Sheet

Es importante hacernos conscientes sobre la proteccion de nuestra información

¿Por qué es importante la información?

La información es el activo más **valioso, costoso y vulnerable**

Diferencia entre datos Personales vs. Organizacionales

Datos Personales	Datos Organizacionales
Datos que solo me interesan a mi	Datos que le interesan a la empresa
Redes Sociales	Datos de Clientes
Cuentas Bancarias	Estructura Organizacional
Facturas	

Rutina de seguridad diaria

- Siempre mantener el celular con un tipo de bloqueo
- No permitir mostrar notificaciones
- Usar sesión en la computadora
- Mantener la computadora bloqueada si no estamos en ella
- Nunca mantener información confidencial en libretas
- Usar un gestor de contraseñas para almacenar las contraseñas
- No mantener las contraseñas en Post-it
- No enviar contraseñas en mensajes de texto o bloc de notas
- No usar la misma contraseña
- Siempre revisar que en la página web exista un https://
- Nunca entrar a publicidad clickbait
- Tener cuidado con las métricas empresariales

- No mantener información personal dentro de la computadora de trabajo
- Siempre mantenerse alerta al momento de ingresar a una red, debido a que una persona puede infiltrarse en nuestra máquina para obtener información que es confidencial
- Usar vpn si es que nos conectamos en redes públicas

Escenarios reales de cyber ataques

En nuestra vida diaria existen diversos momentos en los que podemos ser vulnerables.

Revisar ataques informáticos realizados en la red:

Center for Strategic and International Studies
https://www.csis.org/

Fallos en la seguridad en las empresas

Name	Explicacion
Facebook	Mantenía las contraseñas en un texto plano, por lo que cualquier persona podía acceder. Actualmente esto ha sido cambiado
WhatsApp	Muchos atacantes tuvieron acceso a cámaras y micrófonos por WhatsApp. A través de las llamadas de voz se instalaba un SpyWare que permite estar conectado a la aplicación y obtener información diaria de los usuarios.
WannaCry	Evento sucedido en 2017 aprovechandose en el S.O. Windows que permitia cifrar todos los datos de las computadoras y pedían un rescate con dinero.

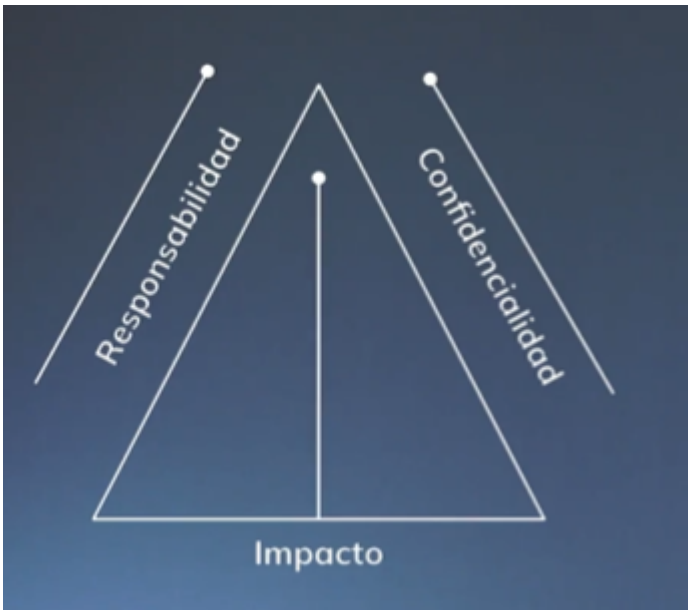
Triangulo CIA: Confidencialidad, Integridad y Disponibilidad

Una cadena es tan fuerte como su eslabón más débil. Debemos tomar el control sobre la seguridad de la empresa. Debemos evitar compartir información personal a través de fotos, publicaciones en facebook, etc.

Estrategias para mantener segura la información

Name	Explicacion
Confidencialidad	Nos asegura que la información que compartimos con otras empresas, es información que será solo accedida por mí y no accedida por sistemas que no están aprobados

Name	Explicacion
Integridad	Propiedad que nos asegura que la información que estamos almacenando, se mantendrá sin mi autorización. Incluso asi yo pida modificar, debe mantenerse un registro de cambios.
Disponibilidad	La información se encuentra disponible para usuarios **AUTORIZADOS**



Cada acción que nosotros realizamos, tiene un impacto sobre la seguridad de nuestra información.

A mayor rango, mayor es la responsabilidad y mayor debe ser la confidencialidad.

Ingeniería social, Phishing y Publicidad engañosa

Ejemplos de hacking que se aprovechan de nuestras vulnerabilidades como seres humanos.

Ingenieria Social: "Hackear al ser humano". Se aprovecha de nuestras debilidades como ser humano (Sociabilidad, facilidad de comunicación).

Phishing: Ingenieria social que nos hace creer que somos importante. Nos brinda clickbaits para "solucionar problemas".

