**FORMATO PARA EL DESARROLLO DE COMPONENTE FORMATIVO**

|  |  |
| --- | --- |
| PROGRAMA DE FORMACIÓN | Implementación de auditoría técnica en continuidad y resiliencia |

|  |  |  |  |
| --- | --- | --- | --- |
| COMPETENCIA | 220601041 - Implementar sistemas de gestión según normatividad y requerimientos técnicos. | RESULTADOS DE APRENDIZAJE | 220601041-03 - Ejecutar los procesos operativos esenciales de la continuidad del negocio de  acuerdo con normativa.  220601042-04 - Implementar un proyecto del SGCN alineado con la normativa y estándares  existentes. |

|  |  |
| --- | --- |
| NÚMERO DEL COMPONENTE FORMATIVO | CF02 |
| NOMBRE DEL COMPONENTE FORMATIVO | Operación, implementación y mejora continua de un SGCN. |
| BREVE DESCRIPCIÓN | Este componente formativo está orientado al estudio de la implementación y operación de un SGCN, teniendo en cuenta los procesos de mejora continua que se puedan requerir a lo largo de su tiempo de vida. |
| PALABRAS CLAVE | Planificación, mejora continua, organización, sistema de gestión, tiempo de vida. |

|  |  |
| --- | --- |
| ÁREA OCUPACIONAL | VENTAS Y SERVICIOS |
| IDIOMA | Español |

1. **TABLA DE CONTENIDOS**

**Introducción**

**1. Planificación y control de operaciones**

1.1. Riesgos disruptivos

1.2. Evaluación de riesgos

**2. ¿Qué es el BIA?**

2.1. Medición del impacto de un BIA

2.2. Estrategias y plan de gestión de incidentes

**3. ¿Qué es un plan de continuidad del negocio?**

3.1. Evaluación de planes de continuidad de negocio

3.2. Características de los planes de continuidad

3.3. Normatividad

**4. ¿Qué es un centro de datos?**

4.1. Riesgos asociados a los centros de datos

4.2. Estrategias para el manejo de un centro de datos

**5. Monitoreo de procesos de continuidad de negocio**

5.1. ¿Qué es una auditoría interna?

5.2. ¿Cómo se aplica una auditoría interna a un SGCN?

5.3. Construcción de planes de mejora continua para un SGCN

5.4. Proceso de certificación de un SGCN

**6. Proyecto de implantación de un SGCN**

6.1 Riesgos al implementar un SGCN

6.2. Problemas frecuentes y solución de problemas

**Síntesis**

1. **INTRODUCCIÓN**

Hoy día para las empresas es necesario garantizar sus procesos de negocio, a través de la aplicación de estrategias basadas en aspectos tecnológicos (*hardware* y *software*) y en sus recursos humanos. La mayoría de los procesos de negocio tienen muchos enemigos, por decirle de alguna manera, aunque si se hace referencia a ellos, de manera técnica, se les conoce como riesgos, los cuales están presentes en cualquier ámbito empresarial y son los causantes de la afectación negativa parcial o total de los procesos de negocio.

Este componente formativo tiene como objetivo principal trabajar los conceptos y la manera en la que se debe implementar y operar un Sistema de Gestión de Continuidad de un Negocio (SGCN) junto con cada uno de los procesos a realizar para que este funcione de manera correcta, y a su vez se esté preparado para recuperarse en caso de sufrir un riesgo que detenga su correcto funcionamiento. El siguiente video presenta cómo la aplicación y apropiación de un SGCN pueden convertirse, además, de un mecanismo de prevención en una ventaja competitiva:

CF02\_video\_introducción

Existen muchos procesos de negocio que son esenciales para las empresas y por tanto se denominan «críticos del negocio». Son aquellos que hacen que la empresa preste los servicios de la manera más eficiente a sus clientes. De ahí que sean precisamente a estos a los cuales se les debe brindar la mayor fuerza de inversión y atención, sobre todo en procesos de continuidad; en otras palabras, son la razón de ser de la organización y la manera en cómo se mantienen presentes en el mercado. Si estos fallan o se detienen, la empresa pierde dinero y posicionamiento.

**1. Planificación y control de operaciones**

Es una estrategia que permite que los SGCN logren los objetivos para los cuales han sido diseñados e implementados: mejorar la confianza y respaldo de los procesos de negocio de la organización.

La planeación es un proceso que permite estructurar de manera organizada y eficiente las actividades que se deben desarrollar para cumplir el objetivo del SGCN. Una buena planificación es la base fundamental del éxito de cualquier proceso empresarial. En el siguiente interactivo se puede apreciar cómo esta se efectúa:

CF02\_1\_interactivo\_desarrollo planificación

|  |  |
| --- | --- |
|  |  |
| Hoy día la planificación lo es todo en una organización, ya que permite aprovechar los recursos de una manera óptima y efectiva. Un mal desarrollo de esta puede arruinar todo un proceso y hasta puede generar inconvenientes de funcionamiento a una organización. | |

El proceso de planificación es una de las etapas más importantes de cualquier proyecto o proceso a ejecutar. Existen diversas situaciones que requieren que los procesos no solo lleven parte de la ejecución de los mismos, sino también realicen una monitorización rigurosa para verificar que se esté cumpliendo de manera correcta con lo establecido.

|  |  |
| --- | --- |
| La lavagna per gestione progetti. Metodo Agile | Herramientas, tales como Trello, permiten gestionar cada proceso y saber en qué estado se encuentra en tiempo real. |

De igual forma, es importante tener en cuenta que las actividades que se relacionan con los SGCN deben sufrir un cambio en el transcurso del tiempo; es decir, su estado actual puede variar de acuerdo con las necesidades de la organización. Por ello, es indispensable tanto su continuo monitoreo como la asignación de un responsable directo, quien no solo debe realizar un acompañamiento y supervisión de las mismas, sino que debe velar porque el equipo de trabajo cuente con las herramientas necesarias para el desarrollo de sus acciones en el sistema de gestión.

Se debe establecer una ruta de trabajo basada en las actividades a realizar y en los tiempos de ejecución necesarios para las mismas, garantizando que estas se desarrollen con el menor traumatismo posible. No se trata de flexibilizar el trabajo sino comprometer al equipo en la importancia de los tiempos y actividades por cumplir en la organización. No obstante, cuando se ha llegado a un estado tal en que cada persona sabe lo que debe hacer, ya puede ser autónomo en su trabajo y corresponder con los entregables. Los procesos de orientación se utilizarán, entonces, para garantizar la correcta integración de todos los componentes en la organización.

