

INFOSEC LATIN AMERICA INC
RNC: 1-30-97411-1

CLIENTE: Dirección General de Impuestos Internos (DGII)
CONTACTO: Juan Matos

Propuesta Económica: Renovación de licencias Portal Terranova para programa de concientización -1 año (1 mayo 2023- 30 de abril 2024)

Item	Número de parte	Descripción	Cantidad usuarios	Precio Unitario	Monto
1	CEU30-I	Plataforma de Concientización Terranova 1 año:	3500	\$ 801.32	\$ 2,804,605.11
		Curso en línea usuarios finales - paquete ultimate 30 temas - 3500 usuarios			
		curso en línea para Directores y Gerentes			
		curso en línea para administradores TI			
		curso en línea para desarrolladores			
		Learning Management System Hosting - Pre y post quiz			
		Micromódulos			
		Nanomódulos			
		Herramientas (posters, boletines, descansapantallas)			
		Personalización de cursos, texto y logo			
Porject Manager terranova (5 horas por año)					
Phishing Ilimitado (12 meses)					
Gestión de soporte capacitación (5 horas por año)					
				Sub total	\$2,804,605.11
				ITBIS	EXENTO
				Sub total	\$2,804,605.11

Términos Generales de la Cotización:	
Moneda:	Precios en Pesos Dominicanos
Validez de la oferta	30 días
Forma de Pago:	30 días contados a partir de la fecha de emisión de la factura

Atentamente,

Dayana Silva
SISAP
O. +1 809 683-6538
C. +1 829 652-8132
dayana.silva@sisap.com



Propuesta técnica

**Renovación de Licencias Portal Terranova para Programa de
Concientización sobre Seguridad de la Información para
Usuarios Finales, Gerentes, Administradores de Ti y
Desarrolladores.**

TERRANOVA

WW CORPORATION

Preparada para:



Impuestos Internos



15 de mayo de 2023

Clasificación: **Confidencial Externo**

www.sisap.com

Tabla de Contenidos

Alcance	3
¿Por qué elegir las soluciones de Terranova?.....	4
I. Capacitación en línea para usuarios finales	5
II. Capacitación en línea para gerentes y directores	12
III. Capacitación en línea para desarrolladores de TI.....	12
IV. Capacitación en línea para administradores de TI.....	13
V. Evaluación de diagnóstico pre y post capacitación.....	13
VI. Plataforma de gestión de concientización en seguridad (Learning management system)	13
VII. Módulos de Micro y Nano aprendizaje	15
VIII. Herramientas de comunicación	16
IX. Personalización de curso de usuarios finales y las herramientas de comunicación.....	19
X. Project Manager Terranova.....	19
XI. Plataforma integrada de simulación de ciberestafa (Phishing)	20
XII. Colaboración para campañas de Phishing	24



Clasificación: **Confidencial Externo**

Alcance

Se contempla el siguiente alcance:

Item	Número de parte	Descripción	Cantidad usuarios
1	CEU30-I	<p>Plataforma de Concientización Terranova 1 año:</p> <p>Curso en línea usuarios finales - paquete ultimate 30 temas - 3500 usuarios</p> <p>curso en línea para Directores y Gerentes</p> <p>curso en línea para administradores TI</p> <p>curso en línea para desarrolladores</p> <p>Learning Management System Hosting - Pre y post quiz</p> <p>Micromódulos</p> <p>Nanomódulos</p> <p>Herramientas (posters, boletines, descansapantallas)</p> <p>Personalización de cursos, texto y logo</p> <p>Porject Manager terranova (5 horas por año)</p> <p>Phishing Ilimitado (12 meses)</p> <p>Gestión de soporte capacitación (5 horas por año)</p>	3500

Se contempla soporte de acompañamiento a la DGII en temas relacionados a este servicio y seguimiento a solicitudes hacia el fabricante de la plataforma de Terranova.



Clasificación: **Confidencial Externo**

¿Por qué elegir las soluciones de Terranova?

Terranova Security Awareness es una empresa privada que brinda soluciones integrales de **capacitación** y de **comunicación** que apuntan a modificar en forma positiva los comportamientos en materia de seguridad de la información. Los productos de Terranova son la base a partir de la cual se crean programas personalizados sobre seguridad de la información que respetan las políticas internas y los requisitos de conformidad de la empresa.

Creada en torno a las mejores prácticas de la industria y fundada por profesionales de seguridad y educación de la tecnología de la información con más de 20 años de experiencia, Terranova ofrece una solución completa e integral sobre sensibilización a la seguridad de la información a empresas y organizaciones gubernamentales en todo el mundo en más de 10 idiomas. ¡Casi 400 empresas ya confían en Terranova! Y más de 2 millones de usuarios realizan nuestros cursos en línea.

Las soluciones y la capacitación de Terranova pueden reducir las pérdidas relacionadas con la seguridad de la información. Los conocimientos, la gestión de riesgos, y las mejores prácticas en combinación con una buena concientización en toda la empresa dan como resultado un verdadero rendimiento de la inversión (ROI).

Terranova ofrece las mejores herramientas de sensibilización, que cubren todas las etapas de la seguridad de la información en su empresa.

Programa de capacitación sobre sensibilización a la seguridad de la información

Los colaboradores de **DGII** deben jugar un rol importante en el programa de Capacitación sobre sensibilización a la seguridad de la información (CSSI). Cada esfuerzo individual contribuye a la mejora en la seguridad de toda la organización.

En SISAP, creemos que un programa de concientización sobre seguridad de la información debe cambiar la forma en que los usuarios ven la seguridad y hacerlos más conscientes de los riesgos potenciales.

Nuestros cursos en línea de concientización sobre seguridad de la información están hechos a medida para cumplir con las expectativas de diferentes tipos de clientes:

- Gerentes;
- Administradores de TI y desarrolladores de TI; y
- Usuarios finales.



Clasificación: **Confidencial Externo**

I. Capacitación en línea para usuarios finales

El curso está diseñado para fortalecer la primera línea de defensa en seguridad de la información. Los participantes de DGII entenderán y sabrán cómo implementar las mejores prácticas en seguridad de la información.

