**INFORME DETALLADO SOBRE LA PLATAFORMA INTERACTIVA DE CONCIENTIZACIÓN EN CIBERSEGURIDAD PARA PERSONAL EMPRESARIAL**

Autoría de: Karol Vanessa Nuñez Vera

Cargo: Aprendiz SENA

Dirigido a: Ángela Patricia Marroquín y Jorge García

Fecha: 8/4/2025

**1. INTRODUCCIÓN**

Vivimos conectados. Usamos teléfonos inteligentes, computadoras, correos electrónicos, redes sociales y servicios en línea todos los días. La ciberseguridad, por tanto, no es solo un asunto técnico: es una parte fundamental de nuestra vida diaria. Desde proteger nuestras contraseñas hasta evitar caer en engaños por internet, todos estamos involucrados.

Por eso, este informe presenta una plataforma digital educativa especialmente diseñada para principiantes. Su propósito es que cualquier persona, sin importar su nivel técnico, aprenda a protegerse y comprenda cómo los riesgos digitales pueden afectar su entorno personal y laboral. El conocimiento en ciberseguridad es poder, y esta herramienta busca brindar ese poder a cada empleado o estudiante.

**2. OBJETIVOS**

**Objetivo General:**

Diseñar e implementar una plataforma digital interactiva de formación continua en ciberseguridad, ajustada al personal, con un enfoque práctico, modular, sencillo, interactivo y gamificado.

**Objetivos Específicos:**

* Incentivar el aprendizaje activo mediante recursos multimedia, ejemplos cotidianos, mini talleres, juegos y pruebas de manera progresiva.
* Establecer jerarquías de usuarios con permisos diferenciados y seguimiento individualizado.
* Medir el avance de la concientización mediante indicadores y reportes.
* Fomentar una cultura preventiva, responsable y proactiva frente a incidentes informáticos.
* Relacionar los contenidos con situaciones reales y ejemplos simples que ayuden a comprender su importancia.

**3. ROLES DEFINIDOS EN LA PLATAFORMA**

**3.1. Administrador General (Jefaturas)**

* Supervisión del sistema y control de usuarios.
* Activación y personalización de módulos.
* Acceso total a informes y simulaciones.
* Definición de campañas y lineamientos de concientización.

**3.2. Instructora (Aprendiz SENA)**

* Curaduría de contenidos.
* Asignación de rutas formativas.
* Seguimiento pedagógico.
* Gestión de foros y generación de reportes.

**3.3. Personal (Empleados)**

* Acceso a módulos asignados.
* Realización de actividades y simulacros.
* Participación activa en foros.
* Obtención de logros, insignias y reporte de incidentes.

**4. TEMÁTICA Y CONTENIDOS MODULARES (50 TEMAS)**

Cada módulo está diseñado para explicar conceptos complejos de manera fácil y accesible. Utiliza teoría aplicada, videos, juegos interactivos, ejemplos cotidianos y ejercicios prácticos para que cualquier usuario pueda aprender y aplicar la ciberseguridad en su día a día. Los temas incluyen:

**Contraseñas y accesos**

1. ¿Por qué “123456” sigue siendo una mala idea?
2. El truco para crear contraseñas fáciles de recordar y difíciles de adivinar
3. ¿Está mal guardar tus contraseñas en el navegador?
4. ¿Qué es un gestor de contraseñas y cómo te puede salvar la vida digital?
5. Qué tan fácil es que adivinen tu contraseña con fuerza bruta

**Phishing y trampas digitales**

1. Cómo detectar correos trampa (phishing) en segundos
2. ¿Te ganaste algo por correo? ¡Probablemente no!
3. WhatsApp: los mensajes más comunes usados ​​para robarte
4. Phishing por SMS: “su cuenta fue bloqueada”, y otras mentiras comunes
5. Quishing: el nuevo phishing con códigos QR

**Ingeniería social y engaños**

1. Cómo los estafadores usan tus redes sociales para engañarte
2. Historias reales de suplantación de identidad y cómo prevenirlo
3. ¿Por qué los hackers no atacan computadores, sino personas?
4. El “falso soporte técnico” que te llama para ayudarte
5. ¿Te han pedido datos personales por llamada? Cómo reconocer engaños

**Redes sociales y mensajería**

1. ¿Debo compartir mi ubicación en tiempo real?
2. Qué tipo de fotos NO deberías publicar nunca
3. Cómo proteger tu cuenta de Instagram en 5 pasos
4. ¿Tus seguidores podrían ser bots o perfiles falsos?
5. Cómo evitar que uses tus fotos para hacer perfiles falsos

**Uso del ordenador y navegación**

1. Señales de que una página web es falsa o peligrosa
2. ¿Qué tan seguras son las redes WiFi públicas?
3. No hagas clic ahí: pop-ups, anuncios y trampas comunes
4. Extensiones sospechosas: lo que no deberías instalar en tu navegador
5. ¿Cuándo fue la última vez que actualizaste tu antivirus?

