**FORMATO PARA EL DESARROLLO DE COMPONENTE FORMATIVO**

|  |  |
| --- | --- |
| PROGRAMA DE FORMACIÓN | Implementación y operación de la ciberseguridad. |

|  |  |  |  |
| --- | --- | --- | --- |
| COMPETENCIA | 220501110 - Implementar el sistema de seguridad de la información según modelo y estándares técnicos. | RESULTADOS DE APRENDIZAJE | 220501110-01. Planificar la implementación de las estrategias de ciberseguridad de acuerdo con el diseño de las mismas. |

|  |  |
| --- | --- |
| NÚMERO DEL COMPONENTE FORMATIVO | 05 |
| NOMBRE DEL COMPONENTE FORMATIVO | Planificación, entrenamiento y concienciación en implementación de ciberseguridad. |
| BREVE DESCRIPCIÓN | A partir del estudio de este componente formativo el aprendiz estará en capacidad de planificar e implementar las diferentes estrategias de ciberseguridad de la organización. Además, podrá entrenarse y despertar conciencia en lo relacionado con el diseño y aplicación de dichas estrategias. |
| PALABRAS CLAVE | Ciberseguridad, concienciación, entrenamiento, formación, planificación. |

|  |  |
| --- | --- |
| ÁREA OCUPACIONAL | Servicios |
| IDIOMA | Español |

1. **Tabla de contenidos**

**Introducción**

**1. Técnicas de planificación**

1.1. Pronósticos cualitativos y cuantitativos

1.2. Planificación, necesidades y contexto organizacional

**2. Entrenamiento y concienciación en ciberseguridad**

2.1. Fundamentos del entrenamiento en ciberseguridad

2.1.1. Generalidades del entrenamiento

2.1.2. Generalidades de la concienciación

2.2. Características del entrenamiento

**3. Defensa en profundidad**

3.1. Conceptos de Defensa en Profundidad DID

3.2. Capas de la defensa en profundidad

3.3. Características de la defensa en profundidad

1. **Desarrollo de contenidos**

**Introducción**



La ciberseguridad se fundamenta en la seguridad de la información en el ciberespacio, mundo digital o cibernético, que apropia la seguridad informática o digital, abarcando aspectos de la geopolítica con alcances, incluso, sociales. Esta es otra razón más por la que es importante realizar una adecuada planificación, entrenamiento y concienciación en ciberseguridad para una adecuada implementación posterior de las estrategias de seguridad digital.

La planeación es un elemento transversal para una mejor administración y gestión, en cualquier tipo de proceso o proyecto. Luego, ha de abordarse la planeación como un aspecto importante de la aplicación de estrategias de ciberseguridad. En este componente de formación se obtendrá una amplia y detallada explicación de los elementos requeridos para los procesos de **Planificación**, **Entrenamiento** y **Concienciación** en la implementación de estrategias de ciberseguridad.

**1. Técnicas de planificación**

Según Robbins y Couter (2005), la planificación consiste en “definir metas, establecer estrategias para alcanzarlas y trazar planes para integrar y coordinar el trabajo de la organización. Se ocupa tanto de los fines, lo que hay que hacer, como de los medios, como hay que hacerlo."(p. 158).



La planificación implica llevar a cabo un análisis detallado y definir los objetivos deseados, teniendo en cuenta los recursos fundamentales necesarios para alcanzarlos; los cuales, incluyen las habilidades y conocimientos de las personas, así como la tecnología, los materiales y otros elementos que se consideren esenciales para el logro de dichos objetivos.

, En razón a ello, es crucial prestar atención a los siguientes aspectos clave sobre la técnicas de planificación, como se presentan a continuación:

CF05\_1\_Tecnicas\_de\_planificacion\_formato\_6\_slide\_diapositivas\_simple\_DI\_2023

* 1. **Pronósticos cualitativos y cuantitativos**

Para Robbins y Couter (2005), “en los pronósticos cuantitativos se aplican reglas matemáticas a conjuntos de datos para predecir resultados. Mientras que los cualitativos están basados en el buen juicio y las opiniones de conocedores para predecir resultados “(p. 208).



Analice la siguiente tabla en la que se identifican las técnicas tanto cuantitativas como cualitativas de los pronósticos en la planeación:

**Tabla 1**

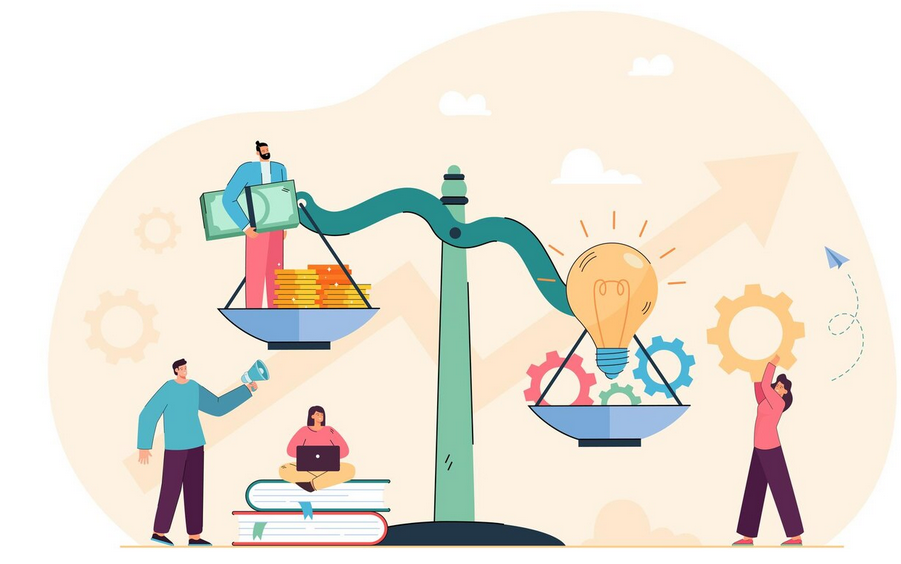
*Técnicas cuantitativas y cualitativas de pronósticos*

| Técnica | Descripción | Aplicación |
| --- | --- | --- |
| *Cuantitativas* | | |
| Análisis de series temporales | Establece una ecuación para una tendencia y la proyecta al futuro. | Pronosticar las ventas del siguiente trimestre con datos de ventas de los cuatro años anteriores. |
| Modelos de regresión | Pronostica una variable a partir de los que se sabe o supone de otras. | Buscar factores que pronostiquen cierto monto de ventas (por ejemplo, precio, gastos en publicidad). |
| Modelos econométricos | Simula con ecuaciones de regresión segmentos de la economía. | Pronosticar el cambio de ventas de autos como resultado de los cambios en las leyes fiscales. |
| Indicadores económicos | Pronostica con uno o más indicadores el estado futuro de la economía. | Pronosticar con cambios en el PIB el ingreso discrecional. |
| Efecto de sustitución | Predice con una fórmula matemática cómo, cuándo y en qué circunstancias un nuevo producto o tecnología sustituirá al actual. | Pronosticar el efecto de los reproductores de DVD en la venta de reproductores de VHS. |
| *Cualitativas* | | |
| Jurado de opinión | Reúne y promedia opiniones de expertos. | Reunir a los gerentes de recursos humanos de la compañía para pronosticar las necesidades de reclutamiento de universitarios el año entrante. |
| Composición de la fuerza de ventas | Combina estimaciones de los vendedores sobre las compras esperadas de los clientes. | Pronosticar las ventas de aparatos de láser individuales el año entrante. |
| Evaluación de los clientes | Combina estimaciones de los clientes habituales. | Un fabricante de entrevistas a los principales distribuidores de autos para determinar los modelos y cantidades de productos deseados. |

Nota. Robbins y Couter (2005)

* 1. **Planificación, necesidades y contexto organizacional**

Las técnicas para la planificación pueden ser aplicadas según las **necesidades** y el **contexto** de la organización. De la misma forma en que se aplica el análisis del punto de equilibrio, la programación lineal o la planeación de escenarios.



A continuación, se analizarán otras técnicas de planificación, teniendo en cuenta las necesidades y el contexto organizacional.

CF05\_1.2\_Planificacion\_necesidades\_y\_contexto\_organizacional\_formato\_4\_video\_DI\_2023

1. **Entrenamiento y concienciación en ciberseguridad**

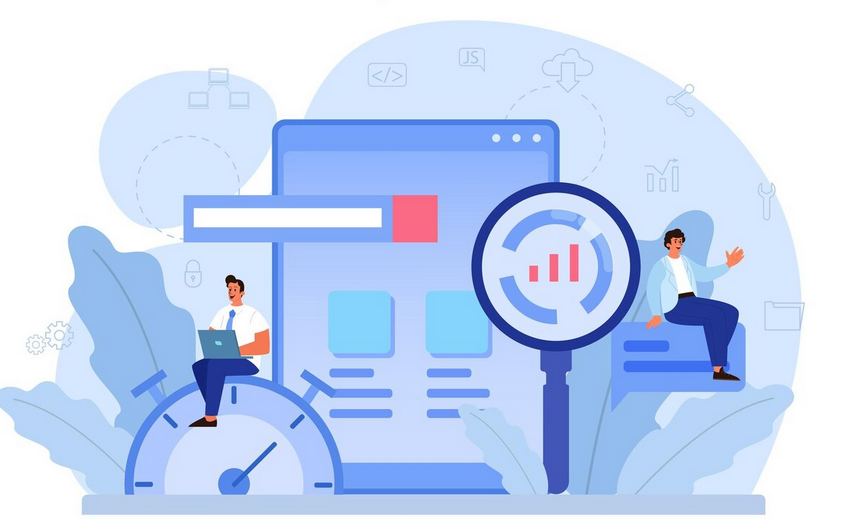
La ciberseguridad se define como la capacidad de minimizar el nivel de riesgo al que están expuestos los sistemas informáticos y sus usuarios, ante amenazas de naturaleza cibernética o digital.

