PERÚ | Presidencia del Consejo de Ministros | Secretaría de Gobierno y Transformación Digital

Siempre con el pueblo

ALERTA INTEGRADA DE SEGURIDAD DIGITAL

Centro Nacional de Seguridad Digital

asbanc
ASOCIACIÓN DE BANCOS DEL PERÚ

Lima, 21 de noviembre de 2022

316-2022-CNSD

La presente **Alerta Integrada de Seguridad Digital** corresponde a un análisis técnico periódico realizado por el Comando Conjunto de las Fuerzas Armadas, el Ejército del Perú, la Marina de Guerra del Perú, la Fuerza Aérea del Perú, la Dirección Nacional de Inteligencia, la Policía Nacional del Perú, la Asociación de Bancos del Perú y el Centro Nacional de Seguridad Digital de la Secretaría de Gobierno y Transformación Digital de la Presidencia del Consejo de Ministros, en el marco de la Seguridad Digital del Estado Peruano.

El objetivo de esta alerta **es informar a los responsables de la seguridad digital de las entidades públicas y las empresas privadas sobre las amenazas en el entorno digital** para advertir las situaciones que pudieran afectar la continuidad de sus servicios en favor de la población.

Las marcas y logotipos de empresas privadas y/o entidades públicas se reflejan para ilustrar la información que los ciudadanos reciben por redes sociales u otros medios y que atentan contra la confianza digital de las personas y de las mismas empresas **de acuerdo con lo establecido por el Decreto de Urgencia 007-2020**.

La presente Alerta Integrada de Seguridad Digital es información netamente especializada para informar a las áreas técnicas de entidades y empresas.

Contenido

Centro Nacional de Seguridad Digital	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 316	Fecha: 21-11-2022
		Página 4 de 10

Componente que reporta	**CENTRO NACIONAL DE SEGURIDAD DIGITAL**		
Nombre de la alerta	Hive Ransomware extorsiona a 1300 empresa		
Tipo de ataque	Ransomware	Abreviatura	Ransomware
Medios de propagación	Red, Internet		
Código de familia	C	Código de subfamilia	C01
Clasificación temática familia	Código malicioso		

Descripción

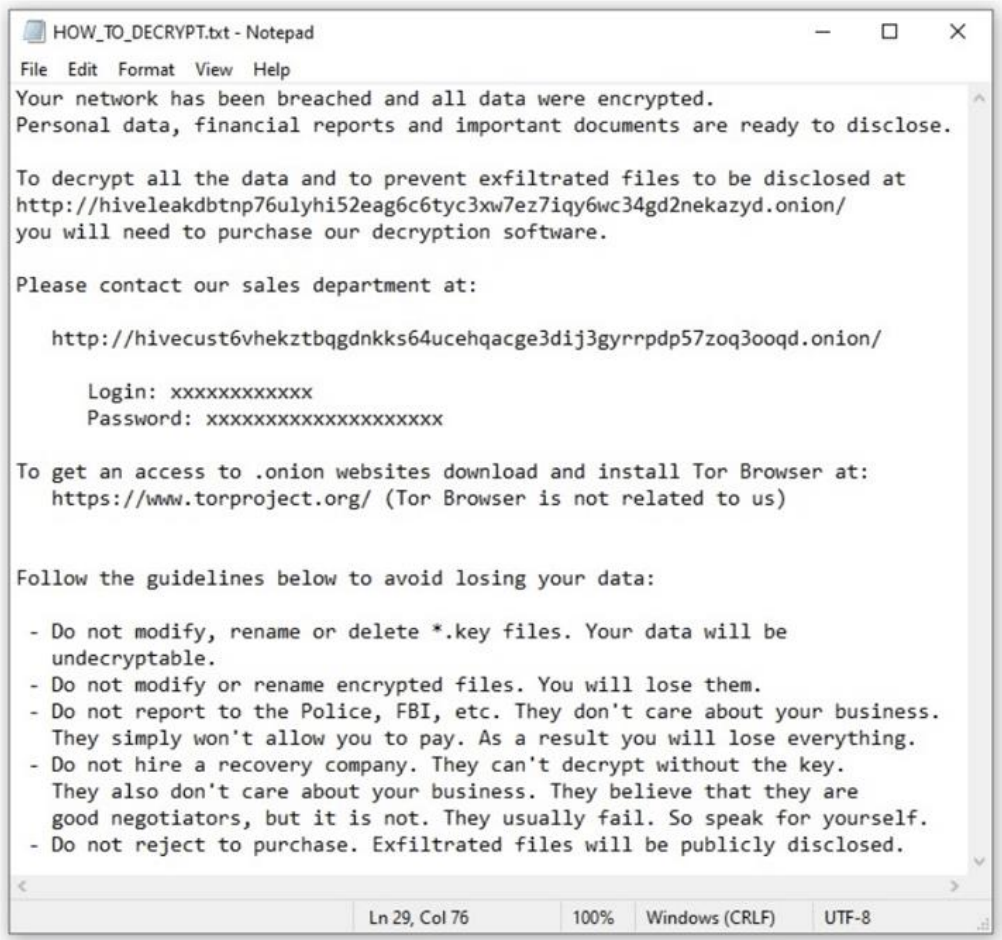
1. RESUMEN:

El grupo cibernético llamado Hive Ransomware esta aumentando su actividad según el FBI, el mundo evoluciona, y los creadores de malware no son menos, hasta el punto de que ya se habla en el mundo de «Ransomware-as-a-service» (Raas), la forma que tienen de monetizar sus actividades criminales. En este caso Hive Ransomware extorsiona a 1300 empresas.

2. DETALLES:

El «modus operandi» de esta actividad ilícita es al de secuestrar un equipo aprovechando alguna vulnerabilidad, ya sea de software o humano, para después pedir un rescate para desbloquear este secuestro si la víctima quiere tener su equipo funcional de nuevo.

Cuando la máquina es infectada, el malware crea un documento en el cual guía a la víctima sobre cómo recuperar su máquina, pasos, como no, para realizar un pago. Tiene un aspecto como el siguiente.



Ahora se ha realizado un ataque en el cual Hive Ransomware extorsiona a 1300 empresas de todo el mundo, llegando a recaudar 100 millones de dólares sólo en noviembre de 2022. Unos pagos, totalmente ilícitos.

Según inteligencia de EE.UU. el objetivo del ataque no ha tenido filtros, afectando desde empresas de infraestructuras hasta otras de atención médica, por lo que puede verse el alcance y la criticidad del ataque. Parece ser que el punto de explotación ha sido unas fallas de seguridad de ProxyShell de Microsoft Exchange Server.

Junto a este fallo de seguridad hay también medidas de anulación de motores antivirus así como ciertas medidas de seguridad de Windows. Según la Agencia de Seguridad, Infraestructuras y Ciberseguridad (CISA), asegura que los actores que han restaurado los sistemas sin realizar el pago, se han visto reinfectados.

3. RECOMENDACIONES:

- Evite hacer clic en enlaces de mensajes de spam o en sitios web desconocidos.
- Evite revelar información personal mediante un mensaje de texto o un correo electrónico de una fuente que no sea de confianza en donde se le solicita información personal.
- Evitar abrir archivos adjuntos de correos electrónicos sospechosos.
- Mantenga sus programas, antivirus y sistema operativo actualizados.

Fuentes de información	▪ hxxps://unaaldia.hispasec.com/2022/11/hive-ransomware-extorsiona-a-1300-empresa.html ▪ hxxps://thehackernews.com/2022/11/hive-ransomware-attackers-extorted-100.html ▪ https://www.bleepingcomputer.com/news/security/fbi-hive-ransomware-extorted-100m-from-over-1-300-victims/

DINI	**ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 316**	**Fecha: 21-11-2022**
		Página 6 de 10

Componente que reporta	**DIRECCIÓN NACIONAL DE INTELIGENCIA**		
Nombre de la alerta	Múltiples vulnerabilidades en productos de Cisco		
Tipo de ataque	Explotación de vulnerabilidades conocidas	Abreviatura	EVC
Medios de propagación	Red, Internet		
Código de familia	H	Código de subfamilia	H01
Clasificación temática familia	Intento de intrusión		

Descripción

1. **Resumen:**
   Cisco ha reportado dos vulnerabilidades de severidad ALTA de tipo inyección SQL y uso de clave criptográfica codificada de forma rígida en la interfaz de administración de interfaz de usuario de próxima generación para Cisco Email Security Appliance (ESA), Cisco Secure Email and Web Manager y Cisco Secure Web Appliance, anteriormente conocido como Cisco Web Security Appliance (WSA). La explotación exitosa de estas vulnerabilidades podría permitir a un atacante remoto elevar los privilegios y/o realizar un ataque de inyección SQL y obtener privilegios de root.