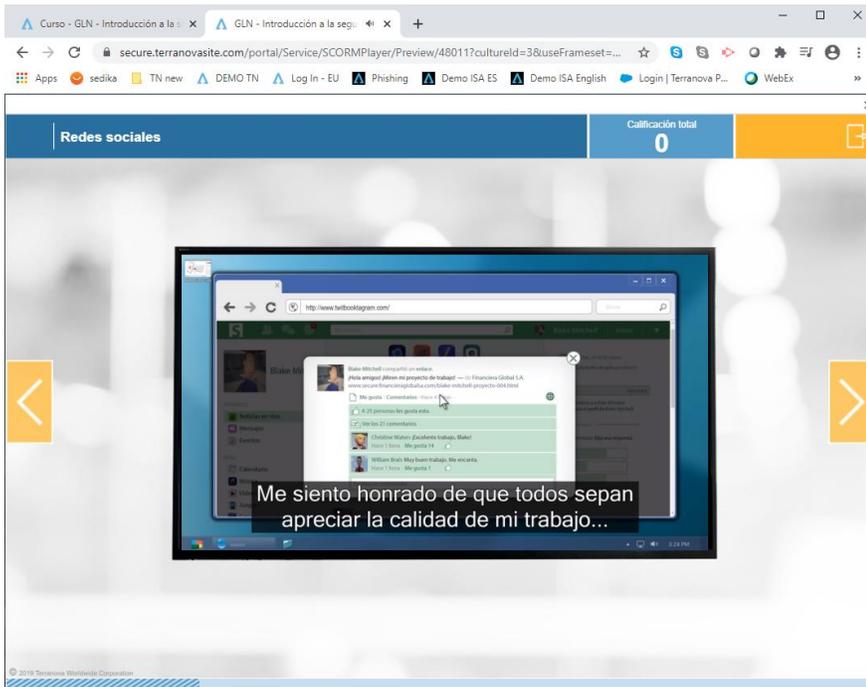
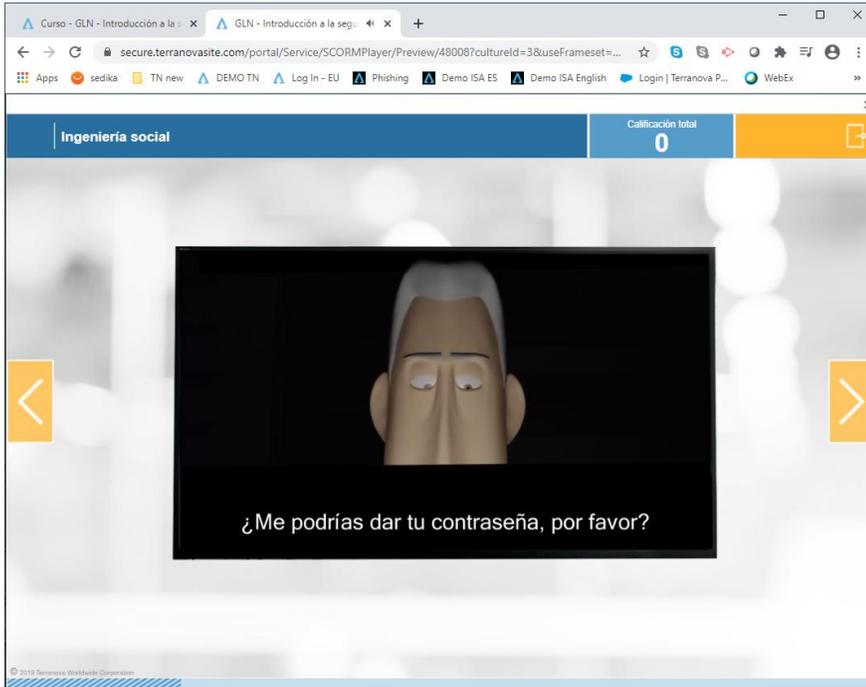
Temas de la capacitación para usuarios finales	
<ul style="list-style-type: none"> • Introducción a la seguridad de la información • Las contraseñas • Correo electrónico • Códigos maliciosos • Ciberestafa (phishing) • Usurpación de identidad • Ingeniería social • Redes sociales • Confidencialidad en la red • Protección de su computadora personal • Teléfonos inteligentes • Trabajo a distancia • Ransomware • Filtración de datos • Reporte de incidentes 	<ul style="list-style-type: none"> • Dispositivos móviles • Viajar con seguridad • Informática en la nube • Principio del escritorio limpio • Seguridad física • Control de acceso • Uso responsable de Internet • "Traiga su propio dispositivo" (TSPD) • Confidencialidad • Clasificación de la información • Ciclo de vida de la información • Propiedad intelectual • Protección de la información de tarjetas de crédito • Amenaza interna no intencionada • Correo electrónico empresarial comprometido

Metodología uniforme de cada tema de curso: Video, Introducción, actividades gamificación, mejores prácticas, actividad de aprendizaje, resumen y evaluación.

