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.

Noviembre 2023

Tabla de contenido

Introducción 1

1. Técnicas de planificación 1

1.1. Pronósticos cualitativos y cuantitativos 3

1.2. Planificación, necesidades y contexto organizacional 4

2. Entrenamiento y concienciación en ciberseguridad 7

2.1. Fundamentos del entrenamiento en ciberseguridad 8

2.2. Características del entrenamiento 14

3. Defensa en profundidad 16

3.1. Conceptos de Defensa en Profundidad DID 17

3.2. Capas de la defensa en profundidad 20

3.3. Características de la defensa en profundidad 23

Síntesis 26

Material complementario 27

Glosario 28

Referencias bibliográficas 29

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 las técnicas de planificación, como se presentan a continuación:

A. **Utilidad de la planificación:** la planificación traza las metas u objetivos en tiempos específicos ya sean en el corto, mediano y largo plazo, en donde se establecen las actividades a realizar con los respectivos responsables, y los medios necesarios para el cumplimiento de las mismas.
B. **Reconocimiento del entorno:** planificar implica, entre otras cosas, una "revisión de grandes volúmenes de información para anticipar e interpretar los cambios del ambiente. Un reconocimiento externo, tal vez revele problemas y preocupaciones que incidan en las actividades actuales o planeadas de la organización." Robbins y Couter (2005).
C. **FODA:** el reconocimiento del entorno puede llevarse a cabo mediante herramientas como la Matriz FODA, que evalúa las Fortalezas, Oportunidades, Debilidades y Amenazas, o mediante el análisis de los aspectos políticos, económicos, sociales, tecnológicos, ecológicos y legales, conocidos como (Análisis PEST-EL).
D. **Pronósticos:** los pronósticos hacen referencia a las "predicciones de resultados; su objetivo es dar a los directivos información que facilite la toma de decisiones. Cuánto más turbulento sea el entorno menos fiable será el pronóstico que se plantee" Robbins y Couter (2005).

1.1. 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.	Establece una ecuación para una tendencia y la proyecta al futuro.
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		

Técnica	Descripción	Aplicación
Jurado de opinión	Reúne y promedias 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)

1.2. 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.

Video 1. Planificación, necesidades y contexto organizacional

Enlace de reproducción del video

Síntesis del video: Planificación, necesidades y contexto organizacional
En el mundo empresarial, la planificación traza las metas u objetivos en tiempos específicos, ya sean en el corto, mediano y largo plazo, en donde se establecen las actividades a realizar con los respectivos responsables, y los medios necesarios para el cumplimiento de las mismas. en donde se establecen las actividades a realizar con los respectivos responsables, y los medios necesarios para el cumplimiento de las mismas. La planeación, siendo un elemento esencial que atraviesa todas las áreas de la administración y gestión, considera tanto las necesidades específicas de la organización como el contexto en el que opera. Ello implica:

1. Reconocimiento del entorno.

2. Pronósticos.

3. Elaboración de presupuestos.

4. Programación.

5. Administración de proyectos.

De acuerdo con lo mencionado, se explican cada uno de estos:

Reconocimiento del entorno: puede realizarse por medio de herramientas como una matriz de fortalezas, oportunidades, debilidades y amenazas (Matriz FODA).

Pronósticos: tienen carácter cualitativo o cuantitativo, y no son más que predicciones de los resultados que se esperan obtener. Con los pronósticos, las directivas de la organización tienen más herramientas de información para tomar decisiones.

Elaboración de presupuestos: implica asignar recursos y guía proyectos. Impactan alcance, objetivos, tiempos y calidad de resultados, siendo esenciales para la planificación efectiva.

Programación: la técnica de programación organiza actividades con detalles de recursos, tiempos y responsables. Utiliza herramientas como Gráficos de Gantt y diagramas PERT para planificar eficientemente.

Diagrama de Gantt: es una representación gráfica de la planificación y programación de procesos. Monitoriza actividades de un proyecto en un período de tiempo, de forma clara y rápida.

Flujo PERT: (Técnica de Evaluación y Revisión de Programas) es un diagrama que muestra la secuencia y duración de actividades en un proyecto. Ayuda al gerente a identificar dependencias y problemas, permitiendo comparar acciones y costos alternativos."

