**PRÁCTICA N°4**

**TEMA: “PREVENCIÓN DE ATAQUES DE INGENIERIA SOCIAL Y SEGURIDAD EN EL ACCESO”**

**1. OBJETIVOS**

1.1 Personalizar y configurar una simulación de ataque de phishing en un entorno controlado.

1.2 Implementar una campaña de concientización y entrenamiento para prevenir ataques de phishing.

1.3 Establecer factores adicionales de autenticación.

**3. REACTIVO**

¿Cuál es una herramienta de simulación de phishing?

1. Kaspersky
2. Human Shield
3. Gophish
4. Nessus

¿Practicas claves para prevenir ataques de phishing?

1. Compartir contraseñas con amigos y compañeros de trabajo.
2. Hacer clic en enlaces e imágenes recibidos por correos no verificados.
3. Verificar la autenticidad del remitente antes de interactuar con un correo.
4. Ignorar las actualizaciones de seguridad del sistema.

¿Qué acciones se debe tomar al recibir un correo sospechoso?

1. Verificar el dominio del remitente
2. Descargar archivos adjuntos para revisar su contenido.
3. Reportar el correo a la unidad de TI o seguridad.
4. No hacer clic en enlaces sospechosos.

¿Selecciones las acciones de un correo legitimo?

1. Uso correcto del idioma y ortografía.
2. Solicitudes de información confidencial como contraseñas.
3. Direcciones de correo que coinciden con los dominios oficiales,
4. Ausencia de sentido de urgencia o amenaza.