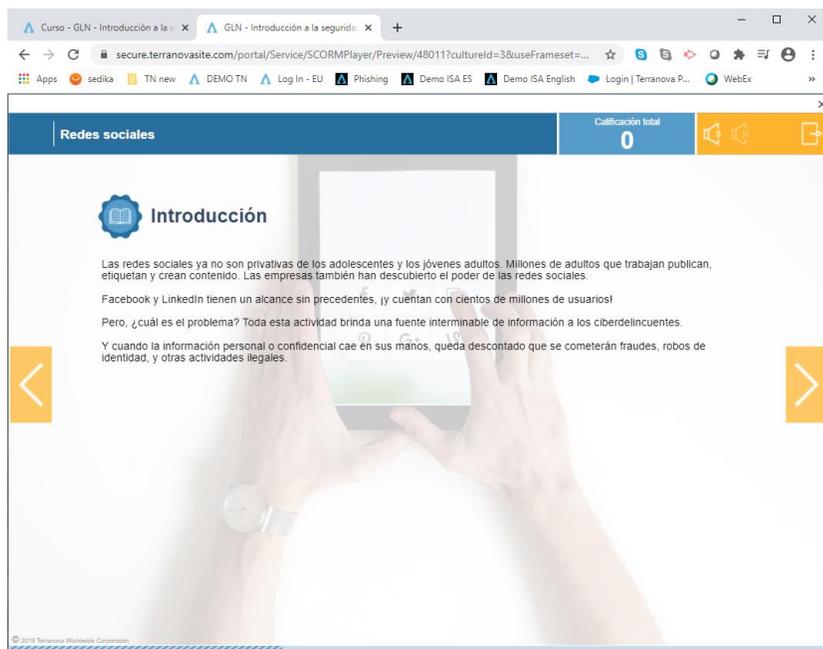
Video integrado en cada tema de usuario



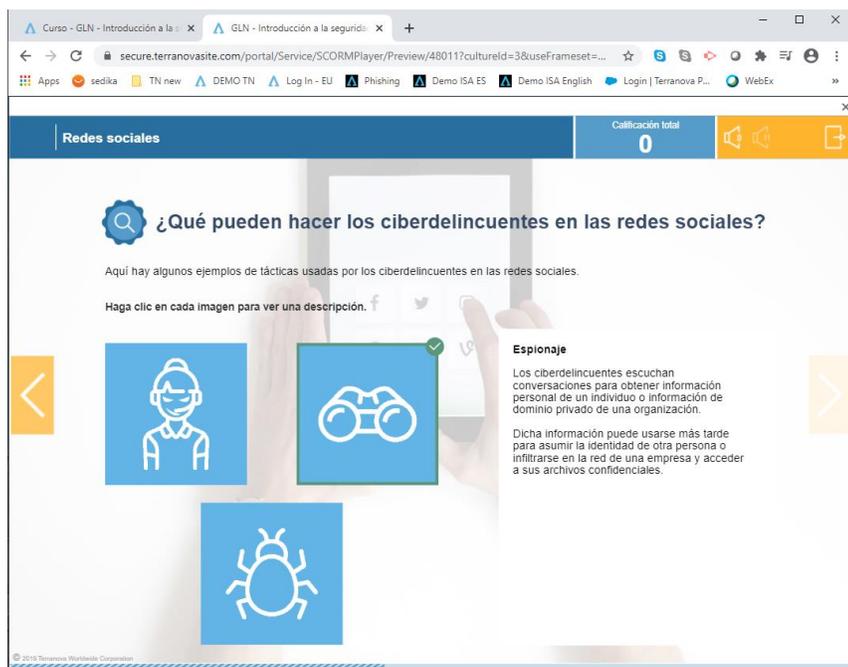
Clasificación: **Confidencial Externo**



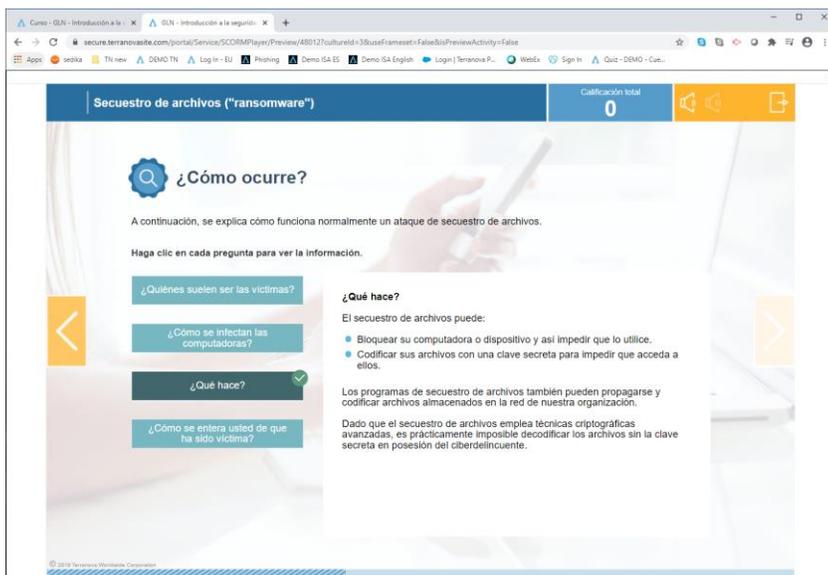
Clasificación: **Confidencial Externo**



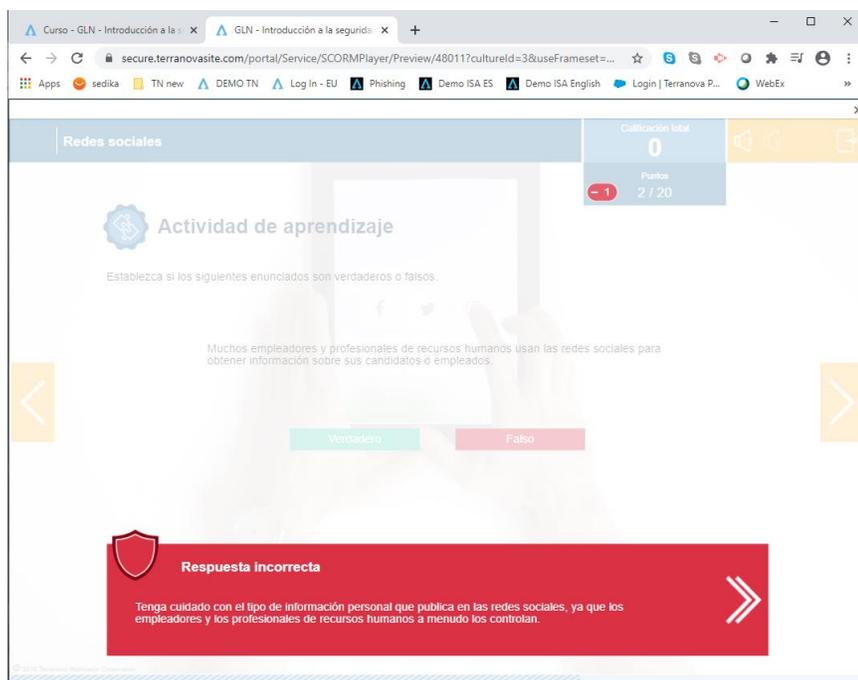
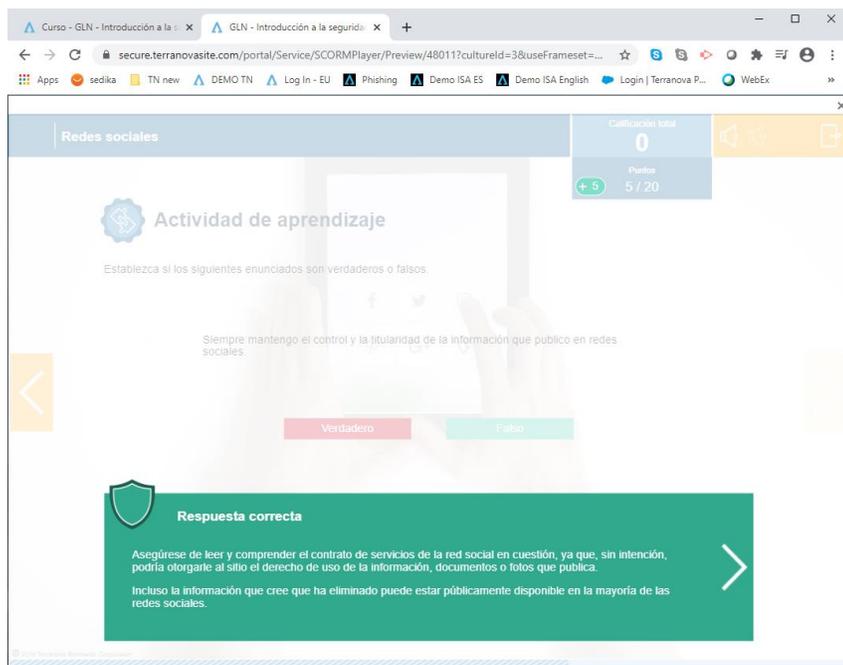
Actividades - Gamificación