Administración de proyectos: implica realizar tareas a tiempo, dentro del presupuesto y según las especificaciones. Un equipo coordina actividades y, al cumplir metas, se reorganiza para nuevos proyectos o roles permanentes.

2. 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:

I. **Ciber-resiliencia:** la ciberseguridad brinda a los gobiernos y las organizaciones la ciber-resiliencia como la capacidad para resistir, proteger y defender los sistemas de ciberataques.

II. **Personal y recursos:** para poder apropiar la ciberseguridad en las organizaciones es importante que se cuente con el personal capacitado y los recursos necesarios.

III. **Formación permanente:** apropiar la ciberseguridad en las organizaciones implica mantener la formación y concienciación permanentes, en ciberseguridad, como estrategia para el cumplimiento y mejora continua.

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 analizarán otras técnicas de planificación, teniendo en cuenta las necesidades y el contexto de la organización.

- **Activo de información:** "Es cualquier información o sistema relacionado con el tratamiento de la misma que tenga valor para la organización, pueden ser procesos de negocio, datos, aplicaciones, equipos informáticos, personal, soportes de información, redes, equipamiento auxiliar o instalaciones. Es susceptible de ser atacado deliberada o accidentalmente con consecuencias para la organización “. Incibe (2021).
- **Vulnerabilidad y amenaza:** la vulnerabilidad es una "Debilidad o fallo de un sistema que puede ser aprovechado con fines maliciosos “. La amenaza, es aquella "Circunstancia desfavorable que puede ocurrir y que cuando

sucede tiene consecuencias negativas sobre los activos provocando su indisponibilidad, funcionamiento incorrecto o pérdida de valor. Si una amenaza acontece, a la vez que existe una vulnerabilidad aprovechando su existencia, puede derivar en un incidente de seguridad." Incibe (2021).

- **Amenaza avanzada persistente (APT):** "También conocido como APT, acrónimo en inglés de “Advanced Persistent Threat”, consiste en un tipo de ataque informático que se caracteriza por realizarse con sigilo, permaneciendo activo y oculto durante mucho tiempo, utilizando diferentes formas de ataque. Suelen estar patrocinados por compañías, mafias o un estado “. Incibe (2021).
- **Ciberataque:** "Intento deliberado de un ciberdelincuente de obtener acceso a un sistema informático sin autorización, sirviéndose de diferentes técnicas y vulnerabilidades para la realización de actividades con fines maliciosos, como el robo de información, extorsión del propietario o simplemente daños al sistema." Incibe (2021).
- **Ciberdelincuente:** "Persona que realiza actividades delictivas en la red contra personas o sistemas informáticos, pudiendo provocar daños económicos o reputacionales mediante robo, filtrado de información, deterioro de “software” o “hardware”, fraude y extorsión. Casi siempre están orientados a la obtención de fines económicos." Incibe (2021).
- **“Malware”:** "Es un tipo de “software” que tiene como objetivo dañar o infiltrarse sin el consentimiento de su propietario en un sistema de información. Palabra que nace de la unión de los términos en inglés de “software” malintencionado: “malicious software”. Dentro de esta definición tiene cabida un amplio elenco de programas maliciosos: virus,

gusanos, troyanos," backdoors", "spyware", etc. La nota común a todos estos programas es su carácter dañino o lesivo." Incibe (2021).

- **Phishing:** "Técnica o tipo de ataque en el que alguien suplanta a una entidad/servicio mediante un correo electrónico o mensaje instantáneo para conseguir las credenciales o información de la tarjeta de crédito de un usuario. Ese correo/mensaje suele tener un enlace (o fichero que contiene ese enlace) a un sitio web que suplanta al legítimo y que usan para engañarlo." Incibe (2021).

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

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.).