Se recomienda tener en cuenta los siguientes aspectos para tener un control adecuado de la ruta de trabajo (ver figura 1):

**Figura 1**

*Recomendaciones*

CF02\_1\_figura\_recomendaciones

|  |  |
| --- | --- |
|  |  |
| Cabe decir que un control adecuado se garantiza cuando se tiene una ruta de trabajo y actividades bien definidas desde el principio. En muchas ocasiones se improvisan actividades y procesos los cuales no estaban en las versiones originales de la ejecución del proceso, trayendo consigo retrasos y problemas de comunicación más adelante y probablemente el fracaso del proyecto o actividades. | |

**1.1. Riesgos disruptivos**

Los riesgos disruptivos son situaciones que colocan en riesgo el correcto funcionamiento de los procesos que desarrolla una organización, los cuales pueden ser de carácter natural o artificial. La siguiente figura 2 presenta en cuáles aplican en cada clasificación:

**Figura 2**

*Tipos de riesgos*

CF02\_1\_1\_gráfico\_tipo de riesgo

Dentro de los riesgos naturales existe un grado de incertidumbre puesto que muchos de ellos son impredecibles; es decir, no se sabe con certeza cuándo se pueden presentar y qué afectaciones pueden generar; en cuyo caso es necesario realizar un análisis y/o investigar cuáles son las causales de riesgo que se pudiesen llegar a presentar, para así realizar medidas preventivas y por ende, planes de contingencia que definan los protocolos a seguir para retornar a los procesos de negocio de manera confiable y segura.

Ahora bien, de acuerdo con el nicho de negocio que la empresa tiene, así serán las causantes que se deben estudiar para establecer los planes de acción a ejecutar. A continuación, se presenta un ejemplo de una matriz de riesgo y la aplicación de los planes de acción a realizar en caso de que ocurra el incidente, medida en su tiempo de recuperación (ver tabla 1):

**Tabla 1**

*Ejemplo de matriz de riesgo*

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Matriz de riesgo y contingencia | | | | |
| Suceso | Frecuencia | Tiempo de recuperación | Atendido por | Observaciones |
| Daño del servidor principal. | Bajo | 30 minutos | Dulfran Montaño, Julio Castaño | Este suceso se ha presentado durante los últimos 5 meses 1 vez. |
| Posibles ataques al sitio web por temporada de promociones de productos. | Medio | 1 hora | Dulfran Montaño. | Este suceso se ha presentado 2 veces en el mes. |
| Falla de energía eléctrica. | Alto | 15 minutos | Julio Castaño | Este suceso se ha presentado 15 veces en lo que va corrido del mes. |

|  |
| --- |
| Como se puede observar, se deben establecer cuáles son los sucesos que pueden ocurrir y colocar en riesgo la continuidad del negocio. Establecer este tipo de riesgos más que analizar los sucesos y su trazabilidad en la contingencia, permite estudiar la competitividad de una empresa, ya que puede que en algunas regiones sean más susceptibles dichos sucesos que en otras, por ejemplo. De ahí la importancia de establecer, de acuerdo con esas realidades, que no se puede dejar a un lado la ejecución de planes de contingencia para la organización. |

Desde un contexto mucho más profundo, establecer la matriz de riesgo puede revelar condiciones que no son observables de manera directa dentro de la organización; es decir, al momento de determinar un suceso de riesgo este a su vez puede aportar una visión mucho más amplia de otros hechos que pueden generarse a raíz de este mismo. Es allí donde toma importancia los detalles del análisis y el estudio del nivel de impacto que pueden ocasionar, el cual se mide desde su frecuencia. Sumado a esto, también es fundamental la definición de acciones a realizar, las cuales se visualizan desde los puntos de vista preventivo y correctivo.

En la siguiente tabla 2, continuando con el ejemplo anterior, se ilustra el registro de sucesos presentados y su frecuencia.

**Tabla 2**

*Ejemplo de frecuencia de sucesos*

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Matriz de riesgo – frecuencia de sucesos | | | | |
| Suceso | Impacto | Plan de contingencia | Responsables | Acciones a realizar |
| Daño del servidor principal. | Alto | Activar el servidor de respaldo mientras se restablece el principal. | Dulfran Montaño, Julio Castaño | Se debe realizar la activación del servidor de respaldo que se encuentra en el rack continuo a las ups. |
| Posibles ataques al sitio web por temporada de promociones de productos. | Medio | Activar la VPN y un *firewall* adicional. | Dulfran Montaño. | Redireccionar todas las conexiones externas a la red de la empresa por la vpn para establecer un canal seguro de comunicación. |
| Falla de energía eléctrica. | Bajo | Encender la planta de energía. | Julio Castaño | Se debe activar la planta eléctrica mientras la ups respalda los equipos. Esta acción se debe realizar en un periodo máximo de 10 minutos que es la autonomía que ofrece la ups. |

|  |
| --- |
| Como se puede observar, se registran todos los eventos o sucesos ocurridos en un determinado periodo de tiempo; esta información es de vital importancia para realizar un seguimiento a todo lo que ocurre en la organización y adicional a ello, cuando se establecen los recursos necesarios para estas eventualidades en el SGCN, se da prioridad a aquellos sucesos que requieren de mayor cuidado y vigilancia. |

Ahora bien, la medición del impacto de un suceso se mide por su solución. Esta puede ser baja (como en el caso de la falla eléctrica de la tabla), por ejemplo, debido a que se cuenta con la contingencia, pero si se suma la frecuencia o la cantidad de veces que se presentó en un periodo de tiempo muy corto, se puede analizar que a lo mejor ciertos procesos de negocio pudieron estar inoperables por un considerable periodo de tiempo (si se sumaran todos los intervalos). En el siguiente video se profundiza en el ejemplo descrito en las tablas, junto con otros casos, sobre estas mediciones particulares:

CF02\_1\_1\_video\_medición de impacto

**1.2. Evaluación de riesgos**

Los procesos de evaluación de los riesgos establecen los diferentes niveles y exposición que tiene el negocio cuando se llega a presentar un incidente. La evaluación del riesgo debe realizar un proceso de análisis no solo del impacto sino también de la frecuencia en la que el negocio se encuentra expuesta por este suceso, a través de una categorización de acuerdo con el daño que pueden ocasionar; luego, se crean los planes de contingencia para tratarlos.

|  |  |
| --- | --- |
| Seismograph and earthquake | En una organización pueden existir riesgos que no pueden ser controlados desde el punto de vista técnico o funcional. Por ejemplo, en un terremoto, que puede suceder en cualquier momento, aunque este no ocurra todos los días, se debe contemplar qué posibilidades existen de su frecuencia debido a la zona en donde se encuentre ubicada la organización. En este caso y de acuerdo con esa realidad se deben adecuar las instalaciones y procesos de negocio de acuerdo con ese contexto de la organización. En algunas ocasiones es difícil pensar que algo pueda ocurrir por el simple hecho de que no ha ocurrido en un determinado lapso de tiempo, pero aunque esto pueda ser algo improbable, se debe igual incluir en los planes de contingencia por muy nula que sea su probabilidad de ocurrir. |

Los riesgos a menudo se pueden ver como posibles causas cuando no se realiza una correcta evaluación de los mismos. Por tanto, la mayoría de veces no se mide por sus consecuencias y el potencial daño que este pueda ocasionar, y lo fuerte que puede resultar para la organización recuperarse de ese suceso infortunado.

