Aarón Espinosa Asencio

Plan de Protección de Ciberseguridad de la Organización

Your delivery!

Principios en materia de Ciberseguridad

En el caso de la empresa *Your delivery!*, al tratarse de una empresa de reparto a domicilio, se ha considerado como lo más imposible la información de pago del cliente, así como la información del mismo, se definen unos principios en el siguiente decálogo que serán imprescindible cumplir para garantizar seguridad, confidencialidad, integridad y disponibilidad de los datos.

- **1. Definir y aplicar una política de ciberseguridad:** Es importante establecer la forma en la que se va a gestionar la seguridad de la información, así como los activos que participan en los procesos.
- **2. Proteger y asegurar la información:** Debemos garantizar la integridad y confidencialidad de la información en todo momento mediante buenas prácticas.

- **3. Uso responsable y seguro de las redes:** Solo se usarán las redes de la empresa, estas contarán con un filtrado de MAC para evitar conexiones ajenas, Es importante navegar de forma segura por el web intentado no introducir información sensible y si es posible usando la navegación en incógnito o en su defecto, borrar toda la información al acabar de usar el navegador.
- **4. Protegerse ante el malware:** La mejor forma para protegerse ante el malware es ser consciente de lo que se hace en todo momento, no descargar programas con extensiones extrañas, de webs de dudosa fiabilidad…
- **5. Uso adecuado del correo electrónico:** Únicamente se abrirán correos corporativos cerciorándose antes que el dominio del que proviene el correo es de la misma empresa, no usar el correo corporativo para fines personales.
- **6. Garantizar acceso remoto y físico seguro:** En cuanto al acceso remoto, acceso mediante protocolos seguros como SSH o SFTP si queremos transferir archivos además de crear un usuario por empleado con una contraseña única. El acceso físico a los dispositivos se realizará mediante una contraseña única que se entregará a cada empleado para su dispositivo.
- **7. Mantener las aplicaciones actualizadas:** Mantener siempre el sistema operativo así como las aplicaciones actualizadas para evitar la explotación de fallas en versiones anticuadas.
- **8. Plan de respuesta a incidentes:** Establecer un plan de acción de respuesta a incidentes en el caso de que los haya.
- **9. Concienciar y formar al personal:** Informar y formar al personal sobre buenas prácticas.
- **10. Asegurar que se aplique todo lo anterior:** Lo más importante de este decálogo, la gobernanza. Establecer cómo se debe cumplir el decálogo y garantizar la implementación de las políticas para minimizar con todo esto el riesgo de la empresa.

Conceptos e Incidentes

A:

- Activo de Información:

- Algoritmos de Cifrado: Consiste en una serie de operaciones matemáticas que utilizadas junto a una clave se aplican sobre un texto en claro y permite obtener un texto cifrado (o descifrarlo) garantizando la confidencialidad e integridad de la información contenida.

- Adware: Programa que mientras su uso o instalación muestra publicidad de forma recurrente al usuario. Por ejemplo, la publicidad que aparece en el videojuego Among Us cada vez que acabas una partida.

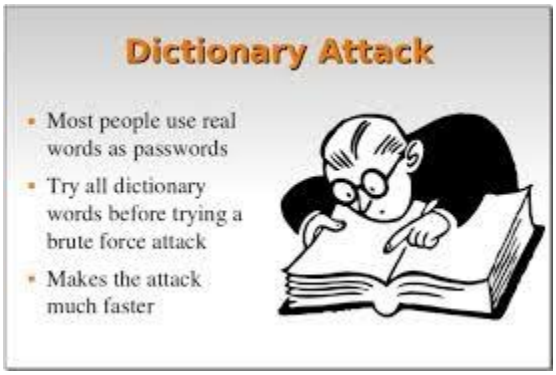
- Agujero de seguridad: Se trata de un fallo o vulnerabilidad en un sistema que puede ser aprovechado para violar la seguridad de este.

Existen diferentes tipos:

- De software
- De hardware
- Del entorno físico
- Del personal
- De procedimientos
- De la red

- Antivirus: Programa informático que se utiliza para prevenir, detectar y eliminar amenazas informáticas, como pueden ser virus, troyanos, worms, etc. El uso de este tipo de programas ha ido decayendo con el tiempo. Como antivirus podemos poner de ejemplo el propio Windows Defender.

- Ataque diccionario: Como su nombre indica, consiste en intentar averiguar una contraseña probando con todas las palabras del diccionario.
  Existen variantes en las que se comprueban las sustituciones típicas (letra por número, intercambio de dos letras, abreviaciones…), así como combinaciones de mayúsculas y minúsculas.



- Ataque de fuerza bruta: Consiste en probar todas las combinaciones posibles hasta dar con la contraseña correcta

B:

- Biometría: método de reconocimiento basado en características fisiológicas de personas (utilizando por ejemplo huella dactilar, reconocimiento facial, iris, etc). Para ello es

necesario que los rasgos sean de carácter universal, diferente a la de cualquier otra persona, ser constante (no variable en el tiempo) y poder ser medida).
Por ejemplo, el acceso biométrico de huella dactilar y reconocimiento facial para desbloquear el móvil y ciertas aplicaciones, o el reconocimiento de voz del Asistente de Google.