****

Algunos elementos fundantes del entrenamiento y la concienciación en ciberseguridad, que se deben tener presentes son:

**2.1. Fundamentos del entrenamiento en ciberseguridad**

Realizar el entrenamiento y los procesos de formación permanente con el personal de la organización, en busca de la mejora continua de la ciberseguridad, vincula la comprensión de algunos conceptos orientadores y regentes, con esto claro como soporte inicial, se garantiza un buen comienzo de procesos de concienciación.



A continuación se presenta información como un excelente punto de partida para aprender sobre los conceptos esenciales del entrenamiento y la concienciación en ciberseguridad. Tómese el tiempo para leer detenidamente y tomar notas para que pueda mejorar su comprensión de este importante tema.

CF05\_2.1\_FundamentosDelEntrenamientoCiberseguridad\_formato\_9\_acordeon\_DI\_2023



Consulte otros conceptos relacionados con el entrenamiento en ciberseguridad, emitidos por el Instituto Nacional de Ciberseguridad de España – **INCIBE**, en el enlace: <https://www.incibe.es/empresas/guias/glosario-de-terminos-de-ciberseguridad-una-guia-de-aproximacion-para-el>

* 1. ***1. Generalidades del entrenamiento.***

El entrenamiento en el marco de la aplicación de estrategias de ciberseguridad, consiste en el proceso de enseñanza estratégica que busca que, además de impartir conocimientos teóricos y prácticos, los mismos sean apropiados estratégicamente por los participantes para que cumplan eficazmente las tareas asociadas a sus actividades, desempeñadas dentro de un entorno (trabajo, sociedad, escuela, universidad, etc.).



<https://cdn.pixabay.com/photo/2020/04/20/20/57/people-discussion-5069845_960_720.jpg>

La importancia del entrenamiento en ciberseguridad radica en su capacidad para abordar una variedad de aspectos cruciales. Este incluye la gestión, las operaciones, la capacitación de usuarios y las entidades facilitadoras, así como diferentes formas y modalidades de enfoque.

A continuación, se pueden observar los aspectos en los que se enfoca el entrenamiento, en el marco de la aplicación de estrategias de ciberseguridad:

CF05\_2.1.1\_Generalidades\_del\_entrenamiento\_conceptos\_formato\_10\_tabs\_horizontales\_DI\_2023

***2.1.2. Generalidades de la concienciación.***

Consiste en la acción de apropiar una responsabilidad directa o indirecta sobre algo que sucede en el entorno; en cierto modo es educar moralmente sobre algo, por ejemplo, sobre la mala alimentación, la tala indiscriminada de árboles, el consumo de sustancias psicoactivas, entre otras muchas realidades.



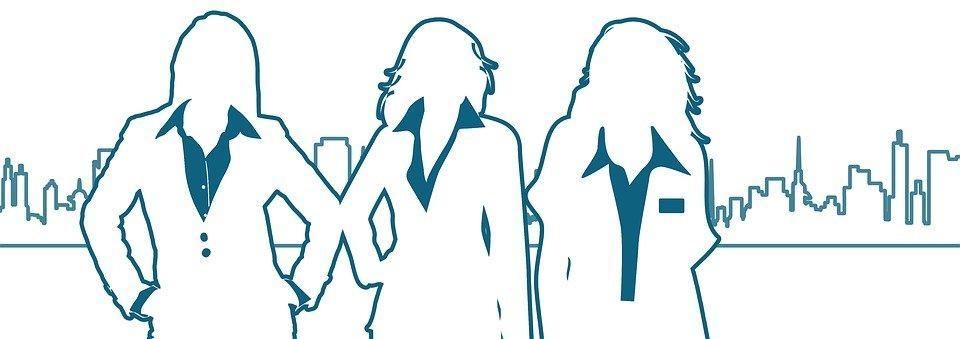
<https://cdn.pixabay.com/photo/2018/03/28/12/44/head-3269125_960_720.png>

En ciberseguridad la concienciación se enfoca en la acción de asumir la responsabilidad directa o indirecta por la confidencialidad, la integridad y la disponibilidad de la información.

En este sentido la concienciación se enfoca a tres grupos de interés claves:

**Los dueños del negocio**

Los dueños de negocio están representados por los gerentes, presidentes y todos los altos cargos de una organización con poder de decisión e influencia sobre todas o ciertas áreas de la misma.



<https://cdn.pixabay.com/photo/2017/04/08/09/02/executive-2212770_960_720.jpg>

Sobre los dueños del negocio, importa reconocer que hay:

**Operadores técnicos**

Se trata del grupo o equipo de técnicos, tecnólogos e ingenieros que se encargan de desarrollar, implementar y operar o mantener los sistemas de información.



<https://cdn.pixabay.com/photo/2018/03/10/12/00/teamwork-3213924_960_720.jpg>

Este grupo se debe mantener muy consciente de la importancia de la ciberseguridad debido a que son responsables por la apropiación de las tecnologías y si no aplican las mejores prácticas, pueden generar brechas o vulnerabilidad de seguridad digital.

