**FORMATO PARA EL DESARROLLO DE COMPONENTE FORMATIVO**

|  |  |
| --- | --- |
| PROGRAMA DE FORMACIÓN | Gestión de negocios y finanzas |

|  |  |  |  |
| --- | --- | --- | --- |
| COMPETENCIA | 260102034 - Medir riesgos del servicio de acuerdo con marcos de referencia y proceso de negocio | RESULTADOS DE APRENDIZAJE | 260102034-02 - Establecer factores de riesgo conforme con escala de valoración.  260102034-03 - Perfilar plan de tratamiento de riesgos de acuerdo con política organizacional. |

|  |  |
| --- | --- |
| NÚMERO DEL COMPONENTE FORMATIVO | CF11 |
| NOMBRE DEL COMPONENTE FORMATIVO | Evaluación y tratamiento del riesgo |
| BREVE DESCRIPCIÓN | La evaluación y el tratamiento del riesgo es responsabilidad de todo funcionario comprometido con el mejoramiento continuo de la organización y la prevención de sucesos que pueden afectar su normal funcionamiento. El análisis del riesgo tiene como objetivo evitar grandes inversiones de recursos en la gestión interna para superar eventos correctivos que afecten la productividad, enfocando esfuerzos en la eficiencia de las operaciones. |
| PALABRAS CLAVE | Riesgo, mapa de riesgo, protección de datos. |

|  |  |
| --- | --- |
| ÁREA OCUPACIONAL | 1 - Finanzas y Administración |
| IDIOMA | Español |

**a. TABLA DE CONTENIDOS**

**Introducción**

1. **Evaluación del riesgo**
   1. Riesgo empresarial
   2. Determinación de ocurrencia
   3. Modelos de estimación
   4. Mapa de riesgos
   5. Tratamiento de riesgos
   6. Normativa técnica
2. **Gestión de la información** 
   1. Protocolos de elaboración
   2. Normativa de protección de datos

**Síntesis**

**Introducción**

Como bienvenida al presente componente formativo, que expone el análisis de la evaluación y tratamiento del riesgo como elemento fundamental para el normal funcionamiento y la mejora continua de las organizaciones, se presenta el siguiente video introductorio:



**b. DESARROLLO DE CONTENIDOS**

**1. Evaluación del riesgo**

Dirigir una compañía implica, en un alto grado de responsabilidad, la gestión y evaluación adecuada de los riesgos a los que se expone a diario la empresa. Dichos riesgos pueden ser internos o externos.



Según la Norma ISO 31000-2018 el proceso de evaluación de los riesgos consta de cuatro pasos básicos: **identificación**, **análisis**, **valoración** y **tratamiento** de los riesgos, que dejan a disposición de la empresa una amplia gama de técnicas para identificar la incertidumbre que puede llegar a afectar a uno o a varios de sus objetivos. A continuación, se describen los cuatro pasos mencionados:



En las empresas es primordial contar con un plan adecuado de prevención y evaluación de riesgos, que permita realizar un diagnóstico acertado y conocer de manera anticipada los sucesos internos o externos que puedan afectar el normal funcionamiento de la compañía. Con base en ello, se ejecutan acciones para minimizar o trasladar el riesgo, así la empresa sería capaz de afrontar sin mayores contratiempos, las consecuencias o pérdidas al materializarse el riesgo (Cristo, 2019).

* 1. **Riesgo empresarial**

La gestión del riesgo empresarial-GRE afecta a los órganos directivos y laborales de la organización (junta directiva, administrativos y empleados) y se diseñó para perfilar eventos que puedan impactar a la entidad, de forma que el riesgo esté en el rango de impacto deseable y razonable que no afecte los objetivos de la organización.

La GRE debe impactar en todos los niveles e incluirse en los modelos de la estrategia organizacional, con el fin de identificar alternativas de solución preventivas y no correctivas enfocadas siempre al cumplimiento de metas, independientemente del departamento al cual se esté aplicando la estrategia.

