

Práctica Pareja 1.4: Auditoría del plan de prevención y concienciación



Trabajo realizado por:

Samuel Romero de los Reyes
Ernesto Saquete Rios

Curso de especialización en:

CETI

Índice

1. Smishing.....	3
2. Notificación de incidentes.....	3
3. Navegación segura en Internet.....	3
4. Uso seguro de redes Wi-Fi.....	4
5. Informe general de concienciación.....	4

1. Smishing

- **Elemento a auditar:** reconocimiento y evitación de SMS fraudulentos
- **Modo de evaluación:** simulacro de smishing mediante envío de SMS controlados
- **Métrica:** % de empleados que pinchan en el enlace del SMS falso
 - Auditoría positiva: menos del 5% pinchan en el enlace. Se considera que la plantilla está bien concienciada
 - Auditoría negativa: más del 5% pinchan en el enlace. Se necesita reforzar esta concienciación

2. Notificación de incidentes

- **Elemento a auditar:** capacidad de los empleados para reportar incidentes
- **Modo de evaluación:** revisión mensual del buzón soporte@saquero.es
- **Métrica:** % de incidentes detectados por empleados vs incidentes detectados por el sistema
 - Auditoría positiva: más del 80% de incidentes notificados por empleados. Se considera que la plantilla está bien concienciada
 - Auditoría negativa: menos del 80% de incidentes notificados por empleados. Se necesita reforzar esta concienciación

3. Navegación segura en Internet

- **Elemento a auditar:** aplicación de buenas prácticas de navegación
- **Modo de evaluación:** simulaciones (páginas falsas, pop-ups, enlaces maliciosos seguros) + encuesta
- **Métrica:** % de empleados que fallan en una prueba de navegación insegura
 - Auditoría positiva: menos del 10% fallan en la prueba. Se considera que la plantilla está bien concienciada
 - Auditoría negativa: más del 10% fallan la prueba. Se necesita reforzar esta concienciación

4. Uso seguro de redes Wi-Fi

- **Elemento a auditar:** uso correcto de redes seguras
- **Modo de evaluación:** registro de conexiones + comprobación de uso de VPN
- **Métrica:** nº de conexiones detectadas desde redes no autorizadas sin VPN
 - Auditoría positiva: 0 a 2 conexiones detectadas desde redes no autorizadas sin VPN. Se considera que la plantilla está bien concienciada
 - Auditoría negativa: más de 2 conexiones detectadas desde redes no autorizadas sin VPN. Se necesita reforzar esta concienciación

5. Informe general de concienciación

- **Elemento a auditar:** cumplimiento global de las buenas prácticas del plan
- **Modo de evaluación:** auditoría trimestral basada en los puntos del informe (p. ej. contraseñas, BYOD, bloqueo, documentos, antivirus)
- **Métrica:** % de incumplimientos detectados respecto al total de controles
 - Auditoría positiva: menos del 15% de incumplimientos detectados respecto al total de controles. Se considera que la plantilla está bien concienciada
 - Auditoría negativa: más del 15% de incumplimientos detectados respecto al total de controles. Se necesita reforzar esta concienciación