- Bomba lógica: Se trata de un trozo de código incluido en algún software que se ejecuta solo cuando se dan una serie de condiciones y realiza una acción maliciosa. Esto puede ser cuando descargas un programa pirata para ahorrarte unos euros y a la tercera vez que lo enciendes te instala un keylogger.

- BUG: Es un error en un programa o software que puede tener consecuencias indeseadas para el sistema, como por ejemplo la exposición de información privada a hackers, crackers, etc.

- BOTNET: Es un conjunto de ordenadores, llamados bots o zombies, que son controlados de forma remota por un atacante para realizar actividades malintencionadas, como ataques de denegación de servicio distribuido, etc. Esta red de ordenadores zombies están conectadas a su vez a un servidor central, quien les da las órdenes y les transmite la información.

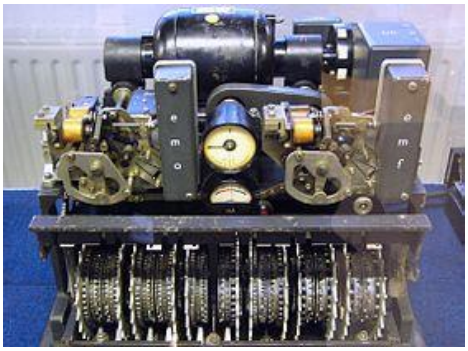
- BULO: Noticias falsas creadas para que se propaguen rápidamente a través de las redes sociales generalmente, para hacer creer a las personas acontecimientos falsos o de dudosa veracidad. Por ejemplo, aquellas personas que propagan que la Tierra es plana.

- Bastionado de Sistemas: Es la implantación de las políticas de seguridad oportunas para prevenir posibles problemas en un futuro tales como de permisos, vulnerabilidades, problemas con el firewall...

C:

- Certificado Digital: Fichero generado por una entidad llamada Autoridad Certificadora (CA), cuya finalidad es confirmar la identidad de una persona física, organismo o empresa en Internet, autenticando al poseedor, aunque también servirá para cifrar las comunicaciones y firmar digitalmente. Dicho fichero tendrá un cifrado para nuestra seguridad, tanto a la hora de instalar, exportar e importar.
  Por ejemplo: Para acceder a nuestro portal de la secretaría virtual de la Consejería de Educación y Deporte, una de las opciones será el acceso mediante certificado digital o electrónico, en este caso generado por la FNMT.

- Criptografía: Habiendo dos tipos de criptografía principales, como la simétrica y la asimétrica o de clave pública, su función es la cifrar un mensaje haciéndolo ilegible para todo aquel que no conozca el sistema con el que se ha cifrado, convirtiendo dicho mensaje en un criptograma.



Máquina alemana de cifrado Lorenz, utilizada en la Segunda Guerra Mundial, para el cifrado de mensajes destinados a generales.

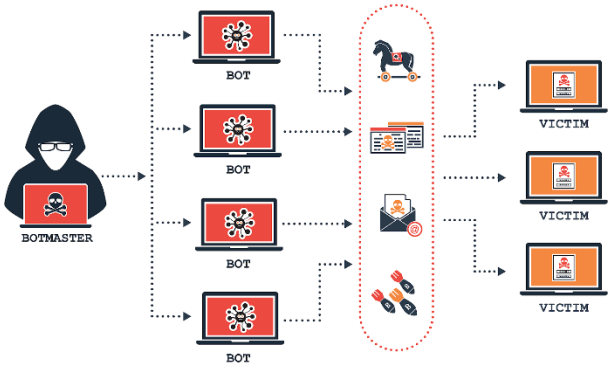
- Control parental: Se trata de una serie de herramientas o medidas que se utilizan para limitar el acceso (generalmente a menores de edad) a cierto tipo de contenido que podría ser inapropiado.

- Cortafuegos: También llamado Firewall, es un sistema de seguridad que está formado tanto por software como por dispositivos hardware, que se colocan en las zonas límites de las redes para así controlar el tráfico entrante y saliente. La función principal es velar por que se cumplan las normas establecidas en cuanto al tráfico de red permitido dentro de una empresa o corporación.

- CRACKER: También conocido como Ciberdelincuente, es una persona con altos conocimientos informáticos, que usa dichos conocimientos para crear caos, para beneficio propio, penetrar en redes e intentar tener acceso a zonas o contenidos reservados (sin autorización). Son completamente diferentes a los HACKERS, perteneciendo al Red Team, o Black Hat.

D:

- Denegación de Servicio: Por un lado, una denegación de servicio (DoS) es un tipo de ataque que consiste en hacer una serie de peticiones a un servicio determinado desde una misma máquina para poder así consumir los recursos que ofrece dicho servicio para colapsarlo.
  Por otro lado, una denegación de servicios distribuidos (DDoS) es un ataque que consiste en colapsar una red utilizando un gran número de equipos para que dicho servicio quede también completamente inaccesible.



- Defacement: Es un ataque dirigido a una página web causando el cambio visual de la apariencia de la misma. Normalmente son producidos por hackers que obtuvieron acceso de alguna forma, por un error de programación o por algún bug o mala administración del servidor. Suelen utilizarse para enviar mensajes activistas o para crear un sitio de malware o phising.