El siguiente esquema presenta el nivel de sofisticación en la gestión el riesgo:

**Figura 1.** Sofisticación del riesgo



**Clasificación de riesgos empresariales**

En el siguiente recurso se presentan dos tipos de riesgo, según su impacto o según la posibilidad de prevenirlos o no:



**Tipos de riesgos y naturaleza**

La forma más eficiente de incrementar o cumplir las metas establecidas es tener siempre presente que existen riesgos que pueden afectar la situación. Antes de definir cualquier estrategia de gestión de riesgos es necesario analizar los posibles riesgos y clasificarlos así:

* **Riesgo sistemático:** integra los elementos socio-político-económicos que afectan el normal funcionamiento de un proyecto o empresa, por ejemplo, crisis financieras, guerras, desplazamientos, entre otros.
* **Riesgo no sistemático:** afecta de manera específica un proyecto o empresa, por ejemplo, mala estrategia de gerencia, mal funcionamiento de una maquinaria, empleados inconformes, entre otros.
  1. **Determinación de ocurrencia**

El análisis de los riesgos permite recopilar la información del sistema y de los procesos que se utilizan en las empresas para mejorar el uso, la manipulación, la protección y la administración de los recursos ante las vulnerabilidades que se pudiesen encontrar. Por tal motivo, es indispensable hacer control a la probabilidad de ocurrencia de los eventos y sus posibles consecuencias.

Existen diversas formas de gestionar un análisis de riesgos, lo más importante es conocer o entender la forma en que se determinará el valor del riesgo. Una forma sería multiplicar la vulnerabilidad por el % de importancia o peso para la empresa, es decir, mientras más vulnerable sea un activo y más importante sea este para la entidad, mayor será su riesgo. Por lo tanto, la inversión en tiempo, dinero o mano de obra será mayor para lograr minimizarlo.

El riesgo concierne a situaciones donde las probabilidades de resultados y sus consecuencias se determinan con técnicas de datos reales, completos y verídicos. Por otro lado, la incertidumbre ocurre cuando los datos utilizados presentan fragmentación, registros incompletos o datos no disponibles.

**Teoría de probabilidades**

Es una herramienta que establece un conjunto de reglas o principios para calcular la ocurrencia de los eventos, asignando un número a la posibilidad de que un evento ocurra. Aproxímese al concepto de teoría de probabilidades a través del siguiente video:



**Análisis de incertidumbre**

La incertidumbre no se puede medir, no es cuantificable. En ocasiones es sencillo hacer “predicciones” que pueden llegar a ser ciertas y tener la falsa sensación de certeza, pero es solo una simple especulación. La incertidumbre al no ser cuantificable, no se puede evaluar completamente, caso contrario al riesgo que se puede medir y evaluar. Basado en lo anterior a continuación se presenta la relación riesgo – incertidumbre:





**Importante:**

* Se debe afrontar la incertidumbre ejerciendo influencia en las situaciones deseadas, en lo que se quiera que ocurra.
* Se deben enfocar los esfuerzos en obtener una alta probabilidad de conseguir los resultados deseados, a pesar de la incertidumbre.
* No se pueden afrontar las situaciones intentando conseguir algo en concreto, sino buscando aumentar las probabilidades de que eso en concreto suceda.
* No se puede eliminar del todo la incertidumbre, pero sí tratar de inclinar la balanza a favor.
  1. **Modelos de estimación**

En el campo de los riesgos previsibles, la estimación trata de valorar la probabilidad de ocurrencia y el nivel de impacto de los riesgos que se componen y que, teniendo en cuenta su materialidad, requieren una valoración y presentan unos niveles de asignación. La asignación distribuye los riesgos según la capacidad de gestión, para que puedan controlarse, administrarse y mitigarse. La valoración determina la estimación que puede ser cualitativa o cuantitativa, tal y como se detalla a continuación:



Es importante cuantificar y categorizar los riesgos, porque según su nivel o puntaje de evaluación o estimación se logran jerarquizar mediante un plan de acción o intervención, tratando de actuar sobre quienes son más críticos y pueden llegar a ser más perjudiciales para el normal desarrollo de un proyecto o funcionamiento de una empresa. Estos niveles jerarquizados se plasman para una mejor lectura y comprensión en un mapa de riesgos.

