DESARROLLO

WEB FULL STACK

-INTERMEDIO

Autor de contenido

Andrés Fernando Pineda Guerra

EMPEZAR

Tabla de Contenido

Presentación

En el curso de desarrollador Full Stack como componente intermedio, podrán adquirir las habilidades y lenguajes necesarios para el desarrollo web, enfocándose en sus grandes pilares, como lo son Front End, Back End, Diseño y modelamiento de aplicaciones y documentación de código.
El curso trata temas emergentes tales como, la seguridad informática, desarrollo de aplicaciones móviles, gestión de base de datos, todo esto basado en la metodología Scrum. De la misma manera, se hace énfasis en el manejo de proyectos tanto en los módulos de desarrollo como los módulos de gestión de proyectos de TI.

Objetivos del curso (competencias)

Objetivo general

Formar a los participantes en el desarrollo web en todo el ciclo de vida del software, en donde adquieran los conocimientos básicos para implementar soluciones web.

Objetivo específico

- Conocer los conceptos y teoría básica del desarrollo web.

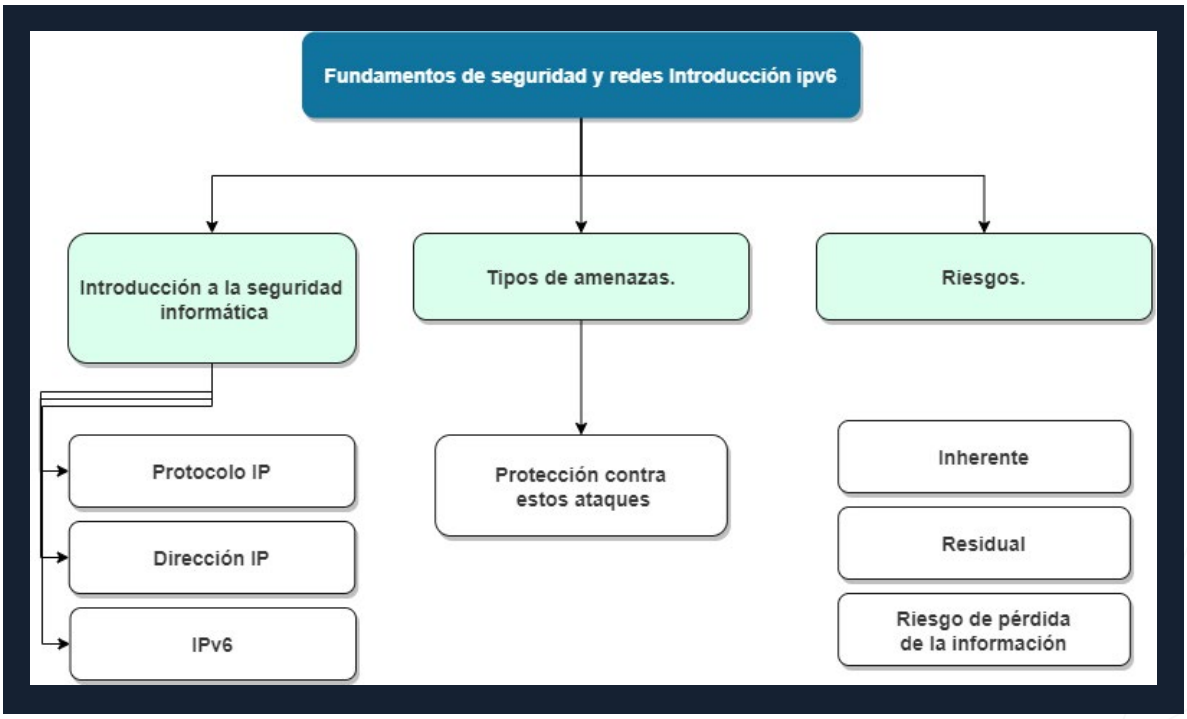
- Identificar y conocer los diferentes lenguajes de programación y herramientas para el desarrollo web.

- Aplicar las diferentes tecnologías web, tendencias y herramientas en el desarrollo de soluciones web enfocadas a proyectos.

- Diseñar, desarrollar e implementar soluciones web básicas en donde se integren los componentes de Front End, Back End, seguridad, redes y buenas prácticas utilizando metodologías ágiles.

- Identificar y conocer los conceptos básicos para el desarrollo móvil, así como aplicar su desarrollo en aplicaciones básicas.

