

CONCIENCIACIÓN A SERVIDORES PÚBLICOS

Objetivo de la Campaña:

La Campaña de Estrategia Comunicacional del mes de abril tuvo como propósito brindar las informaciones de valor que sirvan para fomentar las buenas prácticas que desarrollan la madurez y resiliencia de las instituciones del Estado, garantizando los servicios digitales provistos a la ciudadanía, al margen de asegurar un entorno favorable que permita resguardar la privacidad, disponibilidad e integridad de las informaciones críticas de las entidades y de los ciudadanos que reciben los servicios.



**RESULTADOS
DE LA CAMPAÑA
CIBERSEGURIDAD PARA
EL SECTOR PÚBLICO**

INSTAGRAM, FACEBOOK Y X



INSTAGRAM

Estadísticas de la publicación



41



0



5



7

Resumen ⓘ

Cuentas alcanzadas	1.001
Cuentas que interactuaron	49
Actividad del perfil	0

Alcance ⓘ



INSTAGRAM – FEED

1

#CiberseguridadparaelSectorPúblico



¿Y tú, formas parte del Equipo de concienciación en ciberseguridad?

DESLIZA →



CNCS CENTRO NACIONAL DE CIBERSEGURIDAD REPUBLICA DOMINICANA

Estadísticas de la publicación



73



0



4



14

Resumen ⓘ

Cuentas alcanzadas	1.053
Cuentas que interactuaron	82
Actividad del perfil	14

Alcance ⓘ



INSTAGRAM - FEED

2

¿Y tú, ya formas parte del equipo de concienciación en ciberseguridad?

CIBERSEGURIDAD PARA EL SECTOR PÚBLICO - PRIVADO



Desliza para conocer los roles claves en un equipo de concienciación en ciberseguridad

#CiberseguridadParaElSectorPúblico



CNCS CENTRO NACIONAL DE CIBERSEGURIDAD REPÚBLICA DOMINICANA

Estadísticas de la publicación



Resumen ⓘ

Cuentas alcanzadas	1.271
Cuentas que interactuaron	59
Actividad del perfil	3

Alcance ⓘ



INSTAGRAM – FEED

3



Estadísticas de reels

1.171 24 0 1 1

Resumen ⓘ

Cuentas alcanzadas	907
Interacciones del reel	26
Actividad del perfil	0

Alcance ⓘ

907
Cuentas alcanzadas

23,4%
Seguidores



76,6%
No seguidores

INSTAGRAM - FEED

4



Estadísticas de la publicación

24

0

3

3

Resumen ⓘ

Cuentas alcanzadas	864
Cuentas que interactuaron	27
Actividad del perfil	1

Alcance ⓘ



INSTAGRAM - FEED

5

#CiberseguridadparaelSectorPúblico

¿Qué puedes hacer para
mejorar tu **ciberseguridad**?

 CNCS



Estadísticas de la publicación

35 0 3 2

Resumen ⓘ

Cuentas alcanzadas	1.253
Cuentas que interactuaron	--
Actividad del perfil	--

Alcance ⓘ



INSTAGRAM - FEED

¿QUÉ PUEDES HACER
PARA MEJORAR TU
CIBERSEGURIDAD?



Ciberseguridad para el Sector Público

COLABORACIÓN

Estadísticas de la publicación



47



6



5



3

Resumen ⓘ

Cuentas alcanzadas	972
Cuentas que interactuaron	--
Actividad del perfil	--

Alcance ⓘ



INSTAGRAM - FEED

7

TELETRABAJO Y CIBERSEGURIDAD CONSEJOS



CNCS
CENTRO NACIONAL
DE CIBERSEGURIDAD
REPUBLICA DOMINICANA

Ciberseguridad para el Sector Público

COLABORACIÓN

Estadísticas de la publicación

19

1

2

2

Resumen ⓘ

Cuentas alcanzadas	486
Cuentas que interactuaron	--
Actividad del perfil	--

Alcance ⓘ



INSTAGRAM – FEED

8

DIDA
COMPROMETIDOS
CON TU BIENESTAR
Orienta. Defiende. Informa.

GOBIERNO DE LA
REPÚBLICA DOMINICANA
DIRECCIÓN GENERAL
DE INFORMACIÓN Y DEFENSA DE LOS AFILIADOS
A LA SEGURIDAD SOCIAL
(DIDA)

Asegúrese de que su entidad
es **“Ciberresiliente”**
Ciberseguridad para el
Sector Público

CNCS
CENTRO NACIONAL
DE CIBERSEGURIDAD
REPÚBLICA DOMINICANA

COLABORACIÓN

Estadísticas de la publicación



21



0



3



3

Resumen ⓘ

Cuentas alcanzadas	837
Cuentas que interactuaron	--
Actividad del perfil	--

Alcance ⓘ



INSTAGRAM - FEED

9

¿CÓMO PROTEGERTE CONTRA
LOS ATAQUES **BEC** (*BUSINESS
EMAIL COMPROMISE*)?



CNCS
CENTRO NACIONAL
DE CIBERSEGURIDAD
REPUBLICA DOMINICANA

Ciberseguridad para el Sector Público

COLABORACIÓN

Estadísticas de la publicación

19

0

2

2

Resumen ⓘ

Cuentas alcanzadas	592
Cuentas que interactuaron	--
Actividad del perfil	--

Alcance ⓘ



INSTAGRAM – FEED

10

DIDA
COMPROMETIDOS
CON TU BIENESTAR
Orienta. Defiende. Informa.

GOBIERNO DE LA
REPÚBLICA DOMINICANA
DIRECCIÓN GENERAL
DE INFORMACIÓN Y DEFENSA DE LOS AFILIADOS
A LA SEGURIDAD SOCIAL
(DIDA)

¿Por qué es importante asegurar su acceso y ambiente a sistemas y datos?

Ciberseguridad para el
Sector Público

Asegurar el acceso y proteger la confidencialidad

CNCS
CENTRO NACIONAL
DE CIBERSEGURIDAD
REPÚBLICA DOMINICANA

COLABORACIÓN

Estadísticas de la publicación



41



1



16



5

Resumen ⓘ

Cuentas alcanzadas	1.341
Cuentas que interactuaron	--
Actividad del perfil	--

Alcance ⓘ



INSTAGRAM - FEED

11

¿CÓMO PUEDES
ASEGURARTE DE
QUE TU ENTIDAD ES
CIBERRESILIENTE?



CNCS
CENTRO NACIONAL
DE CIBERSEGURIDAD
REPUBLICA DOMINICANA

Ciberseguridad para el Sector Público

COLABORACIÓN

Estadísticas de la publicación

29 0 2 2

Resumen ⓘ

Cuentas alcanzadas	581
Cuentas que interactuaron	--
Actividad del perfil	--

Alcance ⓘ



INSTAGRAM – FEED

12

DIDA
COMPROMETIDOS CON TU BIENESTAR
Orienta. Defiende. Informa.

GOBIERNO DE LA REPÚBLICA DOMINICANA
DIRECCIÓN GENERAL DE INFORMACIÓN Y DEFENSA DE LOS AFILIADOS A LA SEGURIDAD SOCIAL (DIDA)

Protegiendo tus **Activos Digitales**: Consejos de **Ciberseguridad** para el **Sector Público**

Protegiendo tus activos Digitales: Consejos de Ciberseguridad

CNCS
CENTRO NACIONAL DE CIBERSEGURIDAD
REPÚBLICA DOMINICANA

COLABORACIÓN

Estadísticas de reels

675 32 0 1 2

Resumen ⓘ

Cuentas alcanzadas	471
Interacciones del reel	35
Actividad del perfil	--

Alcance ⓘ



INSTAGRAM - FEED

13



COLABORACIÓN

Estadísticas de la publicación



Resumen ⓘ

Cuentas alcanzadas	1.294
Cuentas que interactuaron	--
Actividad del perfil	--

Alcance ⓘ



INSTAGRAM - FEED

14

¿POR QUÉ ES IMPORTANTE
ASEGURAR SU ACCESO Y
AMBIENTE A SISTEMAS Y
DATOS?



CNCS
CENTRO NACIONAL
DE CIBERSEGURIDAD
REPÚBLICA DOMINICANA

Ciberseguridad para el Sector Público

COLABORACIÓN

Estadísticas de la publicación

67

3

13

4

Resumen ⓘ

Cuentas alcanzadas	1.573
Cuentas que interactuaron	--
Actividad del perfil	--

Alcance ⓘ



INSTAGRAM - FEED

15

PROTEGIENDO TUS ACTIVOS DIGITALES: CONSEJOS DE CIBERSEGURIDAD



CNCS
CENTRO NACIONAL
DE CIBERSEGURIDAD
REPÚBLICA DOMINICANA

Ciberseguridad para el Sector Público

COLABORACIÓN

Estadísticas de la publicación

56 1 1 3

Resumen ⓘ

Cuentas alcanzadas	759
Cuentas que interactuaron	--
Actividad del perfil	--

Alcance ⓘ



INSTAGRAM – FEED

16

#CiberseguridadparaelSectorPúblico



¿Por qué es importante educar a tus colaboradores en ciberseguridad?