* 1. **Mapa de riesgos**

Identifica de forma gráfica los riesgos a los que se expone una empresa, teniendo en cuenta su probabilidad y el impacto que pueden causar.

**Importante:** 

* Compartir y recopilar información de manera clara posibilita reconocer con rapidez los riesgos y actuar de acuerdo con su nivel de importancia.
* Identificar los riesgos de forma correcta permite establecer niveles en diferentes áreas de la empresa, lo que conlleva a establecer el objetivo del mapa de riesgos.

**Pasos para elaborar un mapa de riesgos**

La secuencia ofrecida a continuación detalla los pasos recomendados para la elaboración de un mapa de riesgos:



Los mapas de riesgos se deben revisar periódicamente, teniendo en cuenta que la gestión y los riesgos son dinámicos, es decir, lo que hoy se puede identificar como un peligro, a futuro puede no existir o transformarse en una oportunidad y viceversa. Por eso, el mapa de riesgos debe pasar por revisiones según los cambios o entorno de la empresa, aunque algunas no tienen mayor alteración en sus condiciones, otras entidades proclives a cambios constantes.

Es importante recordar que dentro de las **técnicas de elaboración de un mapa de riesgos** se destacan las siguientes**:**



* 1. **Tratamiento de riesgos**

Está basado en el diseño, la evaluación, la selección e implementación de acciones para plantear los riesgos identificados al interior de una empresa. Según la norma internacional ISO 31000 el tratamiento de riesgos es un proceso cambiante y repetitivo que requiere de actividades de formulación, planeación y evaluación, tales como:



* Formular opciones para el tratamiento de riesgos.
* Seleccionar la opción más adecuada.
* Planificar e implementar el tratamiento de riesgos.
* Evaluar la efectividad de las acciones implementadas.
* Calificar el riesgo residual (aceptable o no aceptable).
* Tratamiento para el riesgo residual no aceptable.

Las opciones del tratamiento de riesgo resultan más efectivas cuando se ponen en una balanza los beneficios y los costos. Los beneficios procedentes de la efectividad de una acción propuesta y los costos del esfuerzo y las desventajas que casualmente surjan como consecuencia de la implementación. Según la Norma ISO 31000 las opciones de tratamiento no son excluyentes entre sí e incluyen algunas de las siguientes acciones:

* Eliminar el riesgo prescindiendo del proceso, la actividad o las circunstancias que lo generan.
* Asumir el riesgo, aún aumentándolo, con el fin de incrementar una posible oportunidad.
* Tomar acciones para disminuir la probabilidad del riesgo.
* Implementar acciones que disminuyan el impacto negativo del riesgo.
* Compartir el riesgo (cláusulas en contratos o comprar pólizas de seguros).
* Retener el riesgo con base en información confiable.

La implementación de los planes de tratamiento de riesgos consiste en determinar y detallar la manera en que tomarán las opciones seleccionadas, de modo que los involucrados entiendan y monitoreen el progreso del plan. De acuerdo con ISO 31000 el plan de tratamiento de riesgos permite reconocer claramente la disposición de la implementación de acciones, de tal forma que integre los procesos de gestión en la empresa, teniendo en cuenta las necesidades identificadas en atención a:

* Justificación para la elección de las opciones de tratamiento, incluyendo beneficios esperados.
* Quiénes son los responsables de aprobar e implementar el plan.
* Las acciones de tratamiento propuestas.
* Recursos requeridos, incluyendo los necesarios en caso de contingencia.
* Mediciones de rendimiento del plan.
* Limitaciones del plan.
* Acciones de monitoreo requeridas.
* Plazos esperados para que se completen las acciones.

Es importante reconocer la existencia de dos estrategias principales para el tratamiento de riesgos, estas son:



* 1. **Normativa técnica**

Son documentos donde se establece por consentimiento y con la aprobación de un ente reconocido algunas cláusulas o directrices mínimas que debe cumplir una empresa en la elaboración de un producto o servicio. Las normas son reglas que se aceptan de manera voluntaria por los interesados y a su vez reflejan la experiencia y el conocimiento de las personas, de acuerdo con su especialidad y las necesidades de las empresas.