Mapa de contenido de la unidad



Módulo 11

Fundamentos de seguridad y redes Introducción ipv6

Ideas clave

Introducción a la Análitica web, importancia, características, pasos para el análisis de sitios web, principales herramientas para realizar análisis web, métricas y KPI´S.

11.1. Introducción a la seguridad informática

Este capítulo comenzará con un Introducción a los fundamentos de seguridad informática y de redes, también explicará cómo ha evolucionado la seguridad a lo largo de los años.

Redes

Una red de computadoras, también llamada red de ordenadores o red informática es un conjunto de equipos conectados por medio de cables, señales, ondas o cualquier otro método de transporte de datos, que comparten información. Así como, finalidad principal para la creación de una red de ordenadores es compartir los recursos y la información en la distancia, asegurar la confiabilidad y la disponibilidad de la información

Red de área personal Personal Area Network (PAN) compuesta por ordenadores usada para la comunicación entre los dispositivos del Ordenador cerca de una persona.
Red de área local Local Area Network (LAN), se limita a un área especial relativamente pequeña tal como un cuarto, un solo edificio. Las redes de área local a veces se llaman una sola red de localización. No utilizan medios o redes de interconexión públicos.
Red de área metropolitana Metropolitan Area Network (MAN) es una red de alta velocidad (banda ancha) que da cobertura en un área geográfica más extensa que un campus, pero aun así limitado. Por ejemplo, una red que interconecte sedes de universidades de un municipio dentro de la localidad por medio de fibra óptica.

¿Qué es el protocolo IP?

El protocolo de Internet en inglés Internet Protocol es un protocolo de comunicación de datos digitales.

- Uso bidireccional en origen o destino de comunicación para transmitir datos.
- Permite la comunicación de por lo menos dos terminales (host) mediante internet.

¿Qué es una dirección IP?

- Una dirección IP es un número que identifica, de manera lógica y jerárquica, a una Interfaz en red de un dispositivo (computador, Tablet, portátil, entre otros.) que utilice el protocolo IP.

¿Qué es IPv6?

- IPv6 o IP versión 6 es el protocolo de Internet de próxima generación que eventualmente reemplazará el protocolo actual IPv4.
- Es la nueva versión del protocolo de internet (IP).
- Busca ser el sucesor de IPv4.
- Tener en cuenta que IPv4 es de 32 bits, si se pone un bit más se tendría el doble de direcciones, si se ponen dos bits más se tendría 4 veces más direcciones, si pusiéramos 3 bits más habría 8 veces más dado que se maneja en potencias de 2.
- El uso de direcciones IP de 128 tamaño fijo, en su mayoría IPv6 se utilizan 64 bits para la dirección de la interfaz de red y 64 para la red, no como en IPv4 que es variable. (Segmentos de subred de tamaño fijo)
- Mayor seguridad Ipsec (Por defecto). Autenticando y/o cifrando cada paquete IP en un flujo de datos
- No mascaras. Si Prefijos /X

$$IPV4 \qquad IPV6$$

$$2^{32} = 4.294.967.296 \qquad 2^{128} \approx 340,282,366,920,938,000,000,000,000,000,000,000,000$$

¿Por qué Utilizar IPv6?

- Es necesario un nuevo protocolo de capa 3 (L3) con direcciones mayores de 32 bits.
- Internet continúa creciendo
- Población mundial a 07 de enero de 2023: 8.009.751 aproximadamente de millones de personas. (https://countrymeters.info/es/World)
- En el año 2014 existían aproximadamente 2000 millones de usuarios de internet 30% de la población.
- A enero de 2023 existen aproximadamente 5.126 millones de usuarios de internet 64% de la población.
- Crecimiento mayor al 400% en la cantidad de usuarios de internet los últimos 10 años.
- Cantidad de dispositivos móviles (smartphones, Tablet, Smart Watches, videoconsolas portátiles, entre otros) al año 2023 aproximadamente 50.000 millones.
- Cantidad de dispositivos móviles a enero de 2023 aproximadamente 8.095 millones, Internet of Things (IOT)

Riesgos de no Implementar IPv6

- Dificultar el surgimiento de nuevas redes.
- Ralentizar el proceso de inclusión digital o reducir la cantidad de nuevos usuarios.