Clasificación: **Confidencial Externo**



Clasificación: **Confidencial Externo**

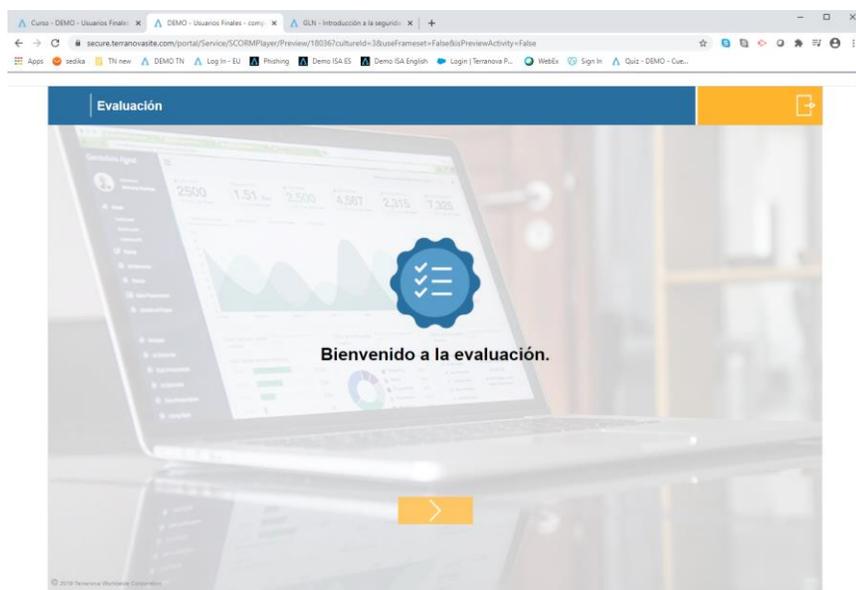


Clasificación: **Confidencial Externo**

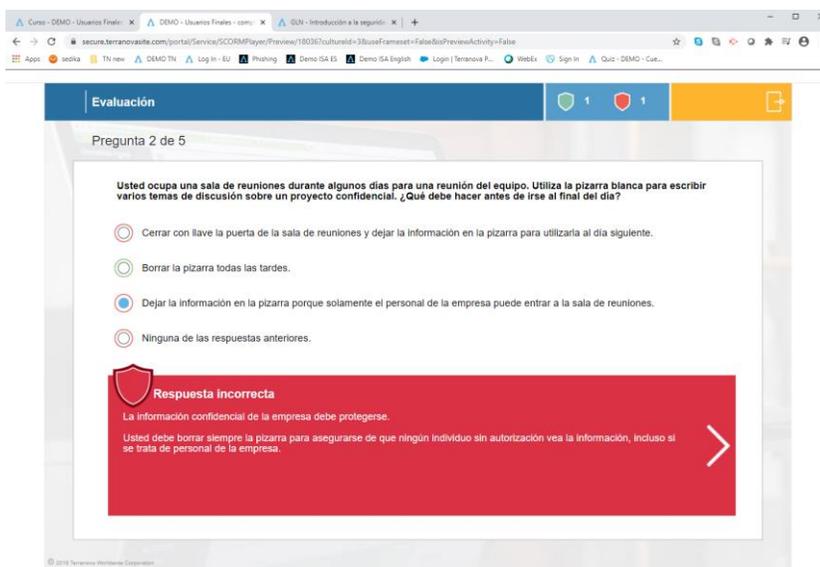
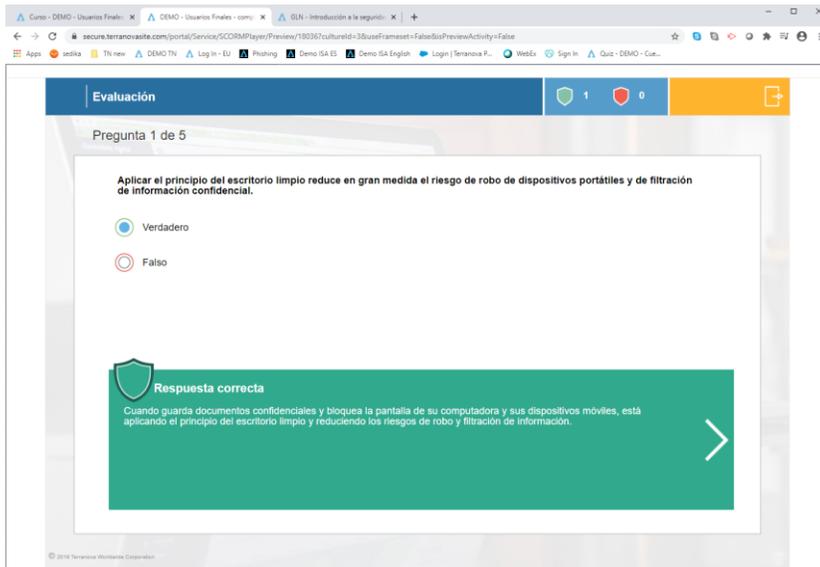
Mejores prácticas



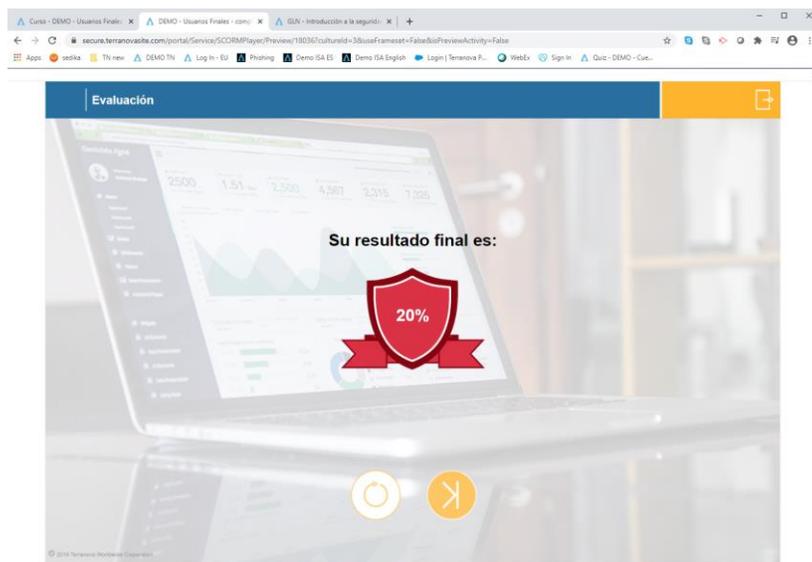
Evaluación



Clasificación: **Confidencial Externo**



Clasificación: **Confidencial Externo**



II. Capacitación en línea para gerentes y directores

Esta capacitación en línea está diseñada para educar a los gerentes y directores de DGII sobre la importancia de la seguridad en su ambiente de trabajo:

- Enfatizando el rol que juegan los directores en el programa de concientización sobre la seguridad; e
- Identificando los roles y las responsabilidades de los directores para asegurar las mejores prácticas en la organización.

Temas de la capacitación para gerentes y directores

- Introducción a la seguridad de la información
- Roles y responsabilidades en la seguridad de la información
- Componentes de un marco de gobierno de la seguridad de la información
- Seguridad de la información y tecnología
- Riesgos de seguridad planteados por las nuevas tecnologías y la movilidad

III. Capacitación en línea para desarrolladores de TI

Este curso está diseñado para educar a los desarrolladores de TI de DGII sobre la importancia de la seguridad en su ambiente de trabajo.

Temas de la capacitación para desarrolladores de TI

- Panorama general de seguridad de las aplicaciones
- Ataques típicos a las aplicaciones
- Desarrollo seguro
- Panorama general de la criptografía

Clasificación: **Confidencial Externo**



IV. Capacitación en línea para administradores de TI

Este curso está diseñado para educar a los administradores de red de TI de DGII sobre la importancia de la seguridad relacionada a las redes y a las bases de datos.

Temas de la capacitación para administradores de TI

- Panorama general sobre seguridad de las redes
- Ataques típicos a la red
- Protección de redes
- Protección de los depósitos de datos

V. Evaluación de diagnóstico pre y post capacitación

DGII tendrá la capacidad de generar evaluaciones previas al curso que brindan un panorama real de los conocimientos de los participantes en materia de seguridad de la información.