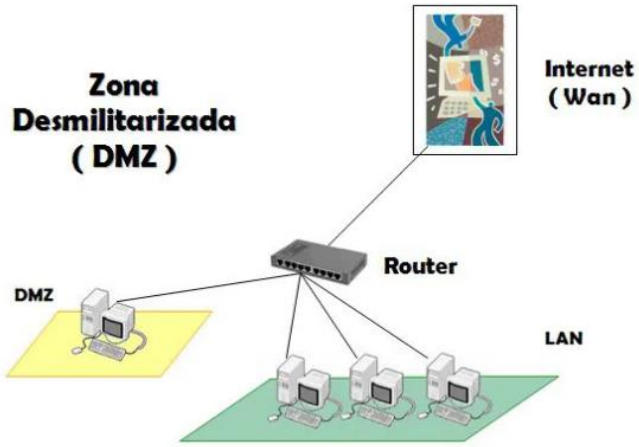
- DHCP: DHCP o Protocolo de configuración dinámica de host es un conjunto de reglas para dar direcciones IP y opciones de configuración a equipos de trabajo en red. Habitualmente un servidor DHCP se encarga de asignar una dirección IP dinámicamente a los equipos clientes.

- Dirección IP: Una dirección IP (Internet Protocol) es un conjunto de números únicos e irrepetibles que identifican a un dispositivo que está conectado a Internet. Se podría decir que una dirección IP es como “una matrícula de un vehículo”.

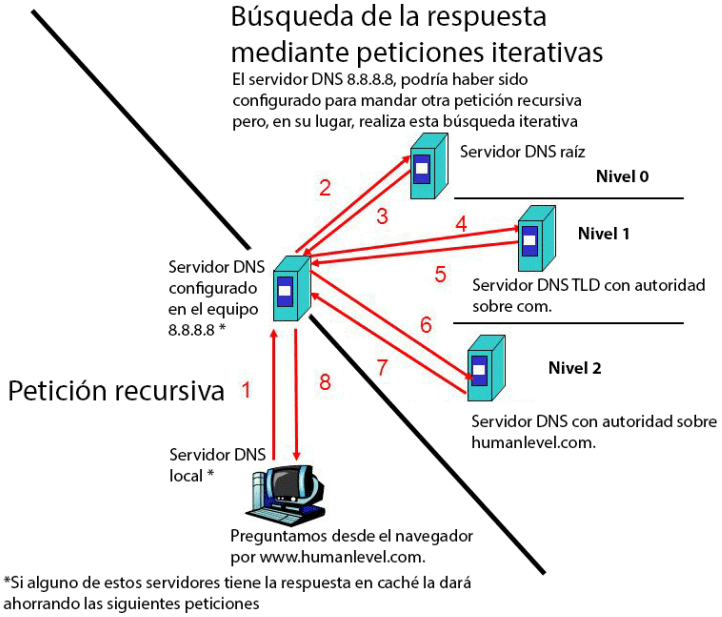
  Dentro de las direcciones IP hay dos tipos: dinámicas (que son aquellas que pueden asignarte una dirección IP completamente diferente a la que tenías previamente) y las estáticas (permanece siempre igual y se configura de manera manual).

- Dirección MAC: Es una dirección física, formada por un valor de 48 bits, que tiene cada dispositivo que esté conectado a una red. Es única e irrepetible para cada dispositivo, ya que se escribe de forma binaria en el hardware de la interfaz de red a la hora de fabricarse.

- DMZ: Zona desmilitarizada o red perimetral, es una red local que se ubica entre la LAN(red interna) y la WAN (red externa). Su objetivo es evitar ejecuciones de programas o acceder a determinados servicios desde el exterior sin permisos o bloquear solicitudes entrantes sospechosas, estas zonas suelen utilizarse para servidores.



- DNS: “Domain Name System”. El servicio DNS asocia un nombre de dominio con información relacionada con ese dominio. Su función más importante es traducir nombres inteligibles para las personas en direcciones IP asociados con los sistemas conectados a la red con el propósito de poder localizar y direccionar estos sistemas de una forma mucho más simple.



E:

- Exploit: Es un programa informático que se aprovecha de una vulnerabilidad para provocar un comportamiento no intencionado en un software, hardware, o cualquier otro dispositivo.

F:

- FTP: Protocolo que consiste en la transferencia de archivos a través de la red. Funciona en el puerto 20 y 21 y su seguridad puede ser mejorada usando SFTP, que se ayuda de SSH para cifrar los datos.

- Fuga de datos: Como su nombre indica se trata de una pérdida de privacidad en cuanto a información privada que puede ser tanto de una empresa como de un particular. Esta información fugada era una información que debería ser privada y debería ser conocida únicamente por las personas autorizadas. Algún ejemplo de esto puede ser un documento de patente que mandemos a algún socio y de repente sepamos que lo ha obtenido la competencia.

G:

- Gusano: Es un malware cuya principal característica es que se propaga fácilmente. El fin de este malware es replicarse a nuevos sistemas informáticos y aprovechando todos los medios posibles, ya sea por correo, por FTP, etc.