Una de las normas más importantes hoy es la Norma ISO 31000, que ayuda a desarrollar y gestionar directrices en empresas de cualquier sector económico, minimizando el impacto de los riesgos en todas sus áreas para mejorar los procesos y gestión de calidad.

A continuación, se presentan sus principales características:



También están los sistemas de gestión de seguridad de la cadena de suministro **ISO 28000** que permiten a las empresas tener la competencia de controlar las vulnerabilidades y las amenazas que lleguen afectar la seguridad. De la Norma ISO 2800 se destaca lo siguiente:

* Aporta un entorno de buenas prácticas para minimizar los riesgos de los responsables y los productos en la cadena de suministro. 
* Gestiona y mitiga la seguridad en la logística, enfocándose a amenazas como el terrorismo, el fraude y la piratería.
* Permite a una empresa amortiguar las consecuencias de los incidentes de seguridad, centrándose en situaciones críticas para gestionar y garantizar los riesgos de seguridad de la cadena de suministro, incluyendo financiación, producción, gestión de la información, transporte, almacenamiento y/o depósito.

Como beneficios de la aplicación de esta norma en una compañía se puede destacar los siguientes:

* Permite identificar los riesgos y las amenazas que atentan contra la seguridad de la cadena de suministro e implementar controles para contrarrestar las amenazas.
* Reduce los niveles de inspección.
* Mejora la gestión del riesgo.
* Contribuye con la seguridad de los empleados.
* Mejora las relaciones y brinda mayor confianza con los organismos reguladores.
* Fortalece la continuidad del negocio.
* Contribuye a gestionar requisitos de otros sistemas de gestión.
* Permite mejorar continuamente la seguridad en la cadena de suministro.
* Generación de ventaja comercial y competitiva.

Las normas técnicas actúan como guías de normalización, unificando procesos y procedimientos que protegen los activos de las empresas, apoyándose en razones éticas, que promueven la calidad, la eficiencia y la seguridad. Su objetivo es la estandarización para un correcto seguimiento, supervisión y desarrollo de los procesos, sin omitir que diferentes normas puedan integrarse y complementarse, razón por la que las normas de gestión de riesgos trabajan junto con las de gestión de calidad de la información.

1. **Gestión de la información**

La Política de Gobierno Digital es una política de Estado liderada por el Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia - MinTIC que tiene como objetivo promover el uso y aprovechamiento de las TIC para fortalecer y garantizar un Estado y ciudadanos innovadores, competitivos y dinámicos, que otorguen valor público en un entorno de confianza digital (MinTIC, 2019, p. 11).

Esta política consiste en dos componentes que se desarrollan mediante tres habilitadores, todos en pro de lograr los cinco propósitos planteados para la implementación de esta política en las entidades públicas:

1. Servicios digitales de confianza y calidad.
2. Decisiones basadas en datos.
3. Procesos internos, seguros y eficientes.
4. Empoderamiento de los ciudadanos a través del Estado abierto.
5. Territorios y ciudades inteligentes a través de las TIC.

En el siguiente esquema se presentan los elementos de la Política de Gobierno Digital:



**Propósitos**

La Política de Gobierno Digital se orienta en la satisfacción de las necesidades y la solución de problemas del Estado y de los ciudadanos a través de la sincronía entre componentes y habilitadores, favoreciendo el logro de los siguientes cinco propósitos:

1. Que las entidades habiliten y mejoren la provisión de servicios digitales de confianza y calidad.
2. Que los procesos internos de las entidades públicas sean seguros y eficientes a través del fortalecimiento de las capacidades de gestión de las tecnologías de la información.
3. Que las entidades públicas tomen decisiones basadas en datos.
4. Que los ciudadanos se empoderen y participen de la consolidación de un Estado abierto.
5. Que se solucionen retos sociales mediante el desarrollo de territorios y ciudades inteligentes.

