**FORMATO PARA EL DESARROLLO DE COMPONENTE FORMATIVO**

|  |  |
| --- | --- |
| PROGRAMA DE FORMACIÓN | Implementación y operación de la Ciberseguridad |

|  |  |  |  |
| --- | --- | --- | --- |
| COMPETENCIA | 220501111 - Controlar sistema de seguridad de la información de acuerdo con los procedimientos y normativa técnica. | RESULTADOS DE APRENDIZAJE | 220501111-01. Establecer indicadores, métricas y alcance de seguimiento de la seguridad digital según normas y estándares internacionales. |

|  |  |
| --- | --- |
| NÚMERO DEL COMPONENTE FORMATIVO | 07 |
| NOMBRE DEL COMPONENTE FORMATIVO | Seguimiento de la seguridad digital. |
| BREVE DESCRIPCIÓN | Con el desarrollo de este componente, el aprendiz estará altamente capacitado en establecer indicadores, métricas y alcance de seguimiento de la seguridad digital, según estándares y metodologías nacionales e internacionales; de igual manera, en realizar el monitoreo de la seguridad digital de acuerdo con los indicadores y métricas establecidos. |
| PALABRAS CLAVE | Alcance, indicadores, métricas, monitoreo, norma técnica. |

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

1. **TABLA DE CONTENIDOS:**

**Introducción**

**1. Métodos de métricas e indicadores de monitoreo**

1.1. Características de las métricas e indicadores

1.2. Tipos de Indicadores

**2. *Testing* y monitoreo de la seguridad digital**

2.1. Tipos de pruebas de efectividad

2.2. Alcance de las pruebas de efectividad

2.3. Procedimiento de las pruebas

**3. *Software***

1. **INTRODUCCIÓN**

Para comenzar el estudio de este componente y enterarse de los contenidos, amplitud y ruta de aprendizaje del mismo, le invitamos a visualizar el siguiente video:



1. **DESARROLLO DE CONTENIDOS:**

**1. Métodos de métricas e indicadores de monitoreo**

La adopción de métodos para la creación de métricas e indicadores de monitoreo está dirigido a la medición de la eficiencia, la efectividad y la eficacia de los componentes de gestión y de implementación, definidos en el plan estratégico de la seguridad y privacidad de la información. Estas métricas e indicadores ayudarán en la formulación de estrategias de mejora continua, permitiendo una mejor toma de decisiones.



<https://cdn.pixabay.com/photo/2018/06/19/10/01/internet-3484137_960_720.jpg>

Esta adopción de métricas e indicadores tiene como principales objetivos, los siguientes:

* **Evaluar la efectividad** de la implementación de los controles de seguridad.
* **Evaluar la eficiencia** del Modelo de Seguridad y Privacidad de la Información al interior de la entidad.
* **Proveer estados de seguridad** que sirvan de guía en las revisiones del modelo de seguridad y privacidad de la información, facilitando mejoras en seguridad de la información y nuevas entradas a auditar.
* **Comunicar valores** de seguridad al interior de la entidad.
* **Servir como insumos** al plan de análisis y tratamiento de riesgos.

Para fundamentar los conceptos abordados, se le recomienda indagar los lineamientos de la **ISO/IEC 27001** – **ISO 27004** y la **Guía 9 de Indicadores de gestión para la seguridad de la información del MINTIC**, que encontrará en el material complementario.

**1.1. Características de las métricas e indicadores**

El escenario de la seguridad digital muestra cómo las amenazas cibernéticas evolucionan de manera permanente; el monitoreo de la seguridad de la información en las organizaciones ha de ser una rutina integral. Las métricas e indicadores orientadas a tal monitoreo, tienen una serie de características que vale la pena identificar, para una mejor aplicación y establecimiento de los mismos.



<https://cdn.pixabay.com/photo/2017/05/08/19/35/cyber-security-2296269_960_720.jpg>

Esas características representativas son:

**Evaluadores**

Las métricas e indicadores son mecanismos o instrumentos utilizados para evaluar si se cumple o no con los objetivos estratégicos.

**Medidores**

Las métricas e indicadores son una unidad de medida gerencial que evalúa resultados de una organización, frente a sus responsabilidades y objetivos.