Publicidad engañosa: Son publicidades dentro de las páginas web que nos hacen creer haber ganado algo pero en realidad es mentira. Actualmente no se ven muchos de estos casos.

Ataques DoS y DDoS, Man in the Middle y Ransomware

Ejemplos de hacking que se aprovechan de vulnerabilidades en nuestros dispositivos.

Ataque DoS o DDoS: La diferencia entre DoS y DDoS es la forma en la que son ejecutados. Si yo intento ingresar a un sitio, es una petición que estoy haciendo a un servidor. Los servidores están equipados con software y hardware que soporten estas solicitudes. Sin embargo, los atacantes pueden realizar peticiones descontroladas y de esa forma el servidor ya no puede responder más.

Man in the Middle: Existen redes públicas sin seguridad, por lo que la información que nosotros realizamos al intentar enviar mensajes, el atacante accede a esta comunicación y mira nuestros mensajes enviados.

Ransomware: Un ejemplo es WannaCry, aprovecha problemas en el S.O. para ingresar a la computadora, encripta la información y el atacante cobra algo a cambio para devolvernos la información. Podemos mantener copias de seguridad de la información y cuando nos atacan simplemente resetamos la máquina.

Virus y Malware, Troyanos, Adware y Spyware

Virus y Malware: Se encuentra pegados a archivos. Se pueden descargar de cualquier lugar, por ejemplo archivos descargables o USB. Los USB pueden tener archivos autorun. Debemos además, tener cuidado con los archivos que estamos descargando.

Troyano: Piezas de software que vienen embebidos dentro de programas y pueden ser perjudiciales para nuestra computadora. Se llaman troyanos debido a que traen algo adentro que puede ser malicioso.

Adware: Nos muestra ventanas de clickbaits hacia publicidad. Ya no suele hacerse mucho debido a que los navegadores tienen protecciones contra estos lugares.

Spyware: Ingresa en nuestros dispositivos debido a que tienen alguna vulnerabilidad. Nosotros como usuarios no nos damos cuenta que tenemos esto. Podemos bloquear el microfono y la cámara para evitar estos problemas

Firewall

Firewall nos permite configurar ciertas reglas que permite que pase o no pase ciertas comunicaciones. Verifica si el mensaje es uno que cumple con las reglas definidas entonces las deja pasar, de otra forma no.

{{search404Captions.content404Title}}
https://support.microsoft.com/es-cl/help/4028544/windows-10-turn-microsoft-defender-firewall-on-or-off

OS X: Acerca del firewall de aplicación
https://support.apple.com/es-es/HT201642

Cookies

Son pequeños pedazos de texto que se envian de nuestro navegador y es enviado al creador del sitio web sobre nuestra información. Al momento de nosotros aceptar, autorizamos que accedan a nuestra información.

Recomendacion: Leer que es lo que están recolectando los sitios web.

Métodos de Defensa: Antivirus, Adblock, Antispam y Web Filter

Antivirus: Software que mantiene base de datos de virus actualizada y permite comparar esta base de datos con cualquier software o navegación en nuestro computador. Cuando es un posible virus nos genera un mensaje que estamos en peligro.

- Avast
- NOD32

Adblock: Bloquea las ventanas Ads.

Antispam: Google ya posee algoritmos de antispam, identifica los correos que pueden ser spam y avisan al usuario que la comunicación es posiblemente spam.

Webfilter: Nos ayuda en la navegación para identificar si la búsqueda es segura o no.

Métodos de defensa: Encriptación

Permite defender de personas inescrupulosas que quieren dañar nuestros equipos.

Encriptación: Transforma dispositivos para que si no tienes la clave de cifrado entonces no pueden acceder.

Métodos de defensa: Two factor authentication

Existe información que sabemos y que tenemos acceso. Cuando ingresamos a la página de la cuenta bancaria, podemos acceder a nuestro login pero al realizar una transacción, algunas entidades bancarias generan una llave dinámica enviada al celular o incluso al movil.

Diseña contraseñas seguras

Uso de sistema de gestión de contraseñas. Permite almacenar las contraseñas y mantener un acceso seguro sobre todos los login.

- No usar palabras obvias: Los atacantes pueden usar ingeniería social para poder acceder.
- Usar por lo menos 8 caracteres: Mayúsculas, minúsculas, símbolos, numeros
- No guardar las contraseñas en lugares visibles: Postit, notas, archivos
- No decir la contraseña a nadie
- No usar la misma contraseña para todo
- Mientras mas larga la contraseña mas segura
- No usar palabras de diccionarios
- No usar palabras o patrones comunes
- Usar un generador de contraseñas

Uso de VPN: Conexión segura en redes

Permite usar una red pública para conectarte a una red privada local. Como cliente realizamos solicitudes a un servidor. Este servidor procesa la información y nos envía una respuesta.

Al usar una VPN creamos un túnel en la comunicación y podemos acceder a la información.

De esta forma si nosotros estamos en Colombia, podemos usar una VPN para que piensen que estamos en otro lugar.

La información está encriptada.