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 reconocer los aspectos en los que se enfoca el entrenamiento, en el marco de la aplicación de estrategias de ciberseguridad:

- **Gestión:** busca mejorar las habilidades y conocimientos para la gestión de la ciberseguridad por medio del entrenamiento en la adopción de estándares y marcos de referencia de ciberseguridad. Se enfoca en fortalecer el liderazgo de la ciberseguridad.
- **Operativo:** fortalecimiento de los conocimientos teórico-prácticos con un enfoque técnico que permita mejorar el desempeño operativo de herramientas, "software" o "hardware", pudiendo mejorar las configuraciones para el rendimiento y eficacia de las mismas. En este sentido, el entrenamiento operativo permite conocer las mejores prácticas técnicas para aplicar controles de ciberseguridad.
- **Usuarios:** así mismo, el entrenamiento operativo puede estar enfocado a los usuarios para que tengan el conocimiento práctico y las habilidades para detectar y reportar posibles vulnerabilidades, eventos e incidentes de seguridad digital.
- **Entes facilitadores:** el entrenamiento puede darse por medio de terceros especializados en la materia y con la acreditación respectiva, tales como instituciones de educación superior profesional, tecnológica y técnica, institutos de educación no formal y profesionales capacitados y certificados.

- **Forma o modalidad:** el entrenamiento puede realizarse en forma de cursos, certificaciones, talleres, asesorías y consultorías.

El entrenamiento en ciberseguridad es importante que se desarrolle previamente, durante y después de la aplicación de estrategias de ciberseguridad según las necesidades.

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.

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:

- **Grupo 1.** 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.
  Sobre los dueños del negocio, importa reconocer que hay:
  - **Principales implicados:** son el primer grupo de interés para concienciar en la importancia de la ciberseguridad.

- ✓ **Con facultad de decisión:** considerando su autoridad para aprobar los recursos esenciales, tienen la capacidad de respaldar la implementación efectiva de estrategias de seguridad digital.
- ✓ **Apoyo fundamental:** juegan un papel crucial como soporte fundamental para implementar políticas de ciberseguridad y asegurar su cumplimiento en toda la organización.

❖ **Grupo 2**. Los 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.

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.

Los operadores técnicos, por principio, han de ser los agentes de la organización más comprometidos con la formación y concienciación permanente en pro de la ciberseguridad.

❖ **Grupo 3.** Los usuarios de los sistemas de información: 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.

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:

a. **Asesoría o consultoría:** 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.

b. **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).
c. **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.
d. **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.
e. **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.
f. 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.

g. **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 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. Es importante explorar la información que se presenta a continuación, así se podrá asimilar de mejor forma los aspectos más relevantes de la defensa en profundidad en capas.

A. **Descubrimiento y gestión de activos:** "Identificar los dispositivos y activos (incluyendo los datos) que deben ser protegidos y monitorearlos. No es posible proteger un activo si no se conoce su existencia, por ello es indispensable tener visibilidad de todos los activos que pertenecen a la organización y que tienen acceso a los recursos de esta. Esto ayudará a identificar la superficie de ataque que se debe proteger y cómo se debe proteger." Raggi (2021).

B. **Protocolo y servicios:** en la apropiación de la tecnología se debe aplicar protocolos y servicios seguros tales como SSL/TLS, HTTPS, SSH, SFTP, DoH/DNSSEC, SMTP, POP3, entre otros.

C. **Sistemas de correlación de eventos o "Logs, Security Information and Event Management" – SIEM:** son herramientas o soluciones que se enfocan en gestionar los eventos, con capacidades para detectar de manera centralizada los logs o registros de los diversos dispositivos en la red, esto ayuda a responder y neutralizar ciberamenazas. También permite tener una visión global de la seguridad de las tecnologías.

D. "**Firewalls**": los cortafuegos son dispositivos de "software" o "hardware" que controlan el tráfico de la red a través del acceso o niegan políticas o reglas. Estas reglas incluyen direcciones IP, direcciones MAC y puertos negros o de listas blancas. También hay firewalls específicos de aplicaciones, como firewalls de aplicaciones web (WAF) y pasarelas de correo electrónico seguras que se enfocan en detectar actividad maliciosa, dirigida a una aplicación en particular.