**Generadores de información**

Las métricas e indicadores son un generador de información que analiza el desempeño de cualquier proceso y verifica el cumplimiento, en términos de resultados.

**Generadores de alertas**

Las métricas e indicadores son un generador de alertas que determinan desviaciones en el cumplimiento de los objetivos.

**1.2. Tipos de indicadores**

Con los lineamientos de las normas **ISO/IEC 27001**, **ISO/IEC 27004** y de la **Guía 9 de indicadores de gestión para la seguridad de la información del MINTIC**, se adopta una serie de indicadores para medir la gestión y el cumplimiento en el avance del modelo de seguridad digital.



<https://cdn.pixabay.com/photo/2015/09/20/15/46/binding-contract-948442_960_720.jpg>

**Indicadores de gestión e indicadores de cumplimiento**

Tanto las normas ISO/IEC 27001 e ISO/IEC 27004, así como la Guía 9 de indicadores de gestión para la seguridad de la información del Ministerio de Tecnologías de la Información y lasComunicaciones , destacan la importancia de estos, para medir la gestión y el cumplimiento en el modelo de seguridad digital de las organizaciones. A continuación, algunas definiciones y orientaciones otorgadas por el MINTIC:

**Se destacan, los tipos de indicadores que se enuncian y definen a continuación:**

* **Indicadores de Gestión:** están relacionados con las razones que permiten administrar un proceso o un sistema. Profundice a continuación sobre los indicadores de gestión:



* **Indicadores de Cumplimiento:** están relacionados con las razones que indican el grado de consecución de tareas. Revise a continuación más información sobre este tipo de indicadores:



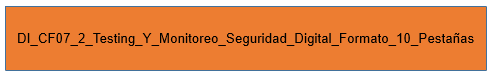
**2. *Testing* y monitoreo de la seguridad digital**

La finalidad de las pruebas de efectividad, frente a la metodología, es comprobar o medir la eficiencia de la ejecución del modelo de seguridad en las entidades; la cual facilita a las entidades la comprensión del desarrollo de las pruebas, los objetivos y el beneficio que se gana al identificar sus etapas y gestionarlas.



<https://image.shutterstock.com/image-photo/finger-touching-tablet-web-technology-600w-1916427485.jpg>

Algunas generalidades del ***testing*** que se deben tener en cuenta, dado su nivel de importancia e implicación, estas son:



Afiance sus conocimientos en lo relacionado con *Testing* y monitoreo, visitando y leyendo, responsablemente, la **Guía No 1 (Guía metodológica de pruebas de efectividad) del MINTIC**.

https://www.mintic.gov.co/gestionti/615/articles-5482\_G1\_Metodologia\_pruebas\_efectividad.pdf

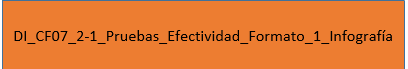
**2.1. Tipos de pruebas de efectividad**

No existe una sola forma de hacer pruebas de efectividad ni tampoco un solo tipo de pruebas; esto significa que no habría marcos de referencia de los niveles de seguridad que se estarían evaluando. Entre otras cosas, un solo tipo de pruebas sería insuficiente para cubrir los diferentes tipos de comprobaciones existentes al interior de la organización. Una sola prueba o tipo de prueba, no tendría arqueo suficiente para evaluar todas las necesidades y eventos de la seguridad y privacidad de la información, que tuviera la entidad. (MINTIC, s.f.).



<https://cdn.pixabay.com/photo/2016/08/13/09/43/data-1590455_960_720.jpg>

Se pueden determinar tres tipos de pruebas de efectividad, teniendo en cuenta el nivel de conocimiento del entorno de la organización, esto es:



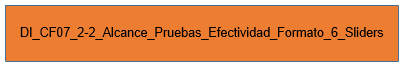
**2.2. Alcance de las pruebas de efectividad**

La metodología de pruebas, desde el inicio de la ejecución, se enfoca en implementar una línea base del estado de seguridad de la organización, con el fin de facilitar la identificación de la brecha en la implementación del modelo de seguridad, teniendo como concepto de línea base, la primera medición.