Establecer una matriz de riesgo permite que la organización tenga un punto de partida para iniciar la creación de la gestión de la continuidad, pues establece una política para la implementación del SGCN y se inicia la apropiación del mismo. Cabe resaltar que los riesgos son, de alguna manera, procesos que se relacionan con los procesos de mejora continua, es decir hoy puede no existir un riesgo, pero mañana puede detectarse y generar causas de detenimiento en los procesos de negocio, por eso la matriz no es fija sino dinámica y debe contemplar la posibilidad de que puedan surgir nuevos riesgos en el transcurso del tiempo.

|  |  |
| --- | --- |
| Métodos para evaluar los riesgos  En este sencillo video se puede comprender los métodos que se implementan para la evaluación de riesgos en un negocio, aunque como se ha comentado no todas las empresas pueden presentar los mismos riesgos. Este recurso también se encuentra en el material complementario. | Ver video |

Los niveles de riesgo se miden por el impacto que puedan causar en los procesos de negocio. A continuación, se describen algunos de ellos.

CF02\_1\_2\_interactivo\_niveles de riesgo

|  |
| --- |
| *Cloud computing* es un modelo de infraestructura tecnológica que propone el uso de servicios tercerizados que garantizan la continuidad del negocio, teniendo en cuenta que son grandes las compañías que respaldan estos servicios en *hardware*, *software*, comunicaciones y energía. Brindan confiabilidad y permiten abaratar los costos de uso de la tecnología, pues no es lo mismo tener un centro de datos donde se debe estar preocupado por la seguridad, por la energía y el mantenimiento de los equipos con los que requiere sostener los procesos de negocio, generando grandes costos e inversión, que con la posibilidad de contratar un servicio en la nube por un precio menor. Además del gran respaldo debido a su centro de datos, que muy seguramente una empresa por sí misma no puede alcanzar. En ese sentido, se vuelve una estrategia más rentable y mejor desde todos los puntos de vista. |

**2. ¿Qué es el BIA?**

El BIA o análisis de impacto en el negocio (por sus siglas en inglés) es un componente del SGCN que mide el tiempo en el cual un proceso de negocio deja de estar disponible u operable. Su finalidad principal es analizar los procesos que tienen mayor impacto en el negocio desde un punto de vista operativo. Se podría decir que pretende visualizar no solo los riesgos que se pueden presentar en el presente sino también tener una estimación de cómo puede ser su comportamiento en el futuro.

Los tiempos en los cuales el sistema no se encuentra operable están estrechamente relacionados con la naturaleza del negocio, es decir no todos los BIA son iguales para las organizaciones, tal como se evidencia a través de los siguientes dos ejemplos:

CF02\_2\_slides\_ejemplos BIA

El BIA se debe realizar en todos los procesos que tiene la organización para luego estimar cuál de ellos requiere mayor atención y recursos, los cuales son necesarios para establecer dichos planes de contingencia.

|  |  |
| --- | --- |
| Checking the operating voltage levels of the solar panel switchgear compartment | Por ejemplo, un negocio tiene problemas constantes de energía. La empresa entonces debe primero realizar un proceso de licitación, luego escoger el proveedor que mejor se ajuste a las necesidades y con la oferta que se tenga, adquirir una planta eléctrica como plan de contingencia y así tener continuidad en el negocio. Esta toma de decisión debe estar justificada en dinero. Es decir, se debe conocer si la inversión es menor a las pérdidas actuales dadas por el suceso y en cuánto tiempo se recuperará. Las organizaciones, entonces, deben garantizar la continuidad de los procesos para funcionar y generar las ganancias trazadas. |

El BIA es un proceso dinámico, por tanto, no existe una fórmula mágica en la cual este proceso funcione igual en todas las organizaciones. Cada una debe construir su propio análisis de impacto de acuerdo con los procesos de negocio y necesidades, el cual inicia dando respuesta a las siguientes preguntas:

* ¿Cuáles son los procesos críticos de negocio?
* ¿Cuál es el impacto que tiene cada riesgo en el negocio?
* ¿Qué recursos se requieren para la implementación del BIA?

Sus respuestas permitirán orientar la ruta de trabajo para iniciar su proceso.

Para un BIA existen diferentes tipos de impactos que se pueden generar, los cuales se deben establecer a partir de un criterio propio para ellos. A continuación, se presentan los diferentes tipos de impactos que se ocasionan en un BIA:

CF02\_2\_interactivo\_impactos BIA

El BIA es una herramienta que brinda la oportunidad de mejorar en los aspectos que realmente lo requiere el negocio y poder alcanzar la mejora continua en todos los aspectos, tanto operativos como administrativos. Por lo que, Para desarrollar efectivamente un plan de continuidad del negocio es importante tener en cuenta las siguientes características:

CF02\_2\_pestañas\_características

|  |  |
| --- | --- |
|  |  |
| Los procesos de negocio se ven afectados a diario por diferentes factores los cuales colocan en riesgo su correcto funcionamiento. Es importante establecer las diferentes estrategias para mejorar la confiabilidad de los procesos de negocio, pues al final lo que se busca, con todos estos procesos, es garantizar el funcionamiento, aun ocurriendo inconvenientes en el mismo. | |

**2.1. Medición del impacto de un BIA**

La medición del impacto de negocio tiene varios procesos a realizar los cuales permiten garantizar que se puedan crear acciones correctivas y preventivas para evitar que el negocio sufra inconvenientes en su operatividad. La medición de impacto inicia con la recolección de información. A continuación, se pressentan algunas consideraciones a tener en cuenta para realizar este proceso:

CF02\_2\_1\_interactivo\_impacto BIA

De igual forma, existen una serie de factores en la conformación del BIA para la medición de los impactos ocasionados al negocio, de acuerdo con MinTIC (2015) y son los mostrados en la siguiente figura 3:

**Figura 3**

*Factores de un BIA*

CF02\_2\_1\_gráfico\_factores BIA

Ahora bien, luego de la recolección de la información, se inicia el proceso para su realización, el cual se evidencia en el siguiente gráfico, en el que se desarrollará en este punto los dos primeros pasos, críticos para su correcto establecimiento:

CF02\_2\_1\_interactivo\_procesos BIA

Ahora bien, en la siguiente tabla se observa un ejemplo de cómo se deben definir los niveles de criticidad de los procesos de negocio de la organización teniendo en cuenta que algunos de ellos son parte integral del negocio y otros no (ver tabla 3):

**Tabla 3**

*Criticidad del proceso en el negocio*

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Función del negocio | Proceso del negocio | Nivel de criticidad | Tiempos de inactividad (Horas) | Especificación |
| Aplicaciones de negocio | Sistema de facturación, inventarios, cartera. | B | 2 | Aplicaciones que llevan los procesos de negocio principal de la organización. |
| Sistema de almacenamiento | Servidor de base de datos | A | 1 | Almacenamiento de los datos. |
| Sitio web | Aplicación de ventas por internet | A | 1 | Compras de catálogo por internet. |
| Comunicaciones | Uso de telefonía. | C | 3 | Llamadas a clientes. |

En dicha tabla se tiene un claro ejemplo de cómo se establecen los niveles de criticidad de acuerdo con el proceso de negocio. Estos valores pueden cambiar dependiendo de cómo evolucione el proceso en el tiempo, ya que el proceso puede tomar menos relevancia dependiendo del nivel de apropiación de los mismos en la organización. Es válido recordar que los procesos de negocio se deben ver desde un punto de vista integral, pues

muchos de ellos se encuentran conectados con otros procesos y, por tal razón, pueden generar mayor afectación dependiendo de qué tan crítico puedan ser.

