar y salvaguardar los bienes y valores que le han sido encomendados y cuidar que sean utilizados debida y racionalmente", y "responder por la conservación de los

útiles, equipos, muebles y bienes confiados a su guarda o administración y rendir cuenta oportuna de su utilización".

2.3.2 Normas que rigen un Plan de Continuidad del Negocio

BS 25999 Parts 1 and 2 Business Continuity Management. Se trata de una norma certificable en la que se tiene como objeto la gestión o plan de continuidad del negocio fundamentalmente enfocado a la disponibilidad de la información, uno de los activos más importantes hoy en día para cualquier organización. La norma se creó ante la necesidad de que actualmente tienen las organizaciones de implementar mecanismos y técnicas, que minimicen los riesgos a los que se está expuesta, para conseguir una alta disponibilidad de las actividades de su negocio. La norma consiste en una serie de "recomendaciones o buenas prácticas" para facilitar la recuperación de los recursos que permiten el funcionamiento normal de un negocio, en caso de que ocurra un desastre. En este contexto, se tienen en cuenta tanto los recursos humanos, como las infraestructuras, la información vital, las tecnologías de la información y los equipos que la soportan.

NIST 800-34, Contingency Planning Guide for Information Technology (IT). El Laboratorio de Tecnologías de la Información (DIT) del Instituto Nacional de Estándares y Tecnología (NIST) promueve la economía de EE.UU. y el bienestar público, proporcionando liderazgo técnico para la medición de la nación y la infraestructura de las normas. ITL desarrolla pruebas, métodos de prueba, datos de referencia, la prueba de las implementaciones de concepto, y el análisis técnico para avanzar en el desarrollo y uso productivo de las tecnologías de la información. Responsabilidades de ITL incluyen el

desarrollo de técnicas, físicas, normas y directrices para la seguridad económica y la privacidad de la información sensible no clasificada en los sistemas informáticos federales administrativos y de gestión. Esta publicación especial los informes de la serie 800 en la investigación de ITL, orientación y divulgación esfuerzos en seguridad informática y de sus actividades de colaboración con la industria, el gobierno y organizaciones académicas.

ITIL Continuity Management, IT Security and Availability Management. La Tecnología de la Información Biblioteca de Infraestructura de TI (ITIL) es un conjunto de prácticas para la gestión de servicios de TI (ITSM) que se centra en la adaptación de los servicios de TI con las necesidades del negocio. En su forma actual (conocido como ITIL edición 2011), ITIL se publica en una serie de cinco publicaciones principales, cada uno de los cuales cubre una etapa del ciclo de vida de ITSM. ITIL sustenta la norma ISO / IEC 20000 (anteriormente BS15000), la Norma Internacional de Gestión de Servicios para la gestión de servicios de TI, aunque las diferencias entre los dos marcos existen. ITIL describe los procesos, procedimientos, tareas y listas de control que no son específicos de cada organización, utilizados por una organización para establecer la integración con la estrategia de la organización, la entrega de valor y el mantenimiento de un nivel mínimo de competencia. Esto permite a la organización para establecer una línea de base desde la que se puede planificar, implementar y medir. Se utiliza para demostrar el cumplimiento y para medir la mejora.

2.4. Marco conceptual

Para el propósito de este proyecto, se aplican los siguientes términos y definiciones:

Estructura organizacional. La estructura organizacional puede ser definida como las distintas maneras en que puede ser dividido el trabajo dentro de una organización para alcanzar luego la coordinación del mismo orientándolo al logro de los objetivos, su función principal de establecer autoridad, jerarquía, cadena de mando, organigramas y departamentalizaciones, entre otras. (Gonzales, 2012)

Tecnología de la información. La Tecnología de la información Abarca todo lo relacionado a la conversión, almacenamiento, transformación, protección, procesamiento, captura y transmisión de la información, además la Tecnología de la Información engloba cualquier tipo de tecnología que permita administrar y comunicar información como la informática, la electrónica y las telecomunicaciones, los avances tecnológicos como la Internet, las comunicaciones móviles y los satélites.(Rodríguez, 2016).

Seguridad de la información Es un conjunto de medidas técnicas, organizativas y legales que permiten a la organización asegurar la confidencialidad, integridad y disponibilidad de su sistema de información. Además consiste en asegurar que los recursos del Sistema de Información de una empresa se utilicen de la forma que se ha decidido y al acceso de información que se encuentra contenida, protegiendo la divulgación e interrupción no autorizada de la misma, así como controlar que la modificación solo sea posible por parte de las personas autorizadas para tal fin y por supuesto, siempre dentro de los límites de la autorización.

Los activos de información son los elementos que la Seguridad de la Información debe proteger. Por lo que son tres elementos lo que forman los activos:

- Información: es el objeto de mayor valor para la empresa.
- Equipos: suelen ser software, hardware y la propia organización.
- Usuarios: son las personas que usan la tecnología de la organización. (Mifsud, 2012).

Auditoria. La auditoría es un proceso sistemático que se realiza para obtener y evaluar de manera objetiva las evidencias relacionadas con informes presentados sobre acciones que tienen que ver directamente con las actividades que se desarrollan en un área o una organización, sea pública o privada.

La auditoría es un proceso sistemático. Esto quiere decir que en toda auditoría debe existir un conjunto de procedimientos lógicos y organizados que se deben cumplir para la recopilación de la información con el fin de emitir una opinión final.(Sánchez Gómez, 2005)

Vulnerabilidad. Es la incapacidad de resistencia cuando se presenta un fenómeno amenazante o para reponerse después de que ha ocurrido un desastre, es el factor complejo de riesgo o el grado de exposición a sufrir algún daño por la manifestación de una amenaza específica. (Ortega Ruiz, 2014).

Recursos informáticos. Los recursos informáticos están conformados por todos aquellos componentes de Hardware y Software que son necesarios para el buen funcionamiento y la optimización del trabajo con ordenadores y periféricos, tanto a nivel Individual, como colectivo u organizativo, sin dejar de lado el buen funcionamiento de los mismos.

Un buen ejemplo de estos pueden ser las aplicaciones, herramientas, dispositivos (periféricos) y capacidades, una computadora que cuenta con una impresora y hace uso de este recurso. (O`Brien, 2016).

Sistemas de información. Los Sistemas de Información (SI) son conjuntos organizados de elementos que procesan y distribuyen información con el fin de cumplir unos objetivos. No es necesario que estén basados en ordenadores. La utilización de aplicaciones informáticas sobre soportes informáticos da lugar a los Sistemas de Información Automatizados (SIA).

Los Sistemas de Información pretenden proporcionar una información oportuna y exacta para el apoyo en la toma de decisiones de la compañía. Además, garantizan la confiabilidad, la integridad y disponibilidad de la información. El uso de Sistemas de Información automatiza procesos operativos y pretenden conseguir ventajas competitivas en el mercado.

Características de los datos en un sistema de información:

- **Integridad:** Para la Seguridad de la Información, la integridad es la propiedad que busca mantener a los datos libres de modificaciones no autorizadas.

- **Confidencialidad:** La confidencialidad es la propiedad de prevenir la divulgación de información a personas o sistemas no autorizados.

- **Disponibilidad:** La Disponibilidad es la característica, cualidad o condición de la información de encontrarse a disposición de quienes deben acceder a ella, ya sean personas, procesos o aplicaciones.(Monte de Paz, 2010)

Base de datos. Es una serie de datos organizados y relacionados entre sí, los cuales son recolectados y explotados por los sistemas de información de una empresa o negocio en particular. Las bases de datos recopilan, almacenan y organizan información, también pueden almacenar información sobre personas, productos, pedidos u otras cosas.

Entre las principales características de los sistemas de base de datos se encuentran:

- Independencia lógica y física de los datos.
- Redundancia mínima.
- Acceso concurrente por parte de múltiples usuarios.
- Integridad de los datos.
- Consultas complejas optimizadas.
- Seguridad de acceso y auditoría.

- Respaldo y recuperación.
- Acceso a través de lenguajes de programación estándar.(Murillo Ovallos, 2016)

Servidor. Es la máquina informática u ordenador que está al servicio de otras máquinas u ordenadores, llamadas clientes. La finalidad de un servidor es suministrar la información o proveer datos que solicitan los clientes y, para ello existen diferentes tipos de servidores, como por ejemplo:

- **servidor Web,** almacena y envía a los clientes documentos en HTML, imágenes, videos, textos, etc.
- **servidor de correo**, como lo indica su nombre se encarga de almacenar, enviar, recibir y realizar todas las operaciones ligadas al correo electrónico,
- **servidor de impresión** se encarga de administrar los diferentes documentos que se envían a imprimir dentro de la red**.**
- **servidor de base de datos** es un sistema que permite almacenar grandes cantidades de información y, el servidor permite almacenar y gestionar o administra la base de datos.
- **servidor de archivos** trata sobre el uso del disco duro compartido por varios usuarios y que sea usado por un único usuario, por ejemplo: cuando varios usuarios intentan acceder a una misma información, el servidor de archivos controla y ordena los accesos a esta, permitiendo el ingreso de un número de usuarios y, a la vez otros se encuentran en espera.

- **servidor proxy** trabaja como un intermediario entre 2 ordenadores, en ocasiones este servidor puede bloquear ciertas peticiones que realiza el cliente debido a que posee ciertas extensiones bloqueadas y, por lo tanto, no se puede acceder a la página solicitada por el cliente.
- **servidor DNS** son las siglas de *Domain Name System*, se asocia una información con un nombre de dominio y, este servidor determina en qué lugar se encuentra esa página web y nos remite a ella, tal como fue solicitado por el cliente. (Fernández, 2015).

Router Es un dispositivo de hardware que permite la interconexión de ordenadores en red. Además es un dispositivo que opera en capa tres de nivel de 3 ya que así permite que varias redes u ordenadores se conecte entre sí, por ejemplo, compartan una misma conexión de internet.

Un router se vale de un protocolo de enrutamiento, que le permite comunicarse con otros enrutadores o encaminadores y compartir información entre sí para saber cuál es la ruta más rápida y adecuada para enviar datos. (Rueda Gonzales, 2016).

Switch. Funciona para la interconexión de redes informáticas, es el dispositivo analógico que permite interconectar redes. Un conmutador interconecta dos o más partes de una red, funcionando como un puente que transmite datos de un segmento a otro. Su empleo es muy común cuando existe el propósito de conectar múltiples redes entre sí para que funcionen como una sola. Un conmutador suele mejorar el rendimiento y seguridad de

una red de área local.

El funcionamiento de un conmutador o switch tiene lugar porque el mismo tiene la capacidad de aprender y almacenar direcciones de red de dispositivos alcanzables a través de sus puertos. A diferencia de lo que ocurre con un hub o concentrador, el switch hace que la información dirigida a un dispositivo vaya desde un puerto origen a otro puerto destino.(Salazar, 2014).

Disco duro. El disco duro o disco rígido es el dispositivo electrónico donde se almacena toda la información que se procesa en la computadora incluyendo el sistema operativo y las aplicaciones. Este emplea un sistema de grabación magnético para almacenar datos digitales y está compuesto por uno o más platos o discos que se unen por un eje que gira a una gran velocidad dentro de una caja metálica que los protege. Cabe destacar que actualmente se está perfeccionando la tecnología de discos en estado sólido o SSD (Solid State Drive) donde la información es grabada y leída gracias a procesos químicos. (Ropero, 2016).

2.5. Marco contextual

Esta investigación se llevó a cabo en el área de T.I (Tecnologías de la Información) del Consorcio Constructor Ruta del Sol - Sector 2 en la ciudad de Aguachica Cesar, Colombia. Se analizó y estudió los procesos de dicha área, su estructura orgánica, sus recursos informáticos y de software, sus riesgos potenciales y vulnerabilidades a las cuales

están expuestas las operaciones de la empresa y se realizó la elaboración de del plan de Continuidad del Negocio el cual fue socializado y entregado al personal correspondiente.

3. Diseño metodológico

3.1. Tipo de investigación

Para la realización de este proyecto de grado el tipo de investigación trabajado fue la investigación de forma descriptiva tipo aplicada.

La investigación descriptiva, tiene como objetivo identificar los riesgos potenciales y las vulnerabilidades a las cuales están expuestas las operaciones de la empresa y analizar el impacto en ella, el estado, las características, factores y procedimientos presentes en fenómenos y hechos que ocurren (Lerma Gonzales, 2009).

Luego se analizó como es y cómo se manifiesta el fenómeno y sus componentes, permitiendo detallarlo, estudiarlo, describir el desarrollo del objeto de estudio y cómo evoluciona respecto a la problemática y demás factores que intervienen en él para resolver problemas prácticos.

3.2. Población y muestra

POBLACIÓN: Una población se precisa como un conjunto finito o infinito de personas u objetos que presentan características comunes, destacamos la afirmación de Levin & Rubin (1996) "Una población es un conjunto de todos los elementos que estamos estudiando, acerca de los cuales intentamos sacar conclusiones".

En este proyecto la población está conformada por las 3 personas que integran el área de TI (Tecnologías de la Información) del Consorcio Constructor Ruta del Sol, Sector 2.

MUESTRA: La muestra es una representación significativa de las características de una población.

- Murria R. Spiegel (1991) afirma "Se llama muestra a una parte de la población a estudiar que sirve para representarla".

- Levin & Rubin (1996) afirman "Una muestra es una colección de algunos elementos de la población, pero no de todos".

Se toma como muestra el 100% de la población involucrada en el proceso por tratarse de una población finita y medible.

3.3.Instrumentos de recolección de datos

Como instrumentos de recolección de datos se utilizó:

3.3.1. Observación directa: "Consiste en el registro sistemático, valido y confiable de comportamientos o conducta, puede utilizarse como instrumento de medición en muy diversas circunstancias" (Hernández Sampieri, Fernández Collado, Baptista Lucio, 1997, p.331).

3.3.2. Lista de chequeo: Permiten realizar un primer inventario o verificación de las características de la empresa, este instrumento permite identificar puntos débiles así como oportunidades de mejora a través de la verificación de un listado de aspectos presentes o no en el área a revisar. (VER ANEXO 1)

3.4. Análisis de información

En el área de T.I del Consorcio Constructor Ruta del Sol, Sector 2 se llevó a cabo una lista de chequeo con el fin de realizar un primer análisis y así identificar el nivel de seguridad de la información del consorcio según ISO/IEC 27002:2013.

Los resultados obtenidos a través de la lista de chequeo aplicada son muy favorables, ya que se logra cumplir con un 81% los dominios presentados en la ISO 27002, obteniendo 43 de los 53 puntos posibles propuestos en esta herramienta de recolección de información, nos permitió identificar puntos débiles que nos permiten tomarlos como oportunidades y así plantear soluciones para su mejora.

4. Presentación de resultados

En este capítulo se desarrollaron las etapas indicadas en los objetivos específicos con el fin de cumplir nuestro objetivo general que corresponde al diseño de un Plan de Continuidad del Negocio para el área de Tecnologías de la Información del proyecto Ruta del Sol – Sector 2.

4.1 Análisis del negocio y evaluación de riesgos potenciales y vulnerabilidades

4.1.1 Reconocimiento de la empresa consorcio constructor ruta del sol, sector 2.

Descripción de la empresa

El Consorcio Constructor Ruta del Sol, Sector 2 - CONSOL, es el principal contratista de la Concesionaria Ruta del Sol S.A.S., ambas están conformadas por la Constructora Norberto Odebrecht de Brasil, EPISOL Y CSS Constructores, estas dos últimas con origen Colombiano; inicialmente el consorcio tiene como objeto contractual el diseño, construcción, mejoramiento y rehabilitación de las obras que comprenden los 528 km del área de influencia desde Puerto Salgar (Cundinamarca) (Sector Sur) hasta San Roque (Cesar) (Sector Norte).

Su objetivo principal es elaborar los diseños, realizar la financiación, obtener las licencias ambientales y demás permisos, adquirir los predios, así como ejecutar las obras para la construcción de la segunda calzada, rehabilitación de la calzada existente,

mantenimiento y operación del proyecto vial en el tramo correspondiente al Sector 2, con una longitud aproximada de 528 kilómetros de doble calzada.

El 14 de enero de 2010 se suscribió con la Agencia Nacional de Infraestructura (ANI) el contrato de concesión 001 de 2010 y a partir del 5 de abril del mismo año se inició la operación y mantenimiento de la vía existente, el diseño detallado de las obras, los estudios de impacto ambiental y la gestión de compra de predios. El evento de inicio de la construcción de la doble calzada se llevó a cabo el 16 de mayo de 2011.

Adicionalmente, el 10 de noviembre de 2014 se firmó el acta de inicio de la Transversal Río de oro-Aguaclara-Gamarra, cuyo objeto son los trabajos de construcción, rehabilitación y mejoramiento de 82 Kilómetros que fueron incluidos al contrato de Concesión 001 de 2010.

El Sector 2 de la Ruta del Sol, hace parte del Proyecto de infraestructura vial más importante de la década en Colombia que unirá en doble calzada al interior del país con la Costa Caribe con una longitud aproximada de 1.071 km.

Este proyecto hace parte de las vías 4g, también llamadas carreteras 4g, y formalmente cuarta generación (4g) de concesiones viales de Colombia, es un programa de infraestructura vial que plantea la construcción y operación en concesión de más de 8,000 km de carreteras, incluyendo 1,370 km de doble calzada y 159 túneles en más de 40 nuevas concesiones. Su objetivo principal es mejorar la competitividad del país, disminuyendo el costo y tiempo de transporte de personas y, en especial, de carga, desde los puntos de

manufactura hasta los puertos de exportación. A octubre de 2015, se han estructurado tres 'olas' de contratos de las Vías 4G.

Es uno de los proyectos más ambiciosos de la historia de la infraestructura en Colombia, con una inversión estimada de $47 billones de pesos (cerca de $18,000 millones de dólares). Se proyecta que las obras se ejecutarán en máximo 6 años a partir de la fecha de su adjudicación.

El proyecto ruta del sol hace parte de los corredores que están en construcción, la troncal se dividió en tres sectores para su construcción y operación:

- Ruta del Sol – Sector 1: Villeta – Guadero – Korán (Puerto Salgar)
- Ruta del Sol – Sector 2: Korán (Puerto Salgar) – San Roque
- Ruta del Sol – Sector 3: San Roque – Y de Ciénaga

El Sector 2 del Proyecto Vial Ruta del Sol, se caracteriza porque el concesionario se obliga por su cuenta y riesgo a elaborar los diseños, obtener el financiamiento, las licencias ambientales y demás permisos; igualmente, a adquirir los predios, rehabilitar y mejorar las vías existentes, construir la nueva calzada, operar y mantener toda la vía.

Desde abril de 2010, la concesión ha trabajado para prestar un servicio de calidad a los usuarios, mejorando las condiciones físicas y de seguridad de la carretera, en pro de una mayor participación y beneficio de las comunidades a lo largo del trayecto.

La Concesionaria Ruta del Sol S.A.S. ha obtenido importantes logros, como el cierre financiero por un monto de 1.4 billones de pesos por cuya estructuración obtuvo el premio "Transportation Deal of the Year", por parte de la publicación Project Finance International (PFI). (Reuters, 2010).

Misión

Es una organización formada por miles de personas de conocimiento, capaces de satisfacer a sus clientes por medio de soluciones innovadoras que contribuyen a un mundo mejor.

Visión

La finalidad de la organización es la generación de riqueza creciente para Clientes, Accionistas, Integrantes y Comunidades, y tiene como rumbo Sobrevivir, Crecer y Perpetuar.

Filosofía

La Tecnología Empresarial Odebrecht (TEO) es un conjunto de principios, conceptos y criterios, con enfoque en la educación y en el trabajo, que provee los fundamentos éticos, morales y conceptuales para la actuación de los Integrantes de Organización. La TEO es una filosofía empresarial volcada al hacer y focalizada en la educación y en el trabajo, valora las potencialidades del ser humano, en particular la disposición para servir, la capacidad y el deseo de evolucionar y la voluntad de superar resultados. Prevé, además, un proceso de delegación planificada, basada en la confianza y en la asociación entre Líderes y Liderados.

Objetivo de calidad la empresa

Establecer compromisos de largo plazo construye relaciones político-estratégicas pautadas en la confianza y se integra en la sociedad, se convierte en motivo de orgullo para las comunidades donde actúa por su contribución al desarrollo sostenible.

Conquistar la confianza de clientes, accionistas y socios externos por su capacidad realizadora, cumplimiento de los compromisos asumidos, excelencia en lo que hace, transparencia y buena gobernanza.

Satisfacer las necesidades de nuestros clientes por medio de soluciones integradas e innovadoras para grandes desafíos globales: disponibilidad de agua, energía, infraestructura, insumos industriales y alimento.

Estructura Organizacional del Área de Tecnologías e Información de Consol, sector 2.

DIRECTOR DE CONTRATO: Marcio Marangoni

GERENTE ADMINISTRATIVO: Jairo Brito

RESPONSABLE ADMINISTRATIVO: Roberto Potrasio

RESPONSABLE TECNOLOGÍAS E INFORMACIÓN: Yuly Contreras

INGENIERO: Gabriel Pabón

INGENIERO: William Escalante

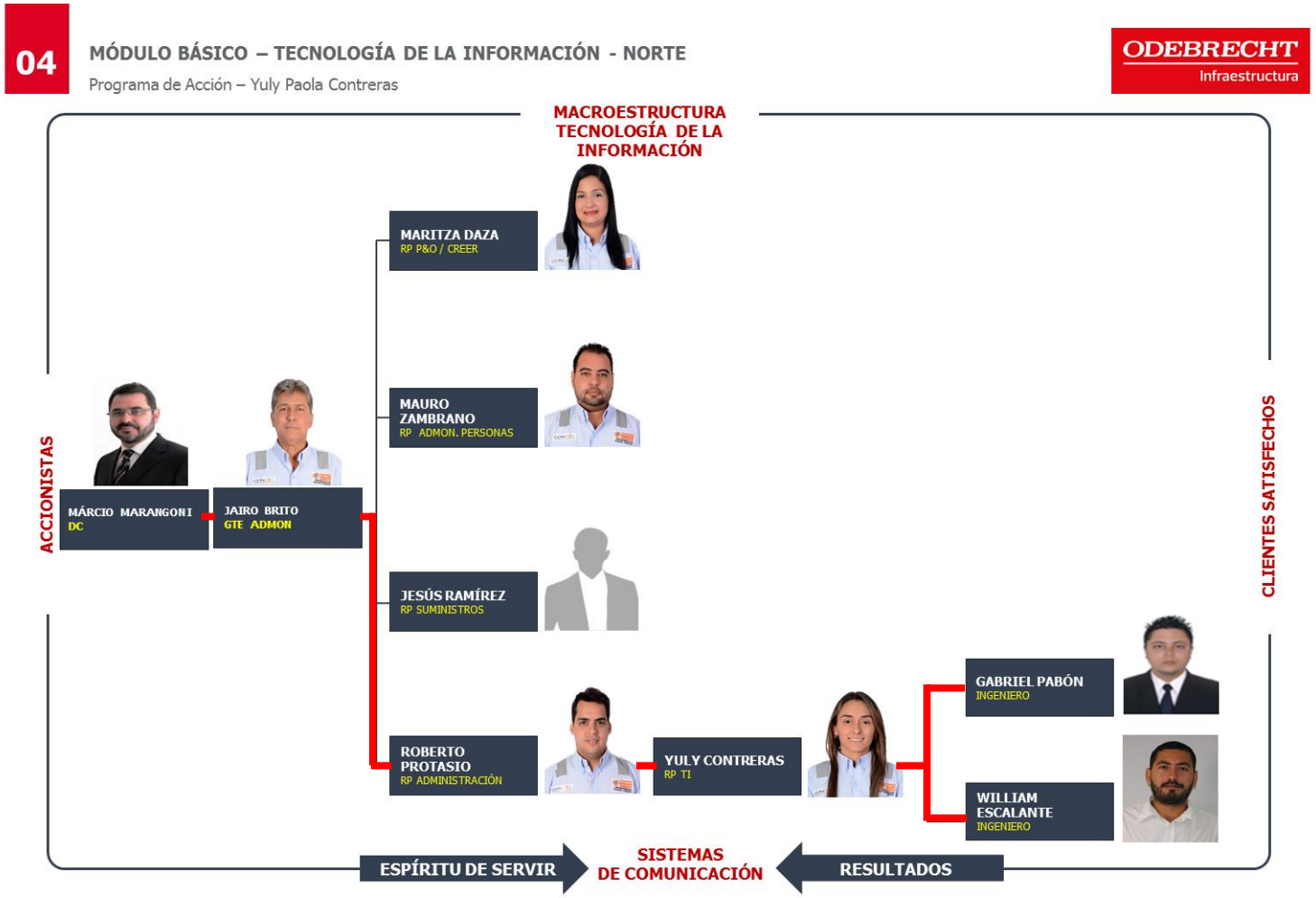


Figura 1. Macroestructura Tecnología de la Información de Consol

Fuente. Modulo Básico – T.I - Consol

Descripción de la dependencia

El área de Tecnologías de la Información de CONSOL es la encargada de administrar eficiente y eficazmente los sistemas de información utilizados para el manejo de los datos de la empresa, analiza, diseña, desarrolla e implementa soluciones tecnológicas para optimizar la productividad.