Así, el MinTIC dispone que, dentro de la sección de políticas TI, las entidades deben actuar junto a lineamientos, guías y estándares que les faciliten la gestión de sus recursos y proyectos, que conlleven a resultados más eficientes.

* 1. **Protocolos de elaboración**



La información es indispensable para abordar diferentes procesos administrativos, académicos, operativos, tecnológicos, etc. El tratamiento de la información en cualquier formato (digital, físico, magnético) es una de las actividades que realizan los sistemas de información que soportan los procesos. Del mismo modo, estos métodos incorporan los datos y los recursos físicos como el papel, o tecnológicos, así como los encargados de realizar estas actividades.

Al hablar de los activos que componen los sistemas de información se pueden reconocer los activos físicos (como los computadores) y los de almacenamiento (como USB, discos, cintas, etc.). No obstante, no es recomendable discriminar los demás activos, que aunque no son tangibles, sí son esenciales para las organizaciones como, por ejemplo, el conocimiento (*know-how*) de los funcionarios, la reputación, el *software* o la propiedad intelectual.

Cuando se habla de los Sistema de Gestión de Seguridad de la Información – SGSI se habla de reconocer la importancia del uso reflexivo de la tecnología y las comunicaciones, entendiendo que su uso irresponsable expone a diario a múltiples amenazas que ponen en riesgo la información y con ello, la operación de las entidades. Dichos riesgos provienen tanto del exterior como del interior. Para poder trabajar en un ambiente seguro es necesario identificar la información, determinar su valor e implementar mecanismos o controles en los procesos, las personas y la tecnología. Con el apoyo e implementación del Sistema de gestión de seguridad y privacidad de la información se puede identificar y gestionar los posibles riesgos que atenten contra la seguridad de la información de la empresa.

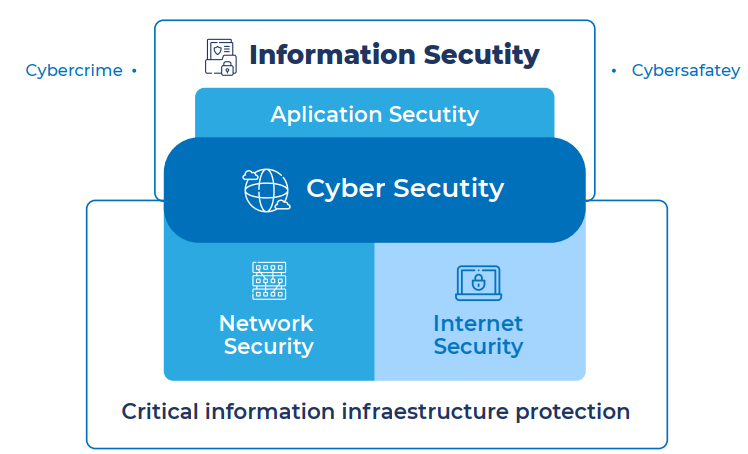
Para hablar del SGSI es importante entender los diferentes conceptos asociados y la diferencia entre seguridad de la información, seguridad informática y ciberseguridad, como se expone a continuación:



La **seguridad informática** permite resguardar la información, por lo que su alcance es mucho más amplio que la **ciberseguridad**; la **SI** protege la información de los posibles riesgos que puedan afectarla, de forma física o digital. Por otro lado, la **ciberseguridad** está orientada a proteger la información digital que se procesa a través de redes, computadores, servidores, etc., por lo que se aproxima mucho a la **seguridad informática**, la cual se preocupa de la protección de la información en cualquier infraestructura computacional o medio informático interconectado o no.

La siguiente figura representa las relaciones entre ciberseguridad y otros dominios de seguridad:

**Figura 2.** Relaciones de ciberseguridad y otros dominios













En conclusión, las bases de datos, los sistemas de información, los reportes, las facturas, los datos personales de contratistas, docentes, proveedores, etc., se deben gestionar de forma diferente, porque no todos tienen la misma relevancia. Por ello, lo más importante en el momento de proteger la información es clasificarla correctamente antes de tomar alguna acción.