De igual forma, se debe tener en cuenta que estos tiempos que se suministran en horas son establecidos de tal manera que la empresa no colapse. Son tiempos tolerables en los cuales no entra en proceso crítico la organización. Es importante que la empresa identifique cuáles son los puntos vulnerables a fallos para evitar que un proceso pueda recaer en criticidad.

**2.2. Estrategias y plan de gestión de incidentes**

Las estrategias son patrones estructurados de actividades que se diseñan para mantener una ruta específica y así lograr un objetivo propuesto. Sin estrategias, en la mayoría de los casos, se puede llegar al colapso de un proceso. Estas están presentes en cada momento que se llega a cometer errores en el proceso, o por causas que podrían ser naturales o de carácter del mismo, pueden ocasionar las interrupciones en el negocio. Es aquí donde surge la garantía de un plan de gestión de incidentes el cual debe activarse, una vez se requiera, para controlar el suceso que se está presentando. Estos planes deben reflejar las acciones a realizar para corregir el daño o proceso que está perjudicando el correcto funcionamiento del proceso de negocio. Todo esto debe ser realizado con previa planificación. En el siguiente recurso se ejemplifica un poco más sobre lo anteriormente descrito:

CF02\_2\_2\_infografia\_plan de gestión de incidentes

Un plan de gestión de incidentes se desarrolla teniendo en cuenta los procesos de negocio que se establezcan en el mismo. En la siguiente figura 4, se presentan cada una de sus etapas:

**Figura 4**

*Etapas de un plan de incidentes*

CF02\_2\_2\_gráfico\_etapas del plan de incidentes

Estas etapas definen cada proceso en los cuales se deben establecer los protocolos a seguir para la aplicación del plan de gestión de incidentes. A continuación, se detallará cada uno de ellos:

CF02\_2\_2\_acordeon\_etapas

**3. ¿Qué es un plan de continuidad del negocio?**

Es la integración de diferentes estrategias para mantener la operatividad de los procesos de negocio de la organización. La mayoría de las veces estas suelen sufrir percances relacionados a posibles sabotajes, riesgos ambientales, humanos y tecnológicos. La continuidad del negocio es tan esencial que asegura el prestigio organizacional y la calidad de los servicios prestados. Contar con un plan de continuidad del negocio no es una obligación exigida para las organizaciones, pero sí es un valor agregado que puede representar una ventaja competitiva para las mismas que lo aplican, tal como se evidencia en los siguientes ejemplos:

CF02\_3\_slides\_ejemplos

La conformación de un plan de continuidad del negocio debe considerar algunos componentes que son esenciales para su implementación y control. A continuación, se examinan cada uno de ellos para ampliar un poco más el panorama referente a estos conceptos:

CF02\_3\_pestañas A\_componentes

**3.1. Evaluación de planes de continuidad de negocio**

|  |  |
| --- | --- |
| Esta debe estar enmarcada en realizar una exhaustiva verificación de cada uno de los procesos involucrados en el plan de continuidad del negocio. Comprueba si estos se ajustan a las necesidades del negocio y da respuesta a los problemas que se puedan presentar a lo largo del funcionamiento de los procesos; eso quiere decir, que se deben incluir cada uno de los riesgos que pueden ser ocasionados en los procesos del negocio para generar una evaluación conjunta de cada uno de ellos, su correlación con otros procesos de negocio y si los planes y estrategias anexados sí solucionan dicha problemática. | Inicio del proceso de trabajo. hombre de negocios que trabajan en la mesa de madera con proyecto de nuevas finanzas. cuaderno moderno en la mesa. pluma, tenencia, mano Foto gratis |

Ahora bien, para realizar de manera correcta la evaluación del plan de continuidad se deben establecer los escenarios mediante los cuales se realizarán las evaluaciones de los casos que se pueden presentar y que se ven representados en los diferentes riesgos que pueden ocurrir en el ejercicio de las funciones sustantivas de la organización. Estos escenarios pueden sugerir el uso de recursos humanos, tecnológicos y financieros, los cuales pueden ser simulados en ambientes controlados o en escenarios reales para verificar el comportamiento de estos en ambas circunstancias.

El uso de los escenarios simulados suele ser mucho más económico que hacerlo en un ambiente natural, puesto que esto requiere que el proceso sea probado en un horario de trabajo y por tanto, se sacrificarán algunos momentos de la producción para realizar su verificación. Un ejemplo de ello se presenta en la siguiente figura:

CF02\_3\_1\_infografia\_ejemplo escenarios

Para ver desde un contexto más detallado la importancia de la evaluación de los planes de continuidad del negocio, a continuación, se presentan algunos aspectos para comprender de una manera muy sencilla los aportes que esto genera a los procesos de negocio de la organización (ver figura 5):

**Figura 5**

*Aspectos que aportan a los planes de continuidad*

CF02\_3\_1\_gráfico\_aspectos

El proceso de verificación del plan de continuidad debe contemplar la característica de mantener una actualización constante para incluir o sacar los procesos que se deben tener en cuenta en el plan. Algo muy importante es que se genere una cultura de actualización constante de los procesos involucrados en el plan de continuidad, ya que estos pueden cambiar en cualquier momento sea para bien o para mal.

**3.2. Características de los planes de continuidad**

Los planes de continuidad, como se ha expuesto, son de vital importancia para las organizaciones ya que estos se encargan de garantizar que los procesos de negocio sigan prestando sus servicios con calidad y eficiencia. Existen muchas maneras de expresar las diferentes características de un plan de continuidad, el cual tiene como objetivo principal garantizar que una vez suceda un incidente este se pueda solucionar en la mayor brevedad posible para no generar eventos críticos en el negocio. En el siguiente recurso se abordan las diferentes características que tienen los planes de continuidad:

CF02\_3\_2\_interactivo\_características

**3.3. Normatividad**

La normatividad permite estandarizar los procesos y acciones que se ejecutan de manera continua en la organización. Cuando se dice que un proceso se lleva a cabo a través de una norma específica se sabe que este utiliza un referente, en la mayoría de los casos internacional, lo que a su vez es referencia para la aplicación de buenas prácticas y mejorar un proceso de negocio o actividad en particular. Así mismo, las normas, de alguna manera, le dan a la empresa el prestigio y reconocimiento no solo a nivel local sino también internacional, ya que se garantiza que todos los procesos que allí se realizan están debidamente documentados y probados.