Su objetivo principal es garantizar que los equipos tecnológicos ofrezcan los niveles precisos de disponibilidad y estabilidad, proporcionando todos los servicios necesarios para garantizar el trabajo de los empleados, gestiona los recursos tecnológicos para su correcto uso, y garantiza una arquitectura de TI coherente y de alto rendimiento.

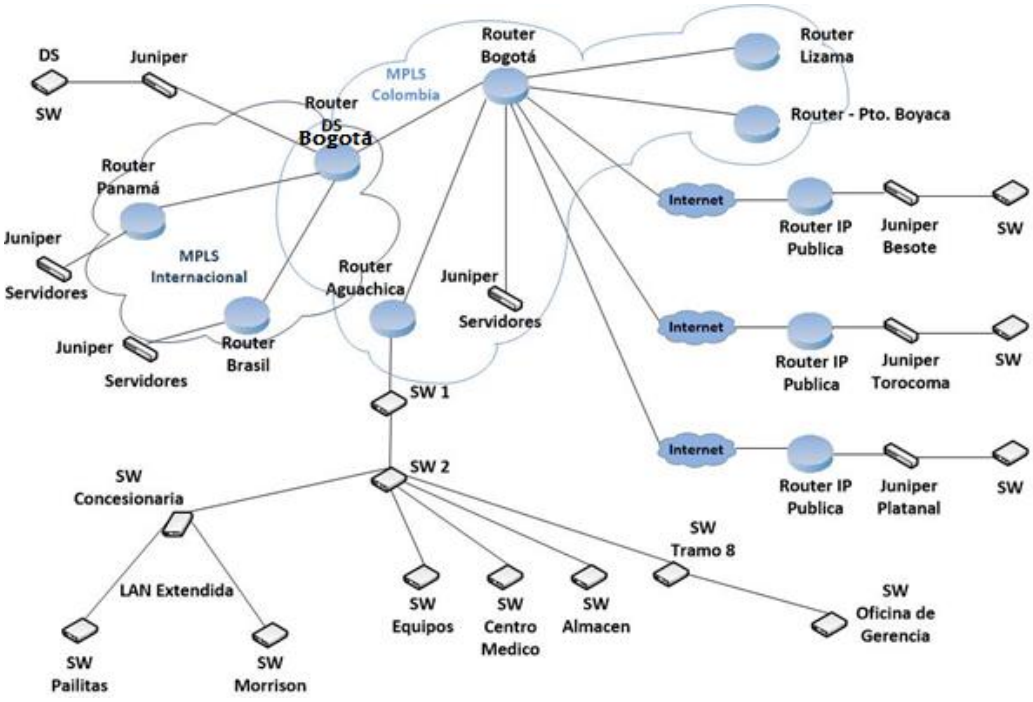


Figura 2. Infraestructura Tecnológica y de Comunicaciones

Fuente: Los Autores.

Siglas:

- **Sw:** Switch
- **Fibris:** Conectores
- **Ds:** Dirección de Superintendencia
- **Mpls:** Multi-protocolo de comunicación mediante etiquetas

Mapa de procesos del Negocio

Es un diagrama que presenta la visión global de la estructura de la empresa, en este caso del área de Tecnologías de la Información, en la cual se presentan todos los procesos que la forman.

Procesos Principales

- Registro y asignación de recursos

Subprocesos:

-Creación de cuenta de dominio: El líder solicita por medio de un formato ya estipulado por la empresa el registro de un nuevo usuario y este debe estar diligenciado con sus datos, la persona ya debe haber sido contratada por la empresa y estar registrado en el sistema de recursos humanos (peopple soft), posteriormente se crea el usuario.

-Creación de cuenta de usuario: Se realiza el mismo procedimiento de la solicitud de creación de usuario de dominio con el fin de registrar la cuenta de usuario de correo

corporativo, este correo se crea como Primernombre.primerapellido ya que son políticas estipuladas por la empresa.

-Activación de sistemas/Servicios: Se realiza el mismo procedimiento de la solicitud de creación de usuario de dominio con el fin dar inicio a la activación de los sistemas y servicios, para esta activación se analiza el perfil, las funciones, el área y las necesidades a la cual va abarcar el empleado.

-Asignación de equipos tecnológicos y de comunicación: Primero se recibe la solicitud y Aprobación por parte del líder, luego se hace un análisis comparativo entre el perfil y las características del equipo solicitado, después se verifica en stock la existencia de dicho elemento y este es asignado atreves de una tarjeta de responsabilidad, de no tener en stock dicho equipo se solicita diligenciar el formato de docmat (formato de compra de materiales), el cual debe tener el visto bueno del responsable de TI para que el área de patrimonio realce la compra.

- Procesos administrativos y control de recursos tecnológicos y procesos informáticos

Subprocesos:

-Administración de servidores de datos: Reciben la solicitud y aprobación por parte del líder de las personas que tendrán acceso a las carpetas, indicando que permiso se le

pueden habilitar ya sea de escritura o de lectura, además atreves de una tecnología llamada escritorio remoto gestionan la manera de acceder al servidor.

-Administración y monitoreo de copia de seguridad: A través de una aplicación llamada copia en Backups se programan las copias de seguridad y se verifica el estado de cada una de ellas, además en la ciudad de Bogotá donde se encuentran el resto de servidores realizan las copias de seguridad en cinta magnética de almacenamiento de datos.

-Administración y monitoreo de red: Se utiliza una herramienta llamada Cisco network assistant para ver el estado de los equipos que estén conectados a esta aplicación, si están encendidos o apagados, si sus puertos están activos o no, además se utiliza una Interfax web de telefónica para observar que tanto ancho de banda se está consumiendo por cada canal.

-Administración de impresoras y tóner: Se crea un usuario para cada empleado dentro de la impresora y se configura para llevar un control de las impresiones y copias de cada persona, al mismo tiempo se centran todas las impresoras para que no impriman de equipo– impresora sino de equipo-servidor-impresora con el fin de que en el servidor también quede un registro de impresiones, al final se saca el resultado que arroja el servidor y se hace una comparación con el resultado de la impresora, estos reportes se envían mensualmente a los gerentes de las áreas con el fin de tener un control financiero en los gastos de papelería y tonner.

-Monitoreo a sistemas/servicios: Al iniciar la jornada laboral se verifica que cada uno de los servicios de los sistemas se encuentren activos (Siseng, ODOS, ADMS, Primavera-Oracle, o2, PeopleSoft).

Para sistema de horas extras ADMS se realiza una depuración del registro cada dos meses.

Para el sistema de Vault-Autodesk al tener un reporte de fallas se realiza una verificación local con los ingenieros del área, si no hay solución se pone en contacto con el proveedor de Autodesk.

Para los sistemas o servicios ubicados en los servidores Bogotá, Panamá y Brasil se hace un llamado a través del portal Help Desk al personal de ODEBRECHT.

Para los problemas en el servidor de correo y al no tener solución al ser intervenidos por los ingenieros del área se solicita apoyo con un especialista de MICROSOFT.

-Control de préstamos de equipos tecnológicos: Al crecer la demanda de préstamos de equipos tecnológicos se vio la necesidad de llevar un control sobre ellos y para esto se creó una aplicación diseñada por los ingenieros de la empresa donde se ingresaban los ítems que se tenían para hacer el préstamo, en este se registraban todo los datos y para buscarlos solo se miraba si el equipo estaba disponible y de inmediato arrojaba toda la información del préstamo.

-Mantenimiento y reparación de equipos de cómputo: Según las políticas y necesidades de la empresa se tiene un cronograma de mantenimiento para suplir todas las

áreas, el cual se llevan a cabo cada 6 meses y se revisa el Hardware y Software de los equipos.

Procesos de Apoyo

- Gestión de recursos de apoyo

Subprocesos

-Asesoría en el proceso de compra de elementos de T-I al área de patrimonio: Cuando un usuario necesita un elemento o equipo de TI, busca al personal encargado de esa área, el cual se encarga de verificar cuales son los mejores precios, las marcas y las características principales que se necesitan para ese equipo, ya que sin el visto bueno de ellos no se puede realizar la compra.

-Apoyo de contratación de T.I al área de A.P (Administración de Personas): Se apoya al área de contratación realizando una prueba técnica (escrita y practica) para verificar como se desenvuelve la persona frente a casos de la vida diaria.

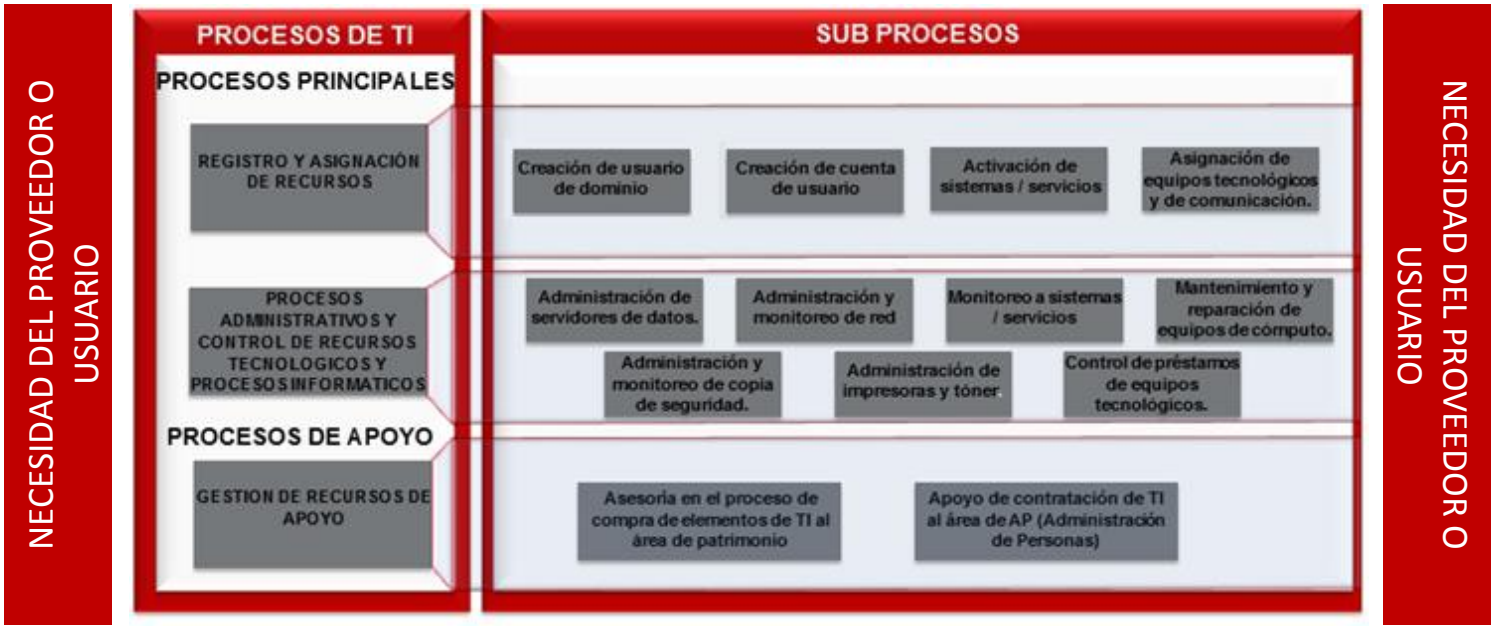


Figura 3. Mapa de Procesos

Fuente. Los Autores.

4.1.2 Identificación y categorización de amenazas, riesgos y vulnerabilidades.

Para este proyecto tomamos como referencia la metodología cualitativa de análisis y gestión de riesgos de seguridad de la información, NIST 800-30.

Guía de gestión de riesgo para los sistemas de Tecnología de la Información

Las organizaciones utilizan la evaluación de riesgos para determinar el alcance de la amenaza potencial y el riesgo asociado con un sistema de tecnología de la información a través del desarrollo del ciclo de vida del sistema. El resultado de este proceso ayuda a identificar los controles adecuados para reducir o eliminar los riesgos durante el proceso de mitigación de los mismos.

La metodología de evaluación de riesgos NIST trabaja bajo nueve pasos principales, que se describen a continuación:

1. Caracterización del Sistema
2. Identificación de amenazas
3. Identificación de vulnerabilidades
4. Análisis de Control
5. Determinación de la probabilidad
6. Análisis de Impacto
7. Determinación de Riesgos
8. Recomendaciones de los controles

9. Documentación de Resultados

Los pasos 2, 3, 4 y 6 se pueden realizar en paralelo después de terminar el 1er paso. La siguiente figura describe los pasos, las entradas y salidas de cada etapa.

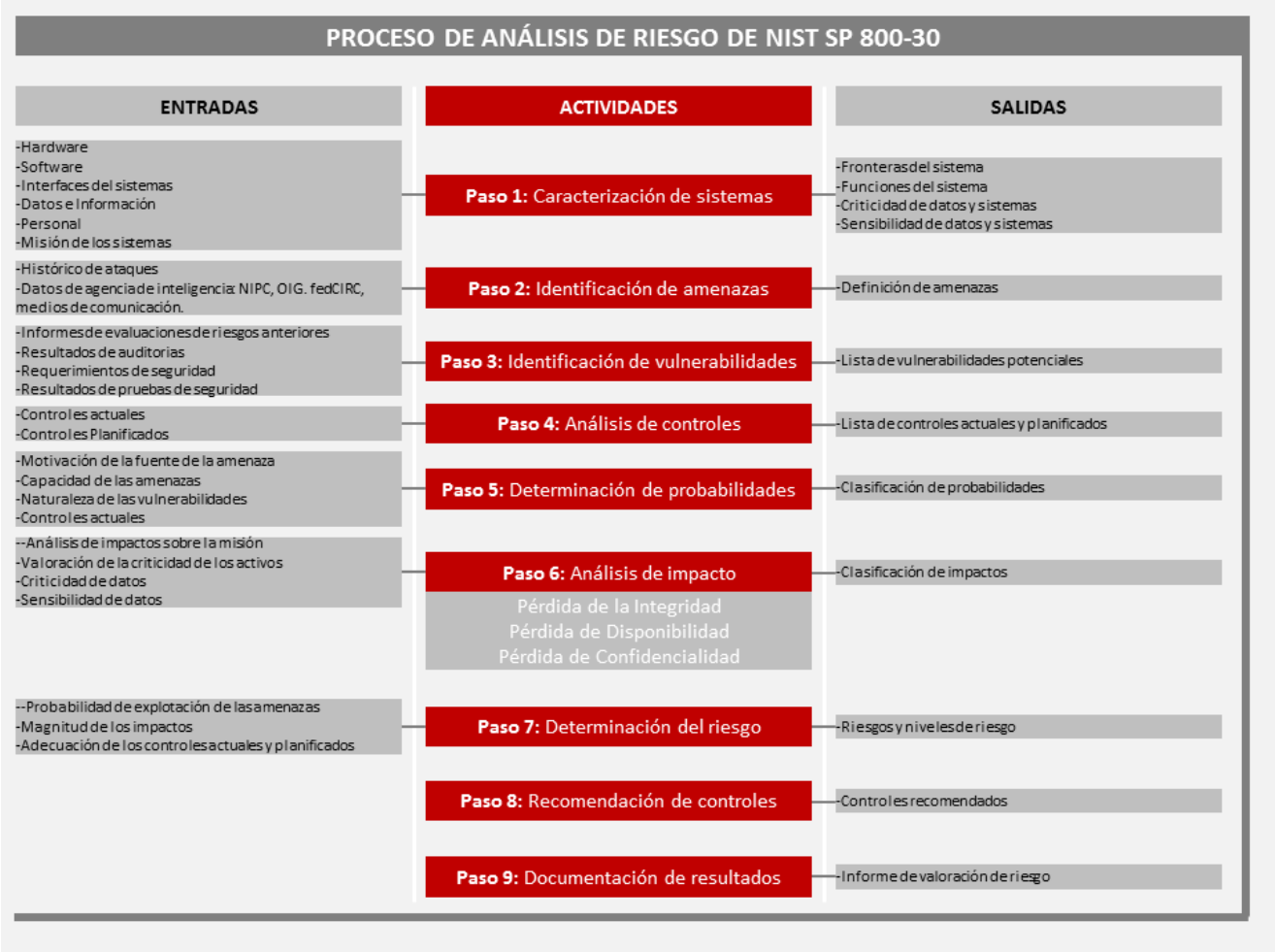


Figura 4. Diagrama de flujo - Metodología de evaluación de riesgos

Fuente. NIST Special Publication 800-30

Los activos a evaluar en la empresa CONSOL ubicados en Aguachica cesar son:

- Dispositivos de cómputo y comunicaciones.

- Información
- Personal

Paso 1: Caracterización del Sistema

Información relacionada con el sistema

El proyecto Ruta del sol Sector 2 a cargo de la empresa Consol abarca una distancia de 528 Kilómetros que va desde Puerto Salgar hasta San Roque, y el contrato adicional de la Transversal Rio de Oro-Aguaclara-Gamarra de 82 Km; cuenta con 2 sedes principales, una ubicadas en Puerto Salgar (Sector sur) y la otra en Aguachica Cesar (Sector Norte). El diseño del Plan de Continuidad del Negocio se encuentra enfocado al sector Norte Aguachica, el cual, cuenta con sistemas y servicios distribuidos así:

Servidores Aguachica:

- Autodesk – Vault: Herramienta para gestionar datos de producto o de proyectos, permite organizar y reutilizar diseños mediante la consolidación de información.
- ADMS: Software para control de ingreso y salida del personal.
- FTP: Transferencia de archivos

Servidores Bogotá:

- Correo Electrónico Consol
- Directorio Activo Consol: Servicio que permite a los administradores establecer políticas a nivel de empresa, desplegar programas en muchos ordenadores y aplicar actualizaciones críticas a la organización, almacenando la información de forma automática entre los servidores.
- FTP: Transferencia de archivos
- Antivirus
- Siseng: Sistema interno para Planificación, Presupuesto y Seguimiento de Obra.
- SGD: Sistema de Gestión Documental.
- Primavera-Oracle: Sistema para gestionar proyectos.

Servidores Panamá:

- O2-Oracle: Sistema de Facturación
- PeopleSoft-Oracle: Gestión de Recursos Humanos

Servidores Brasil:

- Directorio Activo Odebrecht
- Correo Electrónico Odebrecht

A nivel internacional tiene una MPLS “Mecanismo de Transporte de Datos” que conecta a Brasil y Panamá y para Colombia posee otra MPLS encargada de transferir los datos internamente, permitiendo conectar todas las localidades sin necesidad de salir a internet. Esta MPLS conecta a Aguachica, Bogotá, Puerto Boyacá y Lizama, garantizando que el tráfico sea más rápido y que la confiabilidad y estabilidad sea más segura.

En Aguachica Cesar se cuenta con una oficina de TI, que utiliza un Router para el canal de datos para comunicar dentro de la MPLS, este Router se encarga de administrar las direcciones IP que se necesitan para las conexiones.

Se tiene también varios puntos con poco tráfico de información, ubicados en las veredas de Besote, Torcoroma y Platanal, estas cuentan con un dispositivo llamado JUNIPER (Sistema de Seguridad en la Red), que tiene una VPN (Control de comunicaciones) conectada con Bogotá directamente. Para configurar estos dispositivos se necesita una IP publica que se encarga de salir a internet, pasar por varios dispositivos (dependiendo del proveedor) y así llegar hasta Bogotá; también se le asigna una IP local, que garantiza la conectividad y el uso de sus mismos servicios corporativos.

Para el sistema de comunicación entre empleados Consol cuenta con 74 radios de comunicación para la zona montañosa y 1,254 líneas de celulares.

Paso 2: Identificación de amenazas

Histórico de ataques:

La empresa ha sufrido ambientes de protestas por parte de los trabajadores que culminan en bloqueos a las plantas industriales, se han presentado cierres parciales y totales en la vía e impactan el cronograma de obra. (Almario Chávez, 2015).

Una de las instalaciones principales del Consorcio se encuentra ubicado en Aguachica cesar la cual ha sufrido de atentados como papas explosivas detonadas frente a las instalaciones. (Lora García, 2012). Además "En la vía se han presentado quema de maquinaria", (Angarita Parra, 2015, p1).

"La organización no solo se ve afectada por inconvenientes internos, muestra de ello fue el impacto que tuvo el cierre generado por los campesinos del Catatumbo quienes bloquearon un tramo de la ruta del sol", (Morales, 2016, p1).

"En la vereda cerro de los chivos 50 hombres encapuchados paralizaron el tráfico, se presentaron disturbios y enfrentamiento con el ESMAD por más de dos horas". (Bernal, 2013, p1). En otra fecha se presentó bloqueo en la misma vereda la cual queda a 1 Km desde las instalaciones de Consol, donde se bloqueó la vía durante 24 horas obligando a los empleados a evacuar las instalaciones y reanudar actividades luego de día y medio de disturbios, en este punto los campesinos impidieron el paso vehicular y quemaron tres

tractomulas, este disturbio dejo por lo menos 50 personas heridas, la mayoría campesinos y mineros. (Murillo, 2013, p1).

Estas manifestaciones se presentan en el perímetro de los 611 Km que abarca el proyecto Ruta del Sol sector 2, donde se cuentan con estaciones de trabajos para las áreas administrativas ubicadas a lo largo del proyecto como: Puerto Salgar, La Lizama, Besote, Aguachica, Morrison y Pailitas.

Es evidente que a pesar de no presentarse a la fecha ningún tipo de amenaza humada o natural dentro de la empresa o en los puntos donde se encuentran los servidores informáticos y puntos de estación de trabajo critico que puedan poner en riesgo la continuidad del negocio, se evidencia la necesidad de implementar una estrategia que proporcione mecanismos más útiles y adecuados para reaccionar y responder con claridad y fundamento ante un desastre.

Teniendo en cuenta el entorno donde se encuentra ubicada la sede principal del tramo norte de la empresa, y los ataques históricos indicados, las fuentes de amenazas identificadas a través de checklist y observación directa son:

- Amenazas Humanas: delincuencia, allanamiento, sabotaje, robo/hurto, fraude, espionaje, modificación de datos.
- Amenazas Tecnológicas: Accesos no autorizados, Ataques de red, ejecución de software malicioso, fallos en la comunicación, criminales informáticos.

- Amenazas Industriales: Fallos de energía (Sobre carga/baja potencia de electricidad), condiciones inadecuadas de temperatura (Humedad/Incendio) y polvo.
- Amenazas Naturales: Lluvias torrenciales, granizadas y vientos Fuertes.

Tabla 1. Motivaciones y acciones de la amenaza

FUENTE DE AMENAZA	MOTIVOS	AMENAZAS
Amenaza Humana	Vandalismo Intereses económicos Venganza Destrucción infraestructura física Ventaja competitiva Curiosidad Huelga Ego Inteligencia Errores y omisiones no intencionales	Robo de información Robo y destrucción de equipos Actividades fraudulentas Ingeniería social Daños a los activos físicos Asalto a un empleado Soborno
Amenaza Tecnológica	Intereses económicos Venganza Curiosidad Ego Inteligencia Reto Rebelión Ventaja competitiva Espionaje	Hacking Destrucción de Información Divulgación de información Alteración de información Código malicioso Ingeniería Social Acceso no autorizado al sistema Suplantación Penetración al sistema Venta de información Errores del sistema
Amenaza Industrial	Fallos de energía Extremos de temperatura (Incendio/humedad) Polvo	Daños a los activos físicos ,Perdida de información, Errores del sistema, Explosiones Fugas, Derrames

Tabla 1. Continuación

	Lluvias torrenciales	Daños a los activos físicos
Amenaza Natural	Granizadas	Perdida de información
	Vientos Fuertes	Errores del sistema

Fuente. Los Autores.

Nota. La tabla muestra las fuentes de amenazas, los motivos y las amenazas a la cual está sometida la empresa Consol.

Paso 3: Identificación de vulnerabilidades potenciales

Las vulnerabilidades identificadas a través de checklist y observación directa son:

Tabla 2 Vulnerabilidades potenciales en Consol.