DESLIZA →



COLABORACIÓN

Estadísticas de la publicación



60



1



5



12

Resumen ⓘ

Cuentas alcanzadas	1.518
Cuentas que interactuaron	--
Actividad del perfil	--

Alcance ⓘ



INSTAGRAM – FEED

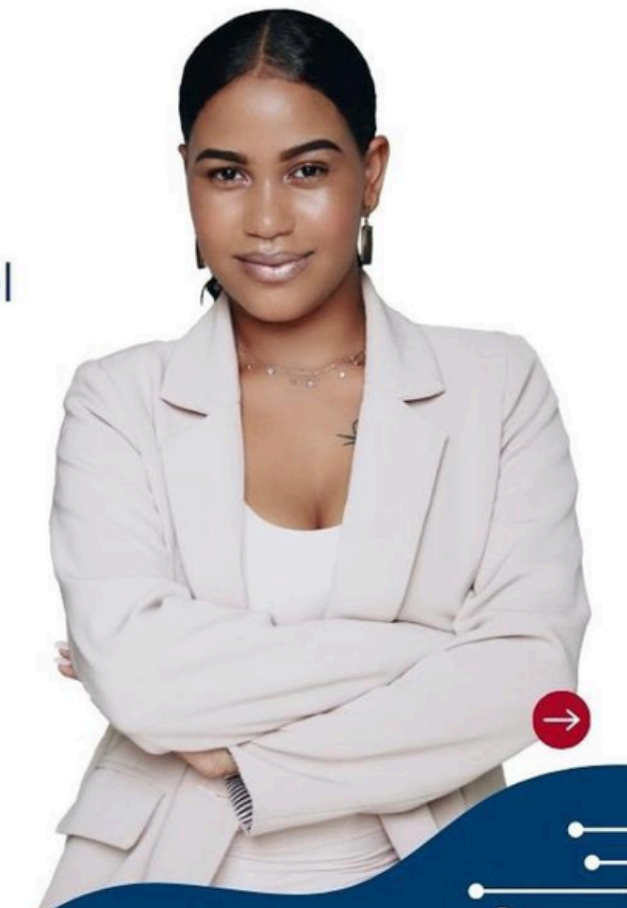
17



¿Y tú, formas parte del Equipo de concienciación en ciberseguridad?

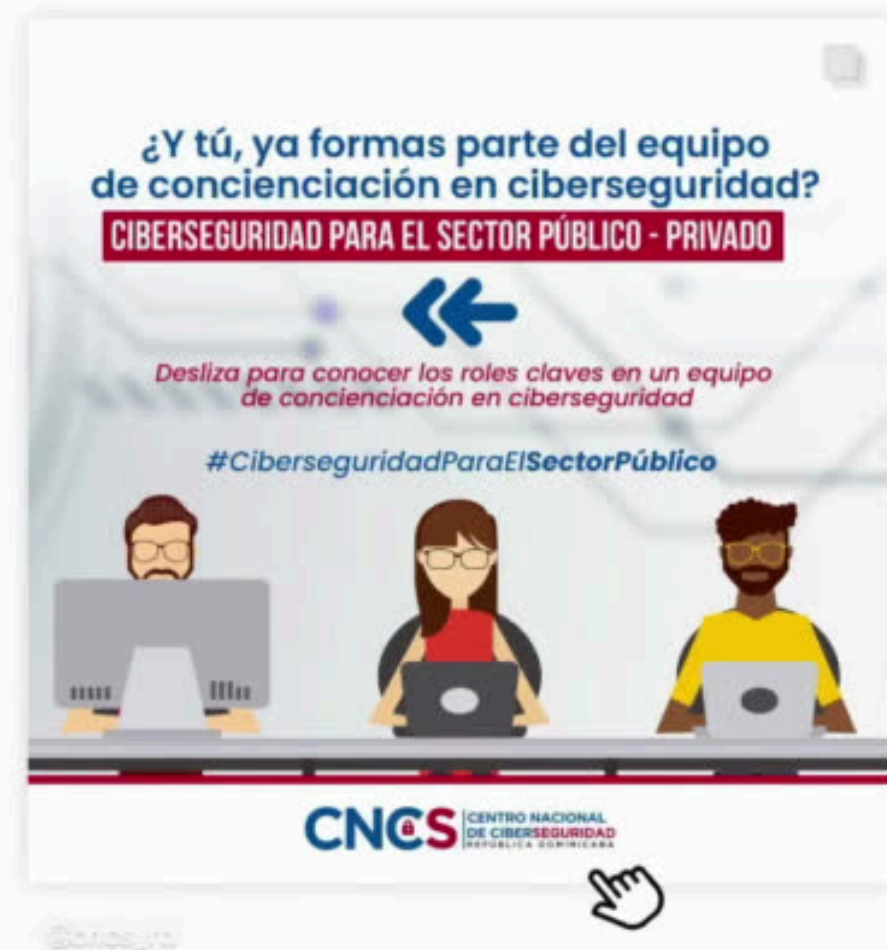
Ciberseguridad para el Sector Público

Ciberseguridad para el Sector Público Roles en el Equipo de Concienciación en Ciberseguridad Implementar una estrategia efectiva de concienciación en ciberseguridad requiere la colaboración de diversos roles especializados.



COLABORACIÓN

INSTAGRAM - HISTORIAS PROPIAS



134 CUENTAS ALCANZADAS

INSTAGRAM – HISTORIAS COMPARTIDAS



CIBERSEGURIDAD PARA EL SECTOR PÚBLICO

¿Por qué es importante educar a tus colaboradores en ciberseguridad?

Los colaboradores juegan un papel crucial en la ciberseguridad de cualquier entidad. ¡Aquí te explicamos por qué es importante concienciarlos sobre los riesgos!

1. Amenazas internas

Los colaboradores pueden ser vulnerables a tácticas de ingeniería social utilizadas por los ciberdelincuentes para obtener información confidencial o instalar software malicioso.

308 CUENTAS ALCANZADAS

2. Importancia de la capacitación

Capacitar a los colaboradores en ciberseguridad los convierte en la primera línea de defensa contra amenazas cibernéticas. Esto les permite reconocer y evitar trampas como el phishing.

3. Ingeniería social

La ingeniería social explota el comportamiento humano para obtener información confidencial. El phishing es un ejemplo común de esta táctica.



225 CUENTAS ALCANZADAS

inapagob



@inapagob

346 CUENTAS ALCANZADAS

INSTAGRAM - HISTORIAS COMPARTIDAS

DIDA
COMPROMETIDOS CON TU BIENESTAR
Orienta, Defiende, Informa.

GOBIERNO DE LA REPÚBLICA DOMINICANA
DIRECCIÓN GENERAL DE INFORMACIÓN Y DEFENSA DE LOS AFILIADOS A LA SEGURIDAD SOCIAL (DIDA)

¿Y tú, formas parte del Equipo de concienciación en ciberseguridad?

Ciberseguridad para el Sector Público

Ciberseguridad para el Sector Público Roles en el Equipo de Concienciación en Ciberseguridad Implementar una estrategia efectiva de concienciación en ciberseguridad requiere la colaboración de diversos roles especializados.

CNCs
CENTRO NACIONAL DE CIBERSEGURIDAD
REPÚBLICA DOMINICANA

404 CUENTAS ALCANZADAS

CNCs
CENTRO NACIONAL DE CIBERSEGURIDAD
REPÚBLICA DOMINICANA

Aquí te presentamos los roles clave:

- 1. Responsable de Ciberseguridad:** Dirige el desarrollo e implementación del programa de seguridad de la información.
- 2. Responsable de Comunicación:** Transmite conocimientos y difunde logros en ciberseguridad entre los empleados.
- 3. Responsable de Tecnología de Sistemas de Información:** Desarrolla, implementa y mantiene sistemas para garantizar la continuidad operativa.
- 4. Responsable del Equipo de Respuesta a Incidentes:** Previene, detecta y responde a incidentes de seguridad en sistemas informáticos.
- 5. Responsable de Recursos Humanos:** Diseña funciones, responsabilidades y requisitos de habilidades para los puestos de trabajo.

DIDA
COMPROMETIDOS CON TU BIENESTAR
Orienta, Defiende, Informa.

GOBIERNO DE LA REPÚBLICA DOMINICANA
DIRECCIÓN GENERAL DE INFORMACIÓN Y DEFENSA DE LOS AFILIADOS A LA SEGURIDAD SOCIAL (DIDA)

365 CUENTAS ALCANZADAS

DIDA
COMPROMETIDOS CON TU BIENESTAR
Orienta, Defiende, Informa.