2. **Detalles:**

   - La vulnerabilidad de severidad **alta** identificada como CVE-2022-20867 en la interfaz de administración de la interfaz de usuario de próxima generación de Cisco ESA y Cisco Secure Email and Web Manager podría permitir a un atacante remoto autenticado realizar ataques de inyección SQL con privilegios de root en un sistema afectado. Para aprovechar esta vulnerabilidad, un atacante necesitaría tener las credenciales de una cuenta de usuario con muchos privilegios. Esta vulnerabilidad se debe a una validación incorrecta de los parámetros enviados por el usuario. Un atacante podría explotar esta vulnerabilidad al autenticarse en la aplicación y enviar solicitudes maliciosas a un sistema afectado. Una explotación exitosa podría permitir a un atacante obtener datos o modificar los datos almacenados en la base de datos subyacente del sistema afectado.

     La vulnerabilidad de tipo inyección SQL se debe a que el software construye todo o parte de un comando SQL utilizando la entrada influenciada externamente desde un componente ascendente, pero no neutraliza o neutraliza incorrectamente elementos especiales que podrían modificar el comando SQL previsto cuando se envía a un componente descendente.

   - La vulnerabilidad de severidad **alta** identificada como CVE-2022-20868 en la interfaz de administración de interfaz de usuario de próxima generación de Cisco ESA, Cisco Secure Email and Web Manager y Cisco Secure Web Appliance podría permitir a un atacante remoto autenticado elevar los privilegios en un sistema afectado. Esta vulnerabilidad se debe al uso de un valor codificado para cifrar un token que se usa para ciertas llamadas a la API. Un atacante podría aprovechar esta vulnerabilidad al autenticarse en un dispositivo afectado y enviar una solicitud HTTP manipulada. Una explotación exitosa podría permitir a un atacante hacerse pasar por otro usuario válido y ejecutar comandos con los privilegios de esa cuenta de usuario. El uso de una clave criptográfica codificada aumenta significativamente la posibilidad de recuperar los datos cifrados.

3. **Productos afectados:**

   - La vulnerabilidad CVE-2022-20868 afecta a Cisco ESA y Cisco Secure Email and Web Manager;
   - La vulnerabilidad CVE-2022-20867 afecta a Cisco ESA, Cisco Secure Email and Web Manager y Cisco Secure Web Appliance.

4. **Solución:**

   - Cisco ha lanzado actualizaciones de software que abordan esta vulnerabilidad.

Fuentes de información	▪ hxxps://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-esasmawsa-vulns-YRuSW5mD

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 316	Fecha: 21-11-2022
		Página 7 de 10

Componente que reporta	**DIRECCIÓN DE INTELIGENCIA DE LA POLICIA NACIONAL DEL PERÚ**		
Nombre de la alerta	Campaña de phishing que tiene como objetivo robar credenciales de acceso de usuarios de la red social Instagram		
Tipo de ataque	Phishing	Abreviatura	Phishing
Medios de propagación	Redes sociales, SMS, correo electrónico, videos de internet, entre otros		
Código de familia	G	Código de subfamilia	G02
Clasificación temática familia	Fraude		

Descripción

1. A través del monitoreo y búsqueda de amenazas en el ciberespacio, se detectó que, los ciberdelincuentes vienen llevando a cabo ataques de envío masivo de emails, que aparenta ser de Instagram**,** en el texto del mensaje advierte lo siguiente ***"se ha detectado una actividad inusual en la cuenta, por lo que será cancela a menos que actualice sus datos personales",*** manipulando a la víctima, que haga clic en un enlace que redirige a un sitio web falso similar al oficial de Instagram, con el objetivo robar credenciales de acceso de inicio de sesión.

- Detalles del proceso de phishing.