Para que una organización empiece un proceso de certificación debe empezar a mejorar y orientar los procesos que esta maneja hacia el referente de la norma, tal como se evidencia en el ejemplo descrito en el siguiente video:

CF02\_3\_3\_video\_ejemplos

La norma ISO 22301 es el estándar establecido para la gestión de la continuidad del negocio la cual se ve reflejada en la utilización de mejores prácticas para lograr que una empresa mantenga su operatividad aun sufriendo riesgos e inconvenientes. Esta norma también garantiza las mejores prácticas para poder recuperar los procesos de negocio de manera efectiva y eficiente. La siguiente figura 6 ilustra cómo funciona la gestión de continuidad del negocio:

**Figura 6**

*Gestión de la continuidad del negocio*

CF02\_3\_3\_gráfico\_gestión de la continuidad

La norma ISO 22301 además, ofrece un espectro amplio de trabajo para mantener los procesos funcionales y evitar que la empresa pueda entrar en crisis. A continuación, se expone un poco más sobre este estándar.

CF02\_3\_3\_interactivo\_ISO22301

|  |  |
| --- | --- |
|  |  |
| Como se pudo apreciar, en un proceso de gestión de la continuidad es importante la gestión de la documentación, pues permite conocer y establecer los procedimientos a seguir y se convierten, además, en la evidencia necesaria para soportar todos los procesos de negocio de la organización. De ahí que todas las dependencias y responsables del proceso participen para lograr una mayor cobertura y ser mucho más eficientes y efectivos al momento de actuar cuando suceda un suceso negativo en el negocio. | |

**4. ¿Qué es un centro de datos?**

Los centros de datos son espacios dedicados donde reposan los dispositivos que se encargan del procesamiento y almacenamiento de la información, los cuales deben ser utilizados mediante unos protocolos y procedimientos específicos para que la información y los dispositivos que allí se encuentran no sean alterados en el proceso de uso y mantenimiento.

|  |  |
| --- | --- |
| Data Center IT Specialist and System administrator Talk, Use Tablet Computer, Wearing Safety Wests. Server Clod Farm with Two Information Technology Engineers checking Cyber Security. | Los centros de datos deben encontrarse en lugares aislados y resguardados donde deben tener unas medidas de seguridad para que solo el personal autorizado y con los conocimientos técnicos de su operatividad sean quienes tengan acceso de acuerdo con los protocolos de acceso de los mismos. |

En algunas organizaciones no se tiene mucho en cuenta el tema de los centros de datos, puesto que si bien son importantes en las organizaciones, requieren de un presupuesto propio para su mantenimiento y cuidado. Muchas empresas optan por no tener centros de datos, sino que dedican un espacio que probablemente no es el más adecuado para su instalación. Uno de los dispositivos más protegidos y resguardado es el servidor los cuales pueden ser de aplicaciones, de bases de datos, de *backups,* entre otros y en algunas ocasiones solo se cuenta con un equipo al cual cualquier persona de la organización puede acceder.

Ahora bien, la normatividad frente al manejo de la información, y para el caso de los centros de datos se deben mantener unos protocolos estrictos para el procesamiento y resguardo de la misma; teniendo en cuenta que la información hoy día es un activo importante para el negocio. Por lo tanto, se debe garantizar que los dispositivos donde esta se almacena y procesa se encuentren en óptimas condiciones y bajo los protocolos y sitios adecuados.

|  |  |
| --- | --- |
| In Data Center: Male IT Technician Running Maintenance Programme on a Laptop, Controls Operational Server Rack Optimal Functioning. Modern High-Tech Telecommunications Operational Super Computer. | La información tiene que estar resguardada en ambientes donde no corra peligros de corrupción de datos y pérdida de la misma. Los centros de datos son, entonces, como las bóvedas donde se almacenan los dispositivos encargados del procesamiento y almacenamiento de la información bajo medidas de seguridad apropiadas. |

Los centros de datos (*Data Center)* son demandados y requeridos por las compañías que manejan y procesan grandes cantidades de información. Su diseño y las medidas de seguridad están concebidos para garantizar la disponibilidad del servicio ante cualquier imprevisto, ya sea un desastre natural o una acción provocada por el hombre. Los centros de datos deben contar con varios elementos para la instalación de los dispositivos que allí se colocan, tal como se aprecia a continuación:

CF02\_4\_interactivo\_elementos

Los centros de datos requieren de muchos cuidados tanto en su operatividad como en su mantenimiento. De ahí la importancia de contar con personal y un análisis de los recursos necesarios para su implementación. Un error muy común que se comete es diseñar un centro de datos futurista y cargado de la última tecnología sin estar orientado a la realidad de la organización tanto en espacio como en costos. Regularmente se diseñan para el uso más no para el mantenimiento. Es como adquirir un vehículo solo concentrado en su precio pero no en su mantenimiento, es decir el precio lo pagas una sola vez pero el mantenimiento se debe seguir realizando en la vida útil; esto mismo que aplica para un centro de datos. Se debe ver no una inversión inicial sino una inversión que requiere un alto costo de mantenimiento y costos de operación. En la siguiente figura 7 se presentan otros aspectos a tener en cuenta:

**Figura 7**

*Aspectos de la implementación de un data center*

CF02\_4\_gráfico\_aspectos\_data center

**4.1. Riesgos asociados a los centros de datos**

Hoy día existen muchos elementos de seguridad tanto a nivel físico como lógico. Los centros de datos se pueden ver afectados tanto por la afectación de un terremoto como por un ataque informático dirigido. En ambas situaciones el riesgo se ve desde el punto de vista de daños asociados, aunque pueden existir diferentes tipos de afectación.