- Dificultar el surgimiento de nuevas aplicaciones.
- Aumentar la utilización de técnicas como NAT.
- El costo de no implementar IPv6 podrá ser mayor que el de implementarlo.
- Los ISP necesitan innovar y ofrecer nuevos servicios a sus clientes.

Seguridad de la información.

Para empezar a hablar de seguridad de la información, primero debemos preguntarnos y definir qué es la información.
Un mensaje no es más que un conjunto ordenado de datos, con un significado específico, enviado de un remitente a un receptor para transmitir información. Lógicamente, el receptor utiliza esta información contenida en el mensaje para actuar sobre su análisis.

Se debe tener en cuenta que la información son datos ordenados. Si estos datos no tuvieran un orden, no serían información.

Ejemplo: (mojado casa tiene la segundo es y grande el piso). Las anteriores palabras son las mismas que están en la siguiente frase, pero mezcladas. Al disminuir la cantidad y claridad de datos, aumenta lo que conocemos como entropía. La siguiente frase tiene poca entropía, dado que tiene información que es entendible y clara lo que permitirán al receptor de esta información conocer y tomar acciones con base en estos mensajes. (La casa es grande y tiene mojado el segundo piso).

Formas de almacenamiento

La información a lo largo de la historia se ha venido almacenando de diversas formas: De forma física: Anteriormente se escribía en tabletas de arcilla y telas, hasta la invención de papel que sigue siendo unos de los medios del almacenamiento físico más utilizado hasta la actualidad.

A inicios del siglo XIX y hasta la fecha la información se ha almacenado en medios electromagnéticos, inicialmente en discos de acetato o también llamados Long Play, donde se guarda música.

Posteriormente se utilizaron cintas de plástico que contenían partículas de metal magnetizadas las cuales podían guardar la información como música, voz y datos. Incluso aún se utilizan en la actualidad. ¿Recuerda los casetes donde venía la música? Incluso las organizaciones utilizan a menudo cintas para hacer copias de seguridad o Backup de información, dado que pueden alojar gran capacidad.

Seguidamente surgieron los Hard Disk Drive (HDD) o discos duros mecánicos, llamados mecánicos porque un motor hace girar sus platos. Hoy en día, estos dispositivos

son de los más usados en nuestros servidores, equipos de escritorio, consolas de video-juegos y cualquier dispositivo que requiera almacenar datos de forma masiva.

Al poco tiempo, surgieron los CD, los DVD, los Blu-ray, sustitutos de los antiguos Long Play. Estos discos plásticos de pequeño tamaño sirven en nuestro mundo informático para almacenar cantidades de información, desde 750MB en el caso de los CD hasta varios 80GB de información en el caso de algunos DVD y los Blu-ray.

En la actualidad hay dispositivo de almacenamiento rápido como Solid-State Drive (SSD) e español discos de estado solido con velocidades de lectura y escritura superio-res a 550 MB/s.

La forma de almacenar información como archivos de texto, imágenes, video, audio, entre otros depende de los diversos formatos como: docx, txt, jpg, bmp, mp4, avi, mp3 o awa

Nota:

MB (Megabytes) Unidad que equivale a 1.024 Kilobytes

GB (Gigabyte) Unidad que equivale a 1.024 Megabytes

Interesante: Lo más valioso para una organización es la información que almacena. Sin la información una organización no tendría sentido de ser pues no se aportaría nada nuevo a una nueva sociedad.

¡Seguridad de la información!

Se puede definir como un conjunto de medidas que deben de tomarse para salvaguar-dar, proteger la información para evitar que pueda ser sustraída, obtenida y/o adultera-da por terceros no autorizados, ya sea mientras esté almacenada o cuando esté siendo transmitida.

Lo anterior, se basa enlos principios básicos de la seguridad informática, tríada CIA por sus iniciales de sus componentes.

Confidentiality (confidencialidad)

Este principio implica que la información se mantenga privada, que no sea expuesta a terceros no autorizados en ella. Dicho de otra forma: la clave de una tarjeta bancaria solamente debe ser conocido por el propietario. Cualquier tercero (otra persona dife-rente es un atacante) que acceda a esta información estará violando el principio de confidencialidad.

Cuando la información es almacenada o trasferida se debe tener en cuenta para prevenir sustracción o robo.

- Cifrado para ocultar la información de quien no tenga las claves de acceso; de la misma forma se deben trabajar los respaldos.
- Cifrado de la comunicación en tránsito como las VPN o los certificados SSL/TLS.
- Cifrado de dispositivos de almacenamiento.
- Uso de solicitud de usuario y clave para acceder a la información.