E. **Sistemas IDS/IPS:** sistemas de detección o prevención de intrusiones (IDS / IPS), un IDS envía una alerta cuando se detecta tráfico de red malicioso, mientras que un IPS intenta prevenir y alertar sobre la actividad maliciosa identificada en la red o en la estación de trabajo de un usuario. Estas soluciones basan el reconocimiento de ataques en firmas de actividad de red maliciosa conocida.

F. "**Endpoint Detection and Response" – EDR:** el "software" o los agentes de EDR residen en el sistema cliente (por ejemplo, la computadora portátil o el teléfono móvil de un usuario) y brindan protección antivirus,

alertas, detección, análisis, clasificación de amenazas e inteligencia de amenazas. Estas soluciones se ejecutan en conjuntos de reglas, es decir, firmas o reglas de firewall o heurísticas, es decir, detección de comportamientos anómalos o maliciosos.

G. **Segmentación de Red:** es la práctica de dividir una red en múltiples subredes diseñadas en torno a las necesidades comerciales. Por ejemplo, esto a menudo incluye tener subredes para ejecutivos, finanzas, operaciones y recursos humanos. Dependiendo del nivel de seguridad requerido, es posible que estas redes no puedan comunicarse directamente. La segmentación, a menudo, se logra mediante el uso de conmutadores de red o reglas de "firewall".

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:

- **Principio de mínimo privilegio:** se requieren políticas y controles técnicos para asignar solo a los usuarios, sistemas y procesos de acceso a los recursos (redes, sistemas y archivos) que son absolutamente necesarios para realizar su función asignada.
- **Contraseñas seguras:** son un mecanismo de autenticación fundamental en la seguridad de la información. La guía moderna de contraseñas implica el uso de la autenticación multifactor para cualquier cuenta de valor, el uso de una frase con varias palabras y la no reutilización de contraseñas.
- **Gestión de parches o "Patch Management":** es el proceso de aplicar actualizaciones a un sistema operativo, "software", "hardware" o

complemento. A menudo, estos parches abordan las vulnerabilidades identificadas que podrían permitir a los CTA el acceso no autorizado a los sistemas o redes de información. CIS (2021).

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).

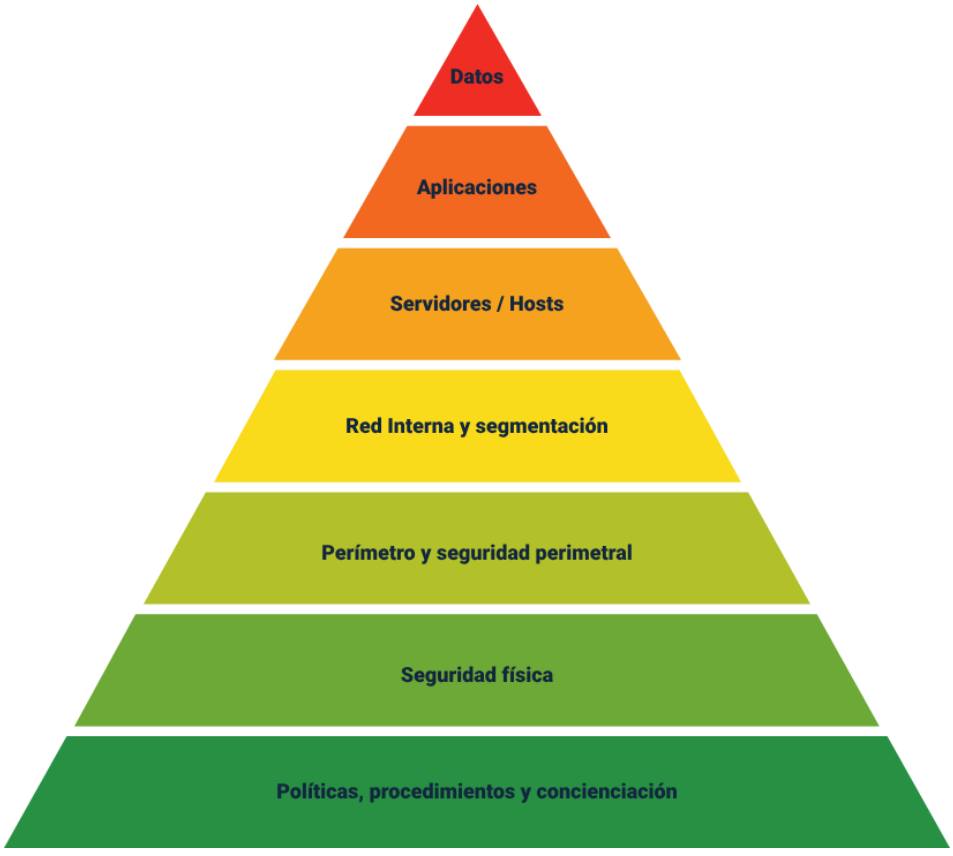
Esta representación tiene las siguientes capas:

- **Directivas y procedimientos**: programas de aprendizaje para los usuarios.
- **Seguridad física:** guardias de seguridad, bloqueos, dispositivos de seguimiento.
- **Perímetro:** servidores de seguridad, sistemas de cuarentena de VPN.
- **Red de internet:** Segmentos de red, IPSec, NIDS.

- **“HOST”:** refuerzo del sistema operativo, administración de revisiones, autenticación, HIDS.
- **Aplicación:** refuerzo de aplicaciones, antivirus.
- **Datos:** ACL, cifrado.

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.



1) **Políticas, procedimientos y concienciación:** en esta capa, se establecen pautas para la gestión, operación y concienciación de la ciberseguridad, incluyendo seguridad física, control de acceso, gestión de redes y cumplimiento legal, entre otros aspectos clave de la seguridad digital.
2) **Seguridad física:** la seguridad física es crucial en la estrategia de ciberseguridad para proteger las instalaciones de sistemas informáticos contra riesgos como robo, ocupación enemiga y denegación de servicios. También implica preparación ante desastres naturales y ataques terroristas, asegurando una respuesta efectiva y protegiendo los activos digitales.
3) **Perímetro y Seguridad perimetral:** el perímetro representa el límite digital de la red corporativa y la internet. Implementar dispositivos de ciberseguridad en este borde es esencial para controlar y asegurar la red. Aunque también se refiere al límite físico, este aspecto se aborda en la capa de seguridad física.
4) **Red Interna y segmentación:** la seguridad de la red corporativa implica una estructura segmentada que incluye redes de servidores, comunicaciones, bases de datos y usuarios. Estos segmentos pueden dividirse por niveles, áreas o pisos. La interconexión se controla mediante firewalls y servicios de seguridad como IDS/IPS y Antimalware para garantizar una composición segura.
5) **Servidores / Hosts:** esta capa protege servidores según la importancia de los datos que manejan, empleando buenas prácticas y políticas de acceso para minimizar riesgos. El "Hardening" o endurecimiento, una técnica clave, implica la aplicación cuidadosa de prácticas para personalizar

servidores, considerando “hardware” y “software”, fortaleciendo así su seguridad.

6) **Aplicaciones:** son vitales en las operaciones empresariales y deben protegerse para garantizar confidencialidad, integridad y disponibilidad. La ciberseguridad en esta capa requiere esfuerzos tanto en el desarrollo como en la operación. Es crucial integrar la ciberseguridad de forma transversal en el proceso de desarrollo de “software” interno.
7) **Datos, usuarios y equipos:** la seguridad de usuarios y equipos es crítica, ya que son vulnerables a ataques de ingeniería social y “malware”. Se requiere una combinación de controles técnicos y capacitación para proteger los datos y los equipos, considerando clasificación, almacenamiento y cifrado. Medidas como antimalware, “Data Loss Prevention” - DLP, cifrado y gestión de comunicaciones son esenciales.

La defensa en profundidad debe ser aplicada considerando las codependencias entre dispositivos, servicios y elementos de una red.

Los datos almacenados en equipos y manipulados por los usuarios deben recibir protección adecuada, considerando la clasificación, almacenado y etiquetado de la información.

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.