GOBIERNO DE LA REPÚBLICA DOMINICANA
DIRECCIÓN GENERAL DE INFORMACIÓN Y DEFENSA DE LOS AFILIADOS A LA SEGURIDAD SOCIAL (DIDA)

Buenas prácticas para fortalecer la Ciberseguridad en tu entidad



Ciberseguridad para el Sector Público

Recomendaciones para Mejorar la Ciberseguridad para los colaboradores.

CNCs
CENTRO NACIONAL DE CIBERSEGURIDAD
REPÚBLICA DOMINICANA

199 CUENTAS ALCANZADAS

INSTAGRAM - HISTORIAS COMPARTIDAS




GOBIERNO DE LA
REPÚBLICA DOMINICANA
DIRECCIÓN GENERAL
DE INFORMACIÓN Y DEFENSA DE LOS AFILIADOS
A LA SEGURIDAD SOCIAL
(DIDA)

COMPROMETIDOS
CON TU BIENESTAR
Orienta. Defiende. Informa.



Aquí te compartimos algunas prácticas recomendadas para fortalecer la ciberseguridad en tu entidad:

- 1. Roles y Responsabilidades Claras:**
Asegúrate de que tus colaboradores entiendan claramente sus roles y responsabilidades en relación con la ciberseguridad.
- 2. Establece un Plan de Trabajo en Ciberseguridad:**
 - Proporciona formación en ciberseguridad a tus colaboradores para crear conciencia.
 - Toma medidas para proteger tus activos de información, incluyendo hardware, software y datos.
 - Asegura el acceso y el entorno para minimizar la entrada no autorizada.
 - Implementa planes para mantener la ciberresiliencia de tu entidad.
- 3. Identifica Riesgos Potenciales y Evalúa las Medidas Implementadas:**
 - Identifica posibles riesgos de ciberseguridad en el entorno de tu entidad.
 - Evalúa si las medidas de ciberseguridad implementadas son adecuadas para proteger tu entidad.



CNCS
CENTRO NACIONAL
DE CIBERSEGURIDAD
REPÚBLICA DOMINICANA

185 CUENTAS ALCANZADAS




GOBIERNO DE LA
REPÚBLICA DOMINICANA
DIRECCIÓN GENERAL
DE INFORMACIÓN Y DEFENSA DE LOS AFILIADOS
A LA SEGURIDAD SOCIAL
(DIDA)

COMPROMETIDOS
CON TU BIENESTAR
Orienta. Defiende. Informa.

¿Por qué es importante educar a tus colaboradores en ciberseguridad?



Ciberseguridad para el Sector Público

Concienciación en Ciberseguridad para tus colaboradores



CNCS
CENTRO NACIONAL
DE CIBERSEGURIDAD
REPÚBLICA DOMINICANA

155 CUENTAS ALCANZADAS




GOBIERNO DE LA
REPÚBLICA DOMINICANA
DIRECCIÓN GENERAL
DE INFORMACIÓN Y DEFENSA DE LOS AFILIADOS
A LA SEGURIDAD SOCIAL
(DIDA)

COMPROMETIDOS
CON TU BIENESTAR
Orienta. Defiende. Informa.

Aquí te compartimos algunas prácticas recomendadas para fortalecer la ciberseguridad en tu entidad:

Los colaboradores juegan un papel crucial en la ciberseguridad de cualquier entidad.

- 1. Amenazas Internas:** Los colaboradores pueden ser vulnerables a tácticas de ingeniería social utilizadas por los ciberdelincuentes para obtener información confidencial o instalar software malicioso.
- 2. Importancia de la Capacitación:** Capacitar a los colaboradores en ciberseguridad los convierte en la primera línea de defensa contra amenazas cibernéticas. Esto les permite reconocer y evitar trampas como el phishing.
- 3. Ingeniería Social:** La ingeniería social explota el comportamiento humano para obtener información confidencial. El phishing es un ejemplo común de esta táctica.



CNCS
CENTRO NACIONAL
DE CIBERSEGURIDAD
REPÚBLICA DOMINICANA

139 CUENTAS ALCANZADAS

INSTAGRAM – HISTORIAS COMPARTIDAS



CIBERSEGURIDAD PARA EL SECTOR PÚBLICO

¿Qué puedes hacer para mejorar tu ciberseguridad?



1. Liderazgo en ciberseguridad:

- Asegúrate de que la ciberseguridad sea una prioridad desde la alta dirección.
- Mantente actualizado sobre los desarrollos en ciberseguridad y apoya las iniciativas de seguridad.
- Establece reglas y directrices claras sobre ciberseguridad para tus colaboradores.

205 CUENTAS ALCANZADAS

2. Capacitación y concientización:

- Implementa un programa de capacitación en ciberseguridad para todos tus colaboradores.
- Personaliza el programa según las necesidades de tu entidad y los diferentes roles.
- Asegúrate de que todos comprendan su importancia como primera línea de defensa contra ataques cibernéticos.

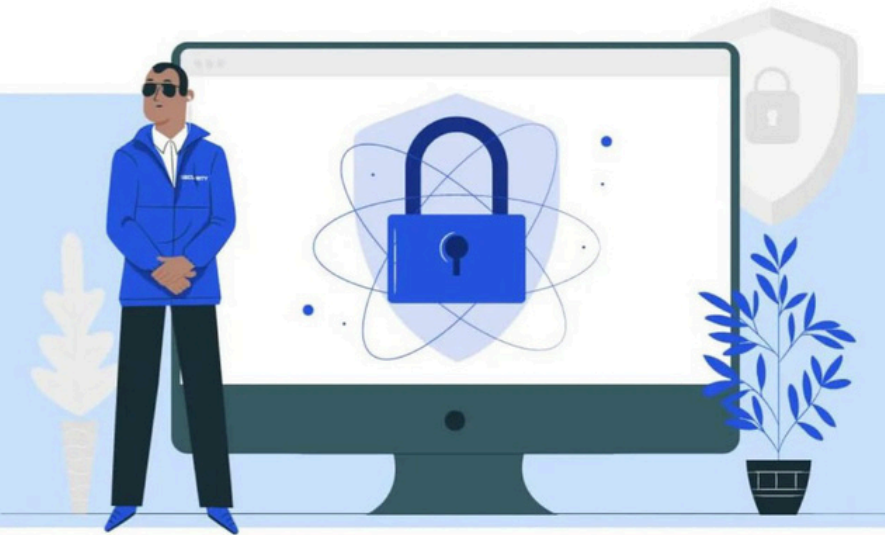


187 CUENTAS ALCANZADAS



CIBERSEGURIDAD PARA EL SECTOR PÚBLICO

**Colaboradores,
¡cuidado con los ataques BEC!**



El BEC es un tipo de ataque de phishing altamente sofisticado que tiene como objetivo engañar a los colaboradores para que realicen acciones dañinas, como transferencias de fondos o divulgación de información confidencial. Aquí hay algunos tipos de ataques BEC que podrían afectar especialmente a los colaboradores:

- Suplantación de identidad.
- Fraude de facturas.
- Cambio de información de pago.

123 CUENTAS ALCANZADAS

INSTAGRAM - HISTORIAS COMPARTIDAS

DIDA
COMPROMETIDOS CON TU BIENESTAR
Ordena. Defiende. Informa.

GOBIERNO DE LA REPÚBLICA DOMINICANA
DIRECCIÓN GENERAL DE INFORMACIÓN Y DEFENSA DE LOS AFILIADOS A LA SEGURIDAD SOCIAL (DIDA)

Protegiendo tus **Activos Digitales**: Consejos de **Ciberseguridad** para el **Sector Público**

Protegiendo tus **activos Digitales**:
Consejos de Ciberseguridad

CNCS
CENTRO NACIONAL DE CIBERSEGURIDAD
REPÚBLICA DOMINICANA

122 CUENTAS ALCANZADAS

DIDA
COMPROMETIDOS CON TU BIENESTAR
Ordena. Defiende. Informa.

GOBIERNO DE LA REPÚBLICA DOMINICANA
DIRECCIÓN GENERAL DE INFORMACIÓN Y DEFENSA DE LOS AFILIADOS A LA SEGURIDAD SOCIAL (DIDA)

Los activos digitales de información son vitales para el funcionamiento diario de tu entidad. Protegerlos contra ciberataques es fundamental para prevenir y minimizar daños. Aquí tienes algunas recomendaciones clave:

- 1. Mantén tus sistemas y software actualizados:**
Evita el uso de sistemas obsoletos y software desactualizados. Garantiza actualizaciones periódicas para mantener tus sistemas seguros y protegidos contra vulnerabilidades.
- 2. Realiza copias de seguridad periódicas:**
Asegúrate de que se realicen copias de seguridad de tus datos con regularidad. Identifica y respalda fuera de línea los sistemas y datos críticos para tu entidad, en una ubicación separada de tus sistemas principales.
- 3. Considera un proveedor de TI:**
Designa a un proveedor de TI para abordar las necesidades de ciberseguridad de tu entidad. Este proveedor puede desarrollar políticas y procedimientos de ciberseguridad, así como implementar y gestionar controles de seguridad para proteger tus activos digitales.