La seguridad es una de las causantes de mayor perdida y daños a la información. Los ataques informáticos, en la mayoría de veces están dirigidos a ocasionar daños particulares, dentro de los cuales se encuentra el robo de información. Las compañías que se encargan de velar porque esto no suceda sufren en algunas ocasiones demandas por la exposición que sufren los datos al ser robados, expuestos o compartidos sin permiso de los dueños. En el siguiente recurso se desarrolla en qué consisten los principales riesgos:

CF02\_4\_1\_interactivo\_riesgos

Los centros de datos deben contener cinco elementos que les permiten realizar un correcto funcionamiento, los cuales son:

CF02\_4\_1\_interactivo\_elementos

Un centro de datos requiere de diferentes capas de seguridad que protejan la infraestructura de amenazas externas o intrusiones, y aunque la zona de alojamiento de un *data center* debe contar con videovigilancia y un control de acceso y seguridad perimetral; también es vital garantizar las cuatro áreas de seguridad primordiales siguientes:

CF02\_4\_1\_interactivo\_seguridad

|  |  |
| --- | --- |
|  |  |
| Un centro de datos tiene muchos factores que pueden afectar su correcto funcionamiento y colocar en riesgo la información que allí se resguarda por eso es importante implementar estrategias las cuales incluyen *hardware* y *software* para mejorar los niveles de seguridad de los mismos. | |

**4.2. Estrategias para el manejo de un centro de datos**

Los centros de datos, como se ha mencionado, son esenciales para los procesos de negocio de las organizaciones y permiten resguardar los datos de una manera adecuada. A continuación, se exponen algunas estrategias que se deben tener en cuenta para que los centros de datos funcionen correctamente:

CF02\_4\_2\_Línea de tiempo D\_estrategias

Es importante muchos aspectos a considerar en el uso y mantenimiento de un centro de datos, entre estos la aplicación de las siguientes recomendaciones que se deben considerar para un centro de datos altamente disponible y que permita ejecutar los procesos de negocio de la manera más efectiva:

CF02\_4\_2\_pestañas\_recomendaciones

|  |  |
| --- | --- |
|  |  |
| Es importante establecer procesos, estudios y pruebas para garantizar el correcto funcionamiento y rendimiento de un centro de datos. | |

**5. Monitoreo de procesos de continuidad de negocio**

El monitoreo de los planes de continuidad del negocio se realiza con el fin de establecer un proceso de pruebas elaboradas y soportadas bajo unos escenarios específicos para garantizar el correcto funcionamiento y ejecución de los SGCN; pues, como se ha mencionado, de nada sirve crear un excelente plan de continuidad sino se prueba y no se verifica que este funciona de la mejor manera. Existen varios factores a analizar en un proceso de monitoreo de un SGCN, los cuales se mencionan a continuación:

CF02\_5\_pestañas\_factores monitoreo

Al realizar un monitoreo se deben registrar todos los acontecimientos que se presentan. Dicho registro permitirá realizar un balance del comportamiento de un proceso implementado. Se debe recopilar información de pruebas realizadas de acuerdo con las eventualidades presentadas; es decir, documentar cada uno de los sucesos generados declarando, además, la manera en cómo este se solucionó y el tiempo que se tomó la operación en darle solución. Luego, estos tiempos deben ser comparados con los tiempos que se tienen registrados en el proceso y de esta manera corroborar si fue que inicialmente se establecieron mal los tiempos o que el proceso realmente requiere mayor espacio de recuperación o, quizás, falta una herramienta para realizar el proceso de manera mucho más efectiva. Todo lo anterior es la forma en la que se corrobora la información y se mejoran los procesos presentados.

El seguimiento que se le realiza a los procesos se debe realizar de una manera específica, tal como se evidencia en la siguiente figura 8:

**Figura 8**

*Proceso de seguimiento*

CF02\_5\_gráfico\_proceso\_seguimiento

Algunas recomendaciones para tener en cuenta con respecto a la documentación de solución de los incidentes presentados, son:

CF02\_5\_interactivo\_documentación

**5.1. ¿Qué es una auditoría interna?**

Es una actividad independiente y objetiva de aseguramiento y consulta concebida para agregar valor y mejorar las operaciones de una organización. Ayuda a una empresa a cumplir sus objetivos aportando un enfoque sistemático y disciplinar para evaluar y mejorar la eficacia de los procesos de gestión de riesgos, control y gobierno.

La auditoría interna está conformada por varias actividades las cuales permiten identificar de manera objetiva e independiente los procesos de negocio y verificar si todos estos se están cumpliendo de manera correcta. La mayoría de las veces va dirigida a realizar la revisión de algunos componentes de un proceso o dependencia de la organización. Sin embargo, si está relacionada con el departamento de contabilidad y la dirección general estos también entran dentro del plan de auditoría para llevar una trazabilidad del proceso.

La independencia está establecida por la estructura de la organización y las líneas de reporte. La objetividad se logra mediante una apropiada actitud mental. La actividad de auditoría interna evalúa la exposición al riesgo del gobierno, las operaciones y los sistemas informáticos de la organización, con respecto a lo siguiente:

CF02\_5\_1\_interactivo\_auditoría

El auditor interno es una persona que debe tener las competencias y en algunos casos la certificación en el proceso que está revisando o auditando. Muchos procesos de auditoría son relativamente transversales a los procesos de la empresa y por tanto, cualquier persona que conozca la documentación, puede realizar un diagnóstico y posteriormente, un informe sobre los hallazgos encontrados. Sin embargo, cuando se habla sobre un procedimiento específico que requiere de unos conocimientos técnicos y propios, se debe contratar a un profesional certificado y con experiencia en el manejo de dichos procesos.

|  |  |
| --- | --- |
| businessman or tax inspector analyzing document with magnifying glass in office. business financial audit concept. copy space | En ocasiones se contratan personas que tienen los conocimientos pero no la certificación para realizar tal actividad y esto puede perjudicar a la empresa porque si se realiza una auditoría externa, este factor se puede convertir en un hallazgo negativo ya que se debe garantizar que la persona que está realizando dicho proceso cumpla con el perfil y conocimientos para realizarlo. |

Una actividad de auditoría interna eficaz es un valioso recurso para la dirección de la organización y su comité directivo o equivalente, así como para el comité de auditoría, debido a su entendimiento de la organización y su cultura, operaciones y perfil de riesgos. Una actividad de auditoría interna eficaz puede proporcionar aseguramiento a otras partes interesadas, tales como los entes de regulación, empleados, proveedores financieros y accionistas. El siguiente video profundiza un poco más sobre este proceso de monitoreo:

CF02\_5\_1\_video\_proceso auditoría

|  |  |
| --- | --- |
|  |  |
| Contar con un sistema de control dentro de la gestión de riesgos permite vigilar y monitorear el funcionamiento correcto de los procesos. Existen diferentes tipos de auditorías, pero es la auditoría interna la que se enfoca en el cumplimiento de los objetivos de la organización. | |

**5.2. ¿Cómo se aplica una auditoría interna a un SGCN?**

La auditoría interna se compone de tres partes, las cuales son el eje central de este proceso dentro de las organizaciones. A continuación, se expone detalladamente cada una de estas:

CF02\_5\_2\_interactivo\_componentes\_auditoría

Cuando las empresas empiezan a tener un crecimiento notable, es cuando se hace más necesaria la auditoría interna porque se vuelve casi imposible tener control directo de todas las operaciones. El proceso de aplicación de un plan de auditoría empieza con una iniciativa de la empresa de validar los procesos que está llevando a cabo y verificar si estos se ajustan a los objetivos que tiene la misma. Para ello, se deben realizar los siguientes pasos para poner en marcha dicho proceso (ver figura 9):