- **“Frameworks”:** La apropiación de controles de ciberseguridad para la defensa en profundidad puede apalancarse en estándares, marcos de referencia o “frameworks”.
- **Capas o barreras de seguridad:** dificultar el avance del agresor, si una barrera falla entonces debe entrar una segunda barrera de protección, y así en la medida de lo posible dentro del contexto, de esta forma se aplica el concepto de defensa en profundidad.
- **Monitoreo, detección y respuesta:** se debe aplicar en todos los controles de defensa y servicios de red, con el fin de detectar eventos extraños y responder ante posibles ciberataques. Se pueden implementar controles o hacer uso de las funcionalidades de las tecnologías de la red corporativa.
- **Aislamiento:** cuando las ciberamenazas avancen, rompiendo la seguridad de las capas de protección, en cualquiera de las capas se pueden aplicar aislamientos parciales o totales según sea necesario, para contener la amenaza. Esto podría indisponer algunas aplicaciones y servicios para algunos o todos los usuarios, pero ayuda a mantener la integridad y la privacidad de la información. Por otra parte, los aislamientos pueden ayudar a reencaminar la amenaza en un lugar de cuarentena controlado.
- **Comunicación:** La comunicación es un elemento clave para informar sobre el estado de la ciberseguridad en cada fase o capa de la defensa. Así, los equipos y responsables de la infraestructura y controles de la red podrán

tomar acciones respectivas de defensa y respuesta a posibles ataques de ciberseguridad.

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.

Material complementario

Tema	Referencia	Tipo de material	Enlace del recurso
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.	Documento en línea	http://polux.unipiloto.edu.co:8080/00002061.pdf

Glosario

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.

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.

Créditos

Nombre	Cargo	Regional y Centro de Formación
Claudia Patricia Aristizábal	Líder del equipo	Dirección General
Liliana Victoria Morales Gualdrón	Responsable de línea de producción	Regional Distrito Capital -Centro de Gestión de Mercados, Logística y Tecnologías de la Información
Rafael Neftalí Lizcano Reyes	Asesoría metodológica y pedagógica	Regional Santander -Centro Industrial del Diseño y la Manufactura
Joaquín Patiño Cerón	Experto Temático	Regional Cauca -Centro de Teleinformática y Producción Industrial
Fabián Leonardo Correa Díaz	Diseñador Instruccional	Regional Tolima -Centro agropecuario La Granja-
Andrés Felipe Velandia Espitia	Revisor Metodológico y Pedagógico	Regional Distrito Capital -Centro de Diseño y Metrología
Gloria Lida Alzate Suarez	Adecuación instruccional	Regional Distrito Capital - Centro de gestión de mercados, Logística y Tecnologías de la información
Alix Cecilia Chinchilla Rueda	Metodología para la formación virtual	Regional Distrito Capital - Centro de gestión de mercados, Logística y Tecnologías de la información
Yuly Andrea Rey Quiñonez	Diseño web	Regional Distrito Capital - Centro de gestión de mercados, Logística y Tecnologías de la información
Luis Jesús Pérez Madariaga	Desarrollo Fullstack	Regional Distrito Capital - Centro de gestión de mercados, Logística y Tecnologías de la información

Nombre	Cargo	Regional y Centro de Formación
Ernesto Navarro Jaimes	Animación y Producción audiovisual	Regional Distrito Capital - Centro de gestión de mercados, Logística y Tecnologías de la información
Lady Adriana Ariza Luque	Animación y Producción audiovisual	Regional Distrito Capital - Centro de gestión de mercados, Logística y Tecnologías de la información
Laura Gisselle Murcia Pardo	Animación y Producción audiovisual	Regional Distrito Capital - Centro de gestión de mercados, Logística y Tecnologías de la información
Yuly Andrea Rey Quiñonez	Diseño web	Regional Distrito Capital - Centro de gestión de mercados, Logística y Tecnologías de la información
Carolina Coca Salazar	Evaluación de contenidos inclusivos y accesibles	Regional Distrito Capital - Centro de gestión de mercados, Logística y Tecnologías de la información
Lina Marcela Pérez Manchego	Validación de recursos educativos digitales	Regional Distrito Capital - Centro de gestión de mercados, Logística y Tecnologías de la información
Leyson Fabián Castaño Pérez	Validación de recursos educativos digitales y vinculación LMS	Regional Distrito Capital - Centro de gestión de mercados, Logística y Tecnologías de la información