<https://cdn.pixabay.com/photo/2013/07/12/17/22/detective-152085_960_720.png>

Estos son algunos alcances de las pruebas de medición en las organizaciones, en relación con el plan de seguridad y privacidad de la información, otorgadas por el ministerio de tecnologías de la información y comunicaciones:



**2.3. Procedimiento de las pruebas**

De la aplicación procedente, responsable y oportuna de las pruebas, depende en gran medida su efectividad y su potencial aprovechamiento. Las pruebas de efectividad han de realizarse por fases, siendo cada una de estas, una acción vinculada consecuentemente con las anteriores o con las posteriores.



Nota: <https://www.mintic.gov.co/gestionti/615/articles-5482_G1_Metodologia_pruebas_efectividad.pdf>

Repase las fases secuenciales de aplicación de las pruebas de efectividad, en procesos de seguridad de la información, como lo propone MINTIC, explorando la información que se expone a continuación:



**Fase de contextualización**

La fase de contextualización se soporta en la identificación de alcances reales de las pruebas y de los procedimientos a ejecutar, con base en las necesidades identificadas.



<https://cdn.pixabay.com/photo/2018/06/08/00/48/developer-3461405_960_720.png>

Tal identificación puede darse por medio de preguntas como:

a. ¿Cuáles serán los objetivos a evaluar?

b. ¿Qué quiere alcanzar la entidad específicamente con estas pruebas?

c. ¿Si desea realizarlo en horas hábiles, no hábiles o fines de semana?

d. ¿Qué direcciones IP internas o externas serán objetivo de las pruebas? (Si aplica).

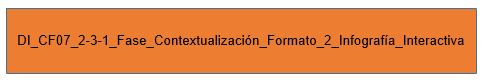
e. En caso de poderse vulnerar el sistema, ¿qué tipo de acciones posteriores solicita realizar? (Pueden ser pruebas de vulnerabilidades en la máquina comprometida, escalamiento de privilegios, etc.).

f. ¿Qué fechas de inicio y finalización de las actividades?

g. ¿Se incluirán temas de ingeniería social?

h. ¿Qué temas de ingeniería social pueden ser válidos para ejecutar estos procedimientos?

Estos son algunos aspectos de suma importancia, desde el ministerio de las TIC, y que se deben tener en cuenta en la fase de contextualización, esto es:



**Fase de reconocimiento del objetivo**

Entre más información pueda obtenerse, más puntos de explotación podrían encontrarse y aprovecharse en las siguientes fases. Para realizar este levantamiento de información pueden utilizarse los tres métodos denominados: pasivo, semi-pasivo y activo (enfocado a los sistemas de información).

Conozca, según la orientación del ministerio de tecnologías de la información y las comunicaciones, las especificaciones y aspectos particulares de los tres métodos para el levantamiento de información en la fase de reconocimiento del objetivo:



**Fase de modelado de amenazas**

“Esta fase maneja la relación “**Atacante Versus activo**”; es decir, el beneficio que el atacante puede obtener si logra su objetivo de penetrar el sistema y modificar, borrar, copiar o destruir algún activo de información”. (MINTIC, s.f.).

A continuación, podrá identificar de manera más detallada esta relación, esto es:



**Fase de análisis de vulnerabilidades**

Dependiendo de la amplitud de los alcances propuestos, el análisis de vulnerabilidad puede variar desde analizar un servicio o host específico o a un inventario completo de máquinas.

Estos procesos de análisis pueden ejecutarse también de las siguientes maneras o métodos:



La fase de análisis de vulnerabilidades implica, además, métodos como análisis de metadatos en archivos publicados en internet, que pueden contener información sobre el tipo de servidor, nombres de dominio, direccionamiento IP, etc. También incluye el monitoreo de tráfico o copiado de tráfico (espejo de puertos) para captura y posterior análisis. (MINTIC, s.f.).

**Fase de explotación**

Esta fase se centra en obtener acceso al sistema, apalancando las debilidades identificadas en la etapa anterior o sobrepasando los controles de seguridad existentes.