**Figura 9**

*Proceso de seguimiento*

CF02\_5\_2\_gráfico\_proceso\_auditoria

|  |  |
| --- | --- |
|  |  |
| La auditoría debe llevar un sello de certificación hacia una norma y/o estándar como referencia de donde se verifican. Si los procesos y procedimientos establecidos en la organización están ajustados a dicha norma, para el caso de los sistemas de continuidad del negocio la norma establecida es la ISO 22301, el auditor debe establecer, a partir del estándar, los ajustes a dichos procesos y buenas prácticas. | |

**5.3. Construcción de planes de mejora continua para un SGCN**

La construcción de los planes de mejora continua debe estar conectada a los procesos ejecutados en la auditoría interna ya que estos deben reflejar los resultados obtenidos en los hallazgos allí encontrados. La mejora continua será el resultado de la aplicación de las recomendaciones dadas en el informe de auditoría, las cuales desde el punto de vista del auditor se deben realizar. El siguiente video expone un ejemplo de esto:

CF02\_5\_3\_video\_ejemplo de hallazgo

Todo esto es un proceso continuo que requiere de mucha paciencia, compromiso de todos (sobre todo de la alta gerencia para asumir los retos en la planificación de los procesos que se deben llevar a cabo en los planes de mejora) y trabajo en equipo para lograr los resultados esperados. Algunos de los elementos esenciales para desarrollar un sistema de mejora continua en un SGCN son (ver figura 10):

**Figura 10**

*Elementos para el desarrollo de un sistema de mejora continua*

CF02\_5\_3\_gráfico\_elementos

**5.4. Proceso de certificación de un SGCN**

Para llevar a cabo la certificación de un SGCN se debe establecer, en primera instancia, el plan de continuidad del negocio como una unidad integral de todos los procesos que componen el plan de gestión, el cual a su vez debe estar orientado hacia la ISO 22301.

Una certificación es un proceso al cual se somete una empresa o persona para validar los conocimientos y procesos que realiza en una determinada tarea. Uno de los procesos más complejos al momento de certificar un SGCN es que este logre ajustarse a las exigencias que puede tener la norma de certificación, para ello siempre es importante establecer qué pide la norma y cuáles son los recursos que se requieren para implementar el SGCN ajustado a la misma. De tal manera que cuando se solicite el proceso de certificación, se tengan las actividades y procesos adecuados al estándar. A continuación, se presenta su paso a paso:

CF02\_5\_4\_pasos\_pasos certificación

El proceso de certificación debe pasar por diferentes etapas las cuales deben garantizar que se cumplen todos los requisitos exigidos por la norma. No se puede certificar al candidato si este no cumple al 100% las actividades y proceso de normatividad. Un paso fundamental en el caso de la certificación de un SGCN es la calidad de la documentación establecida; es decir, los soportes de los procesos que se incluyen en un plan de continuidad de negocio, los cuales son (ver figura 11):

**Figura 11**

*Documentación*

CF02\_5\_4\_gráfico\_documentación

|  |  |
| --- | --- |
|  |  |
| La inspección es la acción dirigida a aquella organización que desea mostrar responsabilidad asegurando que sus equipos, productos y servicios cumplen con la calidad, la seguridad, el respeto al medio ambiente y las responsabilidades sociales imperativas (ya sean de obligado cumplimiento, voluntarias o propias, basadas en sus propios sistemas, normas o necesidades). La evaluación de la conformidad requiere con frecuencia la realización de ensayos de tipo, de vigilancia o de autocontrol sobre los productos que son objeto de algún tipo de certificación. Utilizando las metodologías analíticas más avanzadas, se realizan análisis fisicoquímicos, microbiológicos y sensoriales en productos alimentarios o productos de cosmética, higiene y detergencia, entre otros. | |

**6. Proyecto de implantación de un SGCN**

Los SGCN, como se ha explicado, tienen la capacidad de detectar fallas en los sistemas actuales de la organización y poder detectar nuevas amenazas que se puedan presentar en un futuro cercano. Para la implantación de un sistema de gestión de continuidad del negocio se debe tener en cuenta muchos aspectos tales como las personas que estarán involucradas en los procesos que se llevarán a cabo en cada fase del proyecto, teniendo en cuenta sus conocimientos y experiencia en cada una de las actividades que se desarrollan en el mismo. Algunos pasos a considerar en la implantación de un sistema de continuidad del negocio se exponen a continuación:

CF02\_6\_acordeón\_pasos implantación

|  |  |
| --- | --- |
| ¿Cómo implantar un sistema de gestión de continuidad de negocio?  Los procesos de implantación de un SGCN requieren de un conjunto de actividades organizadas para lograr la integración de cada uno de los procesos que estos soportan. Es importante considerar que todas las actividades deben estar diseñadas para cumplir con el objetivo principal del sistema de gestión y evitar la interrupción de los procesos de negocio que tiene la organización todo esto es esencial para su correcta implantación. En el siguiente video se puede apreciar algunos aspectos a considerar en la implantación de un SGCN. Este recurso también se encuentra en el material complementario. | Ver video |

De acuerdo con la norma ISO 22301 en la implantación de un sistema de gestión de la continuidad del negocio se deben considerar estos aspectos:

CF02\_6\_pestañas\_aspectos implantación

**6.1 Riesgos al implementar un SGCN**

Los riesgos que pueden estar asociados a la implementación de un sistema de gestión del negocio, inicialmente están estrechamente relacionados con los factores humanos. El compromiso de las partes involucradas tiene a ser el principal motivo. A continuación, se exponen algunos riesgos comunes.

CF02\_6\_1\_interactivo\_riesgos

**6.2. Problemas frecuentes y solución de problemas**

Una mala planificación o procesos que no se controlan de manera adecuada pueden generar traumatismos e interrupciones en los procesos de negocio y por ende, en el sistema de gestión. Existen ciertos aspectos a considerar como problemas frecuentes y por tanto, posibles soluciones y controles. Se pueden ver a continuación:

CF02\_6\_2\_pestañas A\_problemas

Estos problemas se presentan en las situaciones en las cuales se requiere de manera inmediata las soluciones. Como bien se ha estipulado, los SGCN son esenciales para el negocio y tanto su diseño, creación y puesta en marcha garantizan la continuidad del negocio, previniendo futuras eventualidades tanto a nivel externo como interno, incluyendo la interacción del equipo de trabajo al momento de su concepción y puesta en marcha. Las soluciones siempre requieren un nivel mayor de comprensión de las diferentes situaciones para poder abordarlas desde los procesos y protocolos implementados por eso siempre es importante estar alerta con todos los sucesos que se puedan presentar en la implementación del SGCN.