H:

- HTTPS: De sus siglas en inglés Protocolo seguro de transferencia de hipertexto (Hipertext Transfer Protocol Secure) es un protocolo de red basado en HTTP pensado para la navegación web. Se suele utilizar en páginas de compras online o que requieran de un extra de seguridad como pueden ser webs de banca o de trading o temas relacionados con la economía en general, así como páginas de compartición de archivos etc.

- Hacker: Comúnmente conocemos como “Hacker” a lo que en castellano conoceríamos como ciberdelincuente. No es más que una persona que comete delitos en internet, ya sea con la vulneración de datos o penetración en redes o suplantación de identidad o otro tipo de delitos virtuales. También nos encontramos con los conocidos como “Hackers éticos” que son personas que son contratadas (o no) para detectar vulnerabilidades u otro tipo de resquicios, que puedan ser aprovechados por los hackers para atacar y cometer delitos, y de aportar soluciones ante estas vulnerabilidades.

I:

- Informática forense: Consiste en la investigación de los sistemas informáticos para buscar cualquier rastro o indicio de delito que pueda ser presentado como prueba en un juicio en caso de ataque a dichos sistemas.

- Incidente de seguridad: Cualquier suceso que afecte a la confidencialidad de la información de una empresa. Ya sea por acceso, divulgación o modificación o destrucción no autorizada de la información

- Inyección SQL: Es un tipo de ataque que se aprovecha de las vulnerabilidades a la hora de autenticar los datos introducidos en un formulario web, para así obtener de forma ilícita las entradas de la base de datos de la organización.

- Ingeniería social: Técnicas usadas para obtener información persuadiendo a las víctimas.

K:

- Keylogger: Software o dispositivo especifico que sirve para registrar todas las acciones realizadas a través del teclado de la víctima.

L:

- Leak: Se produce cuando toda o parte de una información confidencial es liberada en Internet.

M:

- Malware: Es un software diseñado que tiene como objetivo causar daños o infiltrarse sin el consentimiento de la víctima en un sistema de información.

- Metadatos: Es un conjunto de datos que están vinculados a un archivo y que recogen información descriptiva de dicho archivo.

P:

- Parche de seguridad: Como el propio nombre indica se trata de una actualización de seguridad que aplica cambios en el software que tengamos para mantenernos seguros. Suelen desarrollarse por el fabricante del software que estemos actualizando tras detectar vulnerabilidades.

- Phishing: En castellano lo conocemos como estafa. Más que un término de ciberseguridad se trata de una técnica de ingeniería social, siendo el factor humano al final la parte más vulnerable. Algún ejemplo podría ser un supuesto correo electrónico que te pida información personal alegando ser una empresa o entidad que conoces.

- Pharming: Ataque informático que se aprovecha de una vulnerabilidad en el software de los servidores DNS de una organización, que consiste en cambiar o modificar el archivo que contiene los nombres de dominio, cambiando la dirección IP auténtica por otra falsa, de manera que cuando el usuario escriba el nombre de dominio en la barra de direcciones del navegador, el DNS ‘’falso’’ lo redireccionará a una web falsa que suplantará a la auténtica, para así sacar las claves de dichos usuarios.

S:

- Sniffer: software utilizado para monitorizar la red con el fin de capturar información. Este software lo que hace es colocar la tarjeta de red en un modo promiscuo, desactivando así el filtro de verificación de direcciones, y aceptando todos los paquetes de la red donde está situado, sean para este dispositivo o no. Es recomendable utilizar cifrado en nuestras comunicaciones, puesto que nuestro tráfico no va cifrado, este puede ser escuchado por el usuario del sniffer. Por ejemplo, con el software Wireshark podremos ver todo el tráfico de la red, al igual que los dispositivos y protocolos que se utilizan.
- Spoofing: uso de técnicas para la suplantación de identidad, claramente relacionado con usos maliciosos o de investigación, existiendo varios tipos, como por ejemplo:
    - IP Spoofing: siendo el más conocido consiste en sustituir la dirección IP origen de un paquete TCP/IP por otra que deseemos suplantar.
    - ARP Spoofing: suplanta las tramas ARP, se consigue duplicando las tablas que contienen dichas tramas ARP.
    - DNS Spoofing: falsificar una IP para que, mediante nombre DNS, consiga una IP, comprometiendo a un servidor que infecte la caché de otro o modificando las entradas del servidor.
    - Web Spoofing: suplantar una página real por una falsa, para conseguir datos de los usuarios.
    - Email Spoofing: suplantar una dirección de correo electrónico, para el envío de correos hoax como suplemento para el uso de phishing y SPAM.

- SSL: (Secure Sockets Layer) Protocolo criptográfico seguro que asegura las comunicaciones, normalmente cliente-servidor, proporcionando autenticación y privacidad de la información entre extremos. Utiliza clave de cifrado simétrica para garantizar la confidencialidad de la información, y para garantizar la autenticación y seguridad de la clave simétrica, se utilizará algoritmos de cifrado simétrico y certificados X.509. Generalmente, solo se autentica el lado del servidor, ya que para una autenticación mutua será necesaria una infraestructura de claves públicas (PKI) para los clientes.
  Este protocolo ha evolucionado a TLS (Transport Layer Security).