Por eso, la Ley de Protección de Datos Personales declara la protección como derecho de toda persona a conocer, actualizar y rectificar la información recogida en bases de datos propensas a la manipulación y gestión por entidades públicas o privadas. De acuerdo con esto, la información personal se encuentra clasificada así:

* **Pública**: dato público.
* **Clasificada**: dato semiprivado y privado.
* **Reservada**: dato sensible.
  1. **Normativa de protección de datos**

En Colombia a partir de los **Lineamientos de política para ciberseguridad y ciberdefensa** establecidos en el CONPES 3701 del 14 de Julio de 2011 se crearon los equipos especializados en incidentes de seguridad que brindan servicios de respuesta a entidades del Estado, además de contribuir con el fortalecimiento de la seguridad y la generación de confianza ante la ciudadanía.

El siguiente esquema muestra el modelo de coordinación de la comisión intersectorial:

**Figura 3.** Modelo de coordinación comisión sectorial



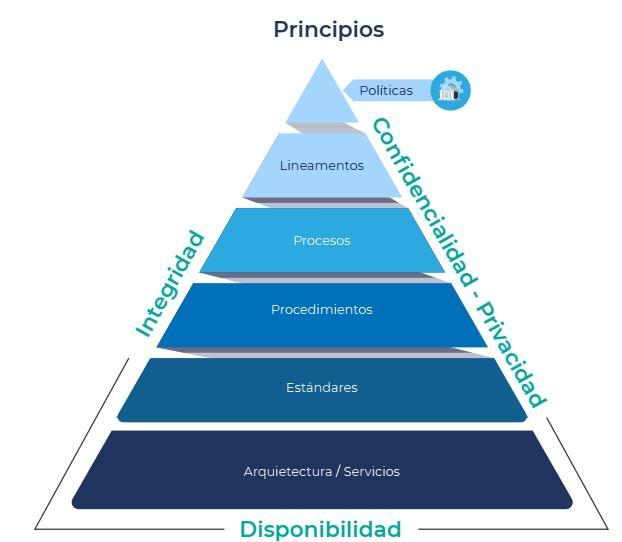
Con el aumento del uso de las tecnologías y los incidentes generados a partir de estas, el Gobierno Nacional inauguró el **CSIRT** de gobierno, un equipo de prevención y respuesta a los incidentes de seguridad informática que afectan a las entidades públicas del país.

La Ley 1712 de 2014 creó la **Ley de Transparencia y del Derecho de Acceso** **a la Información Pública Nacional**, que obliga a publicar en las páginas web tres instrumentos de gestión con el fin garantizar la transparencia y el acceso a la información pública por parte de todos los ciudadanos:

* Registro de activos de la información.
* Índice de información clasificada y reservada.
* Esquema de publicación.

La **NTC-ISO/IEC 27001** es una norma certificable, creada por la ISO con el objetivo de proporcionar una metodología universal para implementar, administrar y mantener la seguridad de la información. De acuerdo con esta norma, el SGSI está conformado por los elementos dispuestos en la siguiente gráfica que representa de modo piramidal las diferentes fases que acompañan los principios del SGSI:

**Figura 4.** *Principios*



La protección de la información se realiza manteniendo los principios (confidencialidad, integridad y disponibilidad) donde esté, incluye los dispositivos que la almacenan, procesan y transmiten y todos los recursos que intervienen en su ciclo de vida, las personas, los procesos y la tecnología que se utilicen; todo esto mediante el uso de políticas, procedimientos, sensibilización y tecnologías.