**Usuarios**

Los usuarios son el elemento con mayor susceptibilidad de ser atacados por los ciberdelincuentes, por lo tanto, deben recibir una atención especial en la concienciación de ciberseguridad, pues estos tienen accesos y privilegios para la manipulación de información en los sistemas de información, dentro de una organización.



<https://cdn.pixabay.com/photo/2018/05/08/08/42/handshake-3382503_960_720.jpg>

En relación con los usuarios, en el marco de la concienciación de ciberseguridad, se debe recordar:

**Lograr vías de concienciación**

Es importante que se apliquen estrategias de concienciación de usuarios por medio de charlas, cursos, talleres prácticos, boletines, entre otras estrategias de comunicación para la concienciación.

**Fortalecer el conocimiento en las personas**

En ciberseguridad se dice que uno de los eslabones más débiles de la cadena son las personas, haciendo alusión a que se pueden tener los mejores controles de seguridad a nivel técnico, pero un error humano por falta de conocimientos o concienciación, puede hacer vulnerable a los sistemas más robustos y protegidos.

**2.2. Características del entrenamiento**

Las características comunes del entrenamiento y concienciación en ciberseguridad se centran en que ambos son elementos claves para instaurar una cultura de ciberseguridad en una organización; ambas se pueden aplicar a cualquier parte interna o externa de la compañía, comparten conceptos de formación y los propósitos de fortalecer el factor humano y la aplicación de mejores prácticas de seguridad en la apropiación de las tecnologías.



A continuación, se detallan algunas características.

**Asesoría o consultoría**

La asesoríao consultoría externa es una herramienta que puede ser utilizada por los equipos líderes de ciberseguridad para brindar entrenamiento y concienciación. Permite la adquisición rápida de conocimientos de formación, gestión y operación, además de facilitar el despliegue de la toma de conciencia a los grupos de interés claves, los dueños de negocio, los operadores técnicos y los usuarios de los sistemas de información.

**Recursos formativos**

Consisten en materiales de texto y multimedia de apoyo para el entrenamiento y concienciación, pudiendo abordar diversas temáticas de ciberseguridad y tecnología en formatos de documentos de texto, presentaciones y recursos multimedia (imagen, audio y video).

**Emulación de ataques dirigidos controlados**

Permite entrenar y concientizar por medio de la práctica de emulación controlada de ataques dirigidos a sistemas y personas, entre estas prácticas se aplican técnicas de la ingeniería social para poder medir el nivel de concienciación de las personas, así como la capacidad de respuesta de los operadores de tecnología.

**Tips y comunicados**

Es una característica que permite preparar y generar conciencia en ciberseguridad de manera ágil y dinámica, de tal forma que los participantes aprenden poco a poco por medio de pequeñas cápsulas informativas de gran valor y fácil de comprender.

**Encuestas de satisfacción**

Cuando se realizan actividades de entrenamiento y concientización se hace útil realizar mediciones para ver el nivel de satisfacción para determinar si las actividades están siendo adecuadas y no suponen una carga más para los grupos de interés. De esta manera se pueden generar actividades dinámicas y eficientes en función de un adecuado entrenamiento y concienciación en ciberseguridad.

**Test de evaluación y retroalimentación**

Permiten reflejar el nivel de conocimientos y concienciación que tienen los grupos de interés, dueños de negocio, los operadores técnicos y los usuarios de los sistemas de información, de tal forma que se pueda realizar la retroalimentación pertinente en los temas de ciberseguridad que se deben fortalecer, así como también permite tomar acciones para certificar, felicitar y motivar a los grupos de interés en la aplicación de las políticas y buenas prácticas en ciberseguridad.

**Proceso continuo**

Otra característica fundamental es que tanto para la concienciación y el entrenamiento en ciberseguridad, se debe mantener como un proceso continuo, debido a los constantes cambios en los factores tecnológicos, los procesos y del personal dentro de la organización.

**3. Defensa en profundidad**

Según Raggi (2021):

Este concepto, al igual que muchos otros, tiene su origen etimológico en el mundo militar siendo, la defensa en profundidad, una estrategia que pretende dilatar y ralentizar el avance de un enemigo en lugar de pensar sólo en un único método para detenerlo de forma absoluta. Esta defensa en profundidad puede retrasar, lo suficiente, el avance de un ejército enemigo haciendo que pierda fuerza e impulso, y proporcionado, además, valioso tiempo adicional para elaborar una respuesta más efectiva.



La defensa en profundidad permite minimizar la probabilidad de ocurrencia de riesgos, causados por ciberataques; permite la apropiación de controles y buenas prácticas de ciberseguridad para el aseguramiento de la infraestructura tecnológica.