El cuestionario permite evaluar las fuerzas y debilidades de la organización para saber qué puntos deben mejorarse a través del programa de capacitación. La evaluación provee toda la información necesaria para desarrollar un análisis práctico de concientización sobre seguridad y así centrar la capacitación en las debilidades identificadas.

Un examen posterior permite evaluar el nivel de cambio en el comportamiento de los participantes.

- La evaluación está compuesta de 20 a 30 preguntas seleccionadas de un banco de 122 preguntas.
- DGII podrá seleccionar el tipo de preguntas que desee: verdadero o falso, de opción múltiple, entre otros.
- La evaluación presenta situaciones reales de comportamientos negligentes o inconscientes.
- DIGII podrá realizar su personalización, modificación o crear sus propias preguntas.

VI. Plataforma de gestión de concientización en seguridad (Learning management system)

Para garantizar la implementación eficiente de su programa de capacitación, este módulo de software administrativo le permitirá a DGII inscribir, administrar y monitorear los participantes. La plataforma es un complemento útil al programa de capacitación y permite realizar un mejor seguimiento y medir adecuadamente los resultados.

Funciones de la plataforma de gestión de concientización

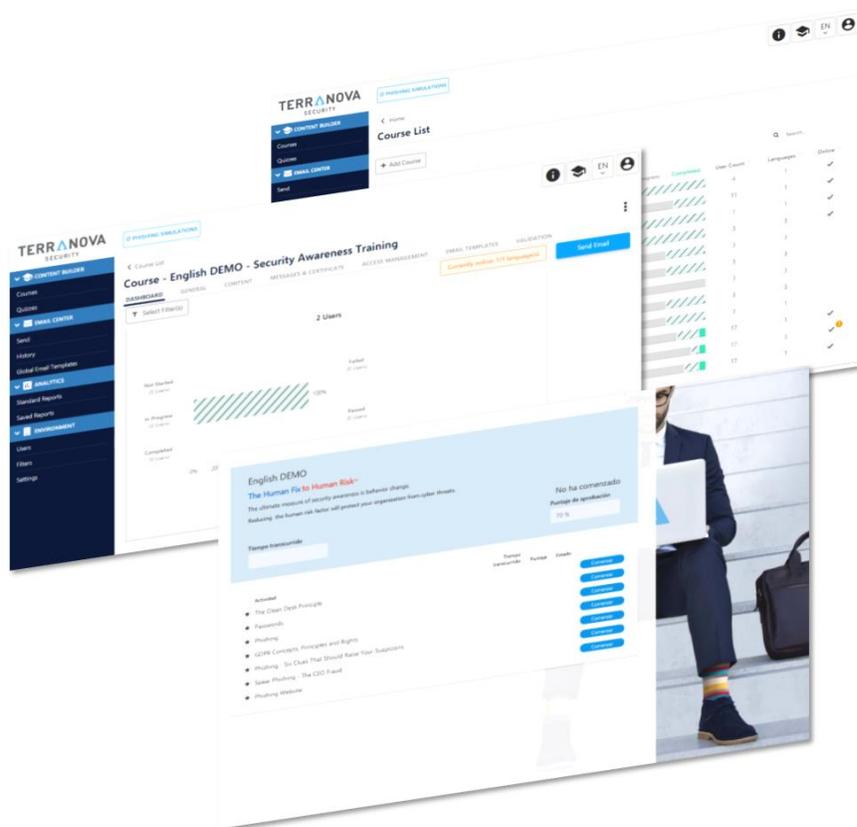
- Permite inscribir, gestionar y supervisar la participación y el rendimiento de los usuarios.

Clasificación: **Confidencial Externo**

- Permite observar el tiempo transcurrido, los módulos completados, la fecha, la hora, el estado de finalización, los resultados de la evaluación y los puntajes de aprobación.
- DGII podrá construir sus propios módulos de concientización en seguridad.
- Permite la gestión centralizada de todos los programas de aprendizaje en línea.
- Interfaz completamente personalizable a la imagen corporativa de DGII.
- DGII podrá enviar correos electrónicos y recordatorios automatizados.
- DGII tendrá la capacidad de generar informes detallados y paneles de control en tiempo real.
- Permite el acceso de inicio de sesión seguro para usuarios y administradores.
- DGII podrá realizar el seguimiento en tiempo real de las actividades de aprendizaje en línea.
- DGII podrá realizar la administración centralizada de todos los programas del aprendizaje en línea.

Beneficios del sistema alojado en forma remota

- No hay costos de servidores ni de software.
- No se requieren certificados SSL.
- No se requiere instalación por parte del departamento de TI.
- Las actualizaciones se realizan de forma automática.



Clasificación: **Confidencial Externo**

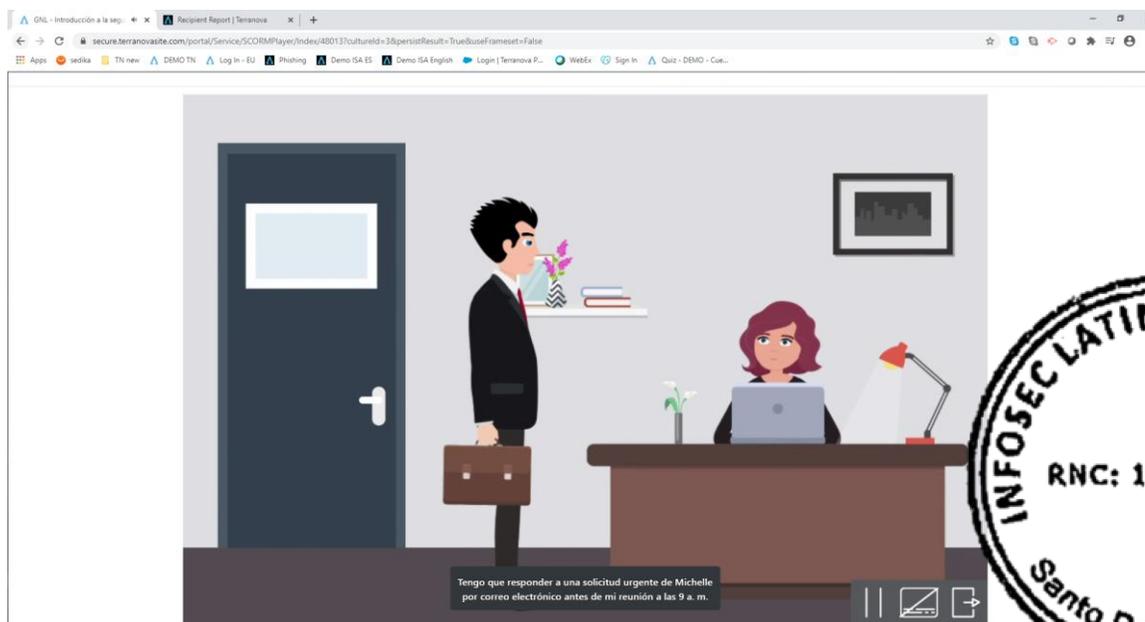
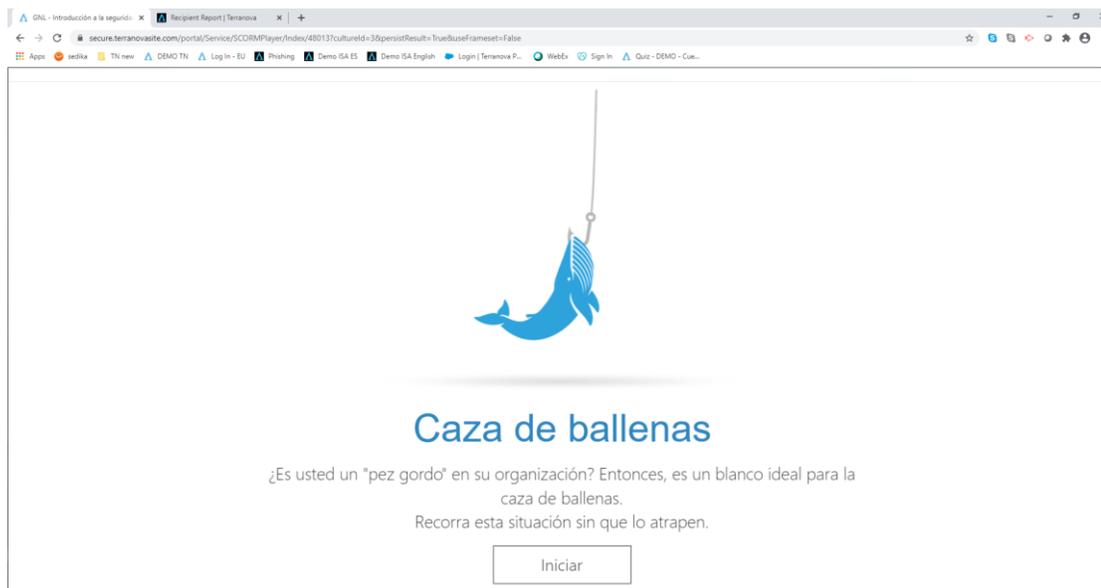
VII. Módulos de Micro y Nano aprendizaje