Integrity (integridad)

La integridad implica garantizar que la información no pueda ser adulterada o modificada por un tercero no autorizado, por ejemplo, si alguien no autorizado entra al sistema de nómina de una organización y logra modificar los valores a girar en una cuenta para hacer que aparezca un valor superior al que debía tener esta cuenta.

Se sugiere que la información almacenada o trasmitida debe contar con mecanismos o herramientas para verificar que no haya sido adulterada.

Availability (disponibilidad)

Es importante que la información pueda ser consultada por los interesados cada vez que se requieran, dado a que muchas veces se concentran esfuerzos a garantizar que la información no sea adulterada (integridad) o que no se filtre (confidencialidad) y se descuidan los aspectos que implica que la información no esté disponible.
De igual manera se debe tener en cuenta para garantizar disponibilidad de la información.

- Sistemas de almacenamiento de alta disponibilidad, redundancia energética, de comunicación y en almacenamiento.

No menos importante es la autenticidad de la información, la cual consiste en que se pueda verificar que la información viene de quien dice ser su emisor, la cual tiene relación directa con la integridad de la información.

Por último, el NO repudio consiste en garantizar que quien haya participado en una comunicación no pueda posteriormente indicar que no lo hizo. Ejemplo, un usuario retira dinero de un cajero automático, y reporta que el no es quien realiza el proceso; sin embargo, queda en registro fotográfico, evidencia que la entidad bancaria presenta al usuario.

Seguridad física

La seguridad física es uno de los aspectos menos se le presta atención por algunas organizaciones y se le da importancia cuando las amenazas se ha materializado.

Es importante adoptar medidas que permitan mitigar o eliminar eventos que afecten la información de una organización y que evita que esta pueda ser sustraída, dañada, modificada, copiada, entre otras.

Los componentes de la seguridad física frente algunos eventos naturales.

- · Cualquier organización pueda estar expuesta como incendios, para este escenario se debe contar con medidas de protección ante incendios (detectores de humo y alarmas, extintores, sistemas contra incendios).
- Inundación, garantizar que la ubicación de espacios informáticos estén en lugares donde el agua no tenga facilidad de acceso, para ello se debe mantener un deshumidificador para evitar que la humedad del ambiente, instalar sensor de agua a nivel del suelo, de forma tal que advierta de una inundación.
- Terremoto, procurar que los espacios como datacenter sean construidos en zonas geológicas de poca probabilidad de riesgo sísmico, al igual la infraestructura física debe cumplir con toda la normatividad antisísmica.
- Plagas de insectos, los insectos a una computadora es un peligro, pueden llegar a ocasionar cortos eléctricos y provocar incendios, para ello contar con redes antiinsectos en las puertas, control de temperatura, los insectos no suelen permanecer en ambientes fríos, por lo que espacios relativamente fríos.
- Descargas eléctricas, los rayos son descargas eléctricas uno peligros en el mundo de la informática, para evitar estos riesgos se debe utilizar cortapicos evitando subidas de tención, instalar un sistema apropiado de puesta a tierra del equipamiento, así como pararrayos. Preferiblemente que la comunicación sea óptica y no electromagnética.

Los componentes de la seguridad física frente algunos eventos no naturales.

- Acceso a sitios, debe estar asegurada contra intrusos y eventos que puedan alterar el normal funcionamiento de los sistemas, disponer con personal de vigilancia, para el acceso a escenarios tecnológicos sea a través de credenciales, tarjetas RFID, biométricas, ópticas, contar con sistemas de cámaras de vigilancia
- Redundancia, la mayoría de los ataques apuntan a la interrupción de los sistemas, energéticos y de conectividad, se debe procurar tener sistemas de redundancia energética como UPS, plantas eléctricas, energía alternativa fotovoltaica, eólica o hídrica, a en redundancia en equipamiento de red.

Lo anteriormente, apunta a tener redundancia en diferentes aspectos, entre ellos el de almacenamiento, con la posibilidad que discos duros suelen fallar y, en este caso, lo menos deseable es que la información se pierda irremediablemente. Para ello se puede usar una tecnología conocida como RAID, sigla de Redundant Array of Inexpensive Disks.

Los siguientes RAID son los más comunes, se verán de manera general.