- SSH tunneling: Consiste en enviar todos los paquetes dentro de paquetes SSH para cifrar los datos y garantizar que no se puedan leer de camino.

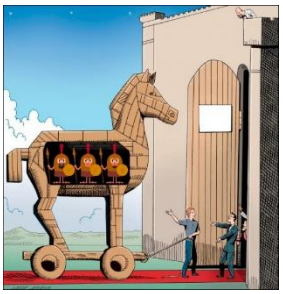
- Suplantación: El atacante se hace pasar por quien no es para cometer otros cibercrímenes tales como fraudes o ciberacoso o ganarse la confianza de la gente para luego obtener más información de ella mediante chantajes por ejemplo, todo esto mediante perfiles falsos o robados de otras personas.

R:

- Ransomware: Es un tipo de malware que impide a los usuarios acceder a un sistema o a unos archivos y que exige el pago de un rescate para poder acceder de nuevo a ellos.
- Rootkit: Son programas maliciosos que se instalan en un sistema. Generalmente son muy difíciles de detectar porque se suelen instalar a muy bajo nivel. Con ellos es posible hacerse con el control de ciertas funcionalidades y acceder a servicios y recursos del sistema vulnerado.

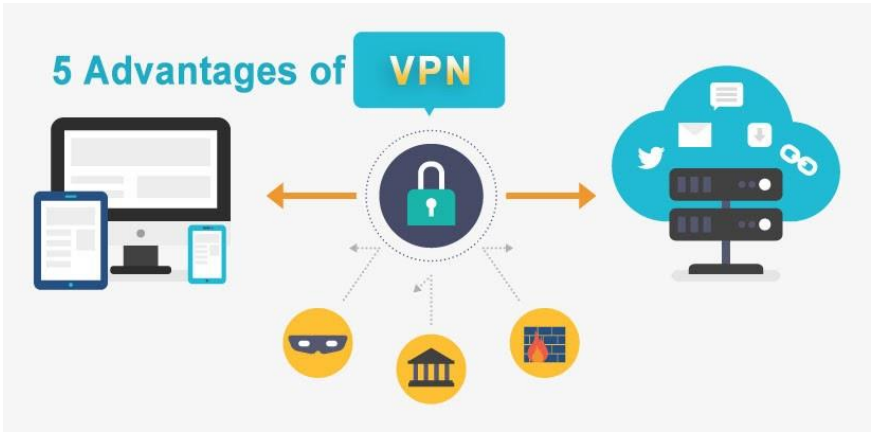
T:

- Troyano: Tipo de malware cuya principal característica es que requiere de ingeniería social para su propagación, es decir, hace falta que un usuario descargue o ejecute el troyano para que sea infectado. Cuando esto ocurre el programa suele dedicarse a abrir canales de comunicación con la computadora del atacante la cual permitirá controlar nuestro sistema.



V:

- VPN: Conocido como Red Privada Virtual, permite una red local segura sobre una red pública. Los datos que pasan por esa red se protegen mediante la autenticación y el cifrado.



- Virus: Un virus es un programa informático diseñado intencionadamente para ejecutarse y replicarse a sí mismo. Esto hace que una aplicación infectada pueda infectar otros archivos.

- Vulnerabilidad: Una vulnerabilidad es una debilidad o un fallo en un programa que permite que un usuario no legítimo acceda a la información o explota de forma intencionada la seguridad de forma remota.

W:

- Wifi: Una red Wifi es aquella que está formada por dispositivos comunicados entre sí de manera inalámbrica a internet mediante un punto de acceso de acceso inalámbrico, esta tecnología inalámbrica funciona bajo el estándar 802.11, este tipo de conexiones van cifradas ya que si no sería fácil acceder a estas comunicaciones haciendo un ataque de man in the middle.

    - existen tres tipos de cifrados para esta conexión:
        - WEP
        - WPA
        - WPA2

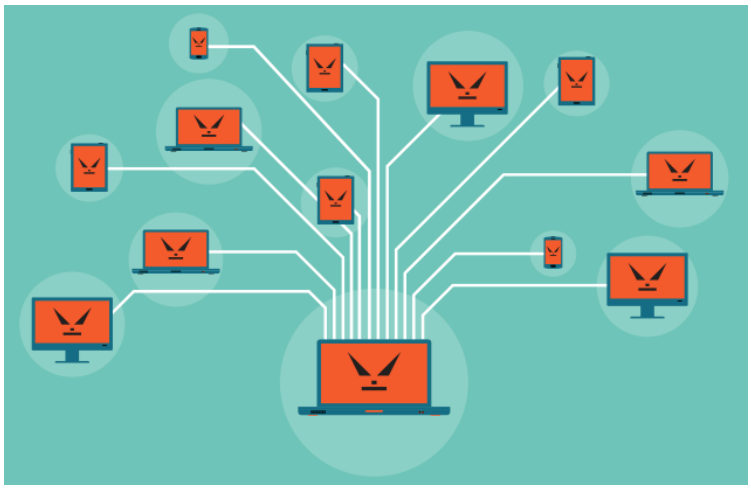
X:

- XSS: Secuencias de comandos en sitios cruzados (Conocido como Cross-site scripting). Es una vulnerabilidad que existe en las páginas web. Al ser una página web dinámica, el usuario puede insertar un código script dentro de los formularios, foros, blogs,lo oculta y lo ejecuta. Una vez hecho el ataque puede cambiar configuraciones, robar cuentas y cualquier acción que pase inadvertida.