DGII estará en la capacidad de integrar los módulos de Mano y Micro aprendizaje en su programa de concientización en la seguridad de la información para aumentar la adquisición de conocimientos y el cambio de comportamiento. Este enfoque se puede utilizar para la capacitación justo a tiempo que se dirige a riesgos específicos y cumple con los objetivos de productividad.

Temas	
<p>Nanolearning Modules (1 a 2 min)</p> <ul style="list-style-type: none"> • Ransomware • Vishing • Phishing - 6 pistas • Phishing Website • Spear Phishing - fraude de CEO • Top Executive Phishing – “Whaling” • Smishing • Protección de la información confidencial • Detección de ataque cibernético • Prevención de violaciones de seguridad • Seguridad Wi-Fi • El robo de identidad • Ingeniería social • Ser consciente de la seguridad • Redes sociales • Spear Phishing • Amenaza interna • Anatomía de un ataque de phishing 	<p>Microlearning Modules (2 a 3 min)</p> <ul style="list-style-type: none"> • Vishing - Has ganado un premio • Web Phishing a través de motores de búsqueda • Phishing en el mercado masivo - Amazon • Phishing a través de SMS - "Smishing" • Spear Phishing • Phishing, Altos directivos - "caza de ballenas" • Suplantación de correo electrónico de nivel C • Informe de incidentes • Amenaza interna • Phishing en el mercado masivo • Malware: claves USB • Seguridad física • Ransomware - Archivos bloqueados • Smishing "Phishing a través de SMS"



Clasificación: **Confidencial Externo**



VIII. Herramientas de comunicación

Con el objetivo del comunicar con más fuerza el programa de entrenamiento y manejar un mensaje coherente a todo DGII, se propone diversas herramientas de comunicación. Con estas herramientas, las posibilidades de éxito de las campañas de entrenamiento en DGII serán muchos mayores, garantizando que a los usuarios les sea recordado de manera divertida e interesante su papel en ayudar a mantener segura su organización.

Clasificación: **Confidencial Externo**



1.1.1. Boletines (archivos PDF)

Ideales para utilizarlos a modo de recordatorio, los boletines de noticias concientizarán a sus usuarios sobre temas de actualidad a lo largo de todo el año. Los boletines están redactados por expertos en seguridad informática, y están disponibles en varios idiomas. Los boletines pueden enviarse por correo electrónico, descargarse a la sección "Seguridad de la Información" de la página Web DGII, enviarse por correo electrónico interno a los empleados, imprimirse en su revista interna, o distribuirse de la forma que se prefiera.

Los boletines se personalizan con el logo de DGII.

Son enviados en un PDF de tamaño carta (8.5x11 pulgadas). Los boletines pueden ser fotocopiados según sea necesario para su uso dentro de DGII.



Introducción a la seguridad de la información



¡SEA UN ESLABÓN FUERTE!

- Ayude a conservar la confidencialidad, integridad y disponibilidad de nuestra información respetando nuestras políticas y medidas de seguridad.
- Tenga en cuenta si la información que usted maneja es sensible y tome las medidas de precaución apropiadas.
- Nunca inhabilite ni eluda las medidas de seguridad existentes, dado que eso pondrá en riesgo la integridad de la información.
- Informe inmediatamente a su supervisor cualquier pérdida o robo de información sensible.

¿Ha visto las noticias? ¡Hubo otro incidente de ciberseguridad!

Si nos ocurriera a nosotros, podría haber un efecto negativo a largo plazo en nuestra organización y su reputación.

¿Qué puede hacer usted acerca de esto? Este es trabajo para nuestro especialista en seguridad de la información, ¿verdad?

¡No! Usted cumple un rol importante en la protección de la información sensible. De hecho, usted es el eslabón más importante en la cadena de seguridad de la información.

¡Piénselo dos veces!

Al mantenerse atento, usted ayuda a proteger nuestra información contra las amenazas que plantean los ciberdelincuentes y el error humano.

© TerraNova WWI Corporation, 2019

1.1.2. Posters (16 x 20 pulgadas, alta resolución, archivos PDF)

Los posters son una de las herramientas más eficaces para incrementar la concientización sobre seguridad en los empleados. Son la principal comunicación no electrónica utilizada para reforzar los mensajes en el plan de comunicación. A medida que se va desarrollando el programa, y en función de los temas tratados, los posters pueden colocarse en los lugares más frecuentados por los usuarios: corredores, salas comunes, salas de conferencia, oficinas, carteleras, etc.

Debido a que los posters están a la vista de todo aquel que ingresa a las instalaciones, tanto el personal interno como los visitantes podrán verlos.



Clasificación: **Confidencial Externo**



¿HA VISTO LAS NOTICIAS?
¡HUBO OTRO INCIDENTE DE
CIBERSEGURIDAD!

¡SEA UN ESLABÓN FUERTE!