VULNERABILIDAD	FUENTE DE AMENAZA	AMENAZA
No existe política y/o medida de soporte de seguridad para el manejo de los riesgos derivados del uso de equipos móviles.	Amenaza Humana y Tecnológica	Por medio de un asalto la información almacenada en este medio puede quedar a disposición de personas para actividades fraudulentas, uso indebido para realizar ingeniería social, soborno, divulgación de información, suplantación, y a través de códigos maliciosos también pueden acceder a dicho dispositivo.
No se realizan capacitaciones sobre la concientización de la seguridad y el adecuado manejo de la información.	Amenaza Humana y Tecnológica	El personal al no tomar conciencia de la importancia de un adecuado manejo de la información puede exponer por error y omisiones no intencionales dicha información de la empresa que puede ser utilizada para actividades fraudulentas, uso indebido para realizar ingeniería social, soborno, divulgación de

Tabla 2. Continuación.

		información y suplantación. Los empleados pueden ejecutar sin conocimiento alguno códigos maliciosos enviados por correos electrónicos y poner a disposición el acceso a criminales informáticos.
No se comunica al empleado que una vez finalizado el contrato permanecerán válidas las responsabilidades y tareas de seguridad de la información a la cual tuvo acceso.	Amenaza Humana	Los ex-empleados por omisión pueden divulgar información que puede ser utilizada para actividades fraudulentas, uso indebido para realizar ingeniería social, soborno, divulgación de información y suplantación.
No existe alarma para detectar humo.	Amenaza Industrial	No hay manera de tener una alerta frente a incidentes que podrían originar un incendio o explosión y así tomar medidas para extinguirlo y evacuar al personal.
No se implementan políticas de escritorio limpio de documentos, medios de almacenamiento removibles y pantalla limpia para la seguridad de la información.	Amenaza Humana	Al tener información expuesta se puede presentar sustracción de información, personal no autorizado que accede a los equipos o a documentación dejada en el escritorio que se expone para robo, destrucción y alteración de información, actividades fraudulentas, soborno.
Equipos de cómputo se encuentran ubicados en el piso de las oficinas.	Amenaza Natural	Daños en los activos físicos por ingreso de lluvia.
Los equipos de cómputo se encuentran expuestos de sufrir algún accidente de caídas libres de objetos pesados.	Amenaza Humana	Daños a los activos físicos.

Tabla 2. Continuación.

Las copias de seguridad de algunos servidores se almacenan en el mismo lugar de los servidores copiados.	Amenaza Humana, Natural, Industrial y Tecnológica	Al sufrir algún tipo de incidente en los servidores también estarían en riesgo los Backups, y no se tendría el respaldo de la información.

Fuente. Los Autores.

Nota. La tabla muestra las vulnerabilidades, fuentes de amenazas y las amenazas a la cual está sometida la empresa Consol.

Prueba de sistemas de seguridad

Se realizó alrededor de hace 3 años un escaneo general de la red identificando los software instalados no permitidos en los equipos de cómputo de la empresa.

Se han realizado escaneo de red por parte de la empresa Odebrecht a los equipos que se encuentran dentro de la MPLS internacional (MultiProtocol Label Switching) solo a los equipos con dominio Odebrecht que se encuentran dentro de la empresa Consol, estos equipos representan el 10% del total, este escaneo identifica el cumplimiento de antivirus, Script, entre otros.

La empresa Autodesk (Compañía dedicada al software de diseño en 2D Y 3d) realiza escaneo aleatorio para verificar el cumplimiento de sus licencias.

Desarrollo de checklist de requerimientos de seguridad

A continuación se presenta una lista de verificación de requisitos de seguridad con los estándares de seguridad básicos que se pueden utilizar para sistemáticamente evaluar e identificar las vulnerabilidades de los activos, procedimientos no automatizados, procesos y transferencias de información asociados a las siguientes áreas de seguridad:

- Administración
- Operacional
- Técnica

Tabla 3. Requisitos y estándares de Seguridad

ÁREA DE SEGURIDAD	CRITERIO DE SEGURIDAD
Administración	• Capacitación seguridad de la información • Capacitación de las responsabilidades del ex-empleado
Operacional	• Control de temperatura
Técnica	• Detección de intrusiones • Auditoria del sistema • Política de seguridad para los equipos móviles

Fuente. Los Autores

Nota. La tabla muestra una lista de verificación de requisitos de seguridad con los estándares de seguridad básicos, que se pueden usar para evaluar e identificar las

vulnerabilidades de los activos, procedimientos no automatizados, procesos y transferencias de información asociados a las áreas de seguridad.

Paso 4: Análisis de controles

Métodos de control

El Consorcio Constructor Ruta del Sol cuenta con los siguientes controles:

- No técnicos en sus procedimientos como: Políticas de seguridad, control en la compra de equipos tecnológicos y sus elementos, seguridad en el ingreso y salida de las instalaciones físicas y control de desechos tecnológicos.

- En controles técnicos cuenta con: para el hardware se maneja tarjeta de responsabilidad y placa de bien patrimonial y en software se maneja asignación de perfiles para acceder a equipos y servidores con cambios periódicos de contraseña, antivirus, cifrado de correo electrónico para gerentes, segmentación de la red por medio de Vlans, control de tráfico para entrar y salir de internet por medio de Juniper y copias de seguridad periódicas en servidores.

Tabla 4. Categorías de control

N°	DESCRIPCIÓN DEL CONTROL	CATEGORÍA	
		Preventivos	**Detección**
1	Políticas de Seguridad.	**X**	
2	Control en compra de equipos tecnológicos y sus elementos.	**X**	
3	Seguridad en el ingreso y salida de las instalaciones físicas.	**X**	
4	Control de desechos tecnológicos.	**X**	
5	Tarjeta de responsabilidad	**X**	
6	Asignación de perfiles	**X**	
7	Cambios periódicos de contraseña	**X**	
8	Antivirus		**X**
9	Cifrado de correo (Gerencia)	**X**	
10	Segmentación de la red	**X**	
11	Control de tráfico de internet a través de Juniper		**X**
12	Copias de seguridad periódicas en servidores	**X**	
13	Control de Bloqueo en Impresiones	**X**	

Fuente. Los Autores.

Nota. La tabla muestra las diferentes categorías de control que se aplican en Consol.

Técnicas de análisis de control

La empresa identifica el cumplimiento de los controles a través de la observación o reporte de algún incidente validando el incumplimiento de algún procedimiento.

Paso 5: Determinación de probabilidades

Existen factores que permite obtener una calificación de verosimilitud global que indique la probabilidad de que una vulnerabilidad potencial puede ejercerse dentro del entorno de amenaza.

- Motivación y capacidad de la fuente de amenaza
- Naturaleza de la vulnerabilidad
- Existencia y efectividad de los controles actuales.

La probabilidad de que una vulnerabilidad potencial pueda ser ejercida por una fuente de amenaza determinada puede ser clasificada como alto, medio o bajo.

Tabla 5. Niveles de probabilidad

NIVEL	DEFINICIÓN DE LA PROBABILIDAD
ALTA	La fuente de la amenaza está altamente motivada y capaz, los controles para prevenir las vulnerabilidades son ineficaces.
MEDIA	La fuente de la amenaza está motivada, pero hay controles que dificultan el ejercicio exitoso de la vulnerabilidad.
BAJA	La fuente de amenaza carece de motivación o capacidad, o los controles previenen, o por lo menos obstaculizan significativamente la vulnerabilidad de ser ejercida.

Fuente. NIST Special Publication 800-30

Nota. La siguiente tabla describe los tres niveles de probabilidad indicadas por la metodología NIST. (Stoneburner, Goguen, Feringa 2002, p, 21).

Paso 6: Análisis de impacto

Se determinará los efectos adversos resultantes al potencializarse una amenaza.

Algunos impactos tangibles se pueden medir cuantitativamente, otros no se pueden medir en unidades específicas, pero pude ser calificado en términos de alta, mediana o bajo impacto como se representa en la siguiente tabla según la metodóloga NIST, la principal ventaja del análisis del impacto cualitativo es la mejora en el tratamiento de las vulnerabilidades.

Este análisis prioriza los niveles de impactos asociados con el compromiso de los activos de información de una organización basados en una evaluación cualitativa o cuantitativa de la sensibilidad y criticidad de dichos activos, una evaluación de la criticidad de los activos identifica y prioriza la información sensible y critica de la organización.

Tabla 6. Magnitud de impacto.

NIVEL	DESCRIPCIÓN DEL IMPACTO
ALTA	La vulnerabilidad ejercida: 1. Puede resultar en la pérdida de un alto costo de los principales activos tangibles o recursos 2. De manera significativa puede violar, dañar, o impedir la misión de una organización, la reputación o los intereses 3. Puede resultar en la muerte humana o lesiones graves.
MEDIA	La vulnerabilidad ejercida: 1. Puede resultar en la pérdida costosa de activos materiales o recursos 2. Pueda violar, dañar, o impedir la misión de una organización, la reputación o los intereses 3. Puede resultar en lesiones.

Tabla 6. Continuación.

BAJA	La vulnerabilidad ejercida: 1. puede resultar en la pérdida de algunos bienes, materiales o recursos 2. Puede afectar notablemente la misión de una organización, la reputación o los intereses.

Fuente. NIST Special Publication 800-30

Nota. la tabla muestra la definición de la magnitud del impacto.

Además, se han establecido Tiempo de Repuesta RTO (Recovery Time Objective): Es el tiempo transcurrido entre una interrupción y la recuperación del servicio, este indica el tiempo disponible para recuperar el sistema y los recursos interrumpidos.

Tabla 7. Tiempo de Respuesta

NIVEL	RTO
ALTA	5 horas
MEDIO	24 horas
BAJO	72 o más horas

Fuente. Los Autores

Nota. La tabla muestra el nivel y el tiempo de recuperación.

Y se estableció un Punto de objetivo de recuperación RPO (Recovery Point Objective):

Es el rango de tolerancia que la empresa puede tener sobre la perdida de datos y el evento de desastre.

Tabla 8. Punto de Recuperación

NIVEL	RPO
ALTA	4 horas
MEDIO	10 horas
BAJO	24 o más horas

Fuente. Los Autores.

Nota. La tabla muestra el nivel y el punto de recuperación.

Paso 7: Determinación del riesgo

Determinación de la matriz de nivel de riesgo

La siguiente matriz es una matriz 3x3 de probabilidad de amenaza (Alto, medio y bajo]) y el impacto de la amenaza (Alto, medio y bajo).

La matriz en la siguiente tabla muestra como los niveles de riesgo global de alto, medio y bajo. Se asigna la probabilidad para cada nivel de probabilidad y un valor para cada nivel de impacto, por ejemplo para la probabilidad asignada para cada nivel de probabilidad es: 1.0 para alto, 0.5 para medio y 0.1 para bajo, y el valor asignado para cada nivel de impacto es 100 para alto, 50 para medio y 10 para bajo como se evidencia en la siguiente tabla:

Tabla 9. Niveles de riesgo

PROBABILIDAD DE LA AMENAZA	**IMPACTO**		
	Bajo (10)	Medio (50)	Alto (100)
Alto (1,0)	**BAJO** 10X1.0=10	**MEDIO** 50X1.0=50	**ALTO** 100X1.0=100
Medio (0.5)	**BAJO** 10X0.5=5	**MEDIO** 50X0.5=25	**MEDIO** 100X0.5=50
Bajo (0.1)	**BAJO** 10X0.1=1	**BAJO** 50X0.1=5	**BAJO** 100X0.1=10

Fuente. NIST Special Publication 800-30

Nota. La tabla muestra el impacto y la probabilidad de la amenaza y a su vez los tipos de niveles de riesgos: escala de riesgo, se multiplica el valor que tiene la probabilidad con el valor que tiene el impacto de la amenaza, se estipulan los siguientes rangos de riesgo: Alta (>50 a 100), Medio (>10 a 50), Bajo (1 a 10).

Descripción del nivel de riesgos

Acá describiremos los niveles de riesgos indicados en la matriz anterior, esta escala de riesgo, con sus calificaciones de Alto, Medio y Bajo representa el grado o nivel de riesgo al que un sistema, instalación o procedimiento podría exponerse si una vulnerabilidad determinada se materializa.

Tabla 10. Descripción de riesgos y acciones necesarias

NIVEL	DESCRIPCIÓN DEL RIESGO Y ACCIONES NECESARIAS
Alta	Si una observación o hallazgo se evalúa como Alto Riesgo, existe una gran necesidad de medidas correctivas. Un sistema existente puede seguir funcionando, pero un plan de acción correctiva debe ser puesto en marcha lo antes posible.
Media	Si una observación es clasificada como Riesgo Medio, se necesitan acciones correctivas y se debe desarrollar un plan para incorporar estas acciones dentro de un período de tiempo razonable.
Baja	Si una observación se describe como Bajo Riesgo, se debe determinar si aún se requieren acciones correctivas o decidir aceptar el riesgo.

Fuente. NIST Special Publication 800-30

Nota. La tabla muestra los niveles de riesgos con su respectiva descripción y las acciones necesarias a implementar.

Evaluación del riesgo

Una vez identificada las amenazas, las fuentes de estas amenazas, las vulnerabilidades potenciales, los controles implementados por la empresa que aplican a cada vulnerabilidad, la probabilidad de ocurrencia y el grado de impacto al potencializarse una amenaza, se determina y evalúa el riesgo que tendría la empresa al materializarse dicha vulnerabilidad.

A través de la siguiente herramienta de control y gestión denominada matriz de riesgo identificamos de manera temprana aquello que amenaza el cumplimiento de los objetivos de la empresa e identificamos las actividades que requieren mayor atención y las áreas críticas de riesgo, cruzamos las amenazas, vulnerabilidades identificadas y los controles para que con esta herramienta determinemos el estado de la empresa con respecto al riesgo.

N	Vulnerabilidad	Fuente de amenaza	Amenaza	Control	Probabilidad de Ocurrencia		Impacto				Riesgo		Descripción nivel del riesgo
					Nivel	Valor	Nivel	Valor	RTO	RPO	Nivel	Valor	
1	No existe política y/o medida de soporte de seguridad para el manejo de los riesgos derivados del uso de equipos móviles.	Amenaza Humana y tecnológica	Por medio de un asalto la información almacenada en este medio puede quedar a disposición de personas para actividades fraudulentas, uso indebido para realizar ingeniería social, soborno, divulgación de información, suplantación, y a través de códigos maliciosos también pueden acceder a dicho dispositivo.	-	ALTO	1.0	ALTO	100	ALTO 5 Horas	ALTO 4 Horas	ALTO	100	Si una observación o hallazgo se evalúa como Alto Riesgo, existe una gran necesidad de medidas correctivas. Un sistema existente puede seguir funcionando, pero un plan de acción correctiva debe ser puesto en marcha lo antes posible.
2	No se realizan capacitaciones sobre la concientización de la seguridad y el adecuado manejo de la información.	Amenaza Humana y tecnológica	El personal al no tomar conciencia de la importancia de un adecuado manejo de la información puede exponer por error y omisiones no intencionales dicha información de la empresa que puede ser utilizada para actividades fraudulentas, uso indebido para realizar ingeniería social, soborno, divulgación de información y suplantación. Los empleados pueden ejecutar sin conocimiento alguno códigos maliciosos enviados por correos electrónicos y poner a disposición el acceso a criminales informáticos.	6,7,8 Y 9	MEDIO	0.5	ALTO	100	ALTO 5 Horas	ALTO 4 Horas	MEDIO	50	Si una observación es clasificada como Riesgo Medio, se necesitan acciones correctivas y se debe desarrollar un plan para incorporar estas acciones dentro de un período de tiempo razonable.
3	No se comunica al empleado que una vez finalizado el contrato permanecerán válidas las responsabilidades y tareas de seguridad de la información a la cual tuvo acceso.	Amenaza Humana	Los ex empleados por omisión pueden divulgar información que puede ser utilizada para actividades fraudulentas, uso indebido para realizar ingeniería social, soborno, divulgación de información y suplantación.	-	ALTO	1.O	ALTO	100	ALTO 5 Horas	ALTO 4 Horas	ALTO	100	Si una observación o hallazgo se evalúa como Alto Riesgo, existe una gran necesidad de medidas correctivas. Un sistema existente puede seguir funcionando, pero un plan de acción correctiva debe ser puesto en marcha lo antes posible.

Figura 5. Matriz de Riesgo

N	Vulnerabilidad	Fuente de amenaza	Amenaza	Control	Probabilidad de Ocurrencia		Impacto				Riesgo		Descripción nivel del riesgo
					Nivel	Valor	Nivel	Valor	RTO	RPO	Nivel	Valor	
4	No existe alarma para detectar humo.	Amenaza Humana	No hay manera de tener una alerta frente a incidentes que podrían originar un incendio o explosión y así tomar medidas para extinguirlo y evacuar al personal.	-	ALTO	1.0	ALTO	100	ALTO 5 Horas	ALTO 4 Horas	ALTO	100	Si una observación o hallazgo se evalúa como Alto Riesgo, existe una gran necesidad de medidas correctivas. Un sistema existente puede seguir funcionando, pero un plan de acción correctiva debe ser puesto en marcha lo antes posible.
5	No se implementan políticas de escritorio limpio de documentos, medios de almacenamiento removibles y pantalla limpia para la seguridad de la información.	Amenaza Humana	Al tener información expuesta se puede presentar sustracción de información, personal no autorizado que accede a los equipos o a documentación dejada en el escritorio que se expone para robo, destrucción y alteración de información, actividades fraudulentas, soborno.	-	ALTO	1.0	ALTO	100	ALTO 5 Horas	ALTO 4 Horas	ALTO	100	Si una observación o hallazgo se evalúa como Alto Riesgo, existe una gran necesidad de medidas correctivas. Un sistema existente puede seguir funcionando, pero un plan de acción correctiva debe ser puesto en marcha lo antes posible.
6	Equipos de cómputo se encuentran ubicados en el piso de las oficinas.	Amenaza Natural	Daños en los activos físicos por ingreso de lluvia.	-	ALTO	1.0	MEDIO	50	MEDIO 24 Horas	MEDIO 10 Horas	MEDIO	50	Si una observación es clasificada como Riesgo Medio, se necesitan acciones correctivas y se debe desarrollar un plan para incorporar estas acciones dentro de un período de tiempo razonable.
7	Los equipos de cómputo se encuentran expuestos de sufrir algún accidente de caídas libres de objetos pesados.	Amenaza Humana	Daños a los activos físicos.	-	ALTO	1.0	MEDIO	50	MEDIO 24 Horas	MEDIO 10 Horas	MEDIO	50	Si una observación es clasificada como Riesgo Medio, se necesitan acciones correctivas y se debe desarrollar un plan para incorporar estas acciones dentro de un período de tiempo razonable.
8	Las copias de seguridad de algunos servidores se almacenan en el mismo lugar de los servidores copiados.	Amenaza Natural, Humana, tecnológica e Industrial.	Al sufrir algún tipo de incidente los servidores también estarían en riesgo los backups, por lo tanto no se tendría el respaldo de la información.	-	ALTO	1.0	ALTO	100	ALTO 5 Horas	ALTO 4 Horas	ALTO	100	Si una observación o hallazgo se evalúa como Alto Riesgo, existe una gran necesidad de medidas correctivas. Un sistema existente puede seguir funcionando, pero un plan de acción correctiva debe ser puesto en marcha lo antes posible.
Clasificación del riesgo del proyecto											ALTO	81.75	

Figura 5. Continuación

Fuente. Los Autores

Se concluyó que la clasificación del riesgo general del proyecto es de 81.75 que según la escala de riesgo es categoría Alta.

Paso 8: Recomendaciones de control

La meta de las recomendaciones de control es reducir el nivel de riesgo identificado, es necesario tener en cuenta los siguientes factores:

- Implementar política y/o medida de seguridad para el manejo de riesgo en el uso de equipos móviles.
- Socializar y certificar que los empleados conocen y acatan plenamente que una vez finalizado el contrato permanecerán válidas las responsabilidades y tareas de seguridad de la información a la cual tuvo acceso.
- Implementar alarma contra incendios.
- Diseñar e implementar programas de capacitación y concientización en las personas sobre la importancia de mantener un escritorio limpio de documentos y el escritorio del equipo de cómputo limpio de carpetas y/o documentos importantes, que los empleados al retirarse de su puesto de trabajo siempre bloqueen sus equipos para evitar acceso de personas externas.
- Almacenar los backups o respaldo de la información en un lugar seguro, ajeno y exterior a la empresa.
- Capacitar al personal sobre la concientización de la seguridad y el adecuado manejo de la información.

- Socializar al empleado la importancia de no abrir correos de remitentes desconocidos o con archivos adjuntos sospechosos e informar inmediatamente al responsable del área de TI.
- Ubicar las torres de los equipos de cómputo en una zona segura libre de incidentes, caídas de objetos pesados o amenazas naturales e informar al personal su importancia.
- Realizar ataques de seguridad constantes provocados por la empresa para chequear constancia y robustez en los servidores que contienen la información.
- Verificar y hacer pruebas periódicas de las copias de seguridad.

Paso 9: Documentación y resultados

El presente informe tiene como objetivo presentar el resultado del análisis de riesgo según la metodología NIST realizado a la empresa CONSOL de Aguachica cesar, Los resultados se presentan con el propósito de identificar situaciones frecuentes y recurrentes que afecta el cumplimiento de los requisitos y controles, para que a partir de ellos los responsables de los procesos formulen acciones de mejora preventivas y correctivas que permitan superarlas de manera eficiente y eficaz en aras del mejoramiento continuo, con este análisis de riesgos identificados se recomienda al área administrativa y gerencial determinar un plan para priorizar las actividades a realizar a partir del análisis acá documentado asignando responsabilidades como lo vea conveniente referente al personal con el que cuenta la empresa.

4.2 Elaboración del plan de continuidad del negocio.

El desarrollo del presente plan toma como referencia la investigación, análisis y comparación de estándares como **ISO/IEC 27001:2005, ISO 27002:2007, NTC 5722, NIST 800-34, NFPA1600:2010 Y ASIS SPC.1:2009** realizada por el Ing. Juan Jose Ortiz vega de la Universidad de Buenos aires, quien desarrollo una guía para la elaboración del plan de continuidad basada en un cuadro comparativo entre las normativas antes nombradas, se utilizó como referencia para establecer un modelo tomando los elementos presentes en dichas normas e identificando las mejores acciones a tomar para la elaboración del plan de continuidad del negocio.

Algunas normativas conocidas existentes para establecer un Plan de Continuidad del Negocio son:

- NIST 800-34 (Contingency Planning Guide for Information Technology Systems)
- ISO27001 (Tecnología de la Información – Técnicas de seguridad – Sistemas de gestión de seguridad de la información – Requerimientos).
- ISO27002 (Tecnología de la información - Código de buenas prácticas para la gestión de la seguridad de la información).
- NTC 5722 (Norma Técnica Colombiana 5722 Gestión De La Continuidad Del Negocio Requisitos).
- NFPA1600:2010 (Standard on Disaster/Emergency Management and Business Continuity Programs).
- ANSI ASIS SPC.1-2009 (Organizational Resilience: Security, Preparedness, And continuity management systems –Requirements with guidance for use)

Para la elaboración de este plan tomamos como referencia la técnica desarrollada por el Dr. Williams Edwards Deming, que se centra en la mejora continua de los procesos de la organización y se basa en 4 fases que ayudan a la evolución adecuada de los procesos de implementación de cualquier proyecto. (Jimeno Bernal, 2013)

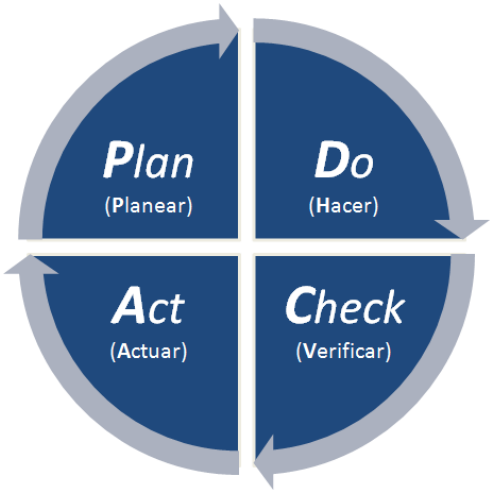


Figura 6. Ciclo PDCA

Fuente. http://www.pdcahome.com/5202/ciclo-pdca/

Las siglas de este ciclo PDCA corresponden a las palabras en inglés, Plan, Do, Check, Act, y en español Planear, Hacer, Verificar, Actuar.

Se toma como referencia elaborar el Plan de Continuidad bajo las cuatro etapas de desarrollo planteadas en el cuadro comparativo de las normas (Anexo 2).

Etapa 1. **Análisis del negocio y evaluación de riesgos potenciales y vulnerabilidades:** Según el ciclo Deming esta es la etapa de Planeación (PLAN). En esta etapa se identificó de

manera detallada como es la organización, las amenazas, riesgos potenciales y vulnerabilidades a los cuales está expuesto. Esta etapa se desarrolló en el capítulo 4.1.2.

Etapa 2. Estrategias para la continuidad y creación de políticas: En esta etapa se definieron las estrategias y políticas, según el ciclo Deming es la etapa Hacer (DO).

Etapa 3. Desarrollo del plan de Continuidad: luego de definir las políticas y las estrategias se desarrolla el BCP (Plan de Continuidad del Negocio) y en el ciclo de Deming es la etapa Hacer (DO).

Etapa 4. Pruebas y Mantenimiento: Según el ciclo Deming es la etapa de Verificar (Check) y Actuar (ACT), se toman los procesos realizados durante el ciclo de vida de las actividades del Plan y se verifica lo realizado, luego se toman los resultados obtenidos y se plantean los cambios para la mejora continua de la organización y del Plan de Continuidad del Negocio.