RAID	Requerimientos	Descripción	Ventajas/Desventajas
0	Se requieren al menos dos discos duros. ()	Se unifican dos discos y lograr un disco con la suma del espacio de ambos. La información no se duplica, sino que se va escribiendo en estos discos como si fueran uno solo: se llena uno y se continúa con el otro hasta que se llene. Es importante mencionar para que no sea utilizado pensando que sirve como redundancia	**Ventajas** No implica una ventaja para asegurar la disponibilidad de la información. **Desventajas** Este tipo de raid en realidad no implica redundancia.
1	Al menos dos discos para este tipo de RAID. Estos discos deben ser idénticos	Dos discos: el 1 y el 2. Al escribirse un byte hacia el disco 1, en RAID 1 la misma información se escribirá inmediatamente hacia el disco 2. Lo mismo ocurrirá al modificarse una información en 1: se modificará de la misma forma en 2 y al eliminarse una información de 1, se eliminará de 2.	**Ventajas** Aumenta el espacio de almacenamiento: se cuenta con cuatro (1, 2, 3 y 4) y se con un espacio de almacenamiento de la suma de dos discos (por ejemplo, 1 y 2). Hay redundancia. Si se dañara un elemento, los otros continuarían almacenando la información en forma degradada. **Desventajas** El costo. No es lo mismo un RAID 1, que tiene dos elementos que un RAID 1+0, que requiere cuatro.

1+0	Al menos cuatro discos, del mismo tamaño si fuera posible.	De los cuatro discos (1, 2, 3 y 4) se toman dos (1 y 2) y se configuraren en RAID 0. Los otros dos (3 y 4), también, de la misma forma, en RAID 0	**Ventajas** Aumenta el espacio de almacenamiento: se cuenta con cuatro (1, 2, 3 y 4) y se con un espacio de almacenamiento de la suma de dos discos (por ejemplo, 1 y 2). Hay redundancia. Si se dañara un elemento, los otros continuarían almacenando la información en forma degradada. **Desventajas** El costo. No es lo mismo un RAID 1, que tiene dos elementos que un RAID 1+0, que requiere cuatro.

11.2. Tipos de amenazas.

Las amenazas se pueden catalogar como un escenario de incidente de latente riesgo frente a posibles vulnerabilidades que usa un atacante y que puede dañar y/o afectar en usuarios, ecosistemas informáticos de manera interna o externa.

Para ello se utilizan diversas técnicas como de ingeniería social que aprovechan vulnerabilidades. mala o poca preparación de los usuarios para detectar intentos de robo de información, esto se da por sistemas desactualizados que permiten la ejecución de programa maligno (malware) en ellos para beneficio de los atacantes, uso de credenciales débiles con cortas de longitud, poca seguridad como “123456”, sin alternar caracteres mayúsculos, minúsculos y especiales como “ads4As46a*/+SAD”