CNCS
CENTRO NACIONAL DE CIBERSEGURIDAD
REPÚBLICA DOMINICANA

108 CUENTAS ALCANZADAS

Planifi
Impulsa y planifica la interrupción de las operaciones diarias causadas por incidentes de ciberseguridad/TI.

Desarrolla un Plan de Respuesta a Incidentes formal que contenga pautas, roles y responsabilidades definidas para abordar

eted_rd_ **CNCS**

158 CUENTAS ALCANZADAS

INSTAGRAM - HISTORIAS COMPARTIDAS

DIDA
COMPROMETIDOS CON TU BIENESTAR
Orienta, Defiende, Informa.

GOBIERNO DE LA REPÚBLICA DOMINICANA
DIRECCIÓN GENERAL DE INFORMACIÓN Y DEFENSA DE LOS AFILIADOS A LA SEGURIDAD SOCIAL (DIDA)

¿Por qué es importante asegurar su acceso y ambiente a sistemas y datos?

Ciberseguridad para el **Sector Público**
Asegurar el acceso y proteger la confidencialidad

CNCs
CENTRO NACIONAL DE CIBERSEGURIDAD
REPÚBLICA DOMINICANA

158 CUENTAS ALCANZADAS

DIDA
COMPROMETIDOS CON TU BIENESTAR
Orienta, Defiende, Informa.

GOBIERNO DE LA REPÚBLICA DOMINICANA
DIRECCIÓN GENERAL DE INFORMACIÓN Y DEFENSA DE LOS AFILIADOS A LA SEGURIDAD SOCIAL (DIDA)

El acceso no autorizado a sistemas y datos críticos puede provocar la pérdida y divulgación de información confidencial.

1. Gestión de Acceso:
Controla el acceso a sistemas y datos críticos según las necesidades del usuario. Es fundamental saber quién tiene acceso y asegurarse de que sea autorizado.

2. Gestión de Proveedores Externos:
Al contratar proveedores externos, asegúrate de que cumplan con los niveles de seguridad acordados. Implementa medidas y acuerdos contractuales para garantizar que cumplan con los requisitos de seguridad y proteger la confidencialidad de tu entidad.

3. Utiliza Frases de Contraseña Seguras y MFA:
Impulsa la importancia de utilizar frases de contraseña robustas y la autenticación multifactor (MFA). **No reutilices contraseñas, no las compartas y habilita MFA, especialmente para cuentas de alto valor.**

CNCs
CENTRO NACIONAL DE CIBERSEGURIDAD
REPÚBLICA DOMINICANA

108 CUENTAS ALCANZADAS

TSS **CNCs**
CENTRO NACIONAL DE CIBERSEGURIDAD
REPÚBLICA DOMINICANA

CIBERSEGURIDAD PARA EL SECTOR PÚBLICO

Entidades Ciberresilientes
Buenas prácticas

++++
++++
++++

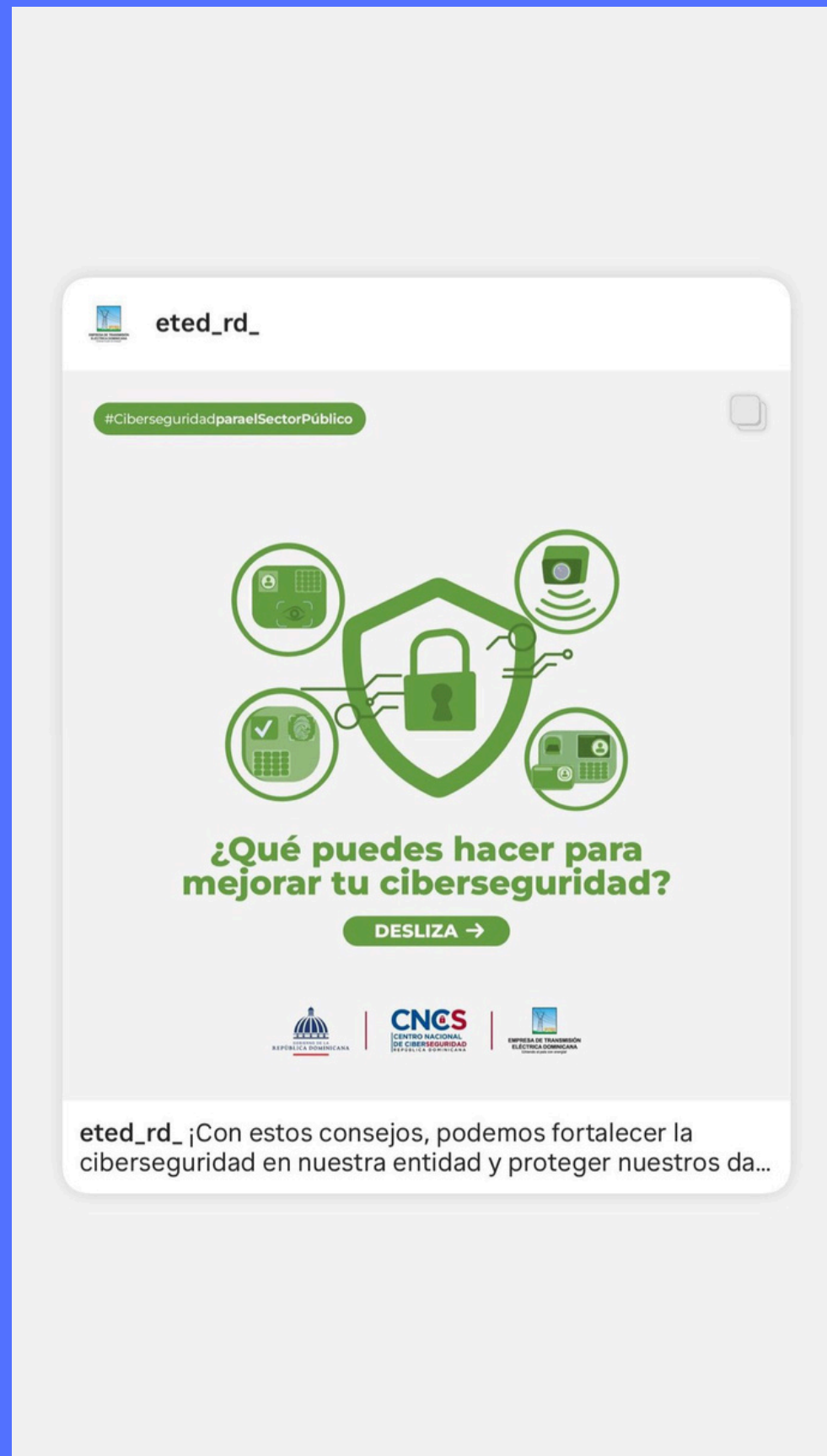
++++
++++
++++
++++

Recomendaciones para mejorar la ciberseguridad y ser ciberresiliente:

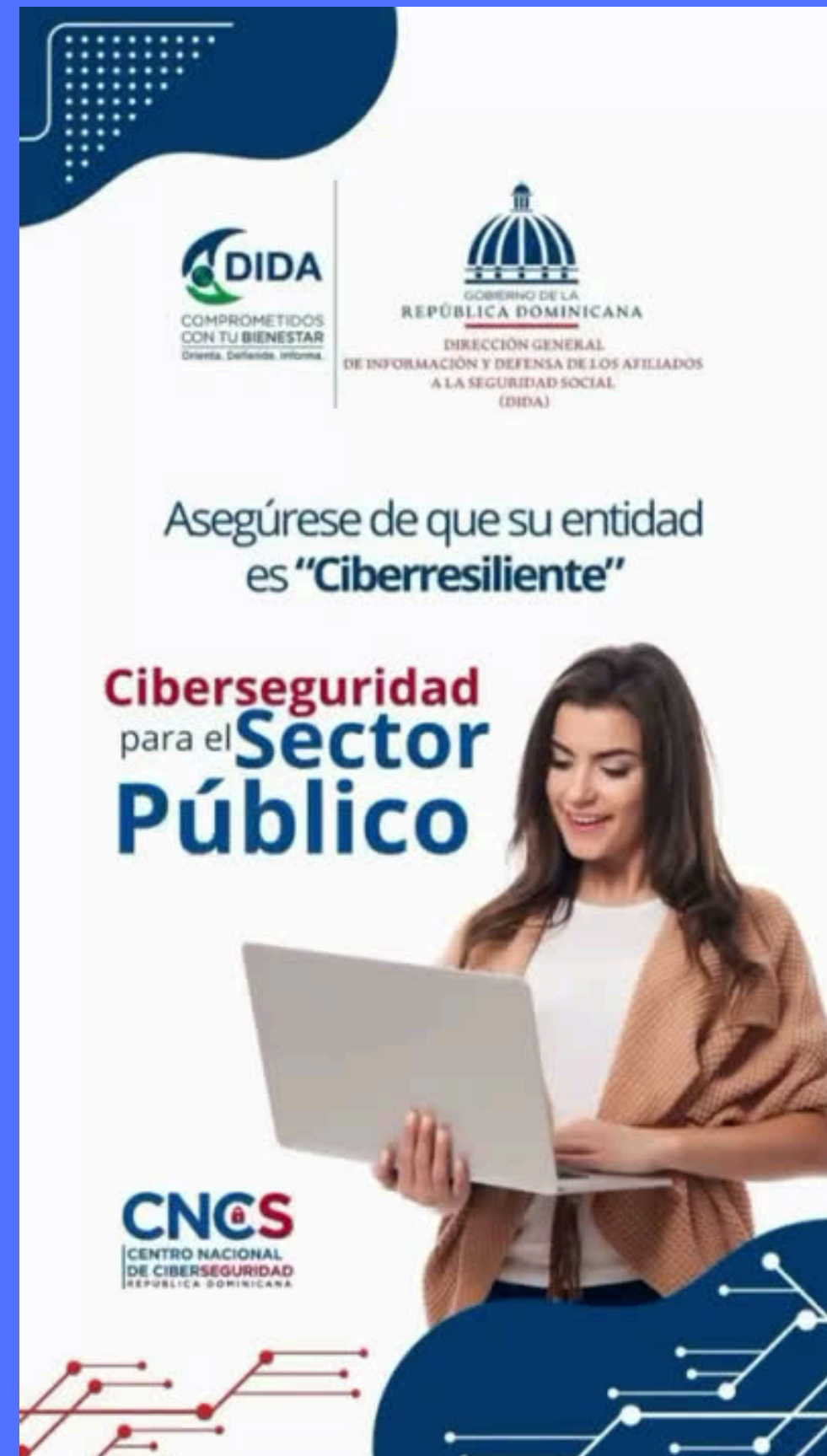
- Planificación de interrupciones operativas.
- Integración de ciberseguridad en el Plan de Continuidad de Negocio (BCP).
- Consideración de escenarios plausibles.