DESARROLLO DE ETAPAS

Etapa 1. Análisis del negocio y evaluación de riesgos potenciales y vulnerabilidades

Esta etapa se desarrolló en el capítulo 4.1.2

Etapa 2. Estrategias para la continuidad y creación de políticas

Con el fin de mantener, restaurar las operaciones y garantizar la seguridad de la información a un nivel aceptable y en las escalas de tiempo requeridas después de cualquier

interrupción se crean estrategias, planes y controles preventivos acordes a las necesidades de la empresa, estas son:

-Definir objetivo y alcance del Plan

-Definir roles funciones/responsabilidades, y personal de apoyo.

-Activación y desactivación del Plan

-Definir procesos y estrategias de recuperación (Acuerdos de continuidad con terceros, establecer lugares alternos para dar estabilidad a las operaciones.

- Objetivos y alcance del Plan de Continuidad del Negocio

Se definen los objetivos y alcance del Plan de Continuidad del negocio con el fin de determinar de manera detallada las actividades a cubrir en caso de emergencia y garantizar en su ejecución la continuidad del negocio.

Objetivos del Plan de Continuidad del Negocio en caso de interrupción:

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

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

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

Alcance del Plan de Continuidad del Negocio en caso de interrupción:

El diseño de este plan solo contempla el área de Tecnologías e información del proyecto Ruta del Sol – Sector 2.

- Definición de funciones, responsabilidades y personal de apoyo.

Personal de apoyo

Es importante conocer cuáles son las personas o áreas que intervienen en las actividades más importantes de la empresa, con el objetivo de ubicar de manera adecuada a este personal en los lugares apropiados para garantizar que con sus conocimientos se podrán mantener en continuidad y funcionamiento las actividades de la empresa.

Para la eficacia de este plan se debe contar con el apoyo del Responsable Administrativo, Gerente Administrativo, Responsable de Seguridad Física y Responsable de Salud y Seguridad en el trabajo, reservas financieras, socialización previa del Plan de Continuidad con el fin de dar a conocer funciones y responsabilidades y mantener comunicación con contactos clave, todos los involucrados deben estar conscientes de todas las actividades a realizar para mitigar las amenazas y riesgos que lograrán una recuperación del negocio de forma rápida y efectiva.

COMITÉS, FUNCIONES Y RESPONSABILIDADES (RESPONSABLES DE LA GESTIÓN DE INCIDENTE)

Se crean responsables de procesos, funciones en la continuidad y personal autorizado para realizar ciertas actividades en caso de presentarse un incidente perjudicial, estas responsabilidades son:

Responsable de la ejecución del Plan de Continuidad del Negocio.

Responsable de T.I – Yuly Paola Contreras Contreras

FUNCIONES Y RESPONSABILIDADES:

-Aprobar el Plan de Continuidad del Negocio.

-Comunicar y gestionar autorización por parte de las directivas los costos para los gastos necesarios y el cronograma para la restauración del ambiente de trabajo.

-Socializar el plan al personal involucrado.

-Dirigir los comunicados de apoyo en la ejecución del Plan de Contingencia a los directivos y responsables de áreas.

-Realizar reuniones periódicas informando actualización o cambios efectuados en el plan original.

-Seguimiento a las pruebas del correcto funcionamiento por lo menos dos veces al año o en el proceso de presentarse cambios que se ameriten.

-Detectar situación que represente riesgo y activar el estado de contingencia y ejecución del Plan de Continuidad.

-Autorizar el procedimiento a seguir en la ejecución del Plan, tomar decisiones correspondientes a la definición de las ubicaciones para instalar los equipos de cómputo alternos.

-Mantener actualizado el directorio de proveedores de servicios con los que cuenta la empresa.

-Dar reporte de los resultados y la evolución del plan de continuidad a las personas involucradas.

-Definir con las áreas correspondientes cuales son los sistemas de información, módulos y/o procedimientos de carácter crítico de la empresa.

-Desactivar el estado de contingencia

Coordinador de Servidores y Sistemas/Servicios

Ingeniero- Gabriel Pabón

-Realizar conexión y pruebas de los equipos de cómputo alternos en el tiempo que se considere necesario.

-Realizar la restauración y conexión alterna de Sistemas/Servicios de la empresa.

- Si se presenta contingencia que afecte a los equipos de cómputo y software es el responsable de restablecer dicho servicio en el menor tiempo posible.

Figura 7. Rol, Funciones y responsabilidades.

Figura 7. Continuación.

Fuente. Los Autores

- Activación y desactivación del Plan

Para activar el Plan de Continuidad del Negocio es necesario detectar una situación que represente riesgo, como las indicadas en la Matriz de Riesgo (Ver Figura 5) e informar al personal involucrado el estado activo de contingencia y ejecutar el Plan, de igual manera, informar cuando a su juicio esa circunstancia que provocaron activar el estado de contingencia desaparezca y se esté en condiciones de continuar con las actividades normalmente, el responsable de la ejecución del Plan de Continuidad del Negocio deberá decidir si se desactiva o se continua en estado activo el Plan luego de realizar una evaluación de la situación.

- Procesos y estrategias de recuperación

Establecer estrategias que no afecten la actividad en los lugares de trabajo, siendo así, la mejor alternativa es elegir lugares alternos y/o acuerdos con terceros que ayudan a la continuidad de las operaciones estableciendo un nuevo centro de operaciones en el menor tiempo.

Es necesario conocer que acciones hay que realizar y como realizarlas en caso de presentarse una situación que paralice y afecte uno o varios procesos de negocio del área de TI.

Se analiza y estudian las alternativas para lograr la recuperación en el tiempo necesario indicado en el Análisis de Impacto del Negocio.

Las diferentes alternativas de estrategias en caso de una situación que se considere crítica y/o con tiempo de recuperación larga consideradas por la norma NIST son:

Hot site, wam site, cold site, mirror, site, sitios móviles y acuerdos recíprocos con otras organizaciones

La empresa debe considerar los costos de tener un lugar alterno y estudiar en detalle la capacidad económica que poseen en la actualidad para adquirir o arrendar sedes donde puedan llevar a cabo la continuidad del negocio.

Tabla 11. Criterios de selección de sitio alterno

SITIO	COSTO	EQUIPO DE HARDWARE	TELECOMUN I-CACIONES	TIEMPO DE PREPARACIÓN	UBICACIÓN	DESCRIPCIÓN
Cold Site (Sitio Frío)	Bajo	Ninguno	Ninguno	Largo	Fijo	Es una segunda ubicación que contiene los elementos físicos para establecer un centro de procesamiento si fuera necesario (cableado eléctrico, aire acondicionado, etc.), pero que no contiene ni las máquinas ni los componentes hardware necesarios para poder levantar los servicios en caso de desastre
Warm Site (Sitio cálido)	Medio	Parcial	Parcial/Full	Medio	Fijo	Es una segunda ubicación de procesamiento, con una configuración adecuada pero que no está suficientemente actualizada como para poder restaurar los servicios sin perder datos. Por tanto, sería necesaria una actualización antes de proceder a una restauración de los servicios en este centro de procesamiento. Los costes son elevados, pero menores que para el Hot Site, ya que el mantenimiento y las pruebas se realizan con menor frecuencia.
Hot Site (Sitio Caliente)	Medio/Alto	Completo	Completo	Corto	Fijo	Es una segunda ubicación de procesamiento que está configurado y suficientemente actualizado como para poder restaurar los servicios correctamente tan sólo unas pocas horas después de la ocurrencia de la interrupción de dichos servicios. Los costes son elevados, pero permiten alcanzar los tiempos establecidos en el BIA casi con seguridad. Los costes podrían ser: Coste básico de suscripción. Cuotas mensuales. Cargos de pruebas. Costes de activación (emergencia real). Cargos por uso por hora o por día (dependiendo del proveedor).
Mobile Site (Sitio Móvil)	Alto	Dependiente	Dependiente	Dependiente	No fijo	Es una segunda ubicación móvil, por ejemplo un remolque, que contiene los elementos necesarios para instalar un centro de procesamiento alternativo. Pueden ser útiles en caso de desastre expandido para constituir áreas de trabajo donde situar PCs y terminales de trabajo.

Tabla 11. Continuación

SITIO	COSTO	EQUIPO DE HARDWARE	TELECOMUNI-CACIONES	TIEMPO DE PREPARACIÓN	UBICACIÓN	DESCRIPCIÓN
Mirror Site (Sitio espejo)	Alto	Completo	Completo	Ninguno	Fijo	Es una segunda ubicación con los recursos necesarios, correctamente configurados y actualizados, donde se realizan las distintas transacciones de cada servicio en paralelo con el centro de procesamiento principal. Esta alternativa supone la necesidad de realizar pruebas periódicas que garanticen la sincronía entre el centro principal y el de respaldo. Debe existir también una correspondencia equitativa de capacidad de trabajo entre ambos centros. Se trata de una alternativa muy costosa, además de ser muy necesario el uso de recursos informáticos y de personal que garanticen la viabilidad de este método.

Fuente. NIST Special Publication 800-34

Acuerdos recíprocos con otras organizaciones: Son acuerdos suscritor con otra empresa (Normalmente se encuentra cerca geográficamente) para proveerse mutuamente de tiempo de CPU e incluso de espacio para poder instalar a algunos trabajadores de forma temporal después de una contingencia.

Este método supone una dificultad de conseguir una configuración y actualización adecuada para poder reanudar los servicios críticos al poco de producirse dicho desastre. El costo de esta alternativa sería el más bajo de todas las presentadas en la metodología NIST.

Estrategia de recuperación elegida:

Luego de analizar con la responsable del área de T.I las estrategias consideradas por la norma NIST y las opciones empresariales se tomó la decisión que llegado el caso de presentarse una situación que se considere crítica, con tiempo de recuperación larga y/o afecte de manera directa las funciones principales se tomará como referencia la alternativa del Warm Site y/o Hot Site; este lugar alternativo no tendría ningún costo de suscripción, cuotas mensuales, cargos por uso, etc., ya que estos puntos serían propios de la empresa, ubicados geográficamente en las veredas de Lizama, Besote, Torcoroma, Platanal y/o Puerto Boyacá, por lo tanto se tendría una ubicación de procesamiento con una configuración adecuada para lograr restaurar los servicios correctamente tan solo a unas pocas horas después de presentarse alguna interrupción sin costo alguno.

La responsable del área de T.I considera importante implementar estas opciones con el fin de tener un lugar alternativo y brindar a los puntos de trabajo como Lizama, Besote, Torcoroma, Platanal y/o Puerto Boyacá su punto alternativo en Aguachica, es decir aprovechar que la empresa tiene varios puntos de trabajo distribuidos en el Departamento para implementar un plan B entre la empresa sin tener costo y con su propia estructura de telecomunicaciones, también informa que una vez restaurada la actividad laboral en el proyecto Ruta del Sol se estudiara e implementara la opción de Mirror Site (Sitio espejo) aprovechando que se tiene varios opciones de ubicación alterna con los recursos necesarios correctamente configurados para lograr realizar las transacciones de cada servicio en paralelo con el centro de procesamiento principal Aguachica, y asignar al coordinador de servidores y sistemas/servicios la realización de pruebas periódicas que garantice la sincronía entre Aguachica y el de respaldo e implementar en aquellos lugares su lugar alternativo en Aguachica.

Se recomienda identificar y establecer con el área de Transporte el equipo necesario para transportar al personal al punto establecido para continuar con las funciones de la empresa.

También, es importante diseñar y definir los protocolos a seguir en caso de presentarse una situación de contingencia que abarque su recuperación en un menor tiempo, se recomienda implementar y socializar los siguientes procedimientos dependiendo de la situación:

Proceso general:

Como prioridad debemos salvaguardar la vida propia y de los compañeros de trabajo, luego, dentro de lo posible es necesario identificar el lugar que origina la emergencia con el fin de ser controlado (si se está en capacidad de hacerlo y no afecte la vida propia o de alguien más)

e informar al área de seguridad física la situación presentada, ellos, según su procedimiento se encargarán de solicitar apoyo a las personas o entidades correspondientes.

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

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

Con el fin de conocer el procedimiento a seguir para cada caso específico, definimos las siguientes situaciones de emergencia que se pueden presentar para el área de T.I: Movimiento telúrico (temblor), Incendio, inundación y/o humedad, interrupción de energía, falla en el servicio de red/Voz, acceso no autorizado a la información lógica, acceso físico no autorizado a las oficinas de T.I, marchas pacíficas, marchas no pacificas o cierre de vía.

- Movimiento telúrico (temblor):

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

Medidas preventivas:

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

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

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

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

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

Durante la situación:

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

-Dé solo los pasos que le permitan colocarse debajo de un lugar seguro, como un escritorio o mesa resistente

-Manténgase alejado de ventanas de vidrio, espejos, puertas o paredes y de todo lo que pueda caerle como lámparas y muebles

Después de la situación:

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

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

-Realizar una inspección física en los puntos donde se encuentran ubicados los Switch (Oficina de T.I, Concesionaria, Oficina de Equipos, Centro medico, Almacén, Ingeniería Tramo 8, Oficina de Gerencia, comunicarse con las veredas de Besote, Torcoroma, Platanal, Morrison, y Pailitas para verificar si físicamente el Switch sufrió algún daño o tiene la probabilidad que ocurra por elementos a su alrededor, con el fin de garantizar la integridad de los activos materiales

Por lo general un sismo afecta únicamente parte de la estructura del edificio, por lo tanto no se verían afectados los datos, sin embargo, es importante verificar que las conexiones a estos dispositivos de comunicación no se hayan afectado.

Usualmente, luego de un movimiento telúrico el sistema de telefónica celular colapsa, por lo tanto es importante implementar algún sistema de comunicación ante alguna situación de emergencia, se recomienda utilizar los siguientes medios de comunicación: Los parlantes de emergencia que se encuentran ubicado en la oficina de Salud y Seguridad del Trabajo, mensajes

cortos de texto (SMS), y/o Comunicación vía internet a través de la cuenta de correo electrónico corporativo.

- Incendio:

Medidas preventivas

-Para el área de T.I se cuenta con 2 extintores de tipo C a base de polvo químico, uno dentro de la oficina y el otro se encuentra ubicado fuera de la oficina, es importante hacerle seguimiento periódico de las fechas de vencimiento de dichas recargas e informar al área de Salud y Seguridad del Trabajo para que tomen las medidas pertinentes de cambio o recarga, y verificar que en las oficinas donde se encuentran los puntos de comunicación existan extintores en completo orden.

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

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

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

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

-Cambiar de ubicación las copias de seguridad, ya que estas se encuentran dentro de la oficina en los mismos servidores, al ocurrir una situación como incendio se correría un gran

riesgo de perder la información vital y sus copias de seguridad, estableciendo una pérdida total del activo más importante que es la Información.

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

Durante la situación:

-Conservar la calma.

-Comprobar el punto donde se genera el incendio.

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

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

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

Después de la situación:

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

-Solicitar a un electricista de la oficina de Servicios Generales inspección del cableado.

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

-Revisar posibles nuevos focos de incendio.

- Inundación/Humedad:

Medidas preventivas:

-Practicar simulacros para identificar los pasos a seguir durante la situación.

-Solicitar la revisión cada cierto tiempo del estado de los desagües y sumideros.

-Verificar situaciones de humedad que pueden desencadenar el crecimiento del moho.

Durante la Situación:

-Evite caminar por aguas en movimiento.

-Suba a un lugar alto y permanezca allí.

-Si el tiempo lo permite, mueva a un lugar seguro los elementos que soportan los procesos críticos o que ayude a restablecerlo para cuando la situación de contingencia se desactive.

-Si la situación lo permite suspenda el servicio de luz, agua y gas y evacue.

Después de la situación.

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

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

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

- Interrupción de energía

Medidas preventivas:

-Revisar periódicamente la carga del UPS (Sistema de Alimentación Interrumpida) para los casos de corte de energía.

-Identificar cuanto es el tiempo que brindaría la UPS de soporte para la empresa teniendo en cuenta el tiempo de deterioro y los usuarios conectados a la corriente.

-Socializar al personal de la empresa la clasificación de conexión donde se especifica que dispositivos deben ir conectados a los tipos de corriente con los que cuenta la empresa (Regulada/No Regulada).

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

Durante la situación:

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

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

Después de la situación:

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

- Falla en el servicio de Red/Voz

Medidas preventivas:

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

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

Durante la situación:

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

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

Después de la situación

-Verificar que el servicio este completamente activo y funcional.

- Acceso no autorizado a la información lógica

Medidas preventivas:

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

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

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

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

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

Durante la situación:

-Realizar cambios de contraseña.

-Bloquear el acceso a la información lógica.

Después de la situación

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

-Realizar cambios de contraseña si se considera necesario.

- Acceso físico no autorizado a las oficinas de T.I

Medidas preventivas:

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

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

Durante la situación:

-Abandonar el lugar donde se encuentra el intruso

-Informar inmediatamente al área de Seguridad Física.

Después de la situación:

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

- Marchas pacificas

Medidas preventivas:

-Solicitar al área de Seguridad Física informar de forma inmediata cuando se esté presentando, o se tenga información de una convocatoria para algún tipo de marcha con el fin de estar alertas.

Durante la situación:

-Cerrar la oficina de T.I

-Informar a las oficinas donde se encuentran los Racks estar alertas para cerrar el acceso físico.

-Estar alerta ante cualquier situación.

Después de la situación:

-Verificar con el área de Seguridad Física que dicha marcha pacífica no se haya salido de control e ingresado a la empresa sin autorización.

- Marchas no pacificas o cierre de vía

Medidas preventivas:

-Solicitar al área de Seguridad Física informar de forma inmediata cuando se esté presentando, o se tenga información de una convocatoria para algún tipo de marcha con el fin de estar alertas.

Durante la situación

-Cerrar la oficina de T.I

-Informar a las oficinas donde se encuentran los Racks estar alertas para cerrar el acceso físico.

-Estar alerta ante cualquier situación.

Después de la situación:

-Verificar con el área de Seguridad Física que los integrantes de la marcha no hayan accedido sin autorización a la empresa y por lo tanto a las oficinas.

Etapa 3. Desarrollo del plan de Continuidad

Según la resolución 1016 del 31 de marzo de 1989, Articulo 11, numeral 18 de la legislación colombiana en materia de Salud Ocupacional establece la obligatoriedad que tienen las empresas en organizar y desarrollar un plan de emergencia.

Teniendo en cuenta todo lo anterior y como producto de este trabajo, nos permitimos referenciar el Plan de Continuidad del Negocio para el área de Tecnologías de la Información del Proyecto Ruta del Sol – Sector 2. (Ver anexo 3)

Etapa 4. Pruebas y mantenimiento

En esta etapa se toman los procesos realizados durante el ciclo de vida de las actividades del Plan y se verifica lo realizado, luego se toman los resultados obtenidos y se plantean los cambios para la mejora continua de la organización y del Plan de Continuidad del Negocio

Una vez realizado el Plan de Continuidad del Negocio para el área de T.I, la responsable del área deberá aprobar dicho Plan, para luego gestionar autorización de dichos costos por parte de las directivas, de ser positiva la aprobación es necesaria su implantación, la cual supondría:

-Socializar el Plan de Continuidad del Negocio al personal involucrado.

-Implantación de medidas preventivas y recomendaciones indicadas en el Plan de Continuidad del Negocio.

-Ejecutar el plan de pruebas y mantenimiento la cual permite tener el Plan de Continuidad del Negocio en la mejora continua.

Plan de Prueba: Permite evaluar la viabilidad de los procedimientos de recuperación descritos anteriormente.

Objetivos a cumplir:

-Medir capacidad del lugar respaldo

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

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

-Evaluar costos de los posibles daños en la empresa

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

-Verificar el cubrimiento del Plan de Continuidad del Negocio.

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

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

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

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

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

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

-Identificación de fallos en la fase de prueba del Plan de Continuidad.

-Cambios en el entorno del Plan de Continuidad, como:

-Renovaciones tecnológicas.

-Cambios estructurales del área de T.I o puntos de trabajo indicados como alternativos de recuperación.

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

4.3 Socialización del plan de continuidad del negocio

Una vez finalizado su elaboración se procede a la socialización del Plan de Continuidad del Negocio a través de una reunión con el personal que integra el área de T.I en la última semana del mes de Abril del 2017 (Ver Anexo 4), después, se llevó a cabo una reunión privada de los 3 (tres) integrantes del área para concretar la aprobación.

La responsable de T.I solicita a Karen Lorena León Pérez, siendo ella integrante de la empresa, como personal de Apoyo al socializar el Plan al personal involucrado y establecer el cronograma para la ejecución de prueba y mantenimiento.

REFERENCIAS

FEMA (Agencia Federal para la Gestión de Emergencias de los Estados Unidos). (2014). Cada empresa debe tener su plan. Recuperado de https://www.fema.gov/media-library-data/1391811186070-60392dd4c49d7f166720fda102db82cc/2014_NegociosBooklet.pdf

Lora García A. (10 de Agosto del 2012). Dos artefactos explotaron simultáneamente en Aguachica. El Pilón, p.1.

Bernal I. (27 de Septiembre del 2013). Bloqueo en el Cerro de los Chivo, Cesar. Las 2 Orillas. p.1.

Murillo A. (27 de Septiembre del 2013). Bloqueo en Aguachica: 50 Heridos. EL HERALDO, p.1.

Angarita Parra J. (13 de Septiembre del 2015). Quemado tractor de la Concesionaria Ruta del Sol CONSOL entre Pelaya y San Roque. Joanpa, p.1.

Angarita Parra J. (12 de Septiembre del 2016). Cae presunto segundo cabecilla SAT-ELN responsable de la quema de maquinaria de CONSOL. Joanpa, p.1.

Montes monte alegre Negro H. (07 de julio del 2016). Reseña Histórica. Súmate, p.1.

DANE. (2015) Información estadística, proyecciones de población municipales por área. Recuperado de http://r.search.yahoo.com/_ylt=A0LEVjwCsOdY2JgAFS3XdAx.;_ylu=X3oDMTByMG04Z2o2BHNlYwNzcgRwb3MDMQRjb2xvA2JmMQR2dGlkAw--/RV=2/RE=1491607682/RO=10/RU=https%3a%2f%2fwww.dane.gov.co%2ffiles%2finvestigaciones%2fpoblacion%2fproyepobla06_20%2fProyeccionMunicipios2005_2020.xls/RK=0/RS=JfzNNsFY2xUsUTLdti3eHnOGsXs-

Sánchez, F. (2002). Bajo el "Efecto 11 de Septiembre". Planes de continuidad del negocio. Recuperado de http://www.networkworld.es/archive/bajo-el-efecto-11-de-septiembre-planes-de-continuidad-del-negocio

Burgos Salazar, J., & Campos, P. (2008). Modelo Para Seguridad de la Información en TIC. CEUR Workshop Proceedings, 234-253.

Gonzales Luisa (23 de Mayo del 2012). Análisis de organizaciones. Recuperado de https://es.slideshare.net/luismarlmg/estructura-organizacional-13045747

Rodríguez Leídy (10 de Enero del 2016). Introducción a la informática. Recuperado de https://es.slideshare.net/leidysRguez001/introduccin-a-la-informtica-56883494

Mifsud Elvira. (26 de maro de 2012). Instrucción a la seguridad informática- seguridad de la información. Recuperado de http://recursostic.educacion.es/observatorio/web/ca/software/software-general/1040-introduccion-a-la-seguridad-informatica?start=1

Sánchez Gómez Adelkys Rosa. (2005, Octubre 7*).* Definición genérica de auditoría y sus etapas. Recuperado de https://www.gestiopolis.com/definicion-generica-auditoria-etapas/

Ortega Ruiz Luis Hernando. (22 de Octubre de 2014). Concepto sobre amenazas, vulnerabilidad, riesgos y desastres. Recuperado de https://prezi.com/jqaa12sg1dq-/conceptos-sobre-amenazas-vulnerabilidad-riesgos-y-desastres/

O`Brien Joyce. (14 de Julio de 2016). Recursos informáticos. Recuperado de http://tocayojunior.blogspot.com.co/2016/

Monte de la Paz, M. (marzo 2010). Seguridad Lógica Y De Accesos Y Su Auditoria (Tesis de grado). Universidad Carlos III de Madrid – Escuela Politécnica Superior, España.