- ☑ Ayude a conservar la confidencialidad, integridad y disponibilidad de nuestra información respetando nuestras políticas y medidas de seguridad.
- ☑ Tenga en cuenta si la información que usted maneja es sensible y tome las medidas de precaución apropiadas.
- ☑ Nunca inhabilite ni eluda las medidas de seguridad existentes, dado que eso pondrá en riesgo la integridad de la información.
- ☑ Informe inmediatamente a su supervisor cualquier pérdida o robo de información sensible.

© Terranova WW Corporation, 2019

1.1.3. Fondos de pantalla sobre la seguridad de la información

Los fondos de pantalla permiten transmitir los mensajes de seguridad directamente a sus empleados por medio de sus propias computadoras. Los mismos constituyen excelentes herramientas de concientización. Los mensajes difundidos y el aspecto visual concuerdan con el conjunto de herramientas de concientización (boletines de información, afiches, videos, etc.) que usted puede utilizar junto con los cursos en línea para obtener un programa excepcional de sensibilización a la seguridad de la información.

Los fondos de pantalla se personalizan con su logo y su eslogan sobre la seguridad de la información.

IX. Personalización de curso de usuarios finales y las herramientas de comunicación

Por medio de un proceso guiado de parametrización DGII estará en la capacidad de personalizar el texto y la inclusión de su logo en los 20 temas de curso para usuarios finales y en las herramientas de comunicación.

X. Project Manager Terranova

Durante el proceso de implementación DGII tendrá el acompañamiento de un gerente de proyecto.

Clasificación: **Confidencial Externo**

XI. Plataforma integrada de simulación de ciberestafa (Phishing)

Las simulaciones de ciberestafa (Phishing) son maneras rápidas de medir la vulnerabilidad de los colaboradores, al tiempo que incrementan la conciencia sobre la gravedad de los riesgos. Utilice nuestra poderosa plataforma para fortalecer sus destrezas de detección e inculcar las prácticas recomendadas de ciberseguridad a los miembros de su organización.

Características clave

- Navegación sencilla e intuitiva.
- Amplia selección de plantilla, páginas de destino y materiales de aprendizaje totalmente personalizables.
- Escenarios fácilmente personalizables y basados en las amenazas más comunes (ingreso de datos, archivos, adjuntos, ataques de doble correo (double barrel), secuestro de archivos, violación de su correo electrónico de negocios y más). Todo listo para su utilización.
- Actualizaciones mensuales de las funcionalidades y escenarios.
- Ciberestafa automatizada y aleatoria.
- Informes detallados y paneles de control en tiempo real.
- Contenido multilingüe y multicultural disponible en 40 idiomas.

Beneficios clave

- Cuantifique la vulnerabilidad de su organización
- Evalúe su nivel de exposición a distintos tipos de riesgos.
- Capacite a sus empleados en tiempo real sobre como identificar y reaccionar a los correos electrónicos fraudulentos.
- Cambie sus conductas e inculque una cultura de seguridad
- Elimine riesgos y convierta a su personal en su línea de defensa mas solida.
- Proporcione niveles crecientes de simulaciones.
- Proteja datos valiosos.
- Mitigue los riesgos relativos a cumplimiento, fraude y reputación.



DGII contará con la plataforma de simulación de phishing para realizar simulaciones ilimitadas durante la duración de la licencia.

Terranova realiza el lanzamiento de un escenario de ciberestafa nuevo mensualmente. En este momento la herramienta cuenta con 190 escenarios diferentes multilinguaje y en el idioma solicitado.

Panel de simulaciones de ciberestafa

El administrador de la plataforma podrá encontrar las características e información en tiempo real de las diferentes simulaciones realizadas.

El administrador podrá consultar la información de:

- Simulaciones en curso
- Escenarios de cada simulación
- Características de la simulación

Clasificación: **Confidencial Externo**

Dashboard

Currently active simulation list

There are no active simulations

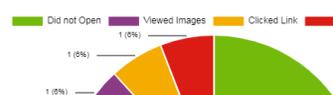
Active/Complete simulation statistics

Simulation: Sedika demo 01 Scenario: Sedika demo 01

[Export to PDF](#)

Summary		Simulation Details	
Scenario - Sedika demo 01 Show filters Total Recipients: 17 Email Processed: 17 Use Landing Page: Yes Use landing page form: Yes Use Feedback Page: Yes Use Attachment: No Use Double Barrel: No		Simulation: Sedika demo 01 Description: Type: Standard Status: Completed Use Outlook plugin: Yes Anonymous: No No. of recipients: 17 Delivery Start: 10/04/2017 13:54:00 (UTC-05:00) Delivery End: 10/04/2017 15:10:00 (UTC-05:00) Data Collect End: 10/11/2017 15:10:00 (UTC-05:00) Created by: Jaime Torres Last Modified by: Jaime Torres	

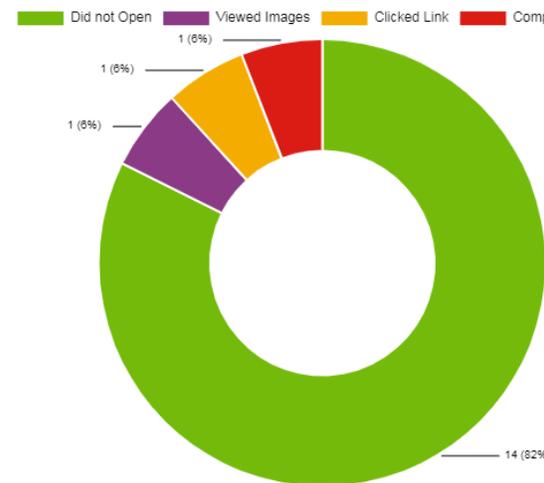
Recipient actions summary



Action	Count	Percentage
Did not Open	14	82%
Viewed Images	1	6%
Clicked Link	1	6%
Completed Form	1	6%

En esta parte, el administrador puede ver una gráfica que le indica las diferentes acciones que tomaron los usuarios y su porcentaje según las siguientes acciones: Los que no abrieron el mensaje, los que vieron imágenes, los que hicieron clic en el link y los que completaron el formulario.

Recipient actions summary



Action	Count	Percentage
Did not Open	14	82%
Viewed Images	1	6%
Clicked Link	1	6%
Completed Form	1	6%

No. of recipients:	17
Delivery Start:	10/04/2017 13:54:00 (UTC-05:00)
Delivery End:	10/04/2017 15:10:00 (UTC-05:00)
Data Collect End:	10/11/2017 15:10:00 (UTC-05:00)
Created by:	Jaime Torres
Last Modified by:	Jaime Torres



Clasificación: **Confidencial Externo**

Continuando con la información del *dashboard*, se muestra una gráfica de embudo, donde se muestran las diferentes acciones tomadas por los usuarios en una simulación: Los que informaron el correo electrónico sospechoso, los que no abrieron el correo electrónico, los que abrieron, pero no ejecutaron más acciones, los que vieron las imágenes, los que dieron clic en el enlace y los que completaron un formulario.