114 CUENTAS ALCANZADAS

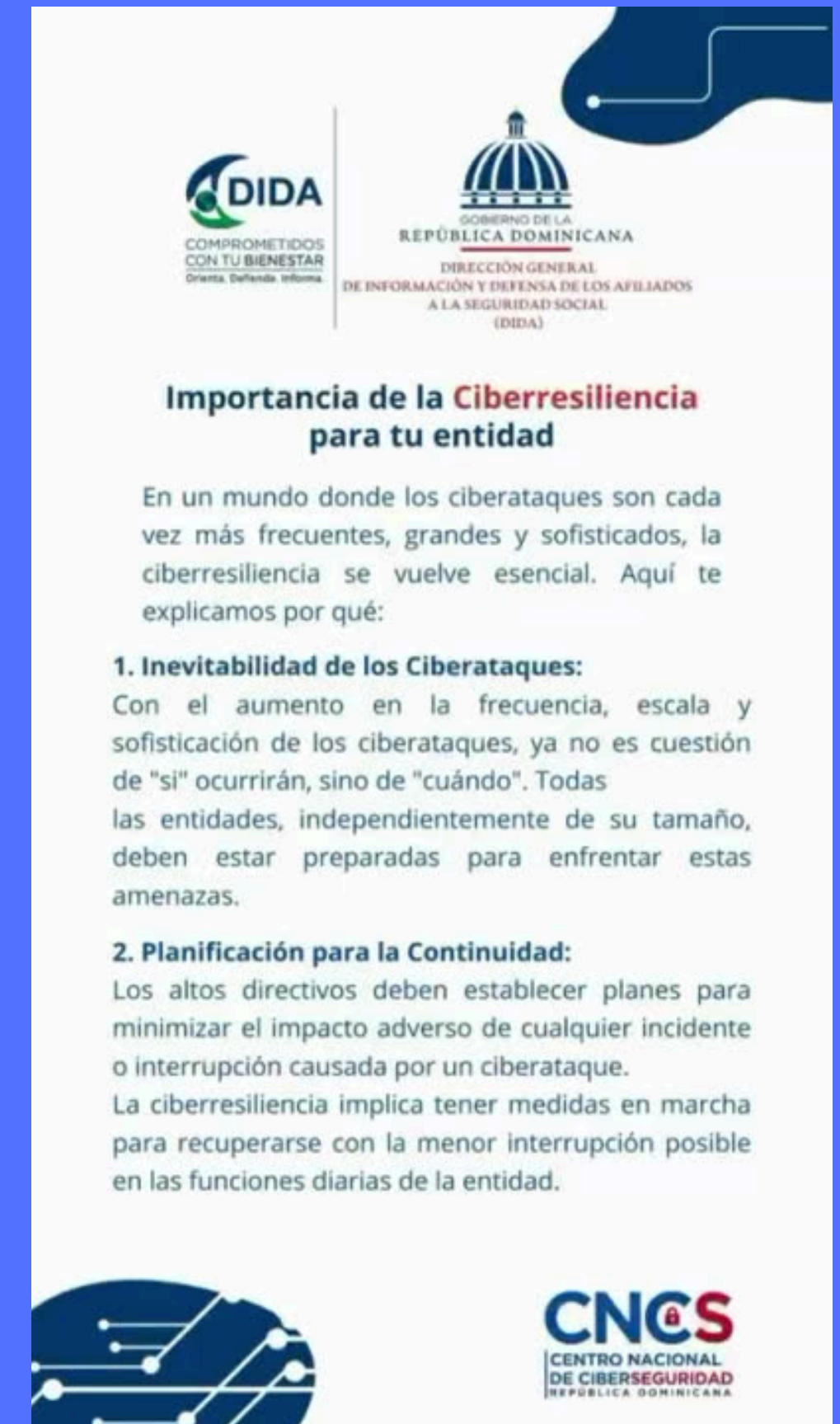
INSTAGRAM - HISTORIAS COMPARTIDAS



187 CUENTAS ALCANZADAS



147 CUENTAS ALCANZADAS



132 CUENTAS ALCANZADAS

INSTAGRAM - HISTORIAS COMPARTIDAS



TSS **CNCS**
CENTRO NACIONAL DE CIBERSEGURIDAD REPÚBLICA DOMINICANA

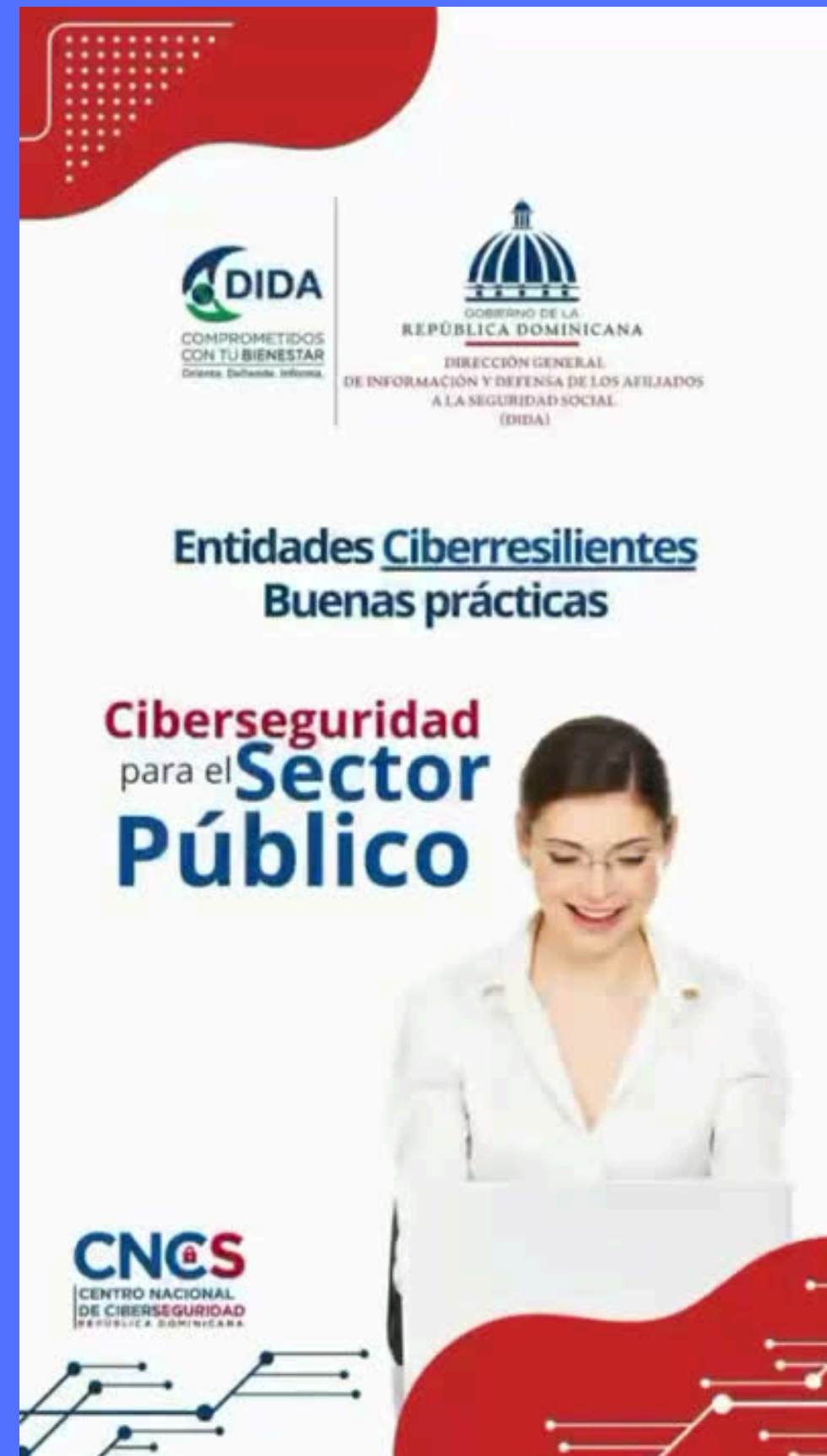
CIBERSEGURIDAD PARA EL SECTOR PÚBLICO

Ransomware: lo que necesitas saber y cómo protegerte

El ransomware es una amenaza grave para nuestras entidades. Aquí te dejamos algunos consejos para evitar ser víctima:

1. Mantén tus sistemas actualizados.
2. Haz copias de seguridad.
3. Sé cauteloso con los correos electrónicos.
4. Usa software de seguridad confiable.
5. Capacita a tu personal.

263 CUENTAS ALCANZADAS



DIDA
COMPROMETIDOS CON TU BIENESTAR
Diversa. Diferente. Informa.

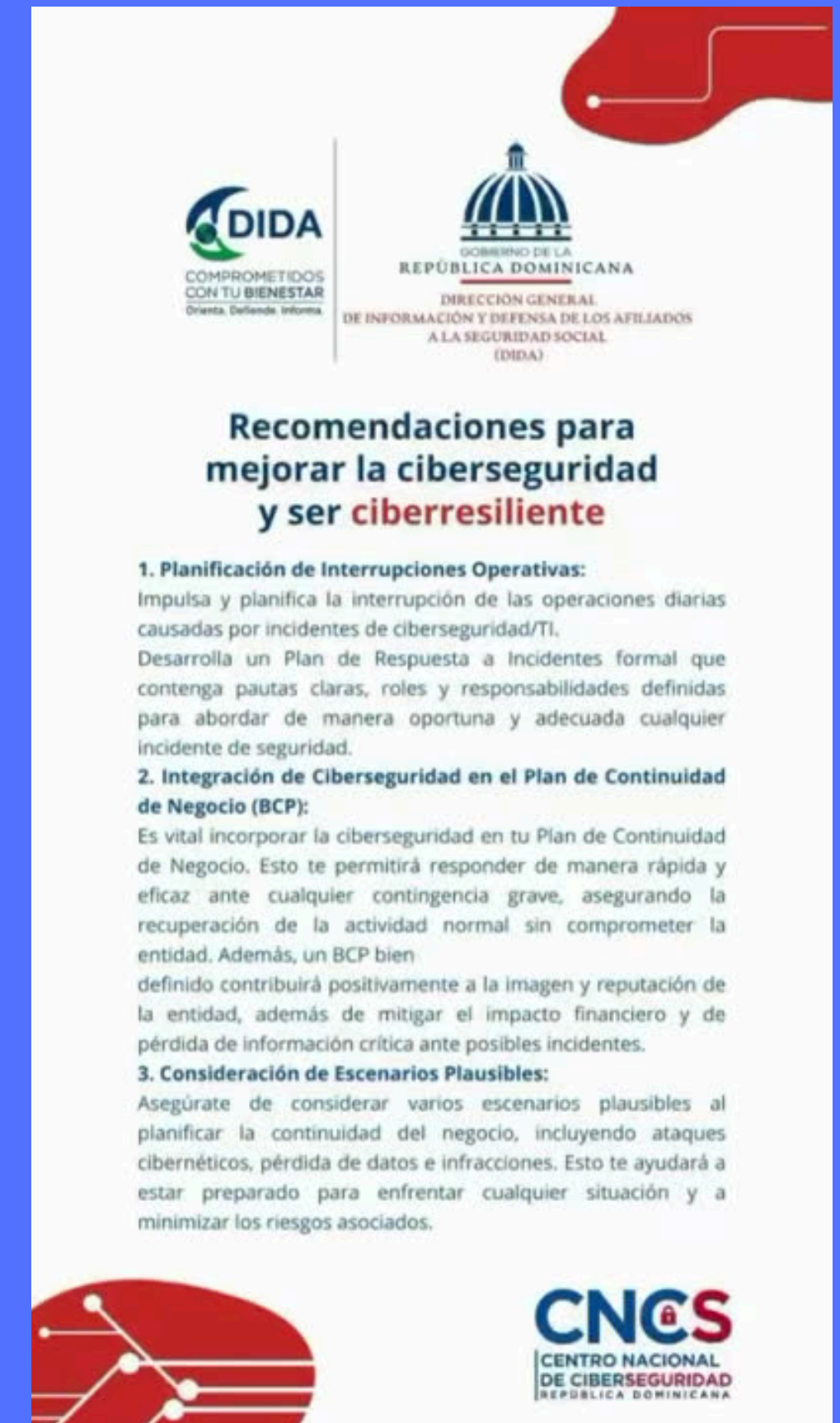
GOBIERNO DE LA REPÚBLICA DOMINICANA
DIRECCIÓN GENERAL DE INFORMACIÓN Y DEFENSA DE LOS AFILIADOS A LA SEGURIDAD SOCIAL (DIDA)

Entidades Ciberresilientes Buenas prácticas

Ciberseguridad para el Sector Público

CNCS
CENTRO NACIONAL DE CIBERSEGURIDAD REPÚBLICA DOMINICANA

137 CUENTAS ALCANZADAS



DIDA
COMPROMETIDOS CON TU BIENESTAR
Diversa. Diferente. Informa.