Murillo Ovallos Katerine. (7 de octubre de 2016). Base de datos. Recuperado de https://prezi.com/avs7sflkf59e/aprendiz/

Fernandez Silvia. (29 de Noviembre de 2015). InformáticaEstudio, Servidores-Tipos de servidores. Recuperado de http://informaticaestudio.com.ar/2015/11/servidores-tipos-de-servidores/#more-972

Ruedas Gonzales Juan. (10 de mayo de 2016). Dispositivos específicos. Recuperado de https://prezi.com/wct3qqjcablm/dispositivos-especificos/

Salazar Alex, (25 de Noviembre del 2014). SWITCH Y ROUTER. Recuperado de https://prezi.com/9mjjm_mf2krg/switch-y-router/

Ropero Sofía. (24 de Agosto de 2016). Tecnología e Informática. Recuperado de http://tcsofiaromero.blogspot.com.co/2016/08/las-partes-del-computador.html

Lerma Gonzales H. D. (2009). Metodología de la investigación: propuesta, anteproyecto y proyecto. Recuperado de https://books.google.com.co/books?id=COzDDQAAQBAJ&printsec=frontcover&hl=es#v=onepage&q&f=false

Levin, R y Rubin, D (1996). Estadística para Administradores. Recuperado de https://books.google.com.co/books/about/Estad%C3%ADstica_para_administradores.html?id=iKT_PAAACAAJ&redir_esc=y

Murria R. Spiegel (1991). Estadistica (Schaum). Recuperado de https://www.elsolucionario.org/estadistica-schaum-murray-r-spiegel-4ta-edicion/#prettyPhoto

Hernández Sampieri, Fernández Collado, Baptista Lucio, (1997) Metodología de la investigación (1890) Recuperado http://www.dgsc.go.cr/dgsc/documentos/cecades/metodologia-de-la-investigacion.pdf.

Ruta del Sol-Concesión vial (2010). Informe de la Ruta del Sol Sector 2. Recuperado de http://rutadelsol.com.co/quienes-somos/que-hacemos/

Almario Chávez M. (30 de Mayo de 2015). Volqueteros protestan contra la Ruta del Sol. Vanguardia, p1.

Morales (10 de Junio de 2016). Cierre generado por los campesinos del Catatumbo quienes bloquearon un tramo de la ruta del sol. Blu radio, p. 1.

NIST (Instituto Nacional de Estándares y Tecnología). (2002). Guía de gestión de riesgos para Sistemas de Tecnología de la Información. Recuperado de http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf

Jimeno Bernal, J (2013). Ciclo PDCA (Planificar, Hacer, Verificar y Actuar): El circulo de Deming de mejora continua. PDCA. Recuperado de http://www.pdcahome.com/5202/ciclo-pdca/

ANEXOS

Anexo 1. Checklist

Checklist

Nombre del Entrevistado: Yuly Paola Contreras Contreras
Cargo: Responsable
Área: Tecnologías de la Información
Empresa: Consorcio Constructor Ruta del Sol
Entrevistador: Karen Lorena León Pérez - Danny Jhoan Rios Barona
Fecha: 15 - Julio - 2016

Objetivo: Recopilar información que sirva para identificar el nivel de seguridad de la información.

Alcance: Verificar el cumplimiento de los dominios según ISO 27002:2013 para lograr un adecuado nivel de protección y calidad de la información.

Nº	Aspecto	Si	No	Observaciones	Req.	PO	%C	0	10	20	30	40	50	60	70	80	90	100
A5	Políticas de seguridad				3	2	67%							■				
A6	Organización de la seguridad				3	1	33%				■							
A7	Seguridad de los recursos humanos				5	3	60%							■				
A8	Gestión de los activos				6	6	100%											■
A9	Control de acceso				4	4	100%											■
A10	Criptografía				1	1	100%											■
A11	Seguridad física y medio ambiental				13	11	85%									■		
A12	Seguridad en las operaciones				7	6	86%									■		
A13	Seguridad de las comunicaciones				3	3	100%											■
A14	Adquisición desarrollo y manteniemiento del sistema				3	3	100%											■
A15	Relación con los proveedores				1	1	100%											■
A16	Gestión de los incidentes de seguridad de la información				2	1	50%						■					
A17	Gestión de los aspectos de la seguridad de la información para la continuidad del negocio				1	0	0%	■										
A18	Cumplimiento				1	1	100%											■

Total numero de requerimientos: 53
Total Puntos Obtenidos: 43
Cumplimiento del objetivo: 81%

Metodología del Check List: Las preguntas están formuladas de tal manera que para que cumpla con el objetivo su respuesta debe ser Positiva (SI), Por cada Nivel evaluado se tiene un total de Numero de Requerimientos (Total de preguntas), y se tiene un total de Puntos Obtenidos (de las preguntas realizadas en dicho nivel cuantas dieron como respuesta una apreciación Positiva (SI), dando como resultado un porcentaje sobre el cumplimiento del Objetivo.

Anexo 1. Continuación

Checklist

Nombre del Entrevistado: Yuly Paola Contreras Contreras
Cargo: Responsable
Empresa: Consorcio Constructor Ruta del Sol
Entrevistador: Karen Lorena León Pérez - Danny Jhoan Rios Barona

Área: Tecnologías de la Información
Fecha: 15 - Julio - 2016

Objetivo: Recopilar información que sirva para identificar el nivel de seguridad de la información.

Alcance: Verificar el cumplimiento de los dominios según ISO 27002:2013 para lograr un adecuado nivel de protección y calidad de la información.

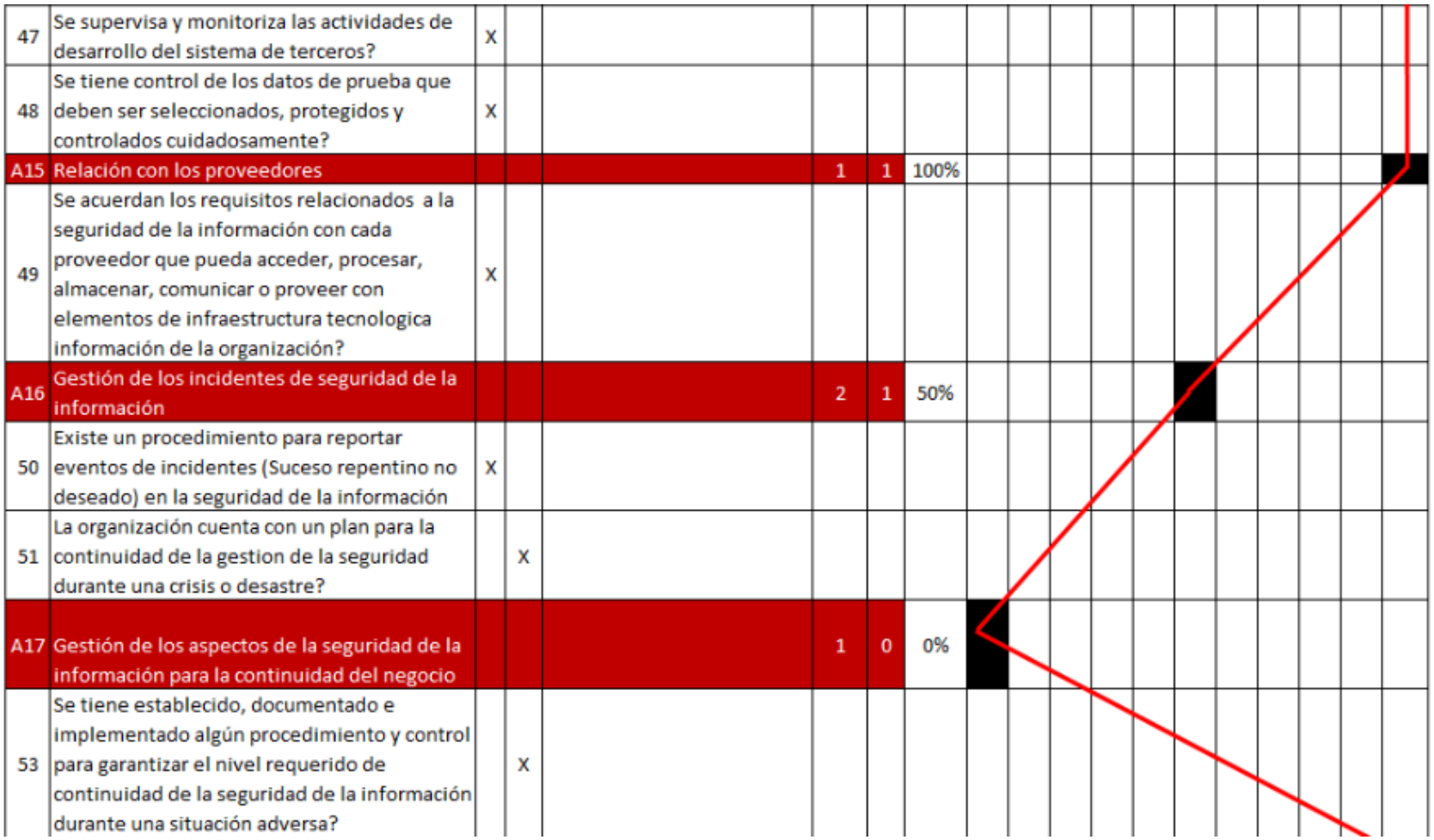
Nº	Aspecto	Si	No	Observaciones	Req.	PO	%C	0	10	20	30	40	50	60	70	80	90	100
A5	Políticas de seguridad				3	2	67%											
1	La empresa cuenta con políticas de seguridad establecidas?	X																
2	Existen mecanismos para la comunicación a los usuarios de estas políticas?		X															
3	Existen controles regulares para verificar la efectividad de las políticas?	X																
A6	Organización de la seguridad				3	1	33%											
4	Se tienen definidas y asignadas las responsabilidades de la seguridad de la información?		X															
5	Existe alguna política y/o medida de soporte de seguridad para el manejo de los riesgos derivados del uso de equipos móviles?		X															
6	Existe control para proteger la información que se encuentra en lugares de trabajo fuera de las instalaciones de la organización?	X																
A7	Seguridad de los recursos humanos				5	3	60%											
7	Se realiza una verificación de los antecedentes de los futuros empleados?	X																
8	Existe un acuerdo de confidencialidad con respecto a la seguridad de la información a la cual accederá?	X																
9	Existen capacitaciones permanentes sobre la concientización de la seguridad y el adecuado manejo de la información?		X															

10	Existe un proceso disciplinario contra los trabajadores que cometen alguna infracción contra la seguridad de la información?	X																
11	Se define y comunica a los trabajadores que una vez finalizado el contrato permanecerán validos las responsabilidades y tareas de seguridad de la información a la cual tuvo acceso?		X															
A8	Gestión de los activos				6	6	100%											
12	Existe un inventario de activos actualizado?	X																
13	Existe un responsable de los activos?	X																
14	Se tiene control de la devolución de estos activos una vez finalizado su empleo, contrato o acuerdo?	X																
15	Se realiza una clasificación de la información según su criticidad y sensibilidad de la misma?	X																
16	Se tienen identificados los archivos con información confidencial?	X																
17	Se tienen procedimientos formales para desechar de manera segura cuando ya no son necesarios los medios de comunicación?	X																
A9	Control de acceso				4	4	100%											
18	En los equipos de computo se debe ingresar usuario y contraseña para poder iniciar sesión?	X																
19	Se tiene control para que los usuarios únicamente puedan acceder a la red o a los servicios que solo han sido autorizados a ingresar?	X																
20	Existe un procedimiento formal de registro o baja de accesos?	X																
21	Existe una política o medida para cambiar la contraseña frecuentemente?	X																
A10	Criptografia				1	1	100%											
22	Se tiene implementado alguna política de uso de controles criptográficos para proteger la información?	X		Aplica solo para usuarios categorizados como criticos, en nuestro caso los Gerentes y el Director de Contrato														

A11	Seguridad física y medio ambiental				13	11	85%													
23	Existen perímetros de seguridad como paredes, tarjetas de ingreso, llaves, etc. Para proteger las áreas que contienen información y las instalaciones de procesamiento?	X																		
24	Existen controles de ingreso para protegerse frente al acceso de personal no autorizado?	X																		
25	Existe alarma para detectar fuego?		X																	
26	Existen extintores adecuados en el área?	X																		
27	Los equipos de cómputo se encuentran lejos de sufrir algún accidente de humedad?	X																		
28	Existen controles frente a fallos en la alimentación eléctrica?	X																		
29	En el ultimo año se han revisado las instalaciones eléctricas?	X																		
30	Existe seguridad en el cableado frente a daños e intercepciones?	X																		
31	Los equipos de cómputo se encuentran fuera de sufrir algún accidente de caídas libres de objetos pesados?	X																		
32	Se lleva un control del mantenimiento realizado y necesario para los equipos de cómputo?	X																		
33	Se lleva un control para los componentes informaticos en garantía?	X																		
34	Se tiene alguna medida de seguridad para los activos utilizados fuera de las instalaciones de la organización?	X																		
35	Se implementan políticas de escritorio limpio de papeles y medios de almacenamiento removibles y pantalla limpia para la seguridad de la información?		X																	
A12	Seguridad en las operaciones				7	6	86%													
36	Se tiene documentado los procesos operacionales y puesto a disposición para los usuarios que lo necesiten?	X																		
37	Los equipos cuentan con antivirus?	X																		

38	El antivirus cuenta con licencia legal establecida y actualizada?	X		Se tiene contrato a través de la T.I. corporativa de Odebrecht, con Trend Micro Office Scan Agent para las actualizaciones automaticas una vez generadas por el sistema de antivirus															
39	Se realizan copias de seguridad?	X		Periocidad: dependiendo del sistema varia entre 8 a 15 dias , Lugar de almacenamiento: Red															
40	Se tiene control para proteger contra la falsificación y el acceso no autorizado a los medios de logeo y la información de logeo?	X		Los equipos que no esten dentro de la red no pueden acceder a los sistemas corporativos.															
41	Se controlan las descargas e instalaciones de programas en los equipos de cómputo?	X																	
42	Se tiene de manera oportuna información sobre las vulnerabilidades o debilidades tecnicas de los sistemas para tomar medidas adecuadas y así manejar los riesgos asociados?		X																
A13	Seguridad de las comunicaciones				3	3	100%												
43	Se administra y controlan las redes para garantizar la protección de la información?	X																	
44	De alguna manera se protege adecuadamente la información enviada mediante mensajes electronicos?	X		Aplica solo para usuarios categorizados como criticos, en nuestro caso los Gerentes y el Director de Contrato															
45	Existen controles para el uso de medios de almacenamiento removibles?	X		Aplica solo para usuarios categorizados como criticos, en nuestro caso los Gerentes y el Director de Contrato															
A14	Adquisición desarrollo y manteniemiento del sistema				3	3	100%												
46	Se tiene control para proteger la información que pasa a tráves de las redes públicas?	X																	

47	Se supervisa y monitoriza las actividades de desarrollo del sistema de terceros?	X						
48	Se tiene control de los datos de prueba que deben ser seleccionados, protegidos y controlados cuidadosamente?	X						
A15	Relación con los proveedores			1	1	100%		
49	Se acuerdan los requisitos relacionados a la seguridad de la información con cada proveedor que pueda acceder, procesar, almacenar, comunicar o proveer con elementos de infraestructura tecnologica información de la organización?	X						
A16	Gestión de los incidentes de seguridad de la información			2	1	50%		
50	Existe un procedimiento para reportar eventos de incidentes (Suceso repentino no deseado) en la seguridad de la información	X						
51	La organización cuenta con un plan para la continuidad de la gestion de la seguridad durante una crisis o desastre?		X					
A17	Gestión de los aspectos de la seguridad de la información para la continuidad del negocio			1	0	0%		
53	Se tiene establecido, documentado e implementado algún procedimiento y control para garantizar el nivel requerido de continuidad de la seguridad de la información durante una situación adversa?		X					



A18	Cumplimiento				1	1	100%											
53	Se tienen procedimientos adecuados para garantizar el cumplimiento de los requisitos legislativos, regulatorios y contractuales relacionados a los derechos de propiedad intelectual y al uso de productos registrados de software (Licencias correspondientes)?	X																

Total numero de requerimientos: 53
Total Puntos Obtenidos: 43
Cumplimiento del objetivo: 81%

Metodología del Check List: Las preguntas están formuladas de tal manera que para que cumpla con el objetivo su respuesta debe ser Positiva (SI), Por cada Nivel evaluado se tiene un total de Numero de Requerimientos (Total de preguntas), y se tiene un total de Puntos Obtenidos (de las preguntas realizadas en dicho nivel cuantas dieron como respuesta una apreciación Positiva (SI), dando como resultado un porcentaje sobre el cumplimiento del Objetivo.

Anexo 2. Comparación de Normas de Continuidad del Negocio

Normas de Continuidad del Negocio	ESTANDAR INTERNACIONAL ISO/IEC 27001-2005 Tecnología de la Información- Técnicas de Seguridad- Sistemas de gestión de Seguridad de la Información - Requerimientos SGSI	PROYECTO NORMA MERCOSUR ISO/IEC 27002: 2007 Tecnologías de la información - Código de Buenas Prácticas para la gestión de la seguridad de la información.	NORMA TECNCA COLOMBIANA NTC 5722 Gestión de la Continuidad del Negocio. REQUISITOS (Adopción Idéntica por Traducción de la BSI 25999-2007).	NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY NIST 800-34 Contingency Planning Guide for Information Technology Systems, Rev 1	STANDARD ON DISASTER/EMERGENCY MANAGEMENT AND BUSINESS CONTINUITY PROGRAMS NFPA1600:2010	ORGANIZATIONAL RESILIENCE ASIS SPC.1-2009: Security, Preparedness, and Continuity Management Systems – Requirements with Guidance for Use
Fecha de publicación	Primera edición 2005-10-15		18/11/2009	Mayo/2010	05/12/2009	12/03/2009
Desarrollador	Comité Técnico Conjunto ISO/IEC JTC 1, Tecnología de la información, Subcomité SC 27, Técnicas de seguridad TI.	Comité Técnico Conjunto ISO/IEC JTC 1, Tecnología de la información, Subcomité SC 27, Técnicas de seguridad TI.	El Instituto Colombiano de Normas Técnicas y Certificación (ICONTEC)	NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY	NFPA - National Fire Protection Association, FEMA - Federal Emergency Management Agency, Nema Electrical Manufacturers Association, IAEM - International association of emergency managers.	American National Standard for Industrial Security
Normas base	La base de esta normativa es la norma BS 7799-2:2002, desarrollada por la entidad de normalización británica, la British Standard Institution (BSI)	La base de esta normativa es la norma ISO/IEC 17799 la cual le fue asignada el número 27002 en el año 2007	La base de esta normativa es la BSI 25999-2:2007 y la Guía Técnica Colombiana (GTC 176).	FIPS 199, NIST 800-53	Esta normativa no especifica si está relacionada con otra normativa.	ISO 73:2002-Risk Management-Vocabulary-Guidelines for use in standards, ISO 9001:2000-Quality management systems, ISO14001:2004-Enviromental management systems
Descripción	Norma creada para fomentar en las organizaciones y sus integrantes, el desarrollo de un ambiente adecuado para establecer la seguridad de la información y donde no se fomenta el despliegue de tecnología o de infraestructura.		Normativa creada para hacer énfasis en la importancia de comprender las necesidades de la continuidad del negocio estableciendo políticas que ayuden a la seguridad de la información y la vida de la organización.	Guía de Planes de Contingencia para la Tecnología de la Información, proporciona instrucciones, recomendaciones y consideraciones para la planificación de contingencia del gobierno de TI.	Normativa creada para ayudar a las instituciones a identificar, analizar y crea soluciones a riesgos presentes en su interior y en el ambiente en que se desempeñan	Esta norma está diseñada para que pueda ser integrada con calidad, seguridad, medio ambiente, seguridad de la información y riesgos.

Función	Educar y enseñar a las organizaciones a **establecer, implementar, operar, monitorear, revisar, mantener y mejorar** los sistemas de gestión de la seguridad de la información SGSI , fomentar estas prácticas como base para el desarrollo de un Plan de Continuidad del Negocio (BCP).	Esta Norma establece recomendaciones y principios generales para **iniciar, implantar, mantener y mejorar la gestión de la seguridad de la información** en una organización. Los objetivos señalados en esta Norma proporcionan recomendaciones generales sobre las metas comúnmente aceptadas para la gestión de la seguridad de la información.	Esta norma técnica colombiana especifica los requerimientos para **planificar, implementar, supervisar, mantener y mejorar** los sistemas de gestión de la continuidad del negocio.	Definir los siete pasos del proceso de los planes de contingencia de la organización y como se integran a los escenarios del ciclo de vida de desarrollo de sistemas. 1. desarrollo de políticas que ayuden a orientar el desarrollo de un plan de contingencia efectivo 1. crear políticas 2. análisis de impacto del negocio (BIA) 3. identificar controles preventivos 4. crear estrategias de contingencia 5. desarrollar el plan de contingencia 6. test del plan de contingencia 7. Realizar mantenimiento del plan de contingencia	Esta normativa abre la mente de las personas integrantes del grupo que desarrollará el programa y ayuda a dejar en claro la identificación, análisis y desarrollo de soluciones de riesgos que ayuden a la continuidad del negocio frente a los riesgos encontrados en el medio o al interior de la empresa.	Esta normativa está enfocada en los sistemas de gestión integral de la seguridad, preparación, respuesta, mitigación, de incidentes perturbadores que resultan en una emergencia, crisis o desastre. Esta normativa se desarrolla enfocada a los procesos para lograr el éxito, esta metodología propende a la mejora continua ya que proporciona la manera de establecer, mantener y mejorar la organización.

Para que se implementa	Se implementa para dar orden a la gestión de la seguridad de la información en la organizaciones.	Se implementa como principios básicos de las practicas de la seguridad	Se implementa para evaluar la capacidad de la organización para cumplir con las necesidades de la continuidad del negocio.	Se implementa esta normativa para el desarrollo efectivo de los planes de contingencia.	Se implementa para establecer de manera clara los pasos para mantener, implementar y desarrollar el programa de prevención	La aplicación de un sistema de procesos dentro de una organización, junto con la identificación e interacciones de estos procesos y su gestión, puede ser referido como un "enfoque de proceso". Que ayuda a: a) Comprender el riesgo de una organización, seguridad, preparación, respuesta, continuidad, y los requisitos de recuperación; b) El establecimiento de una política y objetivos para la gestión de riesgos; c) Implementar y usar los controles para gestionar los riesgos de la organización dentro de la contexto de la misión de la organización; d) Supervisar y revisar el desempeño y la eficacia de la gestión del RO(organizational resilience) sistema; y e) La mejora continua basada en mediciones objetivas.
En que se enfoca la norma?	Esta norma se enfoca en hacer entender a los integrantes de la organización la importancia del desarrollo y mejoramiento de los procesos que gestionan la seguridad de la información	Establecer normativas que ayuden a la organización a controlar los riesgos que afectan a la organización.	Se enfoca en dar a entender cómo crear un sistema de gestión de la continuidad del negocio que sea apropiado para la organización y sus integrantes.	Se enfoca en dar la guía necesaria para el desarrollo de planes de contingencia.	Se enfoca en dar a la persona encargada de la continuidad del negocio los criterios para evaluar los riesgos y poder crear soluciones a los riesgos encontrados.	Esta normativa se enfoca en desarrollo de procesos que permitan la continuidad del negocio y la comprensión y mitigación de riesgos

Objetivos de la norma	Entender las necesidades de la organización. Comprender el objetivo de las políticas de seguridad de la información. Implementar controles que ayuden a la seguridad de la información. Monitorear la efectividad de los cambios y procesos establecidos para la seguridad de la gestión de la información. Mejoramiento continuo de los procesos que garanticen que a futuro no se presentaran problemas de seguridad.	El objetivo de esta norma es establecer controles para iniciar, implementar, mantener y mejorar la gestión de la información y alcanzar los requerimientos de la evaluación de riesgos	Su objetivo es definir los límites a los cuales deben llegar los sistemas de gestión de la continuidad del negocio, dejando claro los procesos que se deben realizar para implementar, mantener y mejorar la gestión de la continuidad.	El objetivo de esta guía es identificar los principios fundamentales de planificación para desarrollar y mantener los planes de contingencia. Este documento sirve de guía para ayudar al personal a evaluar los sistemas de información y las operaciones para determinar los requisitos de contingencia y prioridades.	Propósito. Esta norma establece los criterios fundamentales para desarrollar, implementar, evaluar y mantener el programa para la prevención, mitigación, preparación, respuesta, continuidad y recuperación.	Esta norma permite a una organización:a) Desarrollar un programa de prevención, preparación, respuesta, continuidad y política de recuperación; b) Establecer los objetivos, procedimientos y procesos para alcanzar los compromisos de la política; c) Asegurar la competencia, el conocimiento y la capacitación; d) Establecer indicadores para medir el desempeño y demostrar el éxito; e) Adoptar las acciones necesarias para mejorar el rendimiento; f) Demostrar la conformidad del sistema con los requisitos de esta norma, y g) Establecer y aplicar un proceso para la mejora continua.
Qué modelo adapta para su desarrollo PDCA o SDLC	PDCA	PDCA	PDCA	SDLC o ciclo de vida de desarrollo de sistemas que tiene como fases primordiales: Fase inicial, Desarrollo / fase de adquisición, fase de implementación, fase de operación / mantenimiento, fase de eliminación	PDCA	PDCA
Que es la seguridad informática?	No tiene un concepto fijo de lo que es la seguridad.	La seguridad de la información es la protección de la información contra una amplia gama de amenazas para asegurar la continuidad del negocio, minimizar los daños al negocio y maximizar el retorno de las inversiones y las oportunidades de negocio.	No tiene un concepto de lo que significa la seguridad de la información.	No tiene un concepto de lo que significa la seguridad de la información.	En esta normativa no se especifica el significado de seguridad informática	En esta normativa no se especifica el significado de seguridad informática

Actividades expuestas en la norma que se involucran en el PDCA, SDLC o la metodología usada para el desarrollo del BCP	**Planear**	Desarrollar un plan donde se establezcan las características de la organización, los métodos de evaluación del riesgo, los alcances y como se evaluarán los resultados, además de establecer la prevención de errores, detección y respuestas a las fallas, mantenimiento periódico del plan, revisión y auditoría del mismo y sus funciones primarias.	Determinar los valores, objetivos y principios que la organización ha fijado para dar un apoyo firme a sus procesos, Valoración de los riesgos de la organización, con ésta se identifican las amenazas, se evalúa la vulnerabilidad y la probabilidad de su ocurrencia y se estima como será el impacto para la organización. Toma como fuente el conjunto de requisitos legales, que ayudan al buen desempeño de las funciones de la organizaciones.	Identificar las principales actividades y productos que deben estar dentro de la gestión de continuidad que se desea establecer, determinar las políticas de continuidad del negocio, las metas, objetivos, controles, procesos y procedimientos que se deben realizar para la gestión del riesgo y la mejora de la continuidad del negocio para entregar resultados acordes con las políticas y objetivos generales de la organización.	**Fase inicial**	Se realiza el estudio de cómo será desarrollado el sistema. Se determinará si el sistema será creado para trabajar bajo un entorno controlado o bajo condiciones inusuales, se determinan los requerimientos necesarios para el desarrollo efectivo del sistema, además se debe establecerá el nivel de recuperación que debe tener todo el sistema para garantizar el funcionamiento óptimo de los sistemas a desarrollar.	**planear**	Esta etapa se basa en determinar, el propósito y la aplicación del plan de continuidad a desarrollar. Aquí se definen la metodología a usar, las políticas que regirán a todo el BCP en su desarrollo, implementación y mantenimiento, se determina cual será el coordinador del programa y el comité con el cual se trabajara todo el programa de BCP, además se determinara el tiempo de evaluación del programa.	En esta normativa se destaca la importancia de definir el alcance de las actividades que se desarrollarán en la organización, la misión y visión del BCP, definir los activos a usar, hacer un análisis de riesgos internos y externos que afectan a la organización, además de un análisis de impacto (BIA) que ayudará a definir la gestión de emergencia, desastres y la continuidad del negocio. La organización debe desarrollar políticas donde se haga énfasis en el compromiso, donde se incluya el compromiso de no infringir la ley, donde se establezca la revisión continua de los procesos de la organización en beneficio de la continuidad, todo esto debe ser documentado ya que puede servir para evaluar todas las actividades de la organización, además de determinar los tiempos de recuperación, los costos y los beneficios y llevar un histórico de los riesgos e impactos encontrados.