**3.1. Conceptos de Defensa en Profundidad DID**

El CIS (*Center of Internet Security*) define la defensa en profundidad de la siguiente manera:

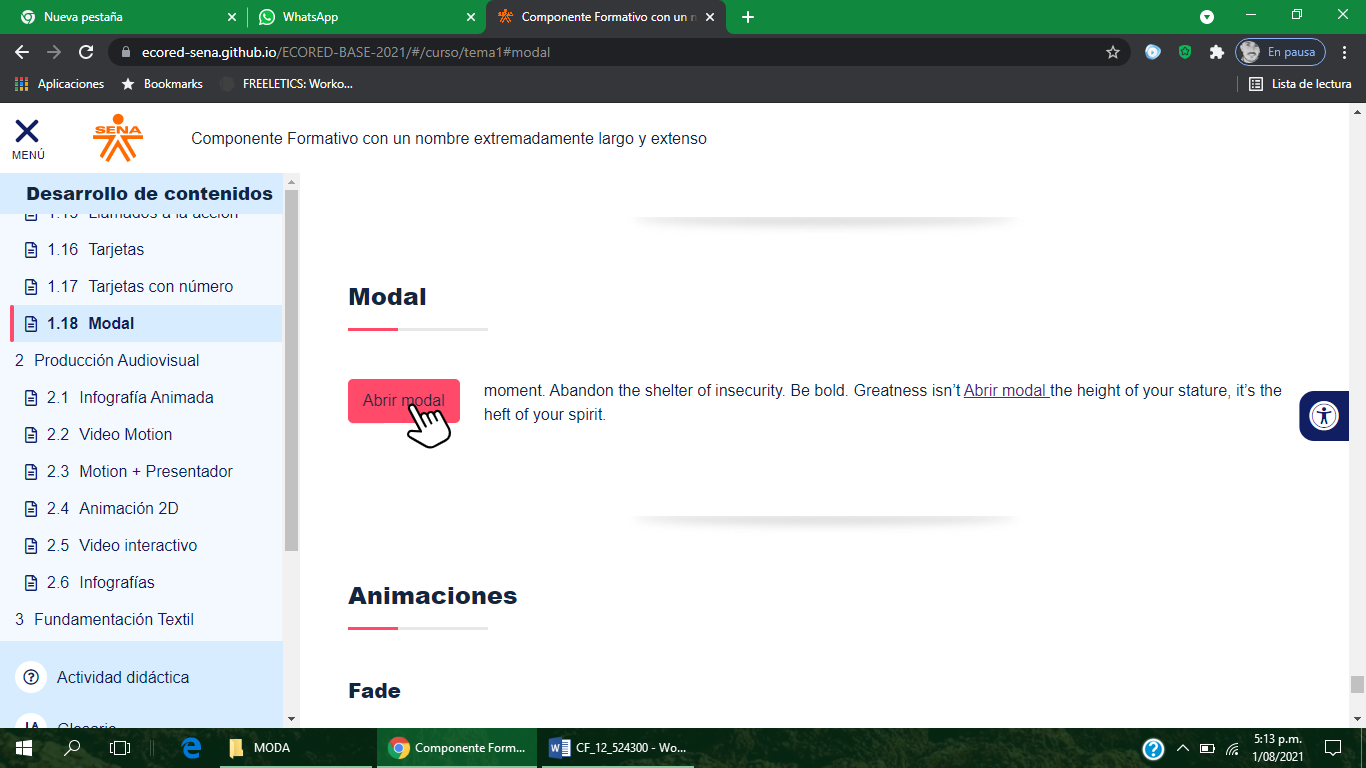
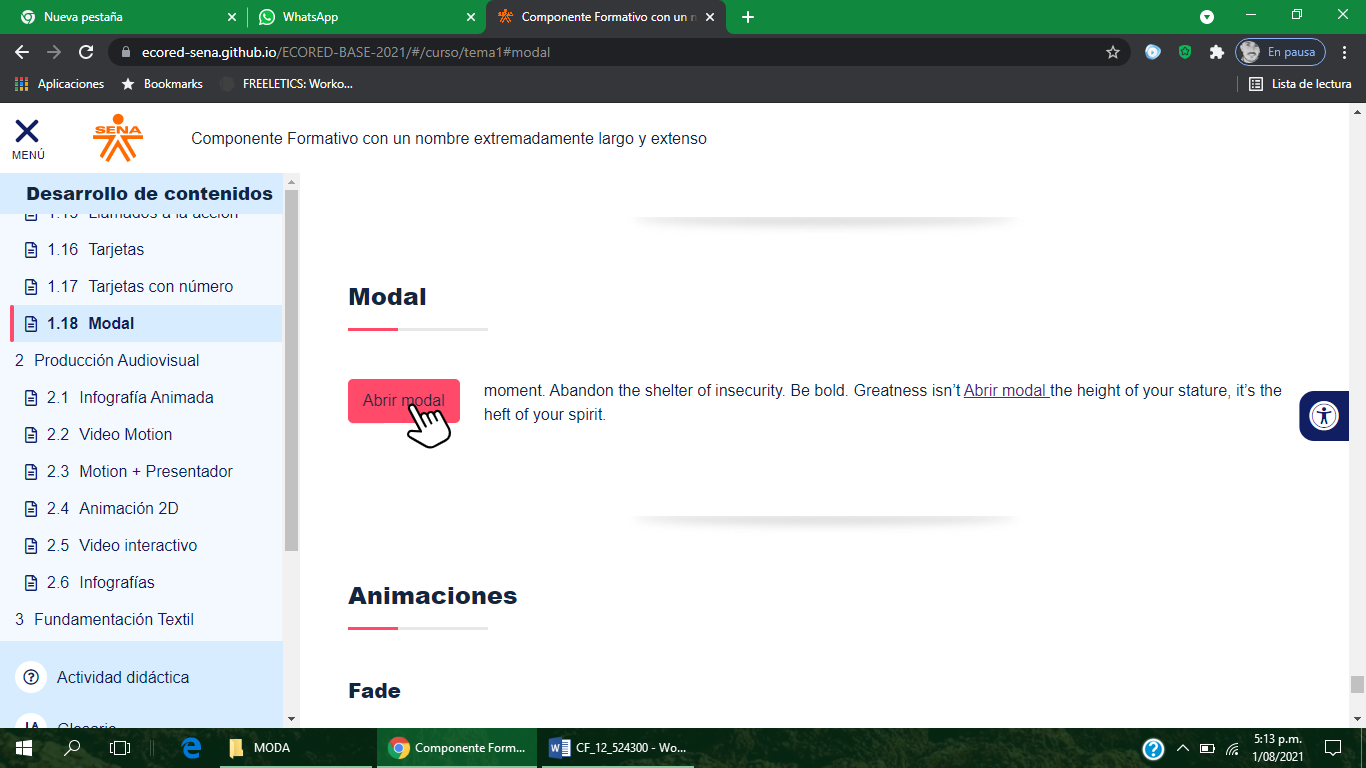
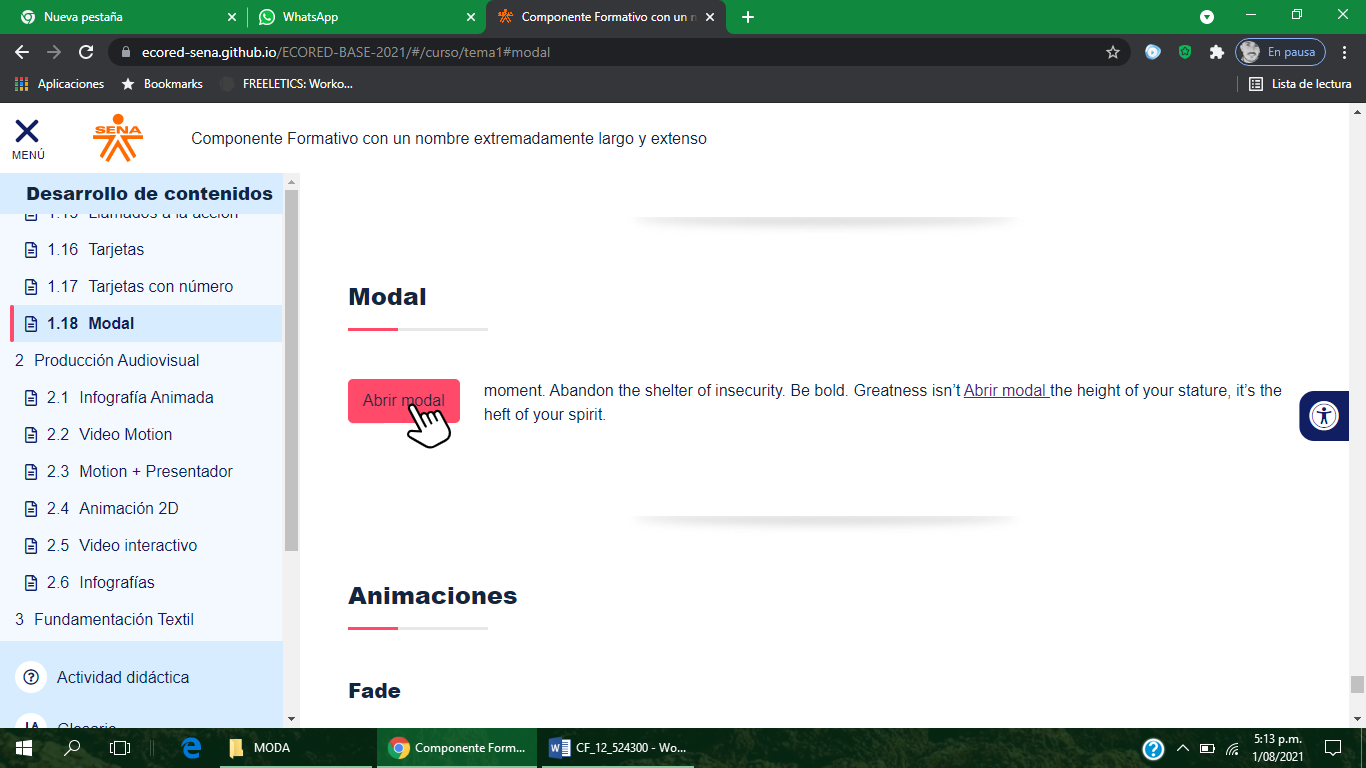
"se refiere a un enfoque de seguridad de la información en el que una serie de mecanismos y controles de seguridad se colocan cuidadosamente en una red de computadoras para proteger la [confidencialidad, integridad y disponibilidad](https://www.cisecurity.org/spotlight/ei-isac-cybersecurity-spotlight-cia-triad/) de la red y los datos que contienen. Si bien ninguna mitigación individual puede detener todas las amenazas cibernéticas, juntas proporcionan mitigaciones contra una amplia variedad de amenazas, al tiempo que incorporan redundancia en caso de que un mecanismo falle. Cuando tiene éxito, este enfoque refuerza significativamente la seguridad de la red contra muchos vectores de ataque". CIS (2021).