Dentro de las técnicas de explotación más utilizadas se encuentran las siguientes:



Existen aún más métodos de ataque, con los cuales se puede intentar lograr el objetivo de vulnerar o acceder a los sistemas. Una vez se logre el objetivo de ingreso, deberán documentarse los hallazgos de una manera evidente y concreta para utilizar la información como herramienta de mejora. (MINTIC, s.f.).

**Fase de post-explotación**

“Es importante tener en cuenta que, a este punto, ya se vulnera el sistema y no es necesario dañarlo o desestabilizar gravemente (a menos que el plan desde el principio así lo indique)”. (MINTIC, s.f.).

Por lo tanto, se debe definir un alcance máximo a ejecutar para las siguientes acciones:

* Escalamiento de privilegios.
* Acceso a datos específicos (bases de datos, repositorios, *fileservers*, ftp).
* Denegación de servicios (CRÍTICO).
* Obtención de *passwords* para otros sistemas.
* Acceso a *logs* de dispositivos.
* Ingreso a servidores Web, DNS, proxy, servidores de impresión.
* Acceso a directorios activos o LDAP, para obtener información de usuarios (cuentas de correo electrónico, extensiones o dependencias donde trabajan), información que puede emplearse para posteriores ataques de ingeniería social.
* Ingreso a las entidades certificadoras, que podría afectar la creación de certificados, revocación e incluso la inscripción de dichos certificados si se llega a comprometer la llave.
* Acceso a los sistemas de almacenamiento, para verificar información sobre tipos de *backup*, medios empleados etc.
* *Ping Sweeps* (Barridos A VLANS para identificar hosts).
* Instalación de *exploits* remotos.
* Instalación de *backdoors* para posterior ingreso y que no se afecten por los reinicios de los hosts.
* Modificación de los servicios.

**Fase de reporte**

“Es necesario documentar todos los resultados obtenidos en cada fase, para tener soportes de las labores realizadas y a su vez la respectiva justificación de los resultados finales”. (MINTIC, s.f.).



<https://cdn.pixabay.com/photo/2019/10/25/10/49/audit-4576720_960_720.jpg>

Por lo anterior, es importante tener en cuenta las audiencias a las cuales se les presentará el reporte, dado que no es conveniente entrar en demasiados detalles cuando la audiencia será de tipo administrativo y así mismo cuando la audiencia es de tipo técnico, no se disponga de un reporte más preciso y específico.

**Tipos de Reporte**

* **Reporte gerencial**

“El reporte gerencial enfoca un plan de trabajo para solucionar todas las falencias encontradas, pueden manejarse plazos trimestrales, semestrales y anuales para determinadas labores que requieran ejecutarse”. (MINTIC, s.f.).



<https://cdn.pixabay.com/photo/2016/12/01/09/12/discussion-1874792_960_720.jpg>

Según las mismas orientaciones de MINTIC, este tipo de reporte debe contener la siguiente información:

* Introducción, justificación y objetivos alcanzados durante las pruebas.
* Calificación de riesgo, ubicando los activos que mayor riesgo pueden traer a la organización con base al criterio del ejecutor de la prueba de efectividad de los controles.
* Motivos o causa raíz de las vulnerabilidades encontradas, entre las cuales se pueden encontrar razones como:
* Máquinas sin parches.
* Sistemas operativos sin el *hardening* adecuado.
* Máquinas con servicios activos no utilizados.
* Contraseñas débiles o fáciles de adivinar.
* Diseños o arquitecturas de sistemas inseguros, servicios de red sin *hardening*.
* Firmware de dispositivos obsoleto.
* **Reporte técnico**

“Este reporte puede contener la información anterior, pero incluyendo los aspectos más importantes a nivel técnico, dado que quienes reciban esta información serían quienes ejecuten las acciones de mejora para cada vulnerabilidad encontrada”. (MINTIC, s.f.).