Actividades expuestas en la norma que se involucran en el PDCA, SDLC o la metodología usada para el desarrollo del BCP	**Hacer**	Formulación del plan de tratamiento de riesgos y actividades de mejoramiento de la seguridad, capacitar a los empleados para su optima reacción. Establecer políticas, objetivos, roles y responsabilidades a los integrantes de la organización que ayuden a la activación del plan de seguridad. Establecer el compromiso que la gerencia tiene en el desarrollo de la gestión de la seguridad describiendo las políticas para el mismo y su responsabilidad, se debe determinar los recursos a usar en el desempeño y mantenimiento de la gestión. Se manejará como base para la integración de la gestión de la seguridad la prevención, la detección, la respuesta inmediata, el mantenimiento, la revisión y auditoría en todas las actividades realizadas.	Desarrollar en el interior de la organización controles que se consideren esenciales para el buen desarrollo de las actividades de la empresa tales como: protección de datos personales, protección de registros de la organización, derechos de propiedad intelectual, documentación de las políticas, asignación de responsabilidades, concientización y capacitación de la información, gestión de la continuidad del negocio, se debe determinar los controles dependiendo de los riesgos que la empresa desea enfrentar y sobre todo los logros que la organización se ha propuesto.	Implementar y ejecutar la política, los controles, procesos y procedimientos de la continuidad del negocio	**Desarrollo / fase de adquisición**	Se deben especificar los requerimientos del sistema, detallar como van a ser sus funciones de manera que se puedan evitar fallas a futuro y donde la corrección de los errores se reduzcan y donde se pueda garantizar la fiabilidad y disponibilidad durante la fase de operaciones.	**Hacer**	Esta fase del PDCA se basa en tener claro la administración de recursos, la comunicación y las alertas anticipadas, la asistencia de terceros con los que se tenga acuerdos, la implementación de los procesos desarrollados para la mitigación de las amenazas, implantar en los empleados la cultura del BCP, en esta etapa se pone en funcionamiento el BCP se gestiona la administración de incidentes y se ponen en práctica las operaciones de emergencia.	En esta etapa las directivas de la organización deben asignar responsabilidades y los recursos necesarios para llevar a cabo las actividades del sistema de gestión, Además se debe realizar entrenamiento continuo sobre el funcionamiento del sistema, se debe comunicar continuamente los cambios sobre el sistema o la organización. La organización debe documentar todo lo sucedido con los procesos actuales o nuevos. Se debe velar por la seguridad de la documentación que servirá como histórico para evaluaciones posteriores, en esta etapa se debe llevar un control de los procesos que van ser activados y de los riesgos encontrados en la etapa de planeación. En esta etapa se desarrolla y se pone en práctica los procedimientos de respuesta desarrollados tras los resultados del BIA.

Actividades expuestas en la norma que se involucran en el PDCA, SDLC o la metodología usada para el desarrollo del BCP	**Chequear**	Se deben realizar procedimientos de revisión continua de las actividades de la gestión de seguridad y si su desempeño está cumpliendo con los objetivos planteados, desarrollar auditorias para verificar si lo dicho anteriormente es verdadero y si cumplen con los requerimientos legales, tras estas revisiones se deben tomar decisiones de modificación, actualización o desarrollo de nuevas políticas o procedimientos que ayuden a la efectividad de la gestión, además de la revisión debe tener en cuenta la prevención, detección, respuesta inmediata y mantenimiento de todo este proceso.	Revisión continua de las políticas de seguridad que ayuden a su mejoramiento, registrar los resultados de la implementación de políticas de versiones anteriores, mejorar continuamente el objetivo de los controles, mejorar la asignación de recursos que ayuden al desarrollo de los procesos de la seguridad de la información, evaluar periódicamente los riesgos actuales y los futuros para determinar su alcance y posibilidad de ocurrencia.	Supervisar y revisar el desempeño frente a los objetivos y la política de continuidad del negocio, reportar los resultados para su revisión y determinar y autorizar las accione destinadas a remediar y mejorar.	**fase operación / mantenimiento**	Se debe establecer la importancia de los sistemas de la empresa para de esta forma diseñar como será el método de recuperación, el plan de recuperación debe actualizarse de manera periódica con las lecciones aprendidas y las mejoras realizadas.	**Chequear**	La entidad debe evaluar los planes, procedimientos y capacidades a través de pruebas periódicas y ejercicios. Las pruebas realizadas deben ser realizadas de manera periódica dependiendo de las necesidades de la empresa. Las pruebas deben ser desarrolladas enfocadas a identificar bondades del BCP o deficiencias del mismo, aclarar funciones y responsabilidades, mejoramiento entre los equipos que intervienen en el BCP, Identificar recursos adicionales y evaluar las políticas y controles implementados en el BCP.	En esta normativa se describe la necesidad de verificar periódicamente con pruebas e informes posteriores a incidentes los la funcionalidad de los procesos, con estas evaluaciones se debe reflejar el cambio inmediato en los procedimientos. La organización debe establecer métricas de rendimiento de los procedimientos que ayuden a medir de forma regular su comportamiento. La organización debe realizar un programa de auditoría planificada, tomando en consideración el estado y la importancia de los procesos y las áreas a auditar, así como los resultados de auditorías previas.

Actividades expuestas en la norma que se involucran en el PDCA, SDLC o la metodología usada para el desarrollo del BCP	**Actuar**	Se deberá mantener y mejorar el sistema de gestión implementado en la empresa al tomar acciones correctivas o preventivas que ayudarán a la eficiencia del Sistema de gestión, se tomará registro de las decisiones tomadas para llevar un control que servirá para estudios posteriores		Mantener y mejorar el sistema de gestión de continuidad del negocio llevando a cabo actividades preventivas y correctivas de los procesos o procedimientos de la organización con base en los resultados de las revisiones hechas sobre todas las actividades y controles implementados en la organización.	**fase de implementación**	En esta fase aunque se sabe que el sistema implementado esta bajo pruebas constantes se debe asegurar que las estrategias a usar sean acordes a las necesidades y si cumplen con lo planeado, para tal caso es debido realizar un plan de pruebas donde se probaran detalladamente las estrategias de la contingencia.	**Actuar**	La entidad debe mejorar la eficacia de los objetivos, políticas y procesos que se establecen en el BCP. En esta etapa del PDCA se evalúa nuevamente cualquiera de las situaciones documentadas desde la activación del BCP hasta el momento donde se llega a la normalidad de las actividades, aquí se corrige el BCP basándose en las lecciones aprendidas.	La dirección revisará el sistema de gestión de la organización y se asegurara de la adecuación y eficacia, con esta revisión debe incluir la mejora y la necesidad de cambios en el sistema. La dirección debe basar la revisión en los resultados de las auditorias anteriores y en el resultado de los procesos implementados, tras la revisión de toda esta información se deben realizar cambios en las políticas y los objetivos que afecten positivamente a la organización.
					fase de eliminación	En esta fase se especifica que los equipos que saldrían de la empresa también deben salir del BCP pero antes debe existir un reemplazo en total funcionamiento de las funciones con las cuales venía trabajando el equipo a reemplazar			

Puntos para dar comienzo al plan	1. Obtener apoyo de la gerencia.	1. La dirección debería apoyar activamente la seguridad dentro de la organización atreves de una orientación clara y la asignación explicita de responsabilidades.	1. Establecer que la dirección tenga un compromiso con las políticas y planes de la gestión de la continuidad del negocio.	1. Se debe tener muy encuentra la opinión de los gerentes y coordinadores para tener éxito en las actividades del plan de contingencia.	1. En primera instancia es importante que la gerencia de vía libre a el coordinador y al comité de programa de desarrollar actividades dentro de la empresa, que contribuyan a la continuidad.	1. Se desarrolla un documento por escrito donde se determine el compromiso de la dirección, donde se establezca que la gerencia está comprometida con el desarrollo del sistema de gestión, donde la gerencia se encargue de comunicar la importancia del sistema de gestión y donde la gerencia proporcione los recursos necesarios para implementar y mantener el sistema de gestión
Puntos para dar comienzo al plan	2. Definir roles y responsabilidades.	2. La asignación de responsabilidades de seguridad de la información debe hacerse de acuerdo a las políticas de seguridad y complementada con guías de implementación y desarrollo	2. Se debe definir y documentar de manera detallada y con claridad los roles, funciones, responsabilidades, competencias y los responsables de activar el plan.	2. Según esta normativa es paso fundamental definir detalladamente los roles y las responsabilidades de las personas que intervienen en el desarrollo del plan de contingencia.	2. Según esta norma en un plan de emergencia se debe asignar responsabilidades a la organización y a los ínvidos para ejecutar acciones especificar en tiempos y lugares predeterminados en caso de emergencia.	2. La alta dirección deberá designar representantes en cada una de las áreas que conforman la empresa, con responsabilidades definidas con las cuales podrá implementar sistemas de gestión.
Puntos para dar comienzo al plan	3. Definir el alcance.	3. Definir hasta donde podrá llegar el plan y en qué casos son los que no cumple con lo requerido.	3. La organización debe determinar el alcance de la gestión de la continuidad del negocio y establecer sus objetivos primordiales.	3. Esta normativa no expone la importancia de definir el alcance del plan a desarrollar.	3. Esta normativa explica la importancia de establecer las metas, objetivos y el alcance del Programa a desarrollar.	3. La organización debe definir los límites del programa, requisitos teniendo en cuenta la misión de la empresa, los escenarios de riesgo.
Puntos para dar comienzo al plan	4. Desarrollo de políticas para el SGSI.	4. Desarrollar un documento con las políticas que se implementaran y los resultados de las mismas después de la puesta en marcha dentro de los procesos de la organización.	4. Establecer un documento detallado donde se haga referencia a los objetivos, alcances y limitaciones de la políticas a implementar, estas deben estar aprobadas por las directivas y debe ser comunicada adecuadamente a todos los integrantes	4. Esta normativa específica que se debe Identificar los requisitos legales o reglamentarios para los planes de contingencia • Declaración de política • Obtener la aprobación de la política • Publicar Desarrollar políticas de Contingencia	4. La entidad debe desarrollar políticas que definen la autoridad competente, la misión y visión, las metas, el manejo de las políticas y procedimientos, las leyes y normas que regirán el programa desarrollado.	4. La organización deberá desarrollar políticas donde se tome la importancia del compromiso de los empleados, el compromiso de la mejora continua, se desarrollarán políticas para garantizar el compromiso con la mejora continua.

Puntos para dar comienzo al plan	5. Definir la metodología para el análisis de riesgos	5. Identificar, cuantificar y priorizar los riesgos contra los criterios de aceptación de riesgo, además de estimar su magnitud y su importancia para esto se debe en primera instancia determinará los activos involucrados y los procesos básicos de la organización.	5. Permitir que la organización determine las actividades criticas y los recursos necesarios que sirven para sus principales servicios. Entender las amenazas a las que están expuestos sus actividades, establecer cuál va a será el método para determinar el impacto de los riesgos encontrados, el tiempo de reacción para reiniciar las actividades, dar niveles de importancia para reinicio de actividades y determinar los activos que son necesarios para iniciar las procesos de recuperación. Todo esto debe estar documentado de tal manera que sea claro para la organización determinar lo que pasaría si una amenaza identificada se vuelva realidad.	5. Esta normativa no especifica qué metodologías deben utilizase para el análisis de los riesgos pero explica la importancia de identificar los procesos, recursos y determinar la prioridad que se debe tener con los recursos críticos de la empresa.	5. Esta normativa explica que la entidad debe identificar riesgos, la probabilidad de ocurrencia y la vulnerabilidad ante los riesgos naturales, tecnológicos y humanos, tras el análisis de estos riesgos se debe analizar el impacto que estos tendrán en la vida continua de la organización.	5. En esta normativa se da mucha importancia a la evaluación y análisis de impacto. Esto se logra con la identificación de los activos y actividades críticas para el funcionamiento de la empresa, además de la identificación y cálculo del impacto de los riesgos es necesario analizar la prioridad de los controles y tratamientos de los riesgos encontrados.

Puntos para dar comienzo al plan	6. Dar solución al riesgo aplicando controles y documentar lo realizado (Histórico).	6. Esta normativa explica que las organizaciones después de evaluar la importancia de los riesgos que las afectan se debe determinar el tratamiento de las mismas, para este caso la organización tendrá la opción de aceptar determinado riesgo dependiendo de los alcances que tenga este riesgo en la organización, otra opción es evitar los riesgos minimizando por completo su ocurrencia y creando estrategias para su control total o parcial.	6. La organización debe conocer en detalle sus actividades criticas y la solución a los riesgos que estas puedan sufrir, los encargados de implementar el SGCN deben poner en práctica soluciones que reduzcan la probabilidad de interrupción y el tiempo de dichas interrupciones, la organización debe implementar soluciones adecuadas al nivel de aceptación del riesgo que se determino en el análisis de riesgos y se debe documentar de tal forma que para futuras interrupciones se pueda responder con eficacia y de forma oportuna a alguna amenaza.	6. Tras determinar los riesgos y lo que estas amenazas afectarían a la empresa, se determina que se debe identificar los controles preventivos y se deben desarrollar estrategias de recuperación como: Backup, lugares alternativos, Reemplazo de equipos, Establecer roles y responsabilidades, esta información debe ser documentada de manera detallada para que sirva como guía a las personas que hacen parte de la implementación del BCP	6. La entidad debe implementar estrategias para eliminar el riesgo o mitigar los efectos del peligro, debe realizar identificación y análisis de riesgos de las amenazas presentes en la naturaleza, en los recursos humanos y la tecnología.	6. La organización tras el estudio de los riesgos está preparada para el tratamiento y la implementación de controles para la mitigación de los riesgos encontrados, para la empresa y las directivas es muy importante la documentación
Puntos para dar comienzo al plan	7. Declarar la aplicabilidad de los controles y explicar en detalle el o los objetivos de estos.	7. Describir los alcances y los objetivos de la estrategia para así ser implementada.	7. La organización debe detallar la forma como se gestionaran los incidentes en el momento y después de que se manifieste.		7. Esta normativa debe definir los objetivos del programa y el modo en la que se relaciona con las políticas de la organización.	7. Los controles establecidos deben ser detallados para no causar confusión a las personas que contribuyen a la implementación y desarrollo del programa.

Puntos para dar comienzo al plan	8. Plan de tratamiento de Riesgos, detalla cómo se va a implementar el control, en qué momento, porque personas, etc.	8. Determinar en detalle que actividades se desarrollaran para mantener la organización en funcionamiento.	8. La organización debe contar con planes documentados que detallen como la organización va a gestionar el incidente, como se recuperara y como se mantendrá en funcionamiento en el momento de una emergencia.	8. Esta normativa trata de identificar los procesos críticos, el tiempo fuera de servicio y las prioridades de recuperación, tras esto se identifican las estrategias de recuperación y se explica en detalle su funcionamiento.	8. Esta normativa habla de manera muy sencilla sobre tratamiento de riesgos y sobre los puntos de vista que se deben tener en cuenta para la identificación, análisis y mitigación de los riesgos y vulnerabilidades e las personas, los bienes, el medio ambiente.	8. la organización debe tener un detallado documento de todas las actividades de la organización y de los tratamientos desarrollados y el resultado obtenido tras aplicar el tratamiento al riesgo encontrado.
Puntos para dar comienzo al plan	9. Definir cómo se va a medir el cumplimiento de los controles propuestos.	9. Desarrollar auditorias de las actividades y resultados de los controles y estrategias implementadas.	9. La dirección debe revisar el SGCN de manera periódica para evaluar las oportunidades de mejora y las necesidades de cambio.	9. Esta normativa no especifica cómo medir el cumplimiento del BCP.	9. Esta normativa no especifica cómo medir el cumplimiento del BCP.	9. La organización debe documentar todo lo realizado y debe tomar datos medibles para probar la eficiencia de los procesos activos y si han cumplido con lo establecido en el programa.
Puntos para dar comienzo al plan	10. Implementar controles y procedimientos que serian obligatorios.	10. Determinar los pasos a seguir de los controles implementados con las actividades de los usuarios de la organización y las partes externas que intervienen en la seguridad.		10. Determina los pasos a seguir en el desarrollo del BIA que sirve para determinar lo métodos de control y el impacto que tienen las fallas en las actividades de la empresa.	10. Aunque no son muy detallados, esta normativa da ideas de cómo se debe controlar y que procedimientos se deben tener en cuenta para el desarrollo de cualquier programa que ayude al mejoramiento y control de los procesos de la empresa.	

Puntos para dar comienzo al plan	11. Capacitar y sensibilizar a los integrantes de la organización con los temas de reforma con la esperanza que todos hagan de forma correcta las actividades de seguridad.	11. Concientizar, educar y formar en seguridad de la información a los empleados de la organización donde se haga hincapié en las responsabilidades, el buen uso de los recursos de la empresa, en la actualización de las políticas y en la importancia de seguir las normativas para que la organización siga en pie ante cualquier emergencia.	11. Asegurarse que se vuelva cultura en la empresa todos los procesos que se establecen en el sistema de gestión de la continuidad, la organización debe ofrecer la concientización, compromiso, formación y entrenamiento a los integrantes de la organización y determinar las competencias necesarias para las personas que estarán bajo el sistemas de la gestión de la organización que se desea implementar, la gerencia debe asegurarse de que los conocimientos del personal sean aptos para su buen desempeño y para el éxito de el SGCN.	11. Esta normativa nos indica que la mejor forma de capacitar a los integrantes de la organización es desarrollando de manera periódica planes de prueba donde se simule la peor situación o la situación con más probabilidad de ocurrencia. Los métodos de capacitación serian en salones de clase simulando casos reales, simulando emergencias en las instalaciones.	11. Esta normativa explica la importancia de realizar capacitaciones a los empleados realizando actividades de prueba en la organización y el objetivo de este plan de capacitación es fomentar conciencia y mejorar el conocimiento y destrezas de las personas de la empresa, se deben llevar registros de capacitación y de los temas tratados como: los impactos potenciales, la preparación a tener en cuenta y la información necesario para desarrollar entre todos un programa de mitigación.	11. La capacitación y el entrenamiento contante de los integrantes de la organización es fundamental para garantizar el desarrollo efectivo los tratamiento realizados ante los riesgos encontrados tras un análisis de los riesgos.
Puntos para dar comienzo al plan	12. Llevar a nivel operativo el SGSI y comenzar con el registro de las actividades.	12. Las actividades realizadas deben ser documentadas con minucioso detalle, dando a conocer los procesos, metodologías utilizadas y manejo de errores, esta información debe estar al alcance de cualquier persona que lo necesite, esta documentación debe ser tratada como un documento formal y debe ser autorizado y realizado			12. en esta normativa no se especifica la menara como se debe activar el programa desarrollado, pero deja claro que es necesario la documentación de las actividades que serán revisadas posteriormente por la gerencia o directivos de la empresa.	12. Esta normativa deja en claro la importancia de llevar registros en la totalidad del desarrollo del programa de gestión.

		por la dirección.				
Puntos para dar comienzo al plan	13. Supervisar las actividades del proyecto SGSI y determinar con los resultados si se cumplen con los objetivos planteados.	13. Revisión independiente a intervalos planificados los procesos, políticas y procedimientos que se enfocan en la seguridad de la información, deben ser registrados y evaluados para determinar si cumplen con la orientación declarada en el documentos de políticas de la seguridad.	13. Al realizar revisiones continuas y de manera programada se determina si se está cumpliendo con lo planificado en el SGCN.	13. Para esta normativa es fundamental la supervisión de los procesos y practicas realizadas sobre el BCP, ya que esta vigilancia continua ayudara a controlar si los procesos y actividades diseñadas logran lo esperado, además tomar lo observado para crear nuevas prácticas o modificaciones del BCP	13. En esta normativa se sugiere la revisión periódica de las actividades del programa implementado, y la necesidad de la documentación del mismo para futuros análisis y mejoras.	13. La gerencia y los integrantes del las áreas encargadas del programa están en la obligación de realizar una revisión permanente de todos los procesos realizados en la activación y después de realizar los tratamientos necesarios sobre las amenazas encontradas.

Puntos para dar comienzo al plan	14. La organización debe desarrollar una auditoría interna periódica donde se vigile detalladamente si los procesos y actividades establecidos en la SGSI cumplen con los objetivos del proyecto y donde muestren las falencias y de proyecten las soluciones.	14 - 15. Revisar el enfoque de la organización hacia la gestión de la seguridad de la información de forma periódica y determinar si las estrategias están bien enfocadas o si es necesario la reevaluación de los controles. Al terminar la revisión se debe documentar los hallazgos y las correcciones realizadas para su buen desempeño	14 - 15. Revisión de las políticas en intervalos planificados y cuando ocurra cambios significativos de las mismas. Además de asegurarse que la organización realice auditoría interna y de autoevaluación del SGCN para revisar la efectividad, la idoneidad de la políticas y objetivos que se plantearon con anterioridad. Las revisiones realizadas en la organización deben ser documentadas para futuras auditorias que permitan determinar si se cumplió o no la mejora de los procesos afectados por las amenazas		14 - 15. Esta normativa revisa periódicamente la disponibilidad de recursos, la infraestructura, los cambios de la organización y todo esto para verificar si se llega a lo esperado o no, y esta auditoría debe ser documentada con las opiniones, y evaluaciones realizadas.	14-15 La gerencia debe formar un equipo de auditores que revisen de manera periódica las actividades y lograr analizar la eficiencia de lo establecido desde el principio del programa de gestión, es de recordar que todo proceso por los auditores debe ser documentado en detalle tras cada actividad realizado y tras cada nuevo hallazgo.