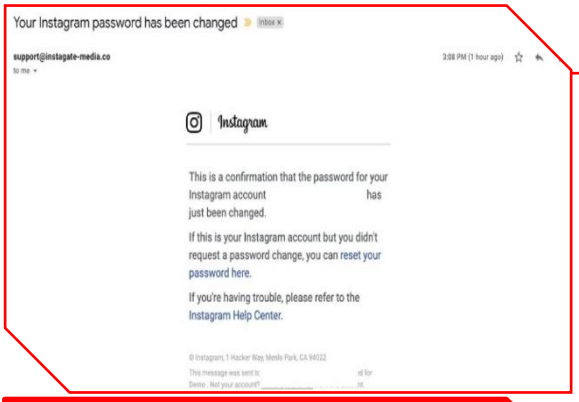


Imagen 1: Correo electrónico que simula ser de Instagram, insta hacer clic en el enlace adjunto.

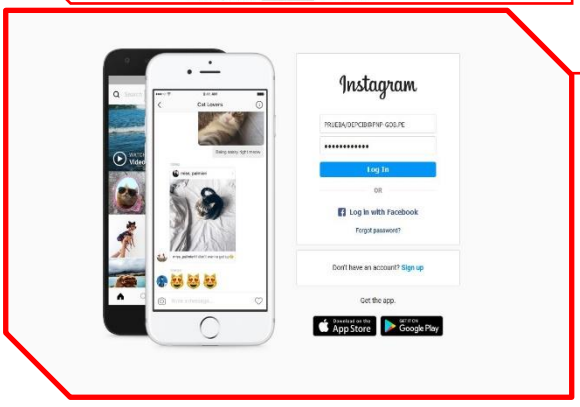


Imagen 2: Estafa, luego requiere proporcionar las credenciales de acceso de inicio de sesión (correo electrónico y contraseña).

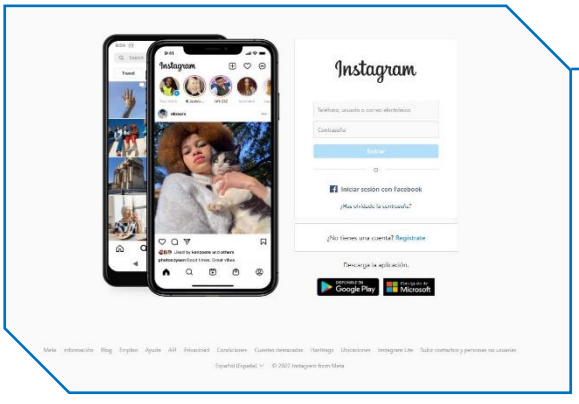
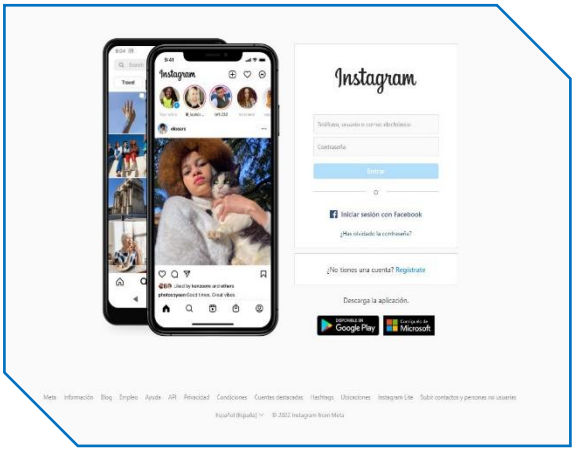


Imagen 3: Una vez ingresada las credenciales de acceso, es redirigido al sitio oficial Instagram, aludiendo un aparente error; sin embargo, los datos fueron capturados.

- Comparación del sitio oficial de Instagram y sitio Falso:

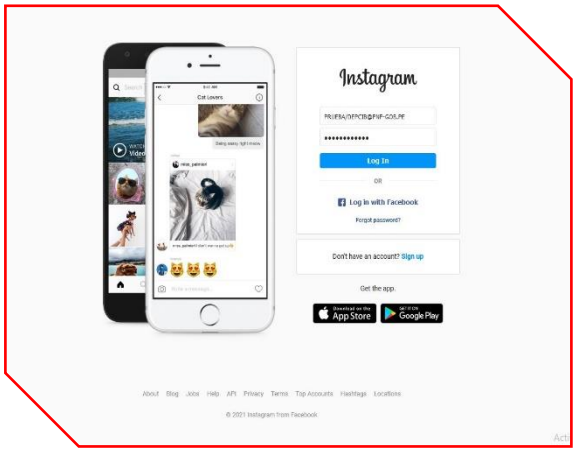
SITIO OFICIAL

URL: https://www.instagram.com/



SITIO FRAUDULENTO

URL: hxxps://douglaso-r[.]github[.]io/instagram-login/

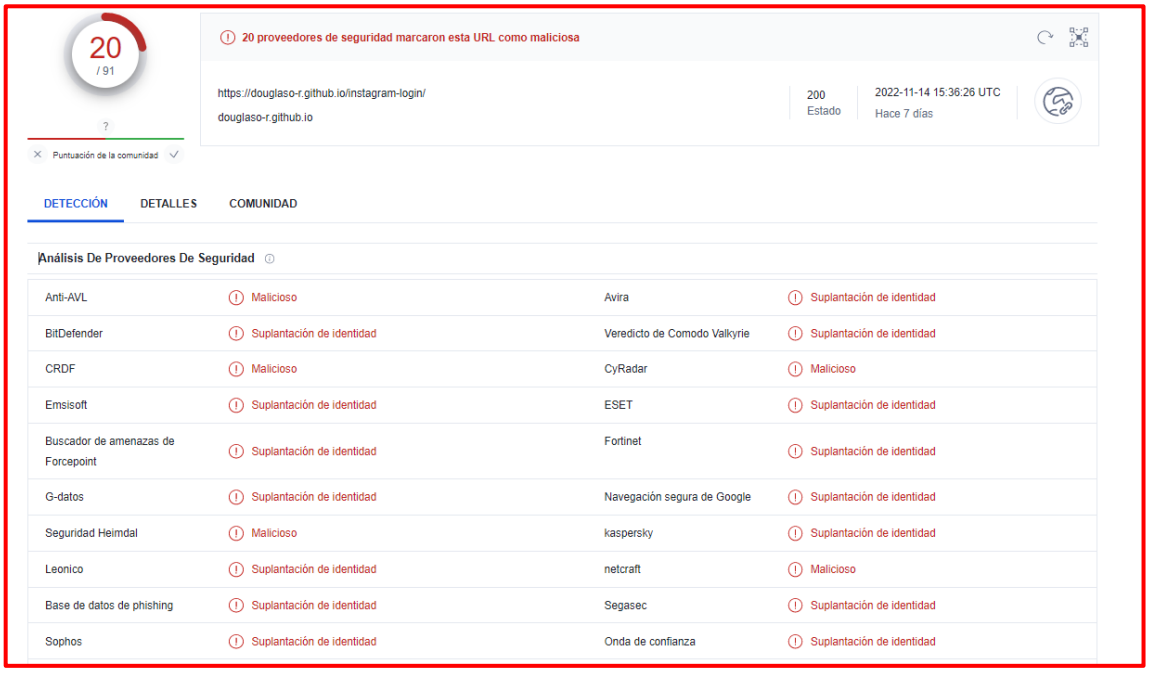


- Existe similitud en imagen de fondo, color y escritura.
- Tiene certificado de seguridad de protocolo HTTPS.
- El dominio se hace pasar por el sitio oficial, pero no coincide.

2. La URL Maliciosa, fue analizada en las diferentes plataformas virtuales de seguridad digital, siendo catalogado como **SUPLANTACIÓN DE IDENTIDAD:**