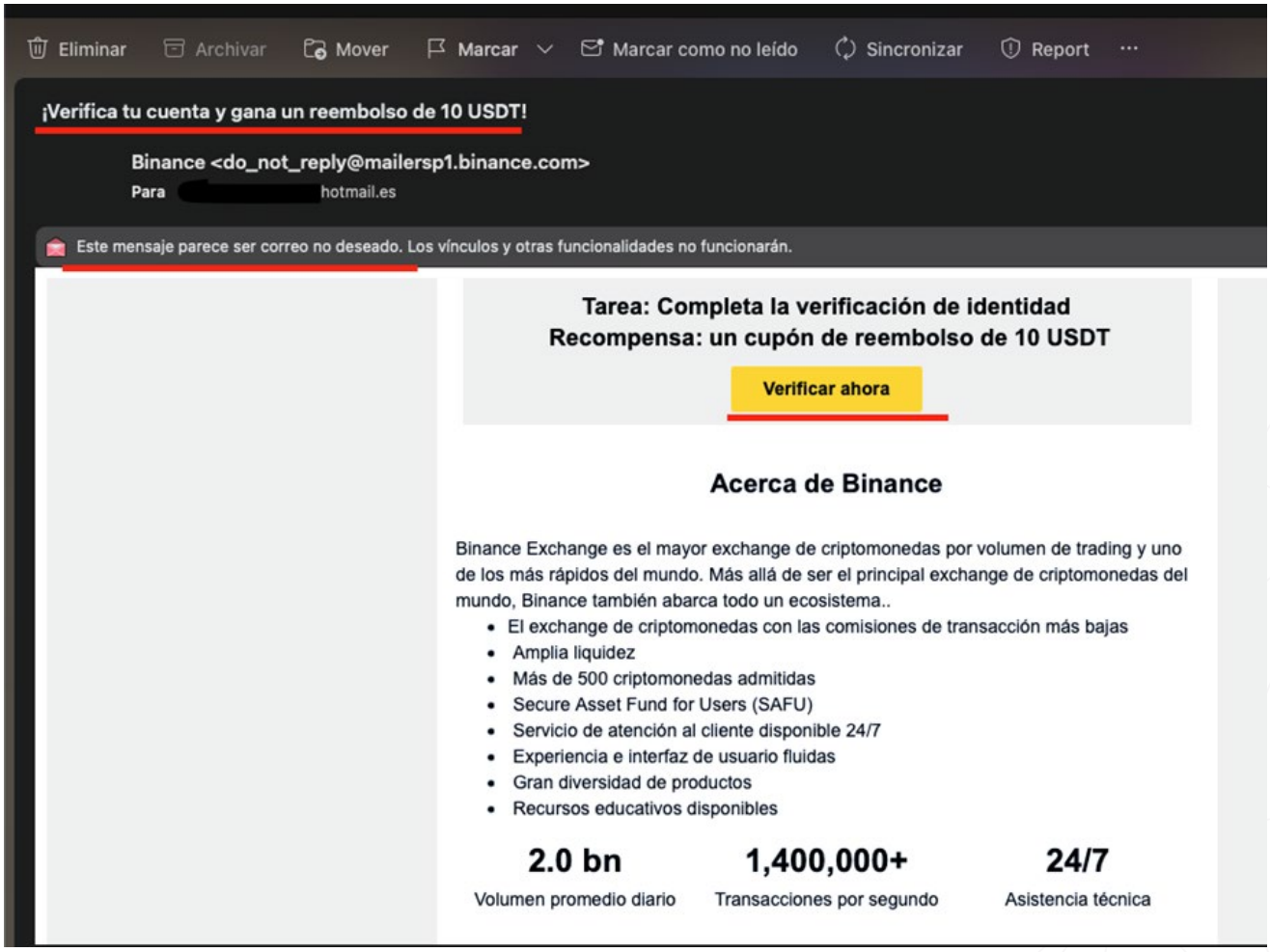
El malware y la forma en que se distribuye hacia los usuarios o victimas ha cambiado con el tiempo y han aparecido nuevos dispositivos y nuevas herramientas para que los atacantes logren instalar estos programas maliciosos, muchas veces los virus se propagaban cuando un usuario son convencidos de bajar un programa pirata a su computador o de hacer doble clic en link, sobre fotos privadas de una personalidad pública. A

continuación, se explica someramente cómo.

- Durante los ochenta y hasta inicio de los años noventa los programas maliciosos se introducían en los equipos a través de dispositivos de almacenamiento contaminados: disquetes y CD.
- A inicios del año 2000 el malware comienza a propagarse por correo electrónico.
- Se empiezan a usarse nuevos dispositivos de almacenamiento para la propagación, como dispositivos de estado sólido (flash, memorias SD, etc.)
- En la actualidad, el phishing ya es algo de todos los días, busca encontrar claves de sistemas que estén almacenadas en la nube o en sitios sociales.
- El malware cuyo objetivo busca convencer a los usuarios de hacer clic en enlaces para que abran formatos pdf, png o doc, entre otros. Al abrirlos se ejecuta el código malicioso que esconden.
- Seguidamente, producto de esto ha surgido una variante llamada ransomware que cifra todos los archivos importantes de un equipo y solicita dinero a cambio de entregar la clave para descifrar los archivos, en pocas palabras un secuertro de onformación.
- El malware ya no solamente alcanza al usuario en sus equipos locales, sino que busca ser ejecutado desde sitios web aprovechando recursos de la máquina del usuario cuando entra a este sitio web.

El concepto de phishing parece venir de password harvesting fishing (recolección y pesca de llaves) y la técnica consiste en convencer al usuario de que debe brindar su usuario y clave por alguna

razón imperiosa y luego hacerse pasar por alguien con poder, como el administrador de la red, de forma de que el usuario entregue sus datos. Siempre se debe estar alertas sobre la información que les llega, hay que dudar, verificar de el remitente de quien proviene y no hacer clic en cualquier enlace que llega por muy legítimo que parezca, como se puede ver en la sigueinte imagen.