<https://cdn.pixabay.com/photo/2018/01/07/20/56/graph-3068300_960_720.jpg>

Lo anterior, teniendo en cuenta:

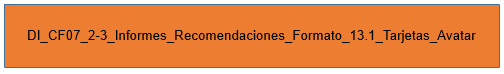
* Recolección de información basada en recursos publicados por la propia entidad.
* Información recolectada en plataformas como *google*, *bing*, páginas de referencia, etc.
* Información que pudo ser recolectada en las plataformas publicadas como, estructura de la organización, unidades de negocio, mercados, proveedores etc.
* Inteligencia con el personal interno, donde se evidencia la información que pudo obtenerse por medio de ingeniería social (solo en primera instancia, no para solicitar claves o accesos).
* Vulnerabilidades encontradas (clasificadas bien sea por los servicios, plataformas o *hosts*).
* Explotación de las vulnerabilidades (cuales fueron apalancadas o pudieron ser aprovechadas en cada *host* y cuáles no).
* Actividades de POST-Explotación efectuadas en cada host comprometido con la prueba.
* Una vez se finaliza el reporte, se espera que la entidad inicie con las actividades propuestas para cerrar las brechas y aumentar la efectividad de los controles implementados o se implementen otros que cumplan con las expectativas de seguridad de la información.
* **Informes y recomendaciones**

En esta fase ya se cuenta con la información resultante del levantamiento de información, pruebas, análisis y evidencias recolectados se han evidenciado las vulnerabilidades técnicas explotables y la línea base de seguridad de la entidad evaluada, su brecha frente a la norma ISO 27001 y en relación con mejores prácticas. (MINTIC, s.f.).



<https://cdn.pixabay.com/photo/2017/12/30/20/59/report-3050965_960_720.jpg>

Estos son algunos aspectos clave que, sobre los informes, deben tenerse en cuenta y ser aplicados, según lo orientado y estipulado por el ministerio de las TIC:



**3. *Software***

Proteger la empresa u organización es más posible cuando se cuenta con herramientas de seguridad digital. Subestimar la importancia de una estrategia de ciberseguridad robusta, es un error que puede costar caro a las organizaciones.



<https://cdn.pixabay.com/photo/2014/02/13/07/28/security-265130_960_720.jpg>

Las estrategias de seguridad digital fortalecidas y desarrolladas bajo normas y estándares son la herramienta que garantiza la protección de las organizaciones.

Conozca, a continuación, algunos de los *softwares* que contribuyen a la seguridad digital, desde la prevención o la mitigación de amenazas:



1. **SÍNTESIS**

Toda empresa u organización debe propender por establecer una política que permita identificar, gestionar e implementar las acciones necesarias que permitan prevenir y mitigar los riesgos de seguridad digital, esto a través de monitoreos métodos e indicadores que permitan su seguimiento constante acorde a las métricas establecidas por la organización que generen seguridad digital.

**Seguimiento de la seguridad digital**

***Software***

**Métricas e indicadores de monitoreo**

***Testing* y monitoreo de la seguridad digital**

Contribuyen a la seguridad digital, desde la prevención o la mitigación de amenazas

La finalidad es comprobar o medir la eficiencia de la ejecución del modelo de seguridad en las entidades

**Tipos**

**Características**

* Evaluadores
* Medidores
* Generadores de información
* Generadores de alertas
* Gestión
* Cumplimiento

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

|  |  |
| --- | --- |
| DESCRIPCIÓN DE LA ACTIVIDAD DIDÁCTICA | |
| Nombre de la actividad | La Seguridad Digital. |
| Objetivo de la actividad | Reconocer los elementos, indicadores, métricas y metodologías necesarios para hacer seguimiento y monitoreo de la seguridad digital, generando con esto el aprovechamiento de los mismos y generando acciones de mejora continua para la seguridad digital. |
| Tipo de actividad sugerida |  |
| Archivo de la actividad  (Anexo donde se describe la actividad propuesta) | Carpeta Anexos |

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 |
| 1. Métodos de métricas e indicadores de monitoreo | Organización Internacional de Normalización (ISO). (2013). *Seguridad de la información, ciberseguridad y protección de la privacidad.* *(ISO 27001)*. | Otro: Norma técnica | <https://www.iso.org/standard/54534.html> |
| 1. Métodos de métricas e indicadores de monitoreo | Organización Internacional de Normalización (ISO). (2016). *Tecnología de la información - Técnicas de seguridad - Gestión de la seguridad de la información - Seguimiento, medición, análisis y evaluación.* (ISO27004). | Otro: Norma técnica | <https://www.iso.org/standard/64120.html> |
| 1. Métodos de métricas e indicadores de monitoreo | Ministerio de Tecnologías de la Información y Comunicaciones (MINTIC). (2015). *Guía de indicadores de gestión para la seguridad de la información.* | Otro: Guía técnica | <https://www.mintic.gov.co/gestionti/615/articles-5482_G9_Indicadores_Gestion_Seguridad.pdf> |

