Plantilla de Evaluación y Eficacia para las Videoconferencias y Transferencias SGSPI.

Este cuestionario es una plantilla del Sistema de Gestión de Seguridad y Privacidad de la Información (SGSPI) diseñada para evaluar la eficacia de las videoconferencias y transferencias de información dentro de la entidad.

Asunto: Plan de Concientización y Sensibilización
Expositor: **Andres del Pilar Gonzalez Hernandez**
Fecha: **26 de Marzo**
Hora: **1:30 p.m - 2: 45 p.m**

Datos de Registro

1. Nombres y Apellidos (Completos) *
LUIS ALBERTO GALICIA GUERRERO

Ingrese su correo Institucional *
galiciag@sena.edu.co

3. Tipo de vinculación *
- (•) Contratista
- ( ) Planta - Carrera administrativa
- ( ) Planta - Provisional
- ( ) Planta - Libre nombramiento y remoción
- ( ) Pasante
- ( ) Aprendiz
- ( ) Otro

Registre su Dependencia.

4. **Dirección General / Regional** *
- ( ) Amazonas
- ( ) Antioquia
- ( ) Arauca
- ( ) Atlántico
- ( ) Bolívar
- ( ) Boyacá
- ( ) Caldas
- ( ) Caquetá
- ( ) Cauca
- ( ) Cesar
- ( ) Córdoba
- ( ) Cundinamarca
- ( ) Chocó
- ( ) Dirección General
- ( ) Distrito Capital
- ( ) Huila
- ( ) Guajira
- ( ) Magdalena
- ( ) Meta
- ( ) Nariño
- ( ) Norte de Santander
- ( ) Quindío
- ( ) Risaralda
- ( ) Santander
- ( ) Sucre
- (•) Tolima
- ( ) Valle del Cauca
- ( ) Casanare
- ( ) Putumayo
- ( ) San Andrés
- ( ) Guainía
- ( ) Guaviare
- ( ) Vaupés
- ( ) Vichada

5. **Tolima** *
- ( ) Centro de Comercio y Servicios (Tolima)
- (•) Centro de Industria y Construcción
- ( ) Despacho Regional Tolima
- ( ) Centro Agropecuario de la Granja

Resultados de la Sesión Realizada.

Se revisará

6. **El phishing** es una técnica de engaño que usan los ciberdelincuentes para que tú mismo les entregues tus datos (contraseñas, números de tarjeta o información personal). *
- (•) Verdadero
- ( ) Falso

Se revisará

7. Ante una anomalía o un incidente de seguridad de la información, ¿cuál es el procedimiento correcto a seguir? *
- ( ) Esperar a la próxima auditoría semestral para mencionarlo.
- ( ) Intentar solucionar el problema por cuenta propia sin avisar a nadie.
- (•) Contactar a la mesa de servicio para reportar el evento.

Se revisará

8. **¿cuál es una de las malas prácticas más comunes que se busca corregir en el SENA?** *
- (•) Almacenar contraseñas en los equipos y lugares inseguros como post-its o agendas
- ( ) Portar el Carnet Institucional
- ( ) Conocer el Manual de Políticas GOR-M-003

Se revisará

9. **Como instructor, ¿cuál es una de sus responsabilidades clave para fortalecer la cultura de seguridad en su Centro de Formación?**
*
- ( ) Crear sus propias políticas de seguridad independientes a la norma ISO 27001.
- ( ) Administrar de forma exclusiva la mesa de ayuda institucional.
- ( ) Reparar físicamente los equipos de cómputo que presenten fallas.
- (•) Replicar los contenidos de 'Martes de Seguridad' en sus grupos de trabajo

Se revisará

10. **¿Qué acción práctica se recomienda para garantizar la seguridad física de la información al alejarse del escritorio?**
*
- ( ) Apagar el monitor pero dejar la CPU encendida y la sesión abierta.
- ( ) Pedirle a un aprendiz que vigile el equipo mientras regresa.
- (•) Bloquear el computador utilizando el comando abreviado Windows + L.
- ( ) Llevarse el teclado para que nadie más pueda escribir.

Se revisará

11. **¿Cuál es el objetivo primordial de la 'Clínica de Contraseñas' ?**
*
- (•) Fomentar el uso de gestores de contraseñas seguros y el segundo factor de autenticación (MFA).
- ( ) Enseñar a los colaboradores a memorizar 50 contraseñas diferentes.
- ( ) Instruir sobre cómo compartir la contraseña de red con el equipo de trabajo.
- ( ) Eliminar la necesidad de usar contraseñas en todos los sistemas del SENA

Se revisará

12. **Contexto:** Un empleado de la empresa recibe un correo electrónico con el asunto: **"URGENTE: Su cuenta de nómina ha sido suspendida".** El cuerpo del mensaje tiene el logotipo oficial del banco de la empresa y dice: *"Estimado usuario, hemos detectado actividad inusual en su cuenta. Para evitar el bloqueo permanente, debe validar su identidad en las próximas 2 horas haciendo clic en el siguiente botón: [VERIFICAR CUENTA AQUÍ].*
Si no realiza esta acción, sus pagos pendientes serán retenidos." Al pasar el cursor sobre el botón (sin hacer clic), el empleado observa que el enlace redirige a: http://servicios-bancarios-seguros.net/login/auth. El remitente del correo es notificaciones@bancopreferido-soporte.com.
¿Qué tipo de ataque está intentando perpetrar el atacante?
*
- ( ) Ransomware
- (•) Phishing
- ( ) Denegación de Servicio (DoS)
- ( ) Inyección SQL

Evaluación de la Sesión.

13. ¿Considera que se abarcaron los temas planteados en el objetivo de la sesión? *
- (•) Si
- ( ) No

14. ¿El expositor o expositores fueron claros con los temas tratados? *
- (•) Si
- ( ) No

15. ¿Las ayudas audiovisuales fueron adecuadas para la sesión? *

1	2	3	4	5

16. ¿Antes de la sesión, tenía dominio de los temas vistos? *
- (•) Si
- ( ) No

17. Después de la sesión, considera que el dominio de los temas vistos: *
- (•) Aumentó
- ( ) Es el mismo

18. ¿Considera que la información de la sesión le es útil para su trabajo? *
- (•) Si
- ( ) No

19. ¿Qué otros temas relacionados con respecto a Seguridad y Privacidad de la información le gustaría profundizar ? *
mas en seguridad

20. En el siguiente espacio escriba sus recomendaciones, observaciones, sugerencias o felicitaciones con respecto a la sesión *
excelente

Microsoft 365

Este contenido lo creó el propietario del formulario. Los datos que envíes se enviarán al propietario del formulario. Microsoft no es responsable de las prácticas de privacidad o seguridad de sus clientes, incluidas las que adopte el propietario de este formulario. Nunca dar tu contraseña.
Microsoft Forms | Encuestas, cuestionarios y sondeos con tecnología de inteligencia artificial Crear mi propio formulario
Privacidad y cookies | Términos de uso