Como se evidencia el sistema de correo indica que este es mensaje parece ser un correo no deseando, primer indicio para sospechar, tambien el remitiente es un correo extenso y poco conocido, por último ofrece un premio o bolsa de dinero con un enlace, muchas de estas solicitudes son imperiosas, ya que indican que si el usuario no hace clic, se le suspenderá el servicio, al igualmentente entre otras cuentan con faltas ortograficas en la el texto del mensaje o asunto.

Las redes sociales tambien se han convertido en un potencial problema para la privacidad de los usuarios. Muchas personas crean cuentas en redes sociales y ofrecen información sobre sí mismas de forma bastante inocente.

Un caso particular fue el escándalo de Cambridge Analytica, el cual se creó una aplicación que permitía determinar ciertos parámetros psicológicos sobre los usuarios que la usaban, pero la aplicación solicitaba más información sobre los usuarios que no era necesaria, incluso información sobre los terceros de los usuarios que ejecutaban el

software. recopilando muchísima información sobre millones de usuarios, que luego fue utilizada para conocer sus perfiles con intenciones de influir en diversas elecciones presidenciales de lo Estados Unidos. Aclarando que sin que el usuario lo supiera de la extracción de la información.

El ransomware es una forma de monetizar las actividades maliciosas, que ya no buscan solamente hacer daño del usuario que haya sido contaminado por él.

Envío de spam es muy usual en el mundo, hay miles de máquinas contaminadas alrededor del mundo es muy difícil de bloquear por la propagación tan fácil y masiva.

Ataques de denegación de servicio distribuido (DDoS): consiste en atacar una red con una o varios equipos contaminados afectando su funcionamiento. Estas máquinas pueden ocuparse de reclutar nuevos equipos en su red o en Internet aprovechando fallas conocidas.

Protección contra estos ataques

Las actualizaciones: no deben evadir, se sugiere que sean obligatorias, ya que los sistemas deben ser actualizados frecuentemente. Los atacantes utilizan fallas de seguridad en sistemas operativos y aplicaciones para lograr sus objetivos. Si se los mantiene actualizados, se habrán eliminado al menos las fallas de seguridad ya conocidas y públicas.

Claves fuertes: muchos dispositivos de Internet de las Cosas en inglés (IOT) siguen teniendo claves sencillas, no robustas simples de adivinar, tener claves fuertes, robustas es una de las mejores protecciones y que los atacantes aprovechan las claves débiles para entrar a los sistemas. Este es un problema que persiste la cual depende de la siguiente.

Educación al usuario: no se debe y bajo ningún concepto se debe ofrecer información que no sea necesaria o compartir con un tercero información confidencial, pues esta puede prestarse para diversos tipos de ataques, virtuales o físicos, esto se fortalece con capacitaciones frecuentes al talento humano de las organizaciones, es cultura de seguridad organizacional. Se sugiere que las compañías tengan un plan de seguridad de la información donde se plasmen políticas y controles para el acceso a ecosistemas digitales.

11.3. Riesgos.

Se puede definir en un enfoque tecnológico, como la posibilidad de que ocurra un acontecimiento que tenga impacto en el alcance de los objetivos. El riesgo se mide en términos de impacto y probabilidad. Por otro lado, peligro es la potencialidad de ocurrencia de un daño, pérdida de información.

- **Inherente:** es aquel que está directamente relacionado con la naturaleza de los procesos desarrollados, en ausencia de controles.

- **Residual** es el riesgo subsistente una vez aplicados los controles.

Riesgo residual = Riesgo inherente – Control
Generalmente los riesgos tienes la siguiente estructura:
Riesgo de….. debido a….. causando….
Ejemplo.

Riesgo de pérdida de la información debido a la falta de ética por parte del personal de la organización causando afectación reputacional a la organización.
Un control se puede definir como una medida que se tome para gestionar, mitigar los riesgos y aumentar la probabilidad de alcanzar los objetivos y metas establecidos.