1. **GLOSARIO:**

|  |  |
| --- | --- |
| TÉRMINO | SIGNIFICADO |
| Activo: | cualquier cosa que tenga valor para la organización. [NTC 5411-1:2006]. |
| Amenaza: | es toda aquella acción o serie de acciones, que aprovechan las vulnerabilidades para romper la seguridad de los sistemas. |
| Control: | medios para gestionar el riesgo, incluyendo políticas, procedimientos, directrices, prácticas o estructuras de la organización que pueden ser de naturaleza administrativa, técnica, de gestión o legal. |
| Política: | toda intención y directriz expresada formalmente por la Dirección. |
| Vulnerabilidad: | te trata de aquella 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:**

Ministerio de Tecnologías de la Información y Comunicaciones (MINTIC). (s.f.). *Guía de indicadores de gestión para la seguridad de la información.* <https://www.mintic.gov.co/gestionti/615/articles-5482_G9_Indicadores_Gestion_Seguridad.pdf>

Ministerio de Tecnologías de la Información y Comunicaciones (MINTIC). (s.f.). *Guía Metodológica de Pruebas de Efectividad.* <https://www.mintic.gov.co/gestionti/615/articles-5482_G1_Metodologia_pruebas_efectividad.pdf>

Organización Internacional de Normalización (ISO). (2013). *Seguridad de la información, ciberseguridad y protección de la privacidad.* *(ISO 27001)*. <https://www.iso.org/standard/54534.html>

Organización Internacional de Normalización (ISO). (2016). *Tecnología de la información - Técnicas de seguridad - Gestión de la seguridad de la información - Seguimiento, medición, análisis y evaluación.* (ISO27004).<https://www.iso.org/standard/64120.html>

1. **CONTROL DEL DOCUMENTO**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | Nombre | Cargo | Dependencia  *(Para el SENA indicar Regional y Centro de Formación)* | Fecha |
| Autor (es) | Pablo Cesar Pardo Ortiz | Experto Temático | Regional Cauca - Centro de Teleinformática y Producción Industrial | Septiembre 2021 |
| Fabián Leonardo Correa Díaz | Diseñador Instruccional | Regional Tolima - Centro agropecuario La Granja | Septiembre 2021 |
| Andrés Felipe Velandia Espitia | Revisor Metodológico y pedagógico | Regional Distrito Capital - Centro de Diseño y Metrología | Septiembre de 2021 |
| Rafael Neftalí Lizcano Reyes | Asesor Pedagógico | Regional Santander - Centro Industrial del Diseño y la Manufactura | Septiembre de 2021 |
| Sandra Patricia Hoyos Sepúlveda | Revisión y corrección de estilo | Centro para la Industria de la Comunicación Gráfica | Septiembre 2021 |

1. **CONTROL DE CAMBIOS**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | Nombre | Cargo | Dependencia | Fecha | Razón del Cambio |
| Autor (es) | Gloria Amparo López Escudero | Adecuadora Instruccional | Regional Distrito Capital - Centro de gestión de mercados, Logística y Tecnologías de la información. | Octubre de 2023 | Adecuación de contenidos de acuerdo con la directriz de Dirección General. |
|  | Alix Cecilia Chinchilla Rueda | Asesora Metodológica | Regional Distrito Capital - Centro de gestión de mercados, Logística y Tecnologías de la información. | Octubre de 2023 | Adecuación de contenidos de acuerdo con la directriz de Dirección General. |
|  | Liliana Victoria Morales Guadrón | Responsable Línea de Producción Distrito Capital. | Regional Distrito Capital - Centro de gestión de mercados, Logística y Tecnologías de la información. | Octubre de 2023 | Adecuación de contenidos de acuerdo con la directriz de Dirección General. |