**Seguridad en el celular**

1. ¿Tu celular tiene contraseña o lo dejas desbloqueado?
2. Qué permisos estás dando sin darte cuenta a tus apps
3. Cómo evitar que te escuchen por cámara o micrófono
4. ¿Vale la pena instalar un antivirus en el celular?
5. Cómo revisar si una aplicación es realmente confiable

**Trabajo, estudio y teletrabajo**

1. Buenas prácticas para no caer en trampas con el correo corporativo
2. ¿Compartes tus contraseñas con compañeros? ¡Grave error!
3. Cómo manejar archivos importantes de forma segura desde casa
4. ¿Dejas tu sesión abierta en el ordenador del trabajo?
5. Archivos “.exe”, “.zip” y otros riesgos en descargas

**Compras, banco y pagos**

1. Cómo saber si una página de compras es confiable
2. Pagos por internet: errores comunes que te pueden costar caro
3. ¿Debería guardar mis datos bancarios en el navegador?
4. El fraude de los falsos domicilios y entregas
5. Cómo evitar caer en estafas con promociones falsas

**Familia, hogar y entorno**

1. Cómo proteger a niños y adultos mayores en el mundo digital
2. ¿Le prestas tu celular a cualquiera? Lo que deberías saber
3. ¿Tus papás usan la misma contraseña para todo? Ayudalos
4. ¿Tus hijos usan TikTok? Esto es lo mínimo que debes revisar
5. ¿Es peligroso tener cámaras de seguridad conectadas a internet?

**Prevención general y conciencia**

1. ¿Qué hacer si crees que te hackearon?
2. Lo que debes revisar cada cierto tiempo en tus cuentas
3. La importancia de hacer copias de seguridad (backups)
4. ¿Sabes qué hacer si alguien te está acosando por redes?
5. Por qué la ciberseguridad **sí es asunto de todos**

Cada contenido se adapta al personal. La prioridad es que todos, desde quienes no saben nada de informática hasta los más avanzados, puedan aprender, participar y sentirse seguros en su entorno digital.

Además, se busca transmitir la idea de que la ciberseguridad no es un tema ajeno ni distante. Es parte de nuestra vida diaria: cuando usamos el cajero automático, cuando hacemos compras en línea, cuando compartimos fotos en redes sociales o simplemente cuando prendemos el computador en la oficina. La ciberseguridad está presente en todo momento, y por eso es fundamental empezar por lo básico y hacerlo de manera práctica, cercana y fácil de entender.

**5. SEGURIDAD DE LA PLATAFORMA**

**Acceso Seguro:**

* Registro con correo.
* Contraseñas encriptadas (bcrypt).
* Recuperación segura.
* Verificación 2FA.
* Restricción por red/IP.

**Protección Web:**

* HTTPS obligatorio.
* Validación de datos para evitar XSS, SQLi.
* CORS configurado.
* Registro de logs.
* Control de sesión por tiempo e inactividad.

**Gestión de Datos:**

* Segmentación de bases de datos.
* Backups automáticos.
* Historial de cambios.
* Control granular de accesos.

**6. FUNCIONALIDADES PRINCIPALES**

* Dashboard por rol.
* Progreso visual e informes.
* Sistema de logros e insignias.
* Retroalimentación automática.
* Calendario integrado.
* Biblioteca multimedia.
* Foros internos.
* Sistema de soporte y reporte.

**7. PROPUESTAS A FUTURO**

* Integración con correo e intranet.
* Aplicación móvil.
* Certificación automática.
* Inteligencia Artificial para alertas.
* Adaptación ISO 27001.

**8. CONCLUSIÓN**

Una organización segura comienza por usuarios informados. Esta plataforma representa un compromiso con la educación digital básica y accesible, promoviendo el desarrollo de habilidades en ciberseguridad desde cero. Está pensada para todos: para quienes usan el computador solo para tareas básicas, para quienes trabajan desde el celular o para quienes aún no están familiarizados con estos temas. La ciberseguridad es de todos y para todos, y con esta herramienta, se hace posible, cercana y comprensible.

**9. ANEXO - Referencias Bibliográficas**

* Instituto Nacional de Ciberseguridad de España (INCIBE). (2023). *Guías de concienciación en ciberseguridad*. Recuperado de [https://www.incibe.es](https://www.incibe.es/)
* International Organization for Standardization. (2013). *ISO/IEC 27001:2013 – Information technology — Security techniques — Information security management systems — Requirements*. ISO.
* Superintendencia de Industria y Comercio. (2012). *Ley 1581 de 2012 - Protección de datos personales*. Recuperado de [https://www.sic.gov.co](https://www.sic.gov.co/)
* OWASP Foundation. (2023). *OWASP Top 10 Security Risks*. Recuperado de [https://owasp.org](https://owasp.org/)
* Agencia Española de Protección de Datos (AEPD). (2022). *Guía para usuarios sobre privacidad y seguridad en Internet*. Recuperado de [https://www.aepd.es](https://www.aepd.es/)

A continuación, se presenta una propuesta de calendario mensual para las capacitaciones en ciberseguridad. Cada tema está pensado para abordar riesgos comunes desde una perspectiva práctica y cercana, con el fin de generar conciencia y promover hábitos seguros en el entorno digital y cotidiano.

|  |  |  |
| --- | --- | --- |
| **CAPACITACIONES MENSUALES** | | |
|  |
| **Mes** | **Tema de la capacitación** | **Enfoque** |  |
| Abril | Phishing: cómo no caer en trampas | Email, SMS, WhatsApp |  |
| Mayo | Redes sociales sin riesgos | Privacidad y suplantación |  |
| Junio | Contraseñas sin estrés | Cómo hacerlas, gestores |  |
| Julio | Ciberseguridad en casa | WiFi, dispositivos compartidos |  |
| Agosto | Celular seguro | Apps, permisos, antivirus |  |
| Septiembre | ¿Están espiando tu cámara? | Seguridad física y digital |  |
| Octubre | Detección de sitios falsos | Navegación segura |  |
| Noviembre | Cómo proteger tus datos bancarios | Compras y pagos |  |
| Diciembre | 5 errores digitales del año | Recordatorio general |  |