Análisis de riesgos

- Involucra prestar consideración a las fuentes de riesgos, sus consecuencias y las probabilidades de que puedan ocurrir esas consecuencias.
- Implica determinar fuentes del riesgo, posibilidad, consecuencias, responsables, acciones.
- Se deben identificar los controles o acciones que ayuden a minimizarlos.
- Cualitativos. Utiliza formatos de palabras o escalas descriptivas para describir la magnitud de las consecuencias potenciales y la probabilidad de que esas consecuencias ocurran.
- Semicuantitativos. El número asignado a cada descripción no tiene que guardar una relación precisa con la magnitud real de las consecuencias o probabilidades.
- Cuantitativos. Uso de datos numéricos para la determinación de los riesgos.

Evaluar riesgos

- La evaluación de riesgos involucra comparar el nivel de riesgo detectado durante el proceso de análisis con criterios de riesgo establecidos previamente.

· El propósito es tomar decisiones basadas en los resultados del análisis de riesgos para su tratamiento y priorización.

IMPACTO						
	Catastrófico	Moderado	Alto	Alto	Extremo	Extremo
	Mayor	Moderado	Moderado	Alto	Extremo	Extremo
	Moderado	Bajo	Moderado	Alto	Alto	Alto
	Menor	Bajo	Moderado	Moderado	Moderado	Alto
	Insignificante	Bajo	Bajo	Bajo	Moderado	Moderado
		Rara vez	Ocasional	Poco frecuente	Frecuente	Muy frecuente
		FRECUENCIA				

Figura. 4 matriz de impacto y frecuencia de riesgos

Probabilidad de ocurrencia. Factores de posible combinación de que un evento ocurra y genere consecuencias frente a una amenaza y/o vulnerabilidad, (Probable, posible, poco probable)
Impacto. Conjunto de consecuencias que se da por la materialización de un riesgo (Catastrófico, moderado, leve).
Véase mejor en las siguientes tablas.

Probabilidad de ocurrencia	**Nivel (Cualitativo)**	**Clasificación (Cuantitativo)**
0-50	Improbable	1
51-70	Posible	2
71-100	Probable	3

Impacto	Nivel (Cualitativo)	Clasificación (Cuantitativo)
0-50	Leve	10
51-70	Moderado	20
71-100	Catastrófico	30

Tratar los riesgos

- Los riesgos involucran identificar el rango de opciones para tratar los riesgos, evaluar esas opciones, preparar planes para tratamiento de los riesgos e implementarlos con el talento humano de las organizaciones.

- Evaluar las opciones para tratar los riesgos con herramientas como matrices FODA, diagramas de flujo de procesos, inventarios de riesgos, entrevistas cuestionarios y lluvias de ideas entre otras.

- Diseñar e implementar un plan de gestión de riesgos en la organización.

Tratamiento de riesgos	
Evitar el riesgo Ejemplo: no tener controles de acceso biométrico en un escenario tecnológico. **Aceptar el riesgo** Evaluar el riesgo según los niveles de tolerancia en el plan de gestión de riesgos	**Combatir el riesgo** Comprar dispositivos de acceso biométricos para el escenario tecnológico. **Mitigar el riesgo** Asegurar la información del escenario tecnológico y generar capacitaciones al talento humano sobre riesgos de acceso no deseado

Otros materiales para profundizar

Recursos de video

NASeros (Director). (2020, mayo 15). Qué es IPv6. Curso de redes desde 0 | Cap 3 |. https://www.youtube.com/watch?v=LQf1azzcG7s

Referencias bibliográficas de la unidad

Key performance indicators for measuring construction success | Emerald Insight. (s. f.). Recuperado 3 de enero de 2023, de https://www.emerald.com/insight/content/doi/10.1108/14635770410532624/full/html?src=recsys&fullSc=1&fullSc=1&fullSc=1&mbSc=1&fullSc=1&fullSc=1

Lntriago, V. A., Fernández, L. A., & Gamboa, A. C. (2016). Análisis de la estrategia de marketing digital mediante herramientas de analítica web. INVESTIGATIO, 7, Art. 7. https://doi.org/10.31095/irr.v0i7.41

Martínez, M. M. (2010). Analítica Web para empresas: Arte, ingenio y anticipación. Editorial UOC.

ALCALDÍA MAYOR
DE BOGOTÁ D.C.
SECRETARÍA DE EDUCACIÓN

ATENEA
AGENCIA DISTRITAL PARA LA EDUCACIÓN
SUPERIOR LA CIENCIA Y LA TECNOLOGÍA

BOGOTÁ

UNIVERSIDAD DISTRITAL
FRANCISCO JOSÉ DE CALDAS
Acreditación Institucional de Alta Calidad