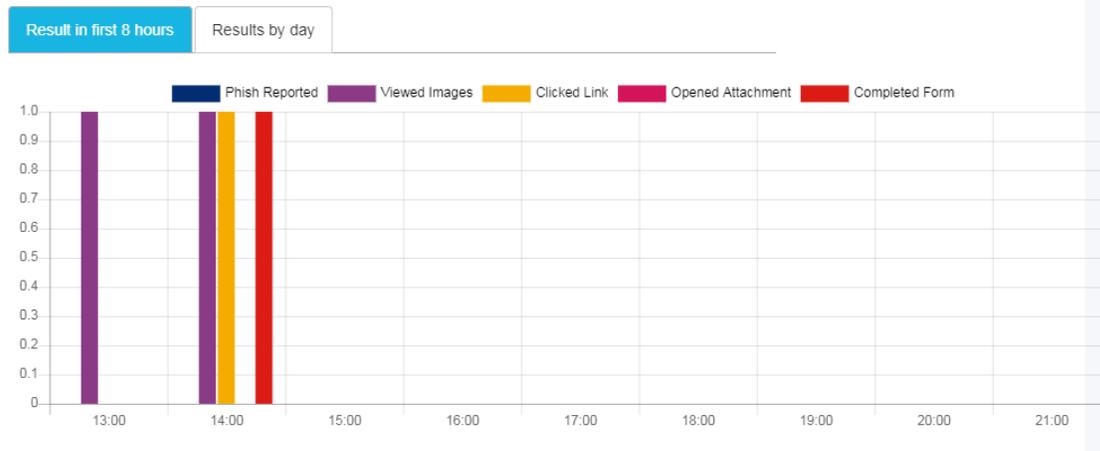
Total actions performed



Results over time

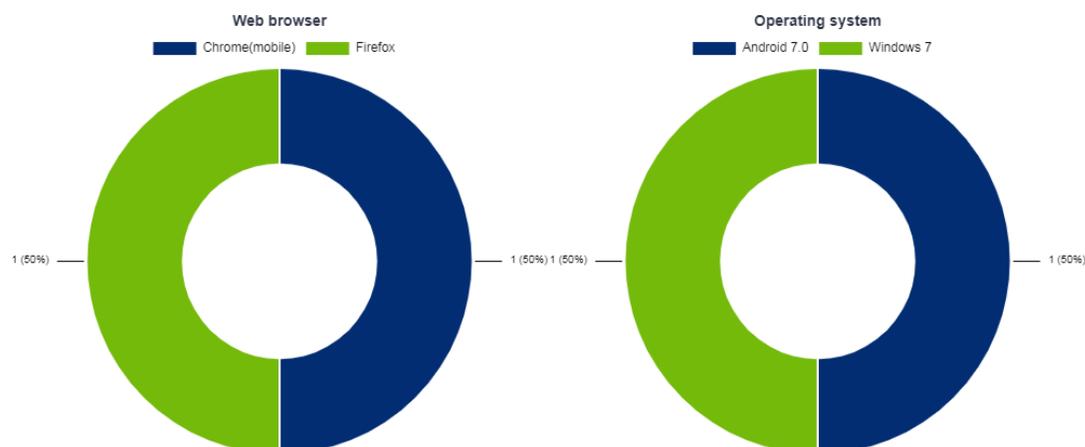
En esta sección se muestra las estadísticas generadas por los usuarios en las primeras 8 horas siguientes después de ser lanzada la simulación. Si el administrador requiere información más específica sobre la tendencia de la simulación en un periodo de tiempo más amplio puede generar un reporte en la sección de reportes de simulación de ciberestafa.

Results over time



Esta parte del informe se muestran los exploradores web y sistemas operativos que fueron utilizados por los usuarios que recibieron los correos electrónicos de ciberestafa.

Web browser and operating system



Finalmente, en la parte de listado de usuario, se muestran todas las estadísticas generadas por usuario en la simulación. Por ejemplo, se muestra información de hora y fecha de recibimiento del correo malicioso, lectura del mensaje, vista de imágenes, acción de clic en el link y si el usuario completó el formulario. Adicionalmente, se muestran los tiempos de duración que el usuario utilizó para tomar el entrenamiento justo a tiempo incluido al final de la página de retroalimentación de un escenario de simulación de ciberestafa.



Clasificación: **Confidencial Externo**

Simulation - Sedika demo 01

Recipient		Simulation details	
First Name	Jaime	Description	
Last Name	Torres	Delivery Start	10/04/2017 13:54:00 (UTC-05:00)
Email	jaime.torres@sedika.com	Delivery End	10/04/2017 15:10:00 (UTC-05:00)
Language	Español (LATAM)	Data Collect End	10/11/2017 15:10:00 (UTC-05:00)
Timezone	SA Pacific Standard Time		
Active	Yes		
Test		Created by	
Ciudad	Santiago	Last Modified by	
Departamento	diseño		
Sucursal	place des arts		

Recipient Events				
Show	10	entries	Q	<input type="text"/>
Scenario ^	Date v	Event d	IP Address d	User Agent d
Sedika demo 01	10/04/2017 14:10:54 (UTC-05:00)	Education Displayed (Education time: 00:00:00)	104.221.93.8	Mozilla/5.0 (Windows NT 6.1; WOW64; rv:56.0) Gecko/20100101 Firefox/56.0
Sedika demo 01	10/04/2017 14:10:53 (UTC-05:00)	Email Form Completed (Education time: 00:01:00)	104.221.93.8	Mozilla/5.0 (Windows NT 6.1; WOW64; rv:56.0) Gecko/20100101 Firefox/56.0
Sedika demo 01	10/04/2017 14:10:31 (UTC-05:00)	Email Link Clicked	104.221.93.8	Mozilla/5.0 (Windows NT 6.1; WOW64; rv:56.0) Gecko/20100101 Firefox/56.0
Sedika demo 01	10/04/2017 14:09:25 (UTC-05:00)	Email Image Downloaded		
Sedika demo 01	10/04/2017 13:59:05 (UTC-05:00)	Email Sent		

Showing 1 to 5 of 5 entries

Previous **1** Next

XII. Colaboración para campañas de Phishing

DGII tendrá el acompañamiento de parte de SISAP.



Clasificación: **Confidencial Externo**



May 16, 2023

To whom it may concern:

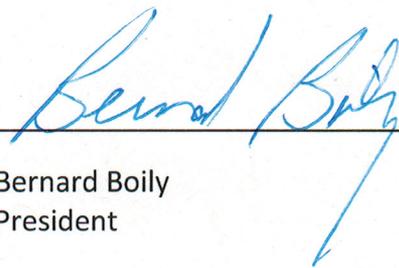
SUBJECT: Authorization to provide Terranova Security Solution courses

Sedika Technologies is the sole authorized distributor of the Terranova Security solutions and services in Latin America.

I hereby would like to confirm that Sistemas Aplicativos, S.A. (SISAP), is the only official reseller authorized to provide Terranova's portfolio of training courses in Dominican Republic.

Terranova Security Solution offers training and comprehensive communication tools that aim to improve behaviors in information security, protect personal information, and help support other aspects related to compliance.

We would like to take this opportunity to greet you and send you our best regards,



Bernard Boily
President