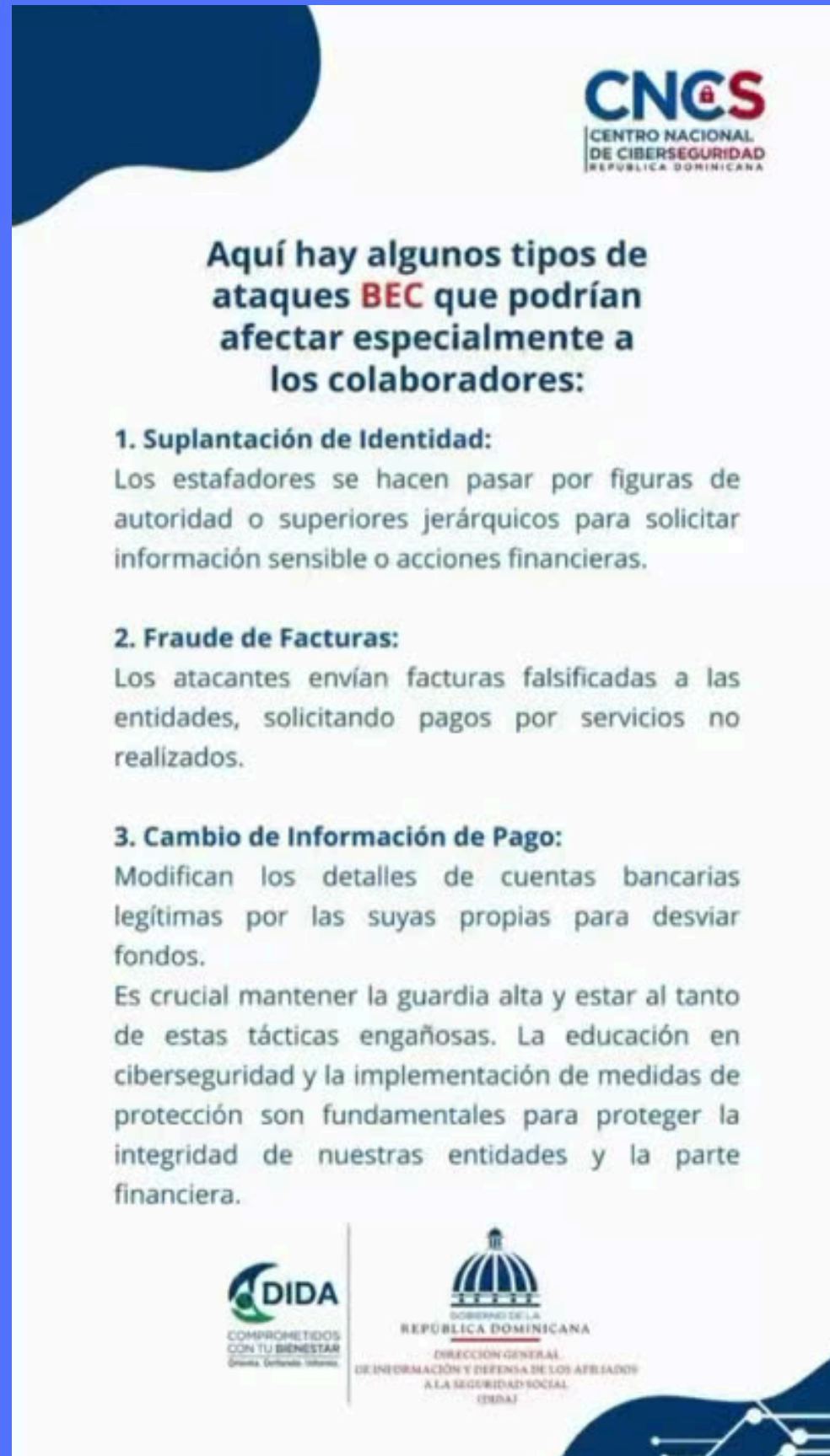
GOBIERNO DE LA REPÚBLICA DOMINICANA
DIRECCIÓN GENERAL DE INFORMACIÓN Y DEFENSA DE LOS AFILIADOS A LA SEGURIDAD SOCIAL (DIDA)

Recomendaciones para mejorar la ciberseguridad y ser **ciberresiliente**

- 1. Planificación de Interrupciones Operativas:**
Impulsa y planifica la interrupción de las operaciones diarias causadas por incidentes de ciberseguridad/TI. Desarrolla un Plan de Respuesta a Incidentes formal que contenga pautas claras, roles y responsabilidades definidas para abordar de manera oportuna y adecuada cualquier incidente de seguridad.
- 2. Integración de Ciberseguridad en el Plan de Continuidad de Negocio (BCP):**
Es vital incorporar la ciberseguridad en tu Plan de Continuidad de Negocio. Esto te permitirá responder de manera rápida y eficaz ante cualquier contingencia grave, asegurando la recuperación de la actividad normal sin comprometer la entidad. Además, un BCP bien definido contribuirá positivamente a la imagen y reputación de la entidad, además de mitigar el impacto financiero y de pérdida de información crítica ante posibles incidentes.
- 3. Consideración de Escenarios Plausibles:**
Asegúrate de considerar varios escenarios plausibles al planificar la continuidad del negocio, incluyendo ataques cibernéticos, pérdida de datos e infracciones. Esto te ayudará a estar preparado para enfrentar cualquier situación y a minimizar los riesgos asociados.

123 CUENTAS ALCANZADAS

INSTAGRAM - HISTORIAS COMPARTIDAS



CNCS
CENTRO NACIONAL
DE CIBERSEGURIDAD
REPUBLICA DOMINICANA

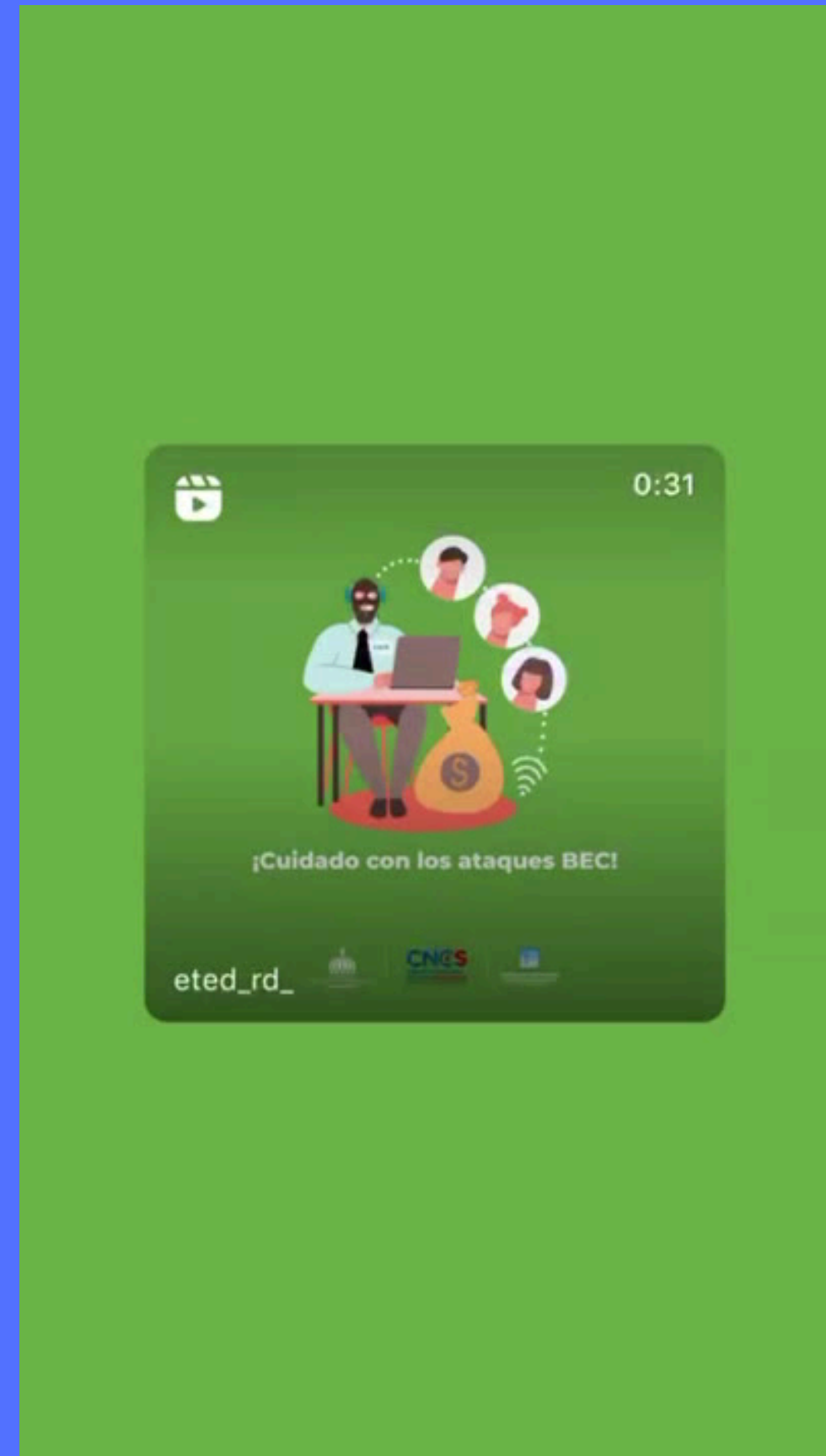
Aquí hay algunos tipos de ataques **BEC que podrían afectar especialmente a los colaboradores:**

- 1. Suplantación de Identidad:**
Los estafadores se hacen pasar por figuras de autoridad o superiores jerárquicos para solicitar información sensible o acciones financieras.
- 2. Fraude de Facturas:**
Los atacantes envían facturas falsificadas a las entidades, solicitando pagos por servicios no realizados.
- 3. Cambio de Información de Pago:**
Modifican los detalles de cuentas bancarias legítimas por las suyas propias para desviar fondos.
Es crucial mantener la guardia alta y estar al tanto de estas tácticas engañosas. La educación en ciberseguridad y la implementación de medidas de protección son fundamentales para proteger la integridad de nuestras entidades y la parte financiera.

DIDA
COMROMETIDOS
CON TU BIENESTAR
Gestión. Cultura. Innovación.