Proteger la información de amenazas que lleguen a afectar la integridad, la confidencialidad y la disponibilidad es lo que se denomina Sistema de información - SI. Conocer los principios de seguridad que se deben proteger permite identificar de manera más fácil las medidas de protección que deben ser aplicadas para evitar su pérdida o alteración, a continuación, se exponen dichos principios:

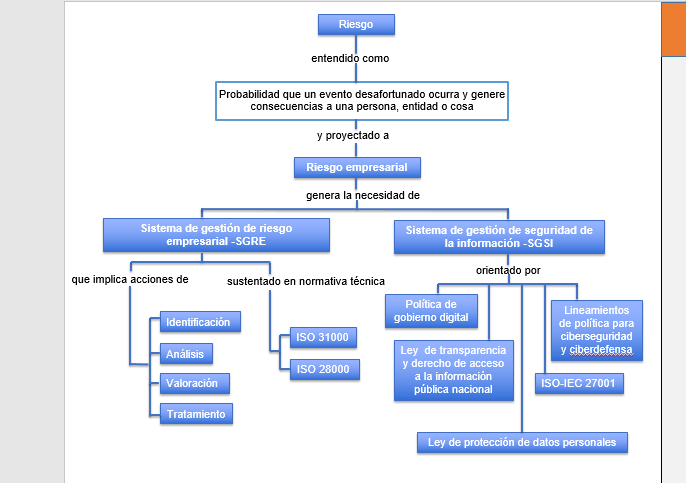


A continuación, se presentan los elementos de la Ley de Protección de Datos Personales y la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional:



**Síntesis**

El siguiente esquema presenta el resumen de las temáticas desarrolladas en el componente formativo, destacando la importancia de los sistemas de gestión del riesgo y la seguridad de la información para el logro de los objetivos empresariales y contribución al proceso de mejora continua de las organizaciones:



**c. ACTIVIDAD DIDÁCTICA**

|  |  |
| --- | --- |
| DESCRIPCIÓN DE LA ACTIVIDAD DIDÁCTICA | |
| Nombre de la actividad | Sistema de gestión del riesgo empresarial y la seguridad de la información |
| Objetivo de la actividad | Verificar la apropiación de la conceptualización básica relacionada con los sistemas de gestión del riesgo empresarial y la seguridad de la información, teniendo en cuenta sus aspectos procedimentales. |
| Tipo de actividad sugerida |  |
| Archivo de la actividad  (Anexo donde se describe la actividad propuesta) | Anexos / CF0011\_Actividad didáctica |

**d. 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 |
| Evaluación del riesgo | Ecuador. Secretaría de Gestión de Riesgos*.* (2012). *Ecuador: referencias básicas para la gestión de riesgos 2013-2014*. Secretaría de Gestión de Riesgos. <https://sena-primo.hosted.exlibrisgroup.com/primo-explore/fulldisplay?docid=sena_elibroELB30908&vid=SENA&search_scope=sena_completo&tab=sena_completo&lang=es_ES&context=L> | Libro | <https://sena-primo.hosted.exlibrisgroup.com/primo-explore/fulldisplay?docid=sena_elibroELB30908&vid=SENA&search_scope=sena_completo&tab=sena_completo&lang=es_ES&context=L> |
| Normativa técnica | Instituto Colombiano de Normas Técnicas y Certificación (Icontec). (2016). *Gestión del riesgo: orientación para la implementación de la NTC-ISO 31000*. Icontec. <https://sena-primo.hosted.exlibrisgroup.com/primo-explore/fulldisplay?docid=sena_aleph000012244&vid=SENA&search_scope=sena_completo&tab=sena_completo&lang=es_ES&context=L> | Libro | <https://sena-primo.hosted.exlibrisgroup.com/primo-explore/fulldisplay?docid=sena_aleph000012244&vid=SENA&search_scope=sena_completo&tab=sena_completo&lang=es_ES&context=L> |
| Normativa de protección de datos | Chaparro, M. (2014). Legislación informática y protección de datos en Colombia, comparada con otros países. *Inventum*, 9(17), p. 32-37. <https://sena-primo.hosted.exlibrisgroup.com/primo-explore/fulldisplay?docid=TN_cdi_doaj_primary_oai_doaj_org_article_d369f2b22f8f479ca3bbdf0c2f4ad238&vid=SENA&search_scope=sena_completo&tab=sena_completo&lang=es_ES&context=PC> | Artículo | <https://sena-primo.hosted.exlibrisgroup.com/primo-explore/fulldisplay?docid=TN_cdi_doaj_primary_oai_doaj_org_article_d369f2b22f8f479ca3bbdf0c2f4ad238&vid=SENA&search_scope=sena_completo&tab=sena_completo&lang=es_ES&context=PC> |