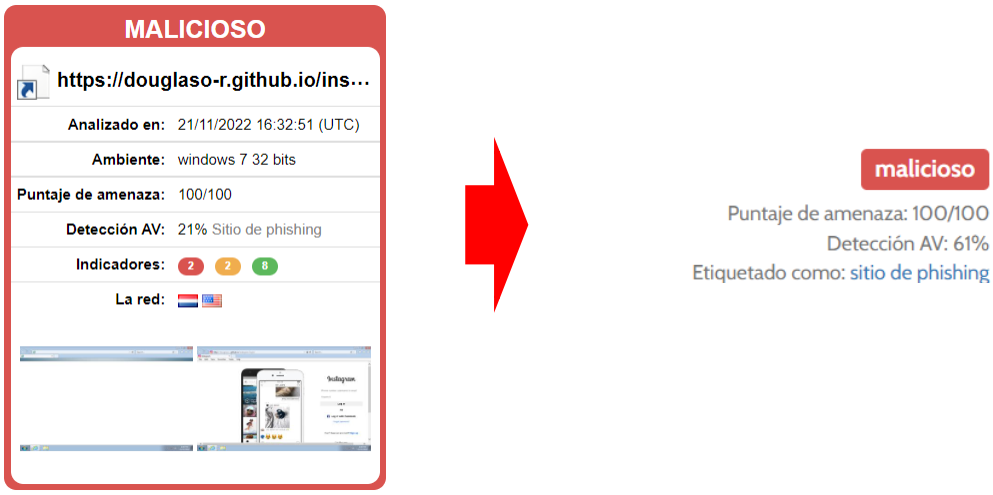
- Indicadores de compromisos:

  - **URL:** hXXps[:]//douglaso-r[.]github[.]io/instagram-login/
  - **Dominio:** douglaso-r[.]github[.]io
  - **Dirección IP:** 185[.]199[.]110[.]153
  - **Código:** 200
  - **Longitud:** 4.23 KB
  - **SHA-256**: 8ee23f2f9065e67357ae2900bb3a7b33fb2b5f2a8fb5c4e022549f7283ccd473

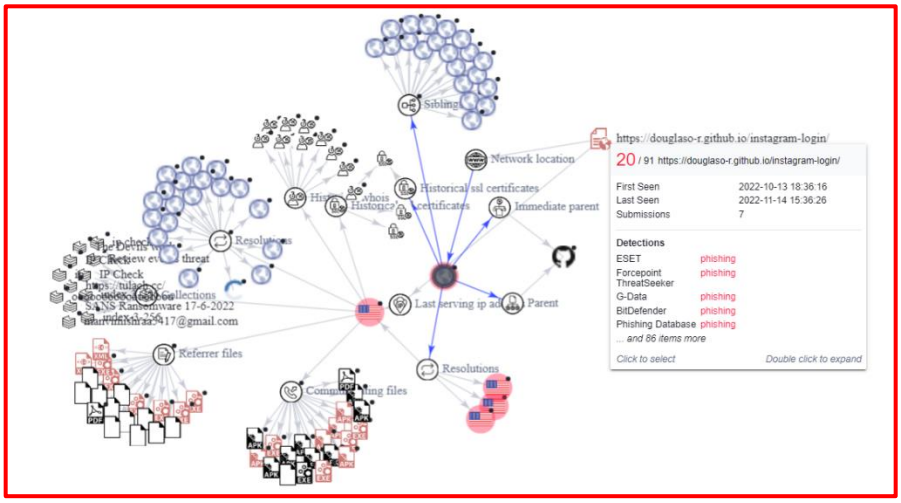


Anti-AVL	Malicioso	Avira	Suplantación de identidad
BitDefender	Suplantación de identidad	Veredicto de Comodo Valkyrie	Suplantación de identidad
CRDF	Malicioso	CyRadar	Malicioso
Emsisoft	Suplantación de identidad	ESET	Suplantación de identidad
Buscador de amenazas de Forcepoint	Suplantación de identidad	Fortinet	Suplantación de identidad
G-datos	Suplantación de identidad	Navegación segura de Google	Suplantación de identidad
Seguridad Heimdal	Malicioso	kaspersky	Suplantación de identidad
Leonico	Suplantación de identidad	netcraft	Malicioso
Base de datos de phishing	Suplantación de identidad	Segasec	Suplantación de identidad
Sophos	Suplantación de identidad	Onda de confianza	Suplantación de identidad

- Otras detenciones de análisis:



- Topología de red:



3. Phishing:

- Es un tipo de ataque de ingeniería social, que consiste en la utilización de envió masivo de email, los cuales se disfrazan para que parezcan proceder de una fuente de confianza. Estos emails están diseñados para engañar a las víctimas y conseguir que proporcionen información personal o financiera.

4. Características:

- Contiene errores ortográficos
- No se respeta el formato (justificado)
- Algunos emails son de alerta o urgencia
- Tienen adjunto documento o URLs