Una estrategia eficaz de defensa en profundidad (**DID**), incluye estas (y otras) **mejores prácticas**, **herramientas** y **políticas de seguridad**:

CF05\_3.1\_Conceptos\_de\_defensa\_en\_profundidad\_formato\_12\_rutas\_DI\_2023

En la era digital, donde la información es un activo invaluable, la seguridad cobra una relevancia sin precedentes. Para salvaguardar datos sensibles y sistemas cruciales, tres principios esenciales han surgido como pilares de la ciberseguridad moderna:

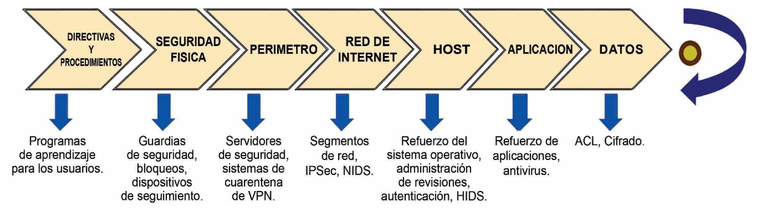
**3.2. Capas de la defensa en profundidad**

La defensa en profundidad aborda la ciberseguridad en capas: en cada capa se aplican controles de seguridad determinados para abarcar todos los aspectos necesarios de proteger, de manera particular y adecuada.

Las capas se pueden representar de distintas maneras y las organizaciones pueden adoptar esta estrategia de ciberseguridad, de acuerdo con su contexto, sus recursos y sus propias necesidades de ciberseguridad.

**Figura 1**

*Representación global del método de defensa en profundidad por capas.*



Rodríguez, Yépez, Peralta y Ortiz (2018).

<https://www.revistaespacios.com/a18v39n42/18394219.html>

En la figura anterior se muestran diversas capas con controles de seguridad asociados, es importante saber que la defensa en profundidad debe ser aplicada considerando las codependencias entre dispositivos, servicios y elementos de una red.

Es esencial comprender las capas de la defensa en profundidad. Para asegurar una protección sólida contra amenazas cibernéticas, explore a detalle en qué consisten estas capas.

CF05\_3.2\_Capas\_para\_la\_defensa\_en\_profundidad\_formato\_2\_infografia\_interactiva\_puntocaliente\_DI\_2023



**3.3. Características de la defensa en profundidad**

La ciberseguridad es el resultado de los procesos ejecutados por las personas haciendo uso de las tecnologías y en defensa en profundidad estos tres elementos (personas, procesos y tecnología) son claves para que la estrategia de defensa en profundidad cumpla con sus objetivos.



A continuación, podrá revisar algunas características clave de la defensa en profundidad en ciberseguridad. Es fundamental comprender estos conceptos para fortalecer la protección de sistemas y datos ante las crecientes amenazas cibernéticas.

CF05\_3.3\_características\_de\_fensa\_en\_profundidad \_formato\_10\_tabs\_verticales(pasos)\_DI\_2023

1. **SÍNTESIS**

En la implementación de ciberseguridad, se enfatizó la planificación utilizando técnicas cualitativas y cuantitativas, considerando pronósticos y el contexto organizacional. Además, se profundizó en la concienciación sobre defensa en profundidad (DID), explorando las capas y características. Esto se traduce en aplicaciones y estrategias efectivas para fortalecer nuestra seguridad cibernética en la empresa.

Diagrama

Descripción generada automáticamente

1. **ACTIVIDADES DIDÁCTICAS (OPCIONALES SI SON SUGERIDAS)**

|  |  |
| --- | --- |
| DESCRIPCIÓN DE ACTIVIDAD DIDÁCTICA | |
| Nombre de la Actividad | Entrenamiento y concienciación en ciberseguridad |
| Objetivo de la actividad | Desarrollar un marco conceptual que permita promover una cultura organizacional centrada en la comprensión y aplicación de principios de seguridad digital. |
| Tipo de actividad sugerida |  |
| Archivo de la actividad  (Anexo donde se describe la actividad propuesta) | Anexos/CF05\_228124\_Formato\_5\_actividad\_didactica\_relacionar\_terminos\_DI\_2023 |