**GOBIERNO DE LA
REPUBLICA DOMINICANA**
DIRECCIÓN GENERAL
DE INFORMACIÓN Y DEFENSA DE LOS AFIADOS
A LA SEGURIDAD SOCIAL
(DIRIAS)

1.064 CUENTAS ALCANZADAS



0:31

¡Cuidado con los ataques BEC!

eted_rd_

CNCS

752 CUENTAS ALCANZADAS



FACEBOOK

85 2 0 0

Resumen i

Alcance	85
Impresiones	85
Reacciones, comentarios y veces que se compartieron las publicaciones	2
Total de clics	5

Reacciones, comentarios y veces que se compartieron las publicaciones i

2 0 0 0 0 0

Reacciones	2
Comentarios	0
Veces que se compartió	0

FACEBOOK

1

#CiberseguridadparaelSectorPúblico



¿Y tú, formas parte del Equipo de concienciación en ciberseguridad?

DESLIZA →



59 2 0 0

Resumen i

Alcance 59

Impresiones 59

Reacciones, comentarios y veces que se compartieron las publicaciones 2

Total de clics 2

Reacciones, comentarios y veces que se compartieron las publicaciones i

2 0 0 0 0 0

Reacciones 2

Comentarios 0

Veces que se compartió 0

FACEBOOK

2

¿Y tú, ya formas parte del equipo de concienciación en ciberseguridad?

CIBERSEGURIDAD PARA EL SECTOR PÚBLICO - PRIVADO



Desliza para conocer los roles claves en un equipo de concienciación en ciberseguridad

#CiberseguridadParaElSectorPúblico



CNCS CENTRO NACIONAL DE CIBERSEGURIDAD REPÚBLICA DOMINICANA

124 2 0 1

Resumen i

Alcance	124
Impresiones	128
Reacciones, comentarios y veces que se compartieron las publicaciones	3
Total de clics	3

Reacciones, comentarios y veces que se compartieron las publicaciones i

4 0 0 0 0 0

Reacciones	2
Comentarios	0
Veces que se compartió	1

FACEBOOK

3



4 18 0 0

Resumen *i*

Alcance	18
Impresiones	18
Reacciones, comentarios y veces que se compartieron las publicaciones	0
Total de clics	0

Ingresos

Configurar

Reproducciones de video *i*

Reproducciones de video de 3 segundos	4
Reproducciones de video de 1 minuto	--
Promedio de minutos reproducidos	00:11
Minutos reproducidos	2

FACEBOOK



Panel para profesionales
Estadísticas de publicaciones

70 1 0 0

Resumen ⓘ

Alcance 70

Impresiones 70

Reacciones, comentarios y veces que se compartieron las publicaciones 1

Total de clics 6

Reacciones, comentarios y veces que se compartieron las publicaciones ⓘ

1 0 0 0 0 0

Reacciones 1

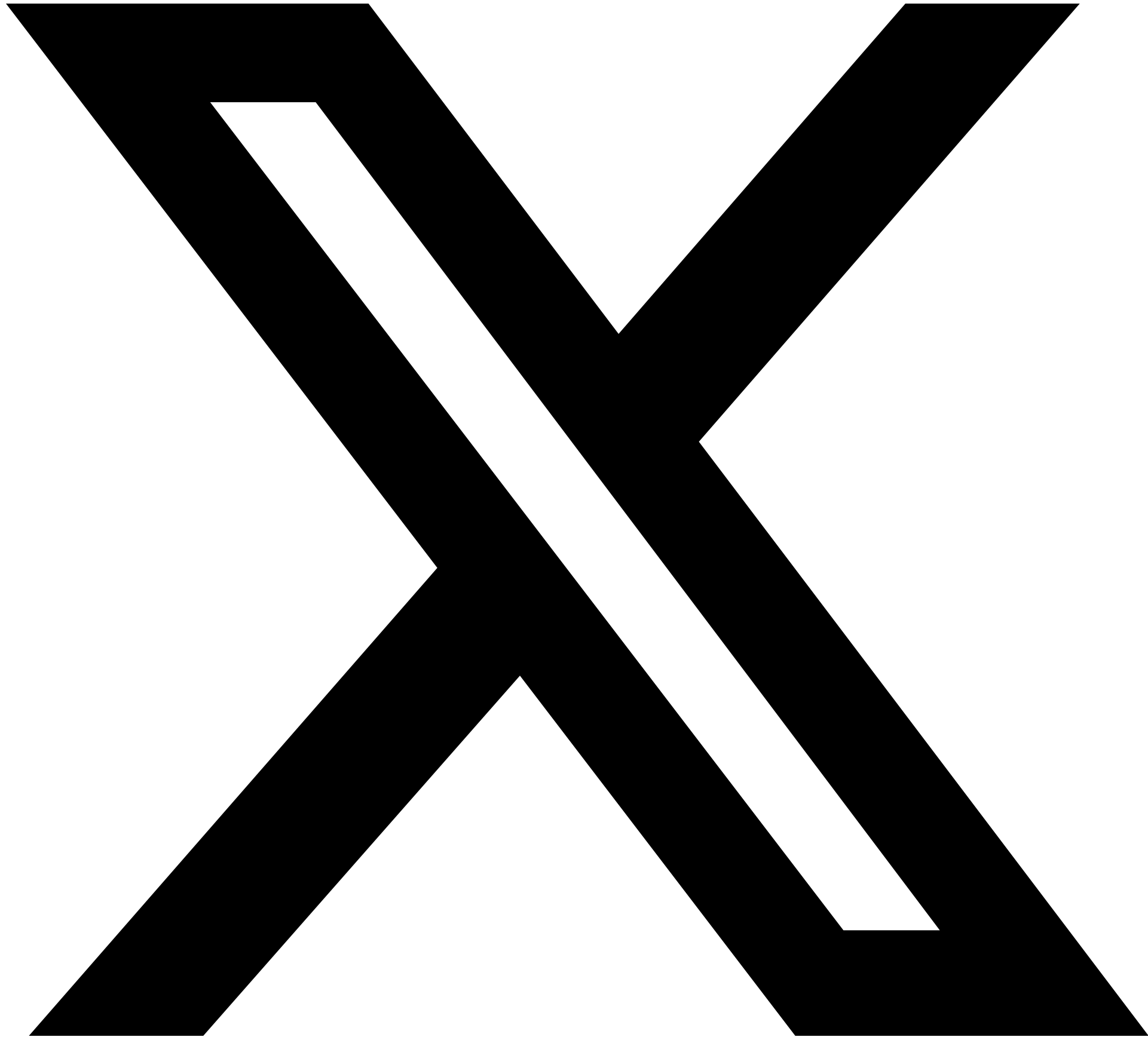
Comentarios 0

Veces que se compartió 0

FACEBOOK

5





Actividad del post

CNCS Centro Nacional de Ciberseguridad @CNCSDR • 15 abr.



Desliza para que conozcas las funciones claves de quienes son los verdaderos héroes de la seguridad digital.

2

3

1

Impresiones ⓘ

245

Interacciones ⓘ

12

Ampliaciones de detalles ⓘ

1

Nuevos seguidores ⓘ

0

Visitas del perfil ⓘ

1

X

1

#CiberseguridadparaelSectorPúblico



¿Y tú, formas parte del Equipo de concienciación en ciberseguridad?

DESLIZA →



CNCS CENTRO NACIONAL DE CIBERSEGURIDAD REPÚBLICA DOMINICANA



Actividad del post

 **Centro Nacional de Ciberseguridad** @CNC: · 17 abr.



Descubre valiosas recomendaciones que puedes implementar en la entidad para la que laboras, con el fin de robustecer la estrategia de Ciberseguridad. ...



0



1



0

Impresiones ⓘ

109

Interacciones ⓘ

4

Ampliaciones de detalles ⓘ

3

Nuevos seguidores ⓘ

0

Visitas del perfil ⓘ

0



2

#CiberseguridadparaelSectorPúblico

Buenas prácticas para fortalecer la Ciberseguridad en tu entidad

 **CNCS**



Video

Métricas del video que compartiste

Reproducciones únicas **32** Reproducciones **35**



Actividad del post

CNCS Centro Nacional de Ciberse @CNC · 22 abr.

¡Concienciar y capacitar a tus colaboradores en materia de ciberseguridad es esencial para proteger tu entidad contra amenazas cibernéticas! 💪🛡️ ...

1

1

0

Impresiones

153

Interacciones

3

Ampliaciones de detalles

0

Nuevos seguidores

1

Visitas del perfil

0





3



Actividad del post

 **Centro Nacional de Ciberse** @CNC: · 23 abr.



¡Con estos consejos, podemos fortalecer la ciberseguridad en nuestra entidad y proteger nuestros datos!  

...



2



4



0

Impresiones ⓘ

195

Interacciones ⓘ

13

Ampliaciones de detalles ⓘ

1

Nuevos seguidores ⓘ

0

Visitas del perfil ⓘ

0



4

#CiberseguridadparaelSectorPúblico

¿Qué puedes hacer para mejorar tu **ciberseguridad**?

 **CNCS**