Puntos para dar comienzo al plan	15. Revisión del SGSI para determinar periódicamente su eficacia, y dando oportunidad de cambio o mejoramiento de las falencias encontradas, además de la documentación de lo encontrado y de las necesidades que servirán para mejorar los procesos.			15 - 16. En esta normativa se explica que el plan de continuidad del negocio debe estar bajo una revisión continua ya que la tecnología y la vida de la empresa y todo lo que la rodea puede cambiar de manera constante, como regla general para todo BCP este debe revisado constantemente y dicha revisión debe centrarse en los siguientes elementos: requisitos operacionales, requisitos de seguridad, procedimientos		

Puntos para dar comienzo al plan	16. Acciones preventivas y correctivas de los errores encontrados, estas acciones deben ser aplicadas en los tiempos y en las actividades correctas y que son vitales para el buen funcionamiento de la organización.		16. La organización debe mejorar la eficiencia del SGCN a través de acciones preventivas que protejan de manera anticipada a la organización de problemas potenciales y acciones correctivas que eliminen las amenazas y que aseguren la no ocurrencia de las mismas, estas acciones deben estar acordes a la magnitudes de la amenaza y deben estar acorde a los objetivos de la organización.	técnicos hardware, software y otros equipos (tipos, especificaciones y cantidad), nombres e información de contacto de proveedores, incluyendo alternativo y fuera de las instalaciones del proveedor, alternativas y requisitos de las instalaciones fuera del sitio estos puntos son utilizados normalmente para conocer el funcionamiento y verificar que los procesos están en correcto estado y si están cumpliendo con los esperado	16. Esta normativa deja en claro que es necesario establecer procesos de acción correctiva para subsanar las deficiencias encontradas, esta normativa no es clara en la manera de desarrollar procedimientos.	16. Tras el análisis de las actividades de la organización, los auditores dan los resultados encontrados y se determina las modificaciones que tendrá el BCP dando como resultado la mejora continua de las actividades realizadas.

Controles de esta norma?	**Políticas de Seguridad de la información**: Esta norma desea controlar que la gerencia desarrolle una documentación completa de la políticas y que periódicamente sean revisadas para proponer cambios o mejoras al mismo.	**Políticas de seguridad, documentación y revisión: E**l objetivo es proporcionar orientación por parte de la dirección, manteniendo en toda la organización normas y leyes que contribuyan a la estabilidad de la misma. La dirección debe demostrar su apoyo y compromiso comunicando en la organización los cambios y nuevas políticas. las políticas deben ser revisadas a intervalos determinados para verificar su eficiencia y suficiencia en los procesos de la organización.	Esta normativa da como objetivo primordial el establecimiento de políticas y actividades de control que ayuden al mejoramiento de las actividades de la organización y que deben ser creadas y administradas por la gerencia como compromiso al buen desempeño de los procesos de la empresa.	Esta normativa sugiere el desarrollo de políticas que abarquen los objetivos generales de empresa, las responsabilidades, el desarrollo de las estrategias y la identificación de los controles preventivos para la planificación de las contingencias.	Esta normativa no expone controles, da la posibilidad al usuario de tener claro lo que se debe hacer y que tener en cuenta pero no expone controles directos para realizar las políticas de seguridad de la información.	La gerencia es la responsable de realiza políticas que abarquen el desarrollo e implementación de BCP y que no intervenga con las metas de la empresa.
Controles de esta norma?	**Organización interna**: lo que se desea controlar es el apoyo continuo de la gerencia en el desarrollo de los planes de seguridad, asignar responsabilidades, reiterar continuamente la confidencialidad a la que están sujetos los integrantes de este plan y hacer en tiempos programados controles de los procesos y actividades especificados en el SGSI.	**Organización de la seguridad:** el objetivo de este control es gestionar la seguridad de la información y crear un marco de referencia para dar comienzo a la seguridad, la dirección como en todos los procesos de la organización debe estar fuertemente ligada y comprometida a apoyar activamente los procesos internos. los procesos deben ser controlados por personal asignado a ellos con roles y responsabilidades aparte	La organización debe realizar controles continuos de sus actividades, debe regir en la al interior de la misma normativas que contribuyan al desarrollo exitoso del SGCN, se debe establecer de forma detallada la participación de las directivas ya que estos son los encargados de hacer cumplir lo impuesto en el plan de la continuidad.	Esta sugiere la participación continua del CIO (Chief Information Officer) y la gerencia de la organización en el desarrollo total del BCP y las políticas que lo rigen.,		En esta normativa surge como punto importante la cooperación de la directiva ya que es responsable de aprovisionar a la organización de los recursos necesarios para el desarrollo del programa, además la gerencia es responsable de asignar responsabilidades y garantizar que comunicar a los empleados la importancia del BCP

Controles de esta norma?	**Organización Externa**: lo que se desea controlar es la identificación de los riesgos que trae dar acceso a la información a agentes externos.	**Partes Externas:** el objetivo es mantener la seguridad de las partes de la organización que son procesadas o en la que intervienen partes ajenas a esta, se desea controlar accesos, procesos y comunicación que debe manejar los agentes externos, también es fundamental mantener la seguridad de todos los recursos de la organización que brindan sus servicios a clientes que usan frecuentemente los recursos de la entidad y dejar de manera escrita y de manera entendible las normativas y los procedimientos para mantener y establecer la seguridad en los tratados con terceros.	Esta normativa no especifica el control que se debe tener sobre los agentes externos o terceros que tienen control y acceso a información vital de la organización.	Esta normativa no especifica el control que se debe tener sobre los agentes externos o terceros que tienen control y acceso a información vital de la organización.	Esta normativa no especifica el control que se debe tener sobre los agentes externos o terceros que tienen control y acceso a información vital de la organización.	Esta normativa no especifica el control que se debe tener sobre los agentes externos o terceros que tienen control y acceso a información vital de la organización.
Controles de esta norma?	**Gestión de Activos**: el objetivo de este control documentar los activos de gran importancia y controlar el buen uso de los mismos.	**Gestión de Activos**: implementar y mantener una adecuada protección a los activos de la organización asignando responsables al cuidado de los mismos, además se debe llevar una documentación adecuada de los activos informáticos, de servicio y físicos.	Esta normativa no especifica cómo realizar la adecuada gestión de activos para el desarrollo efectivo de la seguridad del SGCN.	Esta normativa no especifica cómo realizar la adecuada gestión de activos para el desarrollo efectivo de la seguridad del SGCN.	**Gestión de Recursos:** esta normativa sugiere la creación de un sistema de identificación de activos y recursos como personas, equipos, instalaciones y tecnología que ayude al acceso oportuno de los recursos que contribuyan a la preparación de la continuidad frente a cualquier incidente. La gestión de activos debe incluir las	Aunque no se habla directamente de cómo se deben gestionar los recursos queda muy claro que la importancia del registro de estos es fundamental para la continuidad del negocio.

					siguientes tareas: Inventario de los recursos, clasificación de recursos, recursos de más importancia que ayuden a la continuidad, responsables de los recursos.	
Controles de esta norma?	**Seguridad física y ambiental**: se desea controlar las áreas seguras, estabilidad en las conexiones, control de ingreso de personal y asegurarse que los equipos de cómputo no sean extraídos de la entidad. Establecer áreas donde se los activos no se vean afectados por amenazas ambientales.	**Seguridad física y ambiental:** se desea creas áreas seguras donde se establezcan perímetros de seguridad, controles de acceso físico, seguridad en las oficinas de la organización, donde la protección de los activos frente a amenazas ambientales este establecida y controlar las áreas donde las personas no autorizadas tienen acceso.	Esta normativa no especifica cómo gestionar la seguridad de la infraestructura en la implementación del SGCN.	En esta normativa no se especifica que metodología es la apropiada para gestionar las infraestructura física de la empresa pero toma muy en cuenta la importancia de tener otra sede que cumpla con estándares de seguridad que ayuden a tomar de nueva la continuidad de las actividades de la empresa	Esta normativa no toma muy en cuenta la seguridad de la infraestructura física de la organización.	Esta normativa no toma muy en cuenta la seguridad de la infraestructura física de la organización.

Controles de esta norma?	**Gestión de las comunicaciones y operaciones:** trata de controlar el buen uso de los medios informáticos, controla las forma de dar servicios a terceros, controla que las operaciones dentro de la empresa estén correctamente configuradas para evitar fallas, controlar la seguridad del software, controla el desarrollo de un back-up periódico de los activos de información, control del intercambio de medios y de información con agentes externos, controlar la seguridad de los registros desarrollados en las auditorias.	**Gestión de comunicación y operaciones:** el objetivo es documentar detalladamente todos los procedimientos que se realizan en las operaciones cotidianas de la organización, se debe documentar de manera explícita los cambios realizados en las actividades, los impactos potenciales que tendrían los cambios y controlar que las áreas de trabajo estén separadas para evitar fraudes y cambios inesperados. Además de lo antedicho se desea establecer la capacidad del sistema implementado, los controles sobre código malicioso, los backups de los sistemas actuales, proteger la interconexión entre sistemas en la trasmisión de datos.	Esta normativa pretende que los resultados de la respuesta de la organización ante las emergencias sean comunicadas de manera clara por las personas adecuadas a los integrantes de la organización.	Esta normativa específica la importancia de la buena comunicación de la información entre los integrantes de la empresa, además de la documentación y distribución de la misma entre las personas responsables del BCP	Comunicaciones y Advertencias: la entidad deberá determinar las necesidad de comunicación y alerta, la comunicación debe ser redundante y confiable, la entidad debe tener una central de comunicaciones que ayude con la transmisión de la comunicación en toda las zonas de la entidad.	La organización debe mantener de manera estable la comunicación de todos los interesados en el bienestar de la empresa tanto internos como agentes externos que pueden ser de gran ayuda en el momento de una interrupción. La organización puede determinar si la comunicación llegue al extremo de dar a conocer sus debilidades y riesgos aunque podría ser una ayuda puede ser un riesgo adicional aprovechado por entidades externas y afectaría aun más la seguridad de la organización y sus actividades.

Controles de esta norma?	**Control de acceso:** establecer políticas de seguridad que especifiquen los métodos de acceso a la información y las personas autorizadas para el acceso a la información, revisión periódica de los permisos de acceso.	**Control de Acceso**: el objetivo en establecer políticas que sean viables para el acceso y que fomenten la seguridad del negocio, se debe registrar de manera adecuada los permisos acceso y los usuarios a los cuales afecta, es de gran importancia la gestión de los privilegios asignados y las contraseñas de acceso que son usadas por los usuarios, la directiva deben reevaluar los privilegios asignados y determinar si aun son necesarios, además de la gestión se debe controlar el acceso a la red y su administración, se desea controlar la autenticación correcta de los usuarios del exterior de la empresa, y el comportamiento de los dispositivos de acceso a la misma.	Esta normativa no especifica los métodos adecuados para controlar los accesos al personal de la organización y agentes externos que intervengan en los procesos vitales de la empresa.	Esta normativa no especifica los métodos adecuados para controlar los accesos al personal de la organización y agentes externos que intervengan en los procesos vitales de la empresa.	Esta normativa no especifica los métodos adecuados para controlar los accesos al personal de la organización y agentes externos que intervengan en los procesos vitales de la empresa.	Esta normativa no especifica los métodos adecuados para controlar los accesos al personal de la organización y agentes externos que intervengan en los procesos vitales de la empresa.

Controles de esta norma?	**Adquisición, desarrollo y mantenimiento:** Lo que se desea es saber que la seguridad implementada sea parte de todos los sistemas vitales de la organización, además evitar los errores, pérdidas o modificaciones sin permiso de archivos o código fuente (Uso de Criptografía) de las aplicaciones vitales de la organización. Como punto vital para este control esta registrar los cambios realizados en el software y sistemas operativos, desarrollar pruebas a los cambios realizados para verificar si no impactan en gran medida a los aplicativos fundamentales de la organización.	**Adquisición, desarrollo y mantenimiento de los sistemas de información:** El objetivo es asegurar que la seguridad sea parte fundamental de los sistemas de información, se debe analizar los requerimientos de seguridad, detallar las necesidades y establecer la seguridad necesaria desde el comienzo del plan, tomando como punto de partida establecer el correcto funcionamiento de las aplicaciones, validando los datos de entrada como claves, respuesta adecuada a los errores y la no divulgación de información. Además se desea que los procesos internos de las aplicaciones reduzcan al mínimo la corrupción de información. al realizar pruebas se desea el no uso de bases de datos que contengan información real, realizar controles del código fuente de las aplicaciones que permitan la ubicación de funciones no permitidas.	Esta normativa deja claro que el desarrollo, mantenimiento y mejora de los procesos deben cumplir con los requerimientos plasmados en el inicio del estudio del desarrollo del SGCN, todos los procesos de desarrollo y mantenimiento de los sistemas deben ser documentados de manera clara ya que esta información servirá para futuros procesos de corrección y prevención de fallas.	Esta normativa específica que la mejora continua es la clave para el desarrollo adecuado de las actividades del BCP y que deben ser analizadas contantemente para lograr un equilibrio entre la vida de la empresa y las actividades que se deben hacer frente una amenaza.		

Controles de esta norma?	**Gestión de incidentes en la seguridad de la información:** reportar las debilidades de la seguridad implementada de manera clara que ayude a su corrección inmediata, además asignar responsabilidades a los empleados para asegurar la respuesta inmediata en caso de riesgo.	**Gestión de incidentes de la seguridad de la información:** Se pretende establecer una metodología que ayude al reporte oportuno de incidentes y debilidades de la seguridad, se desea que los empleados o terceros tengan el conocimiento de las responsabilidades de reportar alguna brecha de seguridad, la información de estos reportes deben ser documentados de manera histórica para futuros estudios y establecimiento de debilidades recurrentes que afecten el servicio de la empresa.		Esta normativa no especifica cómo se debe avisar oportunamente los incidentes o riesgos conocidos, solo explica la importancia del desarrollo del BIA y la identificación oportuna de los riesgos que afectan a la empresa, además de los recursos críticos .	La entidad debe desarrolla un sistema de gestión de incidencias que ayude a dirigir, controlar las operaciones de respuesta. Este sistema deberá describir las funciones específicas de la organización, además se deben desarrollar políticas que contribuyan a la mitigación y gestión de incidentes además de mantener una comunicación constante con los interesados en el desarrollo continuo de las actividades de la empresa.	
Controles de esta norma?	**Gestión de la continuidad comercial:** el objetivo de este control es el de evitar que las actividades de la organización se frenen por motivos externos, esto se logra realizando un estudio de los requerimientos de seguridad de todas las actividades vitales de la organización, se debe identificar las principales causas con las cuales se afectaría el funcionamiento de las actividades de la empresa, para lograr que estos hallazgos tengan	Esta norma no establece ninguna metodología o pasos claros para establecer un BCP	Esta normativa determina las actividades necesarias para controlar y gestionar los incidentes y así garantizar la recuperación y tratamiento oportuno de los mismos.	Esta normativa da los pasos necesarios para establecer el proceso de continuidad	Esta normativa muestra los campos a cubrir en el desarrollo de un Programa que colabore con la continuidad del negocio	
			a. Tener un propósito y un alcance	Conocer las políticas y requerimientos necesarios para la implementación del BCP y obtener la aprobación de su implementación	Dejar claro el propósito las metas, las políticas que se utilizaran para el desarrollo del programa.	

	solución se debe desarrollar un Plan donde se mantenga y se asegure que la información estará disponible para asegurar la continuidad del negocio.		b. Tener propietarios que sean responsables de la revisión del SGCN.	Identificar los recursos y actividades críticos y establecer su importancia	Identificar los recursos necesarios y sus propietarios, los recursos deben ser tanto humanos, como tecnológicos, estos recursos deben ayudar a la continuidad del negocio.	Establecer responsabilidades de las personas a interactuar con el sistema y proveer de recursos que sean necesarios para la puesta en marcha del sistema de gestión.
			c. Establecer líneas de comunicación.	Establecer métodos de tratamiento de riesgos y permitiendo a los empleados conocer estos métodos de una manera clara, fomentando la buena comunicación.	La empresa determinara el método de comunicación y redundancia de la misma, además de establecer una comunicación constante entre los integrantes del programa	La organización es responsable por documentar y comunicar los cambios en los planes, sistemas de gestión , los resultados de la evaluaciones y funciones de la organización, debe fomentar la comunicación interna y externa, debe comunicar sobre los riesgos aceptado, el tramite de los riesgos y las inminentes amenazas que afectarían la organización.
			d. Información de tareas principales para la empresa.			Se documentara toda la información de la empresa y sus principales funciones.
			e. Definir grupos o individuos con sus roles y responsabilidades.	Se establece personas adecuado para la implementación y se define que roles tendrá en el BCP	Definir los roles y responsabilidades de las personas a activar y desarrollar el programa.	Se definirán roles y responsabilidades a las personas que integren el grupo que ayudara a la gestión.
			f. Determinar el método y las circunstancias en las cuales se activa el plan.	Determinar estrategias donde se dé solución a los riesgos encontrados.	Determinar cómo se trataran los riesgos, si existe la posibilidad de ayuda externa para lograr la normalidad de las actividades cotidianas	Esta normativa no establece ni la forma ni el momento para activar el plan de gestión.
			g. Proceso de retorno a la normalidad.			

			h. Los detalles para gestionar los incidentes de forma inmediata.	Establecer estrategias que deben ser desarrolladas por la empresa	Esta normativa no establece como deben ser tratados ni tampoco con que tiempo de respuesta pero explica la importancia del BIA y el análisis de riesgos para lograr el control y la continuidad	La organización establecerá la metodología necesario para el análisis y tratamiento por medio de estrategias la gestión de riesgos
			i. Los detalles sobre cómo se le comunican a los empleados lo sucedido con los incidentes.	Se establece una comunicación constante con los personas integrantes de la organización que intervengan en el desarrollo e implementación del BCP	Capacitaciones constantes de los empleados, dando a conocer lo aprendido después de una catástrofe, tomando como recuso más importante la bitácora de los sucedido.	Se deberá comunicar a los empleados de los sucesos encontrados y los eventos por desarrollar en el desarrollo del programa.
			j. Describir el método para registrar la información	Documentar la información de manera clara donde cualquier integrante de la empresa lo pueda usar.	El registro constante de la información ayuda a aprender y conocer de alguna fuente directa lo sucedido tras una catástrofe y conocer que salió bien y que no fue efectivo para el tratamiento de riesgos-.	Esta normativa explica la importancia de la documentación de los eventos, procesos y actividades del programa pero no especifica la metodología a implementar.

TECNOLOGÍAS DE LA INFORMACIÓN

Plan de Continuidad del Negocio

PROYECTO RUTA DEL SOL SECTOR 2

PLAN DE CONTINUIDAD DEL NEGOCIO

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

Para el desarrollo del presente Plan de Continuidad del Negocio se tomó como referencia el análisis y la comparación de las normativas existentes conocidas como ISO/IEC 27001:2005, ISO/IEC 27002:2007, NTC 5722, NIST 800-34, NFPA1600:2010 Y ASIS SPC.1:2009 que permitirá a la empresa establecerlo como un instrumento en la continuidad de las actividades y operaciones tecnológicas, que soporta los procesos más esenciales frente a una crisis que genere interrupción, garantizando las posibilidades de supervivencia y disminuyendo el impacto en las pérdidas que podría afectar la credibilidad de la empresa.

Objetivo.

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

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

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

Alcance.

El diseño de este plan solo contempla el área de Tecnologías e información del proyecto Ruta del Sol – Sector 2.

IDENTIICACIÓN Y CATEGORIZACIÓN DE AMENAZAS, RIESGOS Y VULNERABILIDADES EN LA EMPRESA

-Identificación de amenazas

Teniendo en cuenta el entorno donde se encuentra ubicada la sede principal del tramo norte de la empresa, y los ataques históricos, las fuentes de amenazas identificadas son:

FUENTE DE AMENAZA	MOTIVOS	AMENAZAS
Amenaza Humana	Vandalismo Intereses económicos Venganza Destrucción infraestructura física Ventaja competitiva Curiosidad Huelga Ego Inteligencia Errores y omisiones no intencionales	Robo de información Robo y destrucción de equipos Actividades fraudulentas Ingeniería social Daños a los activos físicos Asalto a un empleado Soborno
Amenaza Tecnológica	Intereses económicos Venganza Curiosidad Ego Inteligencia Reto Rebelión Ventaja competitiva Espionaje	Hacking Destrucción de Información Divulgación de información Alteración de información Código malicioso Ingeniería Social Acceso no autorizado al sistema Suplantación Penetración al sistema Venta de información Errores del sistema
Amenaza Industrial	Fallos de energía Extremos de temperatura (Incendio/humedad) Polvo	Daños a los activos físicos ,Perdida de información, Errores del sistema, Explosiones Fugas, Derrames
	Lluvias torrenciales	Daños a los activos físicos

Amenaza Natural	Granizadas Vientos Fuertes	Perdida de información Errores del sistema

-Identificación de vulnerabilidades potenciales

VULNERABILIDAD	FUENTE DE AMENAZA	AMENAZA
No existe política y/o medida de soporte de seguridad para el manejo de los riesgos derivados del uso de equipos móviles.	Amenaza Humana y Tecnológica	Por medio de un asalto la información almacenada en este medio puede quedar a disposición de personas para actividades fraudulentas, uso indebido para realizar ingeniería social, soborno, divulgación de información, suplantación, y a través de códigos maliciosos también pueden acceder a dicho dispositivo.
No se realizan capacitaciones sobre la concientización de la seguridad y el adecuado manejo de la información.	Amenaza Humana y Tecnológica	El personal al no tomar conciencia de la importancia de un adecuado manejo de la información puede exponer por error y omisiones no intencionales dicha información de la empresa que puede ser utilizada para actividades fraudulentas, uso indebido para realizar ingeniería social, soborno, divulgación de información y suplantación. Los empleados pueden ejecutar sin conocimiento alguno códigos maliciosos enviados por correos electrónicos y poner a disposición el acceso a criminales informáticos.
No se comunica al empleado que una vez finalizado el contrato permanecerán válidas las responsabilidades y tareas de seguridad de la información a la cual tuvo acceso.	Amenaza Humana	Los ex-empleados por omisión pueden divulgar información que puede ser utilizada para actividades fraudulentas, uso indebido para realizar ingeniería social, soborno, divulgación de información y suplantación.
No existe alarma para detectar humo.	Amenaza Industrial	No hay manera de tener una alerta frente a incidentes que podrían originar un

		incendio o explosión y así tomar medidas para extinguirlo y evacuar al personal.
No se implementan políticas de escritorio limpio de documentos, medios de almacenamiento removibles y pantalla limpia para la seguridad de la información.	Amenaza Humana	Al tener información expuesta se puede presentar sustracción de información, personal no autorizado que accede a los equipos o a documentación dejada en el escritorio que se expone para robo, destrucción y alteración de información, actividades fraudulentas, soborno.
Equipos de cómputo se encuentran ubicados en el piso de las oficinas.	Amenaza Natural	Daños en los activos físicos por ingreso de lluvia.
Los equipos de cómputo se encuentran expuestos de sufrir algún accidente de caídas libres de objetos pesados.	Amenaza Humana	Daños a los activos físicos.
Las copias de seguridad de algunos servidores se almacenan en el mismo lugar de los servidores copiados.	Amenaza Humana, Natural, Industrial y Tecnológica	Al sufrir algún tipo de incidente en los servidores también estarían en riesgo los Backups, y no se tendría el respaldo de la información.

-Categorías de Control con los que cuenta la empresa

N°	DESCRIPCIÓN DEL CONTROL	CATEGORÍA	
		Preventivos	**Detección**
1	Políticas de Seguridad.	**X**	
2	Control en compra de equipos tecnológicos y sus elementos.	**X**	
3	Seguridad en el ingreso y salida de las instalaciones físicas.	**X**	
4	Control de desechos tecnológicos.	**X**	
5	Tarjeta de responsabilidad	**X**	
6	Asignación de perfiles	**X**	
7	Cambios periódicos de contraseña	**X**	
8	Antivirus		**X**

9	Cifrado de correo (Gerencia)	**X**	
10	Segmentación de la red	**X**	
11	Control de tráfico de internet a través de Juniper		**X**
12	Copias de seguridad periódicas en servidores	**X**	
13	Control de Bloqueo en Impresiones	**X**	

-Niveles de Probabilidad

La probabilidad de que una vulnerabilidad potencial pueda ser ejercida por una fuente de amenaza determinada puede ser clasificada como alto, medio o bajo.

NIVEL	DEFINICIÓN DE LA PROBABILIDAD
ALTA	La fuente de la amenaza está altamente motivada y capaz, los controles para prevenir las vulnerabilidades son ineficaces.
MEDIA	La fuente de la amenaza está motivada, pero hay controles que dificultan el ejercicio exitoso de la vulnerabilidad.
BAJA	La fuente de amenaza carece de motivación o capacidad, o los controles previenen, o por lo menos obstaculizan significativamente la vulnerabilidad de ser ejercida.

-Análisis de Impacto

Este análisis prioriza los niveles de impactos asociados con el compromiso de los activos de información de una organización basados en una evaluación cualitativa o cuantitativa de la sensibilidad y criticidad de dichos activos, una evaluación de la criticidad de los activos identifica y prioriza la información sensible y critica de la organización.

