1- ¿Correo de Phishing?

1

Riesgo: El usuario hace clic en un enlace malicioso.

Consecuencia: Robo de credenciales, acceso no autorizado a cuentas, y potencial compromiso de sistemas internos.

2- Contraseña Débil

2

Riesgo: Uso de contraseñas como "123456" o "password".

Consecuencia: Acceso no autorizado a sistemas críticos, robo de datos, y potencial para ataques posteriores.

3- Ataque de Ransomware

3

Riesgo: Ejecución de un archivo adjunto malicioso.

Consecuencia: Cifrado de archivos críticos, pérdida de datos, interrupción de operaciones, y demandas de rescate financiero.

4-Dispositivos USB No Autorizados

4

Riesgo: Conexión de un USB infectado a la red corporativa.

Consecuencia: Infección con malware, robo de datos, y posible propagación de virus a otros sistemas.

5-Computadora Desbloqueada

5

Riesgo: Un atacante accede a una computadora desbloqueada.

Consecuencia: Robo de información sensible, acceso no autorizado a sistemas, y alteración de datos.

6-Ingeniería Social

6

Riesgo: Un empleado es engañado para proporcionar información sensible.

Consecuencia: Acceso a cuentas, compromiso de sistemas, y posible filtración de datos.

7-Acceso Remoto No Seguro

7

Riesgo: Conexión a la red corporativa sin usar VPN o cifrado.

Consecuencia: Intercepción de datos sensibles, acceso no autorizado, y posible robo de información.

8-Uso de Wi-Fi Público

8

Riesgo: Conexión a la red corporativa desde una Wi-Fi pública no segura.

Consecuencia: Intercepción de datos, ataques de hombre en el medio, y robo de credenciales.

9-Navegación en Sitios Web No Seguros

9

Riesgo: Visita a un sitio web malicioso que descarga malware.

Consecuencia: Infección con malware, robo de datos, y posible compromiso del sistema.

10-Falta de Actualización de Software

10

Riesgo: No aplicar parches y actualizaciones de seguridad.

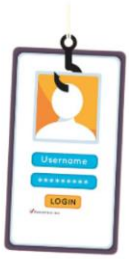
Consecuencia: Vulnerabilidades explotables, acceso no autorizado, y compromisos del sistema.

11-Uso de Aplicaciones No Autorizadas

11

Riesgo: Instalación de software no autorizado o no verificado.

Consecuencia: Infección con malware, pérdida de control de seguridad, y posibles violaciones de datos.



12- Compartir Credenciales

12

Riesgo: Compartir contraseñas con colegas o a través de canales inseguros.

Consecuencia: Acceso no autorizado, robo de información, y aumento del riesgo de compromisos.

13-Exposición de Información en Redes Sociales

13

Riesgo: Publicación de información sensible o detalles sobre el trabajo en redes sociales.

Consecuencia: Uso de la información por atacantes para ingeniería social o acceso no autorizado.

14-Dispositivos Móviles Sin Contraseña

14

Riesgo: Pérdida o robo de un dispositivo móvil sin cifrado.

Consecuencia: Acceso a información corporativa, robo de datos, y posibles violaciones de seguridad.

15-No Uso de Autenticación de Dos Factores (2FA)

15

Riesgo: Dependencia de solo una contraseña para acceder a sistemas.

Consecuencia: Fácil acceso a cuentas comprometidas, robo de datos, y posibles violaciones de sistemas críticos.

16- Reutilización de Contraseñas

16

- **Riesgo:** Uso de la misma contraseña en múltiples cuentas.
- **Consecuencia:** Si una cuenta se ve comprometida, todas las demás también podrían estar en riesgo.

17- Phishing de Voz (Vishing)

17

- **Riesgo:** Un atacante se hace pasar por un soporte técnico legítimo y pide acceso a sistemas a través de una llamada telefónica.
- **Consecuencia:** Acceso no autorizado a sistemas críticos, robo de información, y posibles violaciones de datos.

CONSECUENCIAS GENERALES DE MATERIALIZARSE LOS RIESGOS

Interrupción de Operaciones:
La continuidad del negocio se ve afectada debido a sistemas comprometidos o pérdida de datos.

Pérdida Financiera:
Gastos relacionados con la respuesta al incidente, recuperación de datos, multas, o pagos de rescate.

Daño a la Reputación:
La confianza de clientes y socios comerciales se ve afectada, lo que puede llevar a la pérdida de negocios.

Pérdida de Datos:
Información crítica o sensible se ve comprometida o destruida, lo que puede tener efectos a largo plazo en la empresa.
Impacto en la Seguridad Física:

En casos extremos, un ciberataque puede tener consecuencias en la seguridad física, como en infraestructuras críticas.