UserVerified

La problemática de la seguridad de la información involucra a todo el personal de la empresa, independientemente de su posición en la organización.

✔ Detectar ✔ Reaccionar ✔ Reportar ✔ Mejorar

Es una suite que tiene tres componentes fundamentales para que su organización cuente con usuarios preparados y listos a enfrentar las crecientes ciber amenazas del mundo digital.

## 1. CAMPAÑA

Diseñamos una estrategia efectiva para enfrentar las amenazas.

## 2. FORMACIÓN

Usuarios preparados = empresas fortalecidas

## 3. PRUEBAS

¿Los usuarios les hacen frente a las amenazas de phishing?

# CAMPAÑA DE SEGURIDAD DE LA INFORMACIÓN

Permanentemente el usuario recibirá información clara, continua y atractiva sobre la seguridad de la información. Llevaremos a los usuarios a participar activamente en este programa de concientización.

Al mes se abordarán varios temas de seguridad por medio de un correo semanal, de tal modo que la estructura de esta campaña va ser de modo secuencial, adaptada a las necesidades y políticas de su organización.

| EMAIL SEMANAL | PARTICIPA Y GANA | VIDEO | EMAIL CON ADVERTENCIA SEMANAL |
|---|---|---|---|
| **Consejos de seguridad**<br>**Historias o casos reales**<br>**Políticas del cliente** | **Una vez al mes se envía una encuesta de dos preguntas** | **Video una vez al mes** | **Información de amenazas de seguridad que ponen en riesgo la empresa** |

## ¿De qué se compone?

3 ciclos con una duración de 48 semanas, cada ciclo contiene 16 semanas, a medida que se avanza se profundiza más en los temas

### 16 semanas Nivel 1

- Consejos sobre la protección de la información
- Consejos de seguridad en el correo electrónico
- Qué es el malware, cómo funciona y consejos para evitarlo
- Navegar en internet de forma segura y acceso a redes sociales


### 16 semanas Nivel 2

- Tipos de datos
- Consejos de seguridad basado en las reglas corporativas
- Medidas preventivas contra el malware y casos reales
- Consejos de prevención en internet

### 16 semanas Nivel 3

- Medidas preventivas y conciencia corporativa
- Controles de prevención en el correo electrónico
- Respaldando mi información ante un ataque cibernético
- Seguridad del Home Office y navegación segura en casa

Te apoyamos a definir un plan de sensibilización en seguridad de la información que permita fortalecer las capacidades institucionales para prevenir y dar respuesta a eventos de seguridad.

# CURSO DE SEGURIDAD DE LA INFORMACIÓN

Un contenido desarrollado en el contexto colombiano, con información verificada y actualizada constantemente, que será entregada de una manera dinámica por medio de una plataforma de educación online.

Nuestro curso consta de cuatro módulos donde el usuario aprenderá a identificar cada uno de los ataques cibernéticos a los que se puede exponer en su ambiente de trabajo, con el fin de mitigar los riesgos de eventuales incidentes que se presenten, además de estar en capacidad de actuar de manera oportuna y efectiva para contrarrestar estos tipos de ataques y mejorar la seguridad de la información de su empresa.

## Programa de formación

Encontrará las temáticas de seguridad de la información en cada uno de los módulos:

### MÓDULO 1

Tipos de información, malware y phishing

### MÓDULO 2

Controles corporativos y protección avanzada


### MÓDULO 3

Factores de autenticación y uso de contraseñas


### MÓDULO 4

Ingeniería social

## Presentación del módulo

Cada uno de los módulos consta del siguiente orden:

### PRESENTACIÓN

Obtendrá los contenidos del curso de formación, entre estas encontrará textos con imágenes de forma interactiva.

### VIDEO

Encontrará un contenido de los temas a tratar de una forma clara y explícita para conocer más en detalle la seguridad de la información.

### ACTIVIDAD

Participará en las actividades didácticas que entretienen y enseñan.


### EVALUACIÓN

Debe demostrar su conocimiento de lo que ha aprendido en cada uno de los temas.

## Visión general

Al finalizar el curso el usuario podrá:

- Identificar el malware y sus formas de acción.
- Aplicar corporativa y personalmente el conocimiento adquirido.
- Tomar acciones en caso de incidentes de seguridad de la información mitigando el impacto.

## Incluye

- Acceso a la plataforma virtual
- Certificado de asistencia

# ATTACK USER TEST

## Pruebas de seguridad dirigidas al usuario final

Con **Attack User Test** se pondrán a prueba las capacidades de atención y reacción de los usuarios, usando técnicas estructuradas de alta eficacia. Al final, usted contará con métricas e informes ejecutivos.

Estas pruebas se realizan en un contexto corporativo en donde los usuarios reciben un correo electrónico que intentará engañarlos, usando técnicas de suplantación con el objetivo de evidenciar el riesgo entorno a la seguridad de la información.

- ✔ **Envíos:**
  - Envíos programados en diferentes fechas y diferentes objetivos
- ✔ **Descripción:**
  - Uso de técnicas de suplantación de identidad general y específica
  - Pruebas reales, perfiladas para aumentar la efectividad
  - Objetivo y propósito específico en cada prueba
  - Un sistema de pruebas único para su organización que al final será destruido
  - Un sistema de pruebas Evidencias irrefutables
- ✔ **Dirigido a:**
  - Direcciones de correo electrónico seleccionadas
    Personas o cargos en mayor riesgo

### Pruebas complementarias:

- **Mensajes por WhatsApp**
- **Mensajes de texto**
- **Llamadas telefónicas**
- **Investigación en redes sociales**

### Medición:

- **Clics en enlaces internos**
- **Descargas de adjuntos**
- **Captura de información**
- **Gestión de incidentes**

Para más información, contáctenos:
+57 (601) 744 14 11 comercial@seguridad-it.com
ITS CONSULTORIA INFORMATICA Informática, Tecnología y Seguridad
www.seguridad-it.com