Magnitud del impacto:

NIVEL	DESCRIPCIÓN DEL IMPACTO
ALTA	La vulnerabilidad ejercida: 1. Puede resultar en la pérdida de un alto costo de los principales activos tangibles o recursos 2. De manera significativa puede violar, dañar, o impedir la misión de una organización, la reputación o los intereses 3. Puede resultar en la muerte humana o lesiones graves.
MEDIA	La vulnerabilidad ejercida: 1. Puede resultar en la pérdida costosa de activos materiales o recursos 2. Pueda violar, dañar, o impedir la misión de una organización, la reputación o los intereses 3. Puede resultar en lesiones.
BAJA	La vulnerabilidad ejercida: 1. puede resultar en la pérdida de algunos bienes, materiales o recursos 2. Puede afectar notablemente la misión de una organización, la reputación o los intereses.

Además, se han establecido Tiempo de Repuesta RTO (Recovery Time Objective):

Es el tiempo transcurrido entre una interrupción y la recuperación del servicio, este indica el tiempo disponible para recuperar el sistema y los recursos interrumpidos.

Tiempo de respuesta:

NIVEL	RTO
ALTA	5 horas
MEDIO	24 horas
BAJO	72 o más horas

Punto de recuperación:

NIVEL	RPO
ALTA	4 horas
MEDIO	10 horas
BAJO	24 o más horas

-DETERMINACIÓN DEL RIESGO

La siguiente matriz es una matriz 3x3 de probabilidad de amenaza (Alto, medio y bajo]) y el impacto de la amenaza (Alto, medio y bajo).

La matriz en la siguiente tabla muestra como los niveles de riesgo global de alto, medio y bajo. Se asigna la probabilidad para cada nivel de probabilidad y un valor para cada nivel de impacto, por ejemplo para la probabilidad asignada para cada nivel de probabilidad es: 1.0 para alto, 0.5 para medio y 0.1 para bajo, y el valor asignado para cada nivel de impacto es 100 para alto, 50 para medio y 10 para bajo como se evidencia en la siguiente tabla:

PROBABILIDAD DE LA AMENAZA	**IMPACTO**		
	Bajo (10)	Medio (50)	Alto (100)
Alto (1,0)	**BAJO** 10X1.0=10	**MEDIO** 50X1.0=50	**ALTO** 100X1.0=100
Medio (0.5)	**BAJO** 10X0.5=5	**MEDIO** 50X0.5=25	**MEDIO** 100X0.5=50
Bajo (0.1)	**BAJO** 10X0.1=1	**BAJO** 50X0.1=5	**BAJO** 100X0.1=10

NIVEL	DESCRIPCIÓN DEL RIESGO Y ACCIONES NECESARIAS
Alta	Si una observación o hallazgo se evalúa como Alto Riesgo, existe una gran necesidad de medidas correctivas. Un sistema existente puede seguir funcionando, pero un plan de acción correctiva debe ser puesto en marcha lo antes posible.
Media	Si una observación es clasificada como Riesgo Medio, se necesitan acciones correctivas y se debe desarrollar un plan para incorporar estas acciones dentro de un período de tiempo razonable.
Baja	Si una observación se describe como Bajo Riesgo, se debe determinar si aún se requieren acciones correctivas o decidir aceptar el riesgo.

-Evaluación del riesgo:

Una vez identificada las amenazas, las fuentes de estas amenazas, las vulnerabilidades potenciales, los controles implementados por la empresa que aplican a cada vulnerabilidad, la probabilidad de ocurrencia y el grado de impacto al potencializarse una amenaza, se determina y evalúa el riesgo que tendría la empresa al materializarse dicha vulnerabilidad.

A través de la siguiente herramienta de control y gestión denominada matriz de riesgo identificamos de manera temprana aquello que amenaza el cumplimiento de los objetivos de la empresa e identificamos las actividades que requieren mayor atención y las áreas críticas de riesgo, cruzamos las amenazas, vulnerabilidades identificadas y los controles para que con esta herramienta determinemos el estado de la empresa con respecto al riesgo.

N	Vulnerabilidad	Fuente de amenaza	Amenaza	Control	Probabilidad de Ocurrencia		Impacto				Riesgo		Descripción nivel del riesgo
					Nivel	Valor	Nivel	Valor	RTO	RPO	Nivel	Valor	
1	No existe política y/o medida de soporte de seguridad para el manejo de los riesgos derivados del uso de equipos móviles.	Amenaza Humana y tecnológica	Por medio de un asalto la información almacenada en este medio puede quedar a disposición de personas para actividades fraudulentas, uso indebido para realizar ingeniería social, soborno, divulgación de información, suplantación, y a través de códigos maliciosos también pueden acceder a dicho dispositivo.	-	ALTO	1.0	ALTO	100	ALTO 5 Horas	ALTO 4 Horas	ALTO	100	Si una observación o hallazgo se evalúa como Alto Riesgo, existe una gran necesidad de medidas correctivas. Un sistema existente puede seguir funcionando, pero un plan de acción correctiva debe ser puesto en marcha lo antes posible.
2	No se realizan capacitaciones sobre la concientización de la seguridad y el adecuado manejo de la información.	Amenaza Humana y tecnológica	El personal al no tomar conciencia de la importancia de un adecuado manejo de la información puede exponer por error y omisiones no intencionales dicha información de la empresa que puede ser utilizada para actividades fraudulentas, uso indebido para realizar ingeniería social, soborno, divulgación de información y suplantación. Los empleados pueden ejecutar sin conocimiento alguno códigos maliciosos enviados por correos electrónicos y poner a disposición el acceso a criminales informáticos.	6,7,8 Y 9	MEDIO	0.5	ALTO	100	ALTO 5 Horas	ALTO 4 Horas	MEDIO	50	Si una observación es clasificada como Riesgo Medio, se necesitan acciones correctivas y se debe desarrollar un plan para incorporar estas acciones dentro de un período de tiempo razonable.
3	No se comunica al empleado que una vez finalizado el contrato permanecerán válidas las responsabilidades y tareas de seguridad de la información a la cual tuvo acceso.	Amenaza Humana	Los ex empleados por omisión pueden divulgar información que puede ser utilizada para actividades fraudulentas, uso indebido para realizar ingeniería social, soborno, divulgación de información y suplantación.	-	ALTO	1.O	ALTO	100	ALTO 5 Horas	ALTO 4 Horas	ALTO	100	Si una observación o hallazgo se evalúa como Alto Riesgo, existe una gran necesidad de medidas correctivas. Un sistema existente puede seguir funcionando, pero un plan de acción correctiva debe ser puesto en marcha lo antes posible.

N	Vulnerabilidad	Fuente de amenaza	Amenaza	Control	Probabilidad de Ocurrencia		Impacto				Riesgo		Descripción nivel del riesgo
					Nivel	Valor	Nivel	Valor	RTO	RPO	Nivel	Valor	
4	No existe alarma para detectar humo.	Amenaza Humana	No hay manera de tener una alerta frente a incidentes que podrían originar un incendio o explosión y así tomar medidas para extinguirlo y evacuar al personal.	-	ALTO	1.0	ALTO	100	ALTO 5 Horas	ALTO 4 Horas	ALTO	100	Si una observación o hallazgo se evalúa como Alto Riesgo, existe una gran necesidad de medidas correctivas. Un sistema existente puede seguir funcionando, pero un plan de acción correctiva debe ser puesto en marcha lo antes posible.
5	No se implementan políticas de escritorio limpio de documentos, medios de almacenamiento removibles y pantalla limpia para la seguridad de la información.	Amenaza Humana	Al tener información expuesta se puede presentar sustracción de información, personal no autorizado que accede a los equipos o a documentación dejada en el escritorio que se expone para robo, destrucción y alteración de información, actividades fraudulentas, sobomo.	-	ALTO	1.0	ALTO	100	ALTO 5 Horas	ALTO 4 Horas	ALTO	100	Si una observación o hallazgo se evalúa como Alto Riesgo, existe una gran necesidad de medidas correctivas. Un sistema existente puede seguir funcionando, pero un plan de acción correctiva debe ser puesto en marcha lo antes posible.
6	Equipos de cómputo se encuentran ubicados en el piso de las oficinas.	Amenaza Natural	Daños en los activos físicos por ingreso de lluvia.	-	ALTO	1.0	MEDIO	50	MEDIO 24 Horas	MEDIO 10 Horas	MEDIO	50	Si una observación es clasificada como Riesgo Medio, se necesitan acciones correctivas y se debe desarrollar un plan para incorporar estas acciones dentro de un período de tiempo razonable.

N	Vulnerabilidad	Fuente de amenaza	Amenaza	Control	Probabilidad de Ocurrencia		Impacto				Riesgo		Descripción nivel del riesgo
					Nivel	Valor	Nivel	Valor	RTO	RPO	Nivel	Valor	

.RECOMENDACIONES DE CONTROL

La meta de las recomendaciones de control es reducir el nivel de riesgo identificado, es necesario tener en cuenta los siguientes factores:

- Implementar política y/o medida de seguridad para el manejo de riesgo en el uso de equipos móviles.
- Socializar y certificar que los empleados conocen y acatan plenamente que una vez finalizado el contrato permanecerán válidas las responsabilidades y tareas de seguridad de la información a la cual tuvo acceso.
- Implementar alarma contra incendios.
- Diseñar e implementar programas de capacitación y concientización en las personas sobre la importancia de mantener un escritorio limpio de documentos y el escritorio del equipo de cómputo limpio de carpetas y/o documentos importantes, que los empleados al retirarse de su puesto de trabajo siempre bloqueen sus equipos para evitar acceso de personas externas.
- Almacenar los backups o respaldo de la información en un lugar seguro, ajeno y exterior a la empresa.
- Capacitar al personal sobre la concientización de la seguridad y el adecuado manejo de la información.
- Socializar al empleado la importancia de no abrir correos de remitentes desconocidos o con archivos adjuntos sospechosos e informar inmediatamente al responsable del área de TI.
- Ubicar las torres de los equipos de cómputo en una zona segura libre de incidentes, caídas de objetos pesados o amenazas naturales e informar al personal su importancia.
- Realizar ataques de seguridad constantes provocados por la empresa para chequear constancia y robustez en los servidores que contienen la información.
- Verificar y hacer pruebas periódicas de las copias de seguridad.

ESTRATEGIAS PARA LA CONTINUIDAD Y CREACIÓN DE POLITICAS

Es importante conocer cuáles son las personas o áreas que intervienen en las actividades más importantes de la empresa, con el objetivo de ubicar de manera adecuada a este personal en los lugares apropiados para garantizar que con sus conocimientos se podrán mantener en continuidad y funcionamiento las actividades de la empresa.

Para la eficacia de este plan se debe contar con el apoyo del Responsable Administrativo, Gerente Administrativo, Responsable de Seguridad Física y Responsable de Salud y Seguridad en el trabajo, reservas financieras, socialización previa del Plan de Continuidad con el fin de dar a conocer funciones y responsabilidades y mantener comunicación con contactos clave, todos los involucrados deben estar conscientes de todas las actividades a realizar para mitigar las amenazas y riesgos **q**ue lograrán una recuperación del negocio de forma rápida y efectiva.

-Recursos humanos.

Rol, funciones y responsabilidades

Responsable de la ejecución del Plan de Continuidad del Negocio.

Responsable de T.I – Yuly Paola Contreras Contreras

FUNCIONES Y RESPONSABILIDADES:

-Aprobar el Plan de Continuidad del Negocio.

-Comunicar y gestionar autorización por parte de las directivas los costos para los gastos necesarios y el cronograma para la restauración del ambiente de trabajo.

-Socializar el plan al personal involucrado.

-Dirigir los comunicados de apoyo en la ejecución del Plan de Contingencia a los directivos y responsables de áreas.

-Realizar reuniones periódicas informando actualización o cambios efectuados en el plan original.

-Seguimiento a las pruebas del correcto funcionamiento por lo menos dos veces al año o en el proceso de presentarse cambios que se ameriten.

-Detectar situación que represente riesgo y activar el estado de contingencia y ejecución del Plan de Continuidad.

-Autorizar el procedimiento a seguir en la ejecución del Plan, tomar decisiones correspondientes a la definición de las ubicaciones para instalar los equipos de cómputo alternos.

-Mantener actualizado el directorio de proveedores de servicios con los que cuenta la empresa.

-Dar reporte de los resultados y la evolución del plan de continuidad a las personas involucradas.

-Definir con las áreas correspondientes cuales son los sistemas de información, módulos y/o procedimientos de carácter crítico de la empresa.

-Desactivar el estado de contingencia

Coordinador de Servidores y Sistemas/Servicios

Ingeniero- Gabriel Pabón

-Realizar conexión y pruebas de los equipos de cómputo alternos en el tiempo que se considere necesario.

-Realizar la restauración y conexión alterna de Sistemas/Servicios de la empresa.

- Si se presenta contingencia que afecte a los equipos de cómputo y software es el responsable de restablecer dicho servicio en el menor tiempo posible.

Coordinador de Redes y Comunicaciones
Ingeniero- William Escalante
-Ejecutar los procedimientos a seguir cuando se active el estado de contingencia y estos afectan las comunicaciones, servicios de Internet, correo electrónico, red, etc. -Mantener actualizado los procedimientos en el plan y los requerimientos mínimos necesarios de software, servicios, líneas telefónicas, cuentas de acceso a internet, dispositivos de comunicación (Switchs, Routers, antenas, etc.) -Mantener actualizado el inventario de equipos tecnológicos y de redes con su respectivo responsable, su información de servicio de mantenimiento /reparaciones y garantías. -Efectuar las pruebas de operatividad necesarias para asegurar la continuidad del servicio en caso de un estado de contingencia.

Usuarios y/o Funcionarios del Consorcio Constructor Ruta del Sol.
-Deberá en primera instancia cuando se active el estado de contingencia apoyar para salvaguardar las vidas propias y de sus compañeros de trabajo. -Una vez la situación lo permita deberá contribuir en salvaguardara los bienes como el inmueble, equipos, documentación, etc. Y apoyar en el proceso de inventario de daños cuando sea solicitado. -Con responsabilidad, creatividad y disposición adaptarse a la circunstancia de contingencia que puede generar limitación en espacio, servicios, recursos y equipos de cómputo. -Cuando se declare finalizada el estado de contingencia deberá participar activamente en la

-Activación y desactivación del Plan.

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

-Estrategias de Recuperación para situación que se considere critica o con tiempo de recuperación larga

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

Torcoroma, Platanal y/o Puerto Boyacá, por lo tanto se tendría una ubicación de procesamiento con una configuración adecuada para lograr restaurar los servicios correctamente tan solo a unas pocas horas después de presentarse alguna interrupción sin costo alguno.

La responsable del área de T.I considera importante implementar estas opciones con el fin de tener un lugar alternativo y brindar a los puntos de trabajo como Lizama, Besote, Torcoroma, Platanal y/o Puerto Boyacá su punto alternativo en Aguachica, es decir aprovechar que la empresa tiene varios puntos de trabajo distribuidos en el Departamento para implementar un plan B entre la empresa sin tener costo y con su propia estructura de telecomunicaciones.

Para el proyecto Ruta del Sol se estudiara e implementara la opción de Mirror Site (Sitio espejo) aprovechando que se tiene varios opciones de ubicación alterna con los recursos necesarios correctamente configurados para lograr realizar las transacciones de cada servicio en paralelo con el centro de procesamiento principal Aguachica, y asignar al coordinador de servidores y sistemas/servicios la realización de pruebas periódicas que garantice la sincronía entre Aguachica y el de respaldo e implementar en aquellos lugares su lugar alternativo en Aguachica.
Se recomienda identificar y establecer con el área de Transporte el equipo necesario para transportar al personal al punto establecido para continuar con las funciones de la empresa

-Protocolo para situación de contingencia con tiempo corto de recuperación:

Proceso general:
Como prioridad debemos salvaguardar la vida propia y de los compañeros de trabajo, luego, dentro de lo posible es necesario identificar el lugar que origina la emergencia con el fin de ser controlado (si se está en capacidad de hacerlo y no afecte la vida propia o de alguien más) e informar al área de seguridad física la situación presentada,

ellos, según su procedimiento se encargarán de solicitar apoyo a las personas o entidades correspondientes.

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

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

Con el fin de conocer el procedimiento a seguir para cada caso específico, definimos las siguientes situaciones de emergencia que se pueden presentar para el área de T.I: Movimiento telúrico (temblor), Incendio, inundación y/o humedad, interrupción de energía, falla en el servicio de red/Voz, acceso no autorizado a la información lógica, acceso físico no autorizado a las oficinas de T.I, marchas pacíficas, marchas no pacificas o cierre de vía.

- **Movimiento telúrico (temblor):**

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

Medidas preventivas:

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

-Verificar que los equipos de cómputo y tecnológicos se encuentren fuera de sufrir algún accidente de caída libre de objeto pesado que genere interrupción del proceso de operación normal.
-Practicar simulacros para identificar los pasos a seguir y la ubicación más pertinente para evitar accidente durante el movimiento.
-Conocer dónde y cómo cerrar el paso de la electricidad, el gas y el agua en los interruptores y tomas principales.
-Mantener en la oficina un Kit de emergencia que contenga elementos de ayuda como linterna con pilas, botiquín de primeros auxilios, agua embotellada, pito, etc.

Durante la situación:
-Es importante que en lo posible se mantenga tranquilo y permanezca en un lugar seguro mientras dure el temblor.
-Dé solo los pasos que le permitan colocarse debajo de un lugar seguro, como un escritorio o mesa resistente
-Manténgase alejado de ventanas de vidrio, espejos, puertas o paredes y de todo lo que pueda caerle como lámparas y muebles

Después de la situación:
-Realizar el proceso de evacuación y desplazamiento a un sitio seguro indicados por el área de SST - Salud y Seguridad del Trabajo.
-Cuando la situación lo permita y se den las indicaciones por parte del área de SST volver a los lugares de trabajo.
-Realizar una inspección física en los puntos donde se encuentran ubicados los Switch (Oficina de T.I, Concesionaria, Oficina de Equipos, Centro medico, Almacén, Ingeniería Tramo 8, Oficina de Gerencia, comunicarse con las veredas de Besote, Torcoroma, Platanal, Morrison, y Pailitas para verificar si físicamente el Switch sufrió algún daño o tiene la probabilidad que ocurra por elementos a su alrededor, con el fin de garantizar la integridad de los activos materiales

Por lo general un sismo afecta únicamente parte de la estructura del edificio, por lo tanto no se verían afectados los datos, sin embargo, es importante verificar que las conexiones a estos dispositivos de comunicación no se hayan afectado.

Usualmente, luego de un movimiento telúrico el sistema de telefónica celular colapsa, por lo tanto es importante implementar algún sistema de comunicación ante alguna situación de emergencia, se recomienda utilizar los siguientes medios de comunicación: Los parlantes de emergencia que se encuentran ubicado en la oficina de Salud y Seguridad del Trabajo, mensajes cortos de texto (SMS), y/o Comunicación vía internet a través de la cuenta de correo electrónico corporativo.

- **Incendio:**

Medidas preventivas

-Para el área de T.I se cuenta con 2 extintores de tipo C a base de polvo químico, uno dentro de la oficina y el otro se encuentra ubicado fuera de la oficina, es importante hacerle seguimiento periódico de las fechas de vencimiento de dichas recargas e informar al área de Salud y Seguridad del Trabajo para que tomen las medidas pertinentes de cambio o recarga, y verificar que en las oficinas donde se encuentran los puntos de comunicación existan extintores en completo orden.

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

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

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

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

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

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

Durante la situación:

-Conservar la calma.

-Comprobar el punto donde se genera el incendio.

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

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

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

Después de la situación:

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

-Solicitar a un electricista de la oficina de Servicios Generales inspección del cableado.

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

-Revisar posibles nuevos focos de incendio.

- **Inundación/Humedad:**

Medidas preventivas:

-Practicar simulacros para identificar los pasos a seguir durante la situación.

-Solicitar la revisión cada cierto tiempo del estado de los desagües y sumideros.

-Verificar situaciones de humedad que pueden desencadenar el crecimiento del moho.

Durante la Situación:

-Evite caminar por aguas en movimiento.

-Suba a un lugar alto y permanezca allí.

-Si el tiempo lo permite, mueva a un lugar seguro los elementos que soportan los procesos críticos o que ayude a restablecerlo para cuando la situación de contingencia se desactive.
-Si la situación lo permite suspenda el servicio de luz, agua y gas y evacue.

Después de la situación.
-Realizar la inspección siempre que la situación lo permita y sea seguro, de la situación de la infraestructura de la oficina, haga los arreglos temporales mínimos necesarios.
-Realizar una lista de inventario de los daños y pérdidas, de ser posible tome fotografías, no deseche ninguno de los artículos dañados hasta realizarse el inventario oficial, la compañía de seguro toma en consideraciones todos los daños.
-Verificar que la situación no haya afectado las estaciones de trabajo y dispositivos de comunicación, de ser así, identificar si su daño es físico o lógico para ejecutar el procedimiento establecido.

- **Interrupción de energía**

Medidas preventivas:
-Revisar periódicamente la carga del UPS (Sistema de Alimentación Interrumpida) para los casos de corte de energía.
-Identificar cuanto es el tiempo que brindaría la UPS de soporte para la empresa teniendo en cuenta el tiempo de deterioro y los usuarios conectados a la corriente.
-Social izar al personal de la empresa la clasificación de conexión donde se especifica que dispositivos deben ir conectados a los tipos de corriente con los que cuenta la empresa (Regulada/No Regulada).
-Solicitar al área de Servicios Generales informes del estado y las revisiones periódicas de las instalaciones eléctricas.

Durante la situación:
-Verificar si la falla de energía es solo en un punto, en la empresa, o en toda la ciudad con el fin de informar a los empleados y tomar las medidas necesarias en cuanto al

almacenamiento de información para evitar perdida de datos por apagarse los dispositivos.
-Desconectar los equipos electrónicos que puedan verse afectados al retorno de la energía.

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

- **Falla en el servicio de Red/Voz**

Medidas preventivas:
-Informar en las oficinas donde están ubicados los puntos de comunicación que ante un fallo deben reportarlo y no manipular el Rack, Solo el personal autorizado podrá manipular estos puntos de comunicación.
-Planificar rutas de comunicación alternativas ante las diversas situaciones de fallo.

Durante la situación:
-De no ser posible restaurar la comunicación a través de los ingenieros de la empresa, comunicar al personal de soporte de las empresas que brindan dichos servicios.
-Informar al personal de la empresa el tiempo estimado de recuperación del servicio.

Después de la situación
-Verificar que el servicio este completamente activo y funcional.

- **Acceso no autorizado a la información lógica**

Medidas preventivas:
-Socializar medidas preventivas del buen uso de las herramientas informáticas y el manejo correcto para la seguridad de la información.
-Realizar pruebas del cumplimento de las políticas de seguridad sobre la seguridad de la información.

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

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

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

Durante la situación:

-Realizar cambios de contraseña.

-Bloquear el acceso a la información lógica.

Después de la situación

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

-Realizar cambios de contraseña si se considera necesario.

- **Acceso físico no autorizado a las oficinas de T.I**

Medidas preventivas:

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

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

Durante la situación:

-Abandonar el lugar donde se encuentra el intruso

-Informar inmediatamente al área de Seguridad Física.

Después de la situación:

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

- **Marchas pacificas**

Medidas preventivas:

-Solicitar al área de Seguridad Física informar de forma inmediata cuando se esté presentando, o se tenga información de una convocatoria para algún tipo de marcha con el fin de estar alertas.

Durante la situación:

-Cerrar la oficina de T.I

-Informar a las oficinas donde se encuentran los Racks estar alertas para cerrar el acceso físico.

-Estar alerta ante cualquier situación.

Después de la situación:

-Verificar con el área de Seguridad Física que dicha marcha pacífica no se haya salido de control e ingresado a la empresa sin autorización.

- **Marchas no pacificas o cierre de vía**

Medidas preventivas:

-Solicitar al área de Seguridad Física informar de forma inmediata cuando se esté presentando, o se tenga información de una convocatoria para algún tipo de marcha con el fin de estar alertas.

Durante la situación

-Cerrar la oficina de T.I

-Informar a las oficinas donde se encuentran los Racks estar alertas para cerrar el acceso físico.

-Estar alerta ante cualquier situación.

Después de la situación:

-Verificar con el área de Seguridad Física que los integrantes de la marcha no hayan accedido sin autorización a la empresa y por lo tanto a las oficinas.

PLAN DE PRUEBA

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

Objetivos a cumplir:

-Medir capacidad del lugar respaldo

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

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

-Evaluar costos de los posibles daños en la empresa

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

-Verificar el cubrimiento del Plan de Continuidad del Negocio.

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

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

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

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

Al finalizar la prueba se creará un informe con el fin de evaluar para cada situación de desastre el tiempo empleado para restaurar las funciones afectadas, identificar

problemas de aplicación de los procedimientos de recuperación, evaluación del personal encargado para realizar los procedimientos de recuperación y los recursos necesarios para su ejecución.

PLAN DE MANTENIMIENTO

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

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

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

Anexo 4. Socialización del plan de continuidad del negocio