**e. GLOSARIO**

|  |  |
| --- | --- |
| TÉRMINO | SIGNIFICADO |
| Datos | Cualquier objeto que pueda entregar información o significado para el lector. El dato puede ser manipulable en forma manuscrita o por medio de un computador. Puede ser un caracter capturado desde un teclado, extraído de algún espacio de memoria en el disco, almacenado en la memoria central, etc. |
| Gestión de riesgo | Proceso que afecta a todos los órganos directivos y laborales de la organización (junta directiva, administrativos y empleados). |
| Mapa de riesgos | Identifica de forma gráfica los riesgos a los que se expone una empresa, teniendo en cuenta la probabilidad y el impacto que pueden causar. |
| Riesgo | Probabilidad de que un evento desafortunado ocurra y genere consecuencias a una persona, entidad o cosa. |
| Seguridad de la información | Se encarga de proteger los datos contra robo de información, acceso no autorizado, obstaculización al sistema informático, manipulación y/o eliminación de los datos. |

**f. REFERENCIAS BIBLIOGRÁFICAS**

Comunidad de Madrid. (s.f.) *Tratamiento del riesgo*. Comunidad de Madrid. <http://www.madrid.org/cs/StaticFiles/Emprendedores/Analisis_Riesgos/pages/pdf/metodologia/5TratamientodelRiesgo%28AR%29_es.pdf>

Consejo Nacional de Política Económica y Social. (2011). *Documento CONPES 3701.* *Lineamientos de política para ciberseguridad y ciberdefensa.* Consejo Nacional de Política Económica y Social. <https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3701.pdf>

Cristo, N. (2019). *6 reglas para gestionar riesgos en las empresas*. Grupo Bancolombia. <https://www.bancolombia.com/empresas/capital-inteligente/actualidad-economica-sectorial/6-reglas-gestionar-riesgos-empresariales>

Hopkin, P. (2010). *Fundamentals of risk management: understanding, evaluating, and implementing effective risk management*. Kogan Page Limited.

Londoño, I. (2020). *Mapa de calor: una herramienta para optimizar la gestión de riesgos*. Pirani. <https://www.piranirisk.com/es/blog/mapa-de-calor-una-herramienta-para-optimizar-la-gestion-de-riesgos>

Martínez, J. (2011). *Riesgo e incertidumbre*. ScalabBle. <http://www.scalabble.com/2011/03/riesgo-e-incertidumbre/index.html>

Ministerio de Tecnologías de la Información y las Comunicaciones-MinTIC. (2019). *Manual de Gobierno Digital. Implementación de la Política de Gobierno Digital.* MinTIC. <https://gobiernodigital.mintic.gov.co/692/channels-594_manual_gd.pdf>

**g. CONTROL DEL DOCUMENTO**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | Nombre | Cargo | Dependencia  *(Para el SENA indicar Regional y Centro de Formación)* | Fecha |
| Autor (es) | Abel Fernando Becerra Carrillo | Experto temático | Regional Norte de Santander - Centro de la Industria, la Empresa y los Servicios | Abril de 2022 |
| Maribel Avellaneda Nieves | Diseñadora instruccional | Regional Norte de Santander - Centro de la Industria, la Empresa y los Servicios | Julio de 2022 |
| Andrés Felipe Velandia Espitia | Asesor metodológico | Regional Distrito Capital - Centro de Diseño y Metrología | Agosto de 2022 |
| Rafael Neftalí Lizcano Reyes | Responsable Equipo desarrollo curricular | Regional Santander - Centro Industrial del Diseño y la Manufactura | Agosto de 2022 |
| Julia Isabel Roberto | Correctora de estilo | Regional Distrito Capital - Centro de Diseño y Metrología | Agosto de 2022 |

**h. CONTROL DE CAMBIOS**

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