Z:

- Zero Day: Podemos entenderlo como una vulnerabilidad de algún software en su primer día de lanzamiento. Los posibles atacantes conocen de este problema y los fabricantes suelen lanzar parches de seguridad para solventar este tipo de vulnerabilidades. A este tipo de parches se les conoce como parches de día uno en castellano.

- Zombie: Es nombre dado a los ordenadores que conforman una botnet u ordenadores infectados por un malware en los cuales el Bot master o el ciberdelincuente los usa de una manera ilícita o inapropiada ya sea para propagar el malware hacia otros ordenadores conectados en la misma red o para enviar correos masivos y hacer ataques de denegación de servicios.



Plan de Concienciación

1. Amenazas

En cuanto a amenazas en la empresa, aquellas no físicas conciernen todo lo relacionado con las que se encuentran en internet (phishing, troyanos…) y cualquiera relacionada con la falta de seguridad en la red (puertos abiertos accesibles para cualquiera, contraseñas poco seguras…) En cuanto a las físicas, hay que ser consciente de que pueden intentar atracar el local o a los mismos repartidores cuando van a repartir.

2. Nivel de Peligro

Al tratarse de un local de reparto, en este caso, la CCN-CERT establece que se debería considerar en el nivel 1 de peligrosidad y amenazas, así que es muy importante que se encuentre segura y respaldada en todo momento, pero no con la exhaustividad que se tomaría en otro caso, por ejemplo en una institución financiera.

3. Política de uso de Software

Solo se usará el software que el administrador de la empresa instale en los dispositivos usados. Todos los movimientos en el S.O quedarán registrados, así como aquellos detectados como inusuales serán investigados inmediatamente para verificar que no existen anomalías.

4. Instalación de Software

La instalación de software correrá a cargo del administrador de la empresa, ante cualquier cambio, notificar al mismo o seguir las pautas básicas: Instalar solamente software obtenido de fuentes oficiales, tales como la tienda de Microsoft o las páginas oficiales de los mismos.

5. Guía de buenas prácticas

5.1. Software

El software deberá estar siempre actualizado, tanto como los programas utilizados como el sistema operativo, además de contar con el último sistema operativo en cuestión, o al menos alguno que aún siga ofreciendo soporte. Se deberá ser estrictos con las políticas de seguridad y firewall de los sistemas operativos, en especial de aquellos usados por los terminales donde los clientes pueden realizar operaciones para evitar posibles futuros problemas o ataques. Importante que todos los sistemas sean monitoreados y revisados constantemente para garantizar un correcto funcionamiento de estos.

5.2. Usuario

Es importante que los usuarios sean conscientes de donde trabajan y lo que implica, por ello, es importante que eviten dejar a la luz o al alcance de cualquier información sensible como datos sobre usuarios, en especial, la dirección o número de tarjeta de los clientes.

5.3. Navegación por red (externa e interna)

La navegación se hará siempre a través de la red privada de la empresa que previamente tiene configuradas las restricciones y políticas pertinentes, se evitará acceder a sitios webs de dudosa fiabilidad, así como proporcionar cualquier tipo de información relacionada con la empresa. Se usará un navegador web actualizado y seguro, configurado correctamente para garantizar una navegación lo más segura posible.

5.4. Uso de correo electrónico

El correo electrónico corporativo solo se usará con fines administrativos e informativos hacia los usuarios, muy a tener en cuenta la procedencia de los correos, evitar a toda costa hacer clic sobre enlaces en correos electrónicos y descargar archivos de estos. Para analizar un email entrante podemos usar algunas páginas o apps para ello como “Dante”s Gates Mobile” donde introduciendo el email, mediante técnicas OSINT (inteligencia de fuentes abiertas) nos dará información sobre el email además de decirnos si es sospechoso o no, en caso de ser sospechoso, deberíamos descartarlo automáticamente, ya que con tan solo hacer un clic en algún enlace o descargando algún fichero del email fraudulento, podríamos correr el riesgo de sufrir phishing o algún tipo de ataque a nuestro sistema. Los emails fraudulentos suelen usar nombres muy similares al original, es importante ver el remitente de los correos y cerciorarse de que es una fuente fiable, también y esto en el 99% de los casos, usan un dominio de correo propio, así que, si vemos un email con dominio “@gmail, @outlook, etc…” deberemos sospechar de inmediato.

5.5. Uso de dispositivos móviles

Es importante proteger asimismo los dispositivos móviles entregados por la empresa, dado que contienen información sensible.

Deberemos establecer un método seguro para desbloquear el dispositivo, tal como por ejemplo un patrón, o si es posible biometría (huella dactilar, escáner iris o facial).

Deshabilitar cualquier tipo de conexión si no se está utilizando (datos móviles, wifi, bluetooth).

Ignorar cualquier tipo de SMS no proveniente de la empresa y asegurarse que, una vez recibido un SMS, es realmente la empresa quien lo envía. Descarga de aplicaciones únicamente de tiendas oficiales y revisando previamente los permisos.