1. **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 |
| 2.1. Fundamentos del entrenamiento en ciberseguridad | Instituto Nacional de Ciberseguridad (2021). *Glosario de términos de ciberseguridad: una guía de aproximación para el empresario.* Incibe. | Glosario | <https://www.incibe.es/empresas/guias/glosario-de-terminos-de-ciberseguridad-una-guia-de-aproximacion-para-el> |
| 3.Defensa en profundidad | Viveros, J. (2015). *Defensa en profundidad para proteger la información de la red corporativa.* <http://polux.unipiloto.edu.co:8080/00002061.pdf> | Documento en línea | <http://polux.unipiloto.edu.co:8080/00002061.pdf> |

1. **GLOSARIO:**

|  |  |
| --- | --- |
| TÉRMINO | SIGNIFICADO |
| Amenaza: | se define como toda aquella acción o serie de acciones que aprovechan las vulnerabilidades para romper la seguridad de los sistemas. |
| Ciberseguridad: | se define como la capacidad para minimizar el nivel de riesgo al que están expuestos los sistemas informáticos y sus usuarios, ante amenazas de naturaleza cibernética o digital. La ciberseguridad brinda a los gobiernos y las organizaciones la ciber-resiliencia como la capacidad para resistir, proteger y defender los sistemas de ciberataques. |
| Control o salvaguarda: | medida de protección o control para contrarrestar amenazas. |
| Infraestructura TI: | consiste en los componentes de *hardware* y *software* requeridos para gestionar y operar entornos tecnológicos que pueden ser implementados en instalaciones de la organización o en sistemas en la nube, Cloud Computing. |
| Riesgo: | "contingencia o proximidad de un daño". RAE (2021) |
| Vulnerabilidad: | en informática, se define como una debilidad o fallo de seguridad que se presenta en un sistema de información, que puede estar compuesto por software, hardware y otros componentes y servicios tecnológicos, generando riesgos de seguridad de la información. |

1. **REFERENCIAS BIBLIOGRÁFICAS:**

Center for Internet Security (2021). *Foco de seguridad electoral - Defensa en profundidad (DiD).* CISECURITY. <https://www.cisecurity.org/spotlight/cybersecurity-spotlight-defense-in-depth-did/>

Raggi, N. (2021). *Defensa en profundidad: cómo implementar esta estrategia de ciberseguridad.* WELIVESECURITY. <https://www.welivesecurity.com/la-es/2021/03/26/defensa-profundidad-que-es-como-implementar-estrategia-ciberseguridad/>

Robbins, R. & Couter, M. (2005). *Administración.* <https://www.auditorlider.com/wp-content/uploads/2019/06/Administracion-8ed-Stephen-P.-Robbins-y-Mary-Coulter-1.pdf>

Rodríguez, A., Yépez, J., Peralta, T. & Ortiz, M. (8 de junio de 2018). Defensa en profundidad aplicado a un entorno empresarial*. Revista Espacios,* 39 (42), 19. <https://www.revistaespacios.com/a18v39n42/a18v39n42p19.pdf>

Rodriguez, L. (2014). *Planificación estratégica II: Diagrama de Gantt pasaje de grado de comisario a comisario inspector (PA) (PE) (PT)*. Docplayer.es. <https://docplayer.es/84386006-Planificacion-estrategica-ii-diagrama-de-gantt-pasaje-de-grado-de-comisario-a-comisario-inspector-pa-pe-pt.html>

1. **CONTROL DEL DOCUMENTO**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | Nombre | Cargo | Dependencia  *(Para el SENA indicar Regional y Centro de Formación)* | Fecha |
| Autor (es) | Joaquín Patiño Cerón | Experto Temático | Centro de Teleinformática y Producción Industrial - Regional Cauca | Septiembre de 2021 |
| Fabián Leonardo Correa Díaz | Diseñador Instruccional | Regional Tolima - Centro agropecuario La Granja | Septiembre de 2021 |
| Andrés Felipe Velandia Espitia | Revisor Metodológico y Pedagógico | Centro de Diseño y Metrología -Regional Distrito Capital | Septiembre de 2021 |
| Rafael Neftalí Lizcano Reyes | Asesor Pedagógico | Centro Industrial del Diseño y la Manufactura - Regional Santander | Septiembrede 2021 |

1. **CONTROL DE CAMBIOS**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | **Nombre** | **Cargo** | **Dependencia** | **Fecha** | **Razón del Cambio** |
| **Autor (es)** | Gloria Lida Alzate Suarez | Adecuador Instruccional | Centro de gestión de mercados, Logística y Tecnologías de la información- Regional Distrito Capital | Octubre de 2023 | Adecuación de contenidos de acuerdo con la directriz de Dirección General. |
| Alix Cecilia Chinchilla Rueda | Metodología para la formación virtual | Centro de gestión de mercados, Logística y Tecnologías de la información- Regional Distrito Capital | Octubre de 2023 | Adecuación de acuerdo con la directriz de Dirección General. |
| Liliana Victoria Morales Guadrón | Responsable Línea de Producción Distrito Capital. | Centro de gestión de mercados, Logística y Tecnologías de la información- Regional Distrito Capital | Octubre de 2023 | Adecuación de contenidos de acuerdo con la directriz de Dirección General. |