1. **SÍNTESIS**

Recuerde que la organización debe mejorar continuamente la eficacia de un SGCN mediante la revisión de la política de continuidad de negocio y los objetivos, resultados de la auditoría, eventos analizados, acciones correctivas y preventivas y la revisión por la dirección de la organización. El siguiente esquema ilustra esto, así como todos los contenidos desarrollados en el componente:

CF02\_esquema\_síntesis

1. **ACTIVIDADES DIDÁCTICAS**

|  |  |
| --- | --- |
| DESCRIPCIÓN DE ACTIVIDAD DIDÁCTICA | |
| Nombre de la Actividad | Implementación de un SGCN |
| Objetivo de la actividad | Poner a prueba los conocimientos adquiridos alrededor de la implementación de un SGCN teniendo en cuenta la normatividad existente. |
| Tipo de actividad sugerida |  |
| Archivo de la actividad  (Anexo donde se describe la actividad propuesta) | El documento se encuentra en la carpeta Formatos DI con el nombre: CF02\_Actividad didáctica |

**E. MATERIAL COMPLEMENTARIO**

|  |  |  |  |
| --- | --- | --- | --- |
| Tema | Referencia APA del Material | Tipo de material  (Video, capítulo de libro, artículo, otro) | Enlace del Recurso o  Archivo del documento o material |
| 1.2. Evaluación del riesgo. | Grupo Proikos. (2021). *Métodos para evaluar los riesgos.* [Video]. YouTube. <https://www.youtube.com/watch?v=qYWBhFbN-zs> | Video | <https://www.youtube.com/watch?v=qYWBhFbN-zs> |
| 2. ¿Qué es el BIA? | INCONTEC. (2017). *Seguridad de la sociedad = sistemas de gestión de la continuidad de negocio: directrices para el análisis de impacto en el negocio (BIA).* <https://sena-primo.hosted.exlibrisgroup.com/permalink/f/1j5choe/sena_aleph000101443> | Libro | <https://sena-primo.hosted.exlibrisgroup.com/permalink/f/1j5choe/sena_aleph000101443> |
| 3. ¿Qué es un plan de continuidad del negocio? | Olarte Rojas, A. D. (2017). Propuesta metodológica para la evaluación de la madurez del sistema de gestión de continuidad del negocio en el sector financiero bancario colombiano bajo el enfoque de la norma ISO 22301:2012. *SIGNOS 8(1)*, 31-44. <https://sena-primo.hosted.exlibrisgroup.com/permalink/f/1i756fj/TN_cdi_dialnet_primary_oai_dialnet_unirioja_es_ART0001302199> | Artículo | <https://sena-primo.hosted.exlibrisgroup.com/permalink/f/1i756fj/TN_cdi_dialnet_primary_oai_dialnet_unirioja_es_ART0001302199> |
| 5.1. ¿Qué es una auditoría interna? | Montes Salazar, C. A., Porras Cuellar, C., Muñoz Valle, R. y Dextre Flores, J. (2017). Auditoría Interna y Gestión Organizacional. *Proyecciones,* (12). https://sena-primo.hosted.exlibrisgroup.com/permalink/f/1i756fj/TN\_cdi\_doaj\_primary\_oai\_doaj\_org\_article\_ffdf450c064a494faa07e01e182d58d8 | Artículo | <https://sena-primo.hosted.exlibrisgroup.com/permalink/f/1i756fj/TN_cdi_doaj_primary_oai_doaj_org_article_ffdf450c064a494faa07e01e182d58d8> |
| 6. Proyecto de implantación de un SGCN | GlobalSUITE Solutions. (2020). *ISO 22301: ¿Cómo implantar un sistema de gestión de continuidad de negocio?* [Video] YouTube. <https://www.youtube.com/watch?v=LTZLxE1UHfE> | Video | <https://www.youtube.com/watch?v=LTZLxE1UHfE> |

1. **GLOSARIO**

|  |  |
| --- | --- |
| TÉRMINO | SIGNIFICADO |
| Certificación | Proceso de verificación de un producto o proceso en el cual se realiza la inspección de las actividades que se efectúan en una empresa, las cuales deben estar alineadas con un referente internacional. |
| Continuidad | Se comprende como el proceso de garantizar que las actividades que se están realizando no pierdan su inercia y ejecución. |
| Gestión | Proceso de realizar un adecuado uso de los recursos con los que cuenta una organización o persona natural. |
| ISO 22301 | Es una norma internacional que permite la gestión de la continuidad del negocio en las organizaciones. |
| Negocio | Lugar donde se ofrecen servicios y productos a diferentes clientes o empresas. |
| Organización | Se entiende como el referente de función que realiza actividades en beneficio de una comunidad o personal. |
| Plan | Secuencia organizada de acciones para lograr un objetivo común. |
| Planificación | Proceso que comprende la organización de las diferentes actividades que se llevarán a cabo en un proyecto o proceso a implementar. |
| Riesgo | Situación que se puede presentar y que en la mayoría de las ocasiones si no se controla a tiempo puede causar traumatismos y problemas en los procesos de negocio de una organización. |
| SGCN | Es un proceso que permite controlar las acciones que se realizan para garantizar la gestión de los riesgos y la continuidad del negocio. |
| Sistema | Conjunto de elementos que se utilizan para un fin u objetivo general. |

1. **REFERENCIAS BIBLIOGRÁFICAS**

GlobalSUITE Solutions. (2020). *ISO 22301: ¿Cómo implantar un sistema de gestión de continuidad de negocio?* [Video] YouTube. <https://www.youtube.com/watch?v=LTZLxE1UHfE>

Grupo Proikos. (2021). *Métodos para evaluar los riesgos.* [Video]. YouTube. <https://www.youtube.com/watch?v=qYWBhFbN-zs>

ISO 22301 (2019). *Sistemas de Gestión de Riesgos y Seguridad*. <https://www.isotools.org/normas/riesgos-y-seguridad/iso-22301/>

MinTIC. (2015). *Guía para realizar el Análisis de Impacto de Negocios BIA*. <https://www.mintic.gov.co/gestionti/615/articles-5482_G11_Analisis_Impacto.pdf>

1. **CONTROL DEL DOCUMENTO**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | Nombre | Cargo | Dependencia  *(Para el SENA indicar Regional y Centro de Formación)* | Fecha |
| Autor (es) | Dulfran Antonio Montaño Montaño | Experto Temático | Regional Distrito Capital - Centro de diseño y Metrología | Mayo de 2022 |
| Miroslava González Hernández | Diseñadora Instruccional | Regional Norte de Santander – Centro de la Industria, la Empresa y los Servicios | Mayo de 2022 |
| Andrés Felipe Velandia Espitia | Asesor Metodológico | Regional Distrito Capital - Centro de Diseño y Metrología | Mayo de 2022 |
| Rafael Neftalí Lizcano Reyes | Responsable Equipo Desarrollo Curricular | Regional Santander - Centro Industrial del Diseño y la Manufactura | Mayo de 2022 |
| Jhon Jairo Rodríguez Pérez | Corrector de estilo | Regional Distrito Capital - Centro de Diseño y Metrología | Mayo de 2022 |

1. **CONTROL DE CAMBIOS**

**(Diligenciar únicamente si realiza ajustes a la Unidad Temática)**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | Nombre | Cargo | Dependencia | Fecha | Razón del Cambio |
| Autor (es) |  |  |  |  |  |