5.6. Uso de redes

La red inalámbrica de la empresa deberá ser gestionada por el administrador asegurándola mediante varias configuraciones, tales como la modificación del SSID, cambio de la contraseña por defecto, habilitando un filtrado de MAC para que únicamente los dispositivos empresariales puedan conectar y limitación de puertos únicamente a los que realmente se usan

5.7. Uso de mensajería instantánea

Se usará la plataforma rocket chat, donde el administrador, en este caso quien redacta el documento, creará un servidor con un usuario por cada empleado de la empresa y las pertinentes medidas de seguridad, la aplicación móvil se encuentra en la tienda de cada dispositivo, en ordenadores, se puede obtener a través de su página oficial. La aplicación solo se usará para fines empresariales y no se podrá compartir información personal.
https://rocket.chat/es/

5.8. Uso de redes sociales

Está prohibido el uso de las redes sociales por todos los empleados excepto el CM (community manager) de la empresa, quien se encargará mediante Twitter en este caso, de proporcionar información sobre los productos, redirigir las incidencias a los empleados de la empresa y hacer publicidad de la misma.

5.9. Uso de Internet Of Things

Dispondremos de un sistema de alarma inteligente en el caso de robo o forzado de cajeros, que automáticamente enviará un reporte a la policía.
Los vehículos de entrega estarán geolocalizados en todo momento para que los clientes puedan ver el estado de su pedido en todo momento.

6. Auditoría

Software

Se realizará una auditoría cada 2 meses para comprobar el estado de los programas instalados en los sistemas, se realizará un escaneo en remoto por parte del administrador para detectar que no hay apps no autorizadas o algunas con vulnerabilidad así como aquellas no actualizadas. En general se seguirán los siguientes pasos:

1. Conocer los servicios y sistemas que se van a auditar.
2. Verificar en qué grado la empresa cumple con los estándares de calidad.
3. Identificar todos los dispositivos y sistemas operativos de la empresa.
4. Analizar los programas que están en uso.
5. Comprobar las vulnerabilidades.
6. Plantear un plan de mejora con medidas específicas.
7. Implementar un plan de desarrollo y mejora, consecuencia de la auditoría.

Usuario

Se designará a un empleado cada mes que se encargará de que se cumplan las directrices de los usuarios mediante breves cuestionarios cada 3 meses.

Navegación por red (externa e interna)

Se verificará semanalmente que el navegador web está actualizado así como las políticas existentes por si hubiera que modificarlas o hacerlas más restrictivas.

Uso de correo electrónico

Se verificará que los empleados están concienciados y que han cambiado la contraseña del email cada mes.

Uso de dispositivos móviles

Verificación de que todo funciona correctamente y no hay software instalado de fuentes desconocidas semanalmente.

Uso de redes

Se revisará y monitorizará constantemente los dispositivos conectados a la red, también se rotará de contraseña trimestralmente.

Uso de mensajería instantánea

En el caso que se use, se revisarán los logs de inicio de sesión mensualmente y se aplicarán nuevas políticas si así lo requiriese.

Uso de redes sociales

El CM hará una lista trimestralmente de las incidencias más reportadas así de las campañas publicitarias que más repercusión han causado para así poder enfocarse más en las mismas.

Uso de Internet Of Things

Se recogerá la información de las rutas usadas para diferentes direcciones para que la próxima vez no se solicite al cliente y así ofrecer una mejor experiencia, se verificará que la compartición de localización de los repartidores sea lo más precisa posible, todo esto semanalmente.

Material y recursos de concienciación

PLAN DE CONCIENCIACIÓN SOBRE LA CIBERSEGURIDAD

No, un príncipe nigeriano no te ha contactado para donarte una herencia millonaria a cambio de tus datos personales.

PLAN DE CONCIENCIACIÓN SOBRE LA CIBERSEGURIDAD

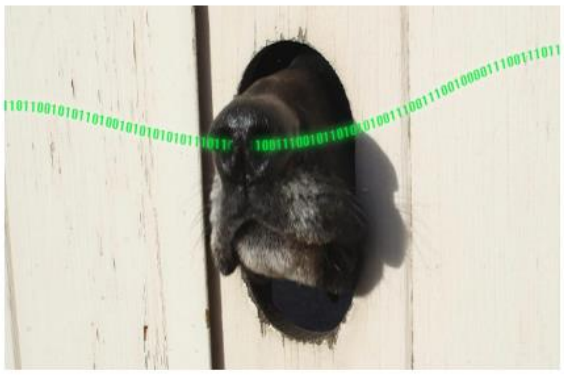
No, tu banco no te ha bloqueado la tarjeta y mucho menos te va a enviar un enlace para que revises el cargo pidiéndote el login de tu cuenta.

PLAN DE CONCIENCIACIÓN SOBRE LA CIBERSEGURIDAD

No, tampoco Microsoft te va a llamar por teléfono con un acento español extraño y con muchos errores a la hora de hablar para obtener acceso remoto de tus dispositivos.

PLAN DE CONCIENCIACIÓN SOBRE LA CIBERSEGURIDAD

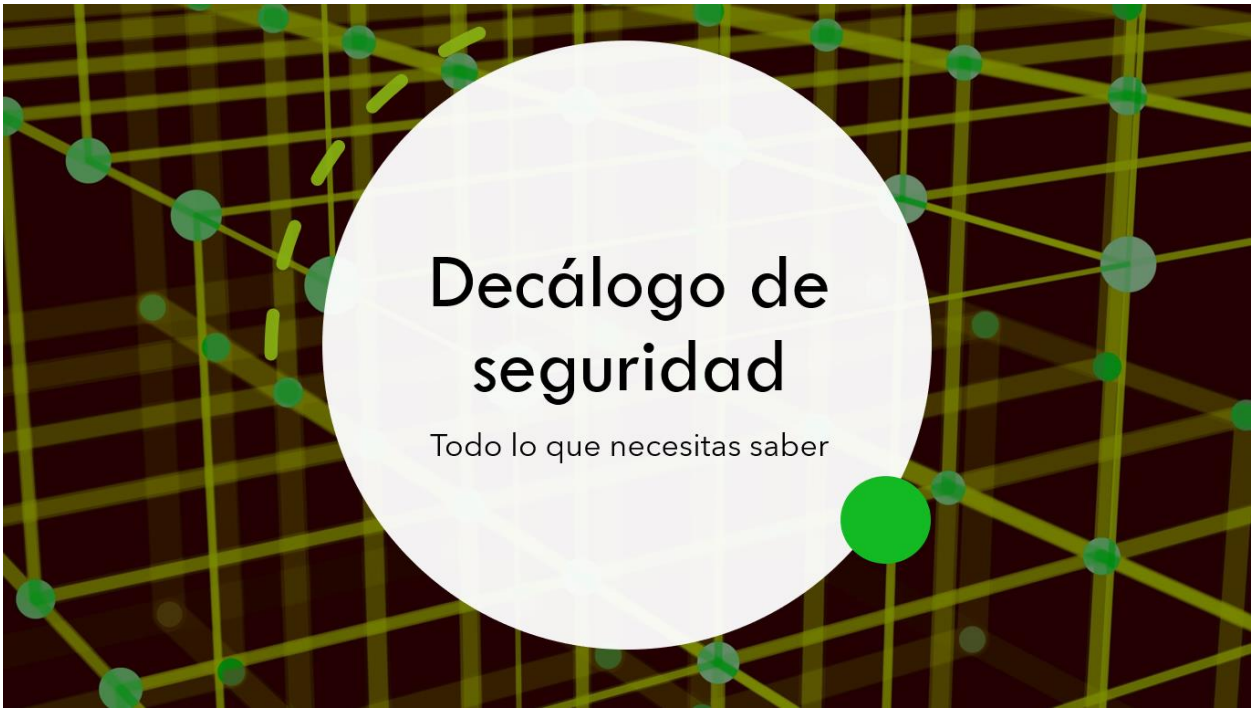
Evita conectarte a redes públicas, pueden estar "viendo" todo lo que haces y lo que transmites a través de la red.



Recomendaciones del CCN (video resumen)

https://www.youtube.com/watch?v=VfZVGFgRI4g&feature=emb_logo

Decálogo de seguridad



Decálogo básico de seguridad

A continuación veremos las bases para establecer una buena cultura de la seguridad en la empresa

1. Definir y aplicar una política de ciberseguridad

- Es importante establecer la forma en la que se va a gestionar la seguridad de la información así como los activos que participan en los procesos.

2. Proteger y asegurar la información

- Debemos garantizar la integridad y confidencialidad de la información en todo momento mediante buenas prácticas.

3. Uso responsable y seguro de las redes

- Solo se usarán las redes de la empresa, estas contarán con un filtrado de MAC para evitar conexiones ajenas,
- Es importante navegar de forma segura por la web intentado no introducir información sensible y si es posible usando la navegación en incógnito o en su defecto, borrar toda la información al acabar de usar el navegador.

4. Protegerse ante el malware

- La mejor forma para protegerse ante el malware es ser consciente de lo que se hace en todo momento, no descargar programas con extensiones extrañas, de webs de dudosa fiabilidad…

5. Uso adecuado del correo electrónico

- Únicamente se abrirán correos corporativos cerciorándose antes que el dominio del que proviene el correo es de la misma empresa, no usar el correo corporativo para fines personales.

6. Garantizar acceso remoto y físico seguro.

- En cuanto al acceso remoto, acceso mediante protocolos seguros como ssh o sftp si queremos transferir archivos además de crear un usuario por empleado con una contraseña única.
- El acceso físico a los dispositivos se realizará mediante una contraseña única que se entregará a cada empleado para su dispositivo.

7. Mantener las aplicaciones actualizadas

- Mantener siempre el sistema operativo así como las aplicaciones actualizadas para evitar la explotación de fallas en versiones anticuadas.

8. Plan de respuesta a incidentes

- Establecer un plan de acción de respuesta a incidentes en el caso de que los haya.

9. Concienciar y formar al personal

- Informar y formar al personal sobre buenas prácticas.

10. Asegurar que se aplique todo lo anterior

- Lo más importante de este decálogo, la gobernanza.
- Establecer cómo se debe cumplir el decálogo y garantizar la implementación de las políticas para minimizar con todo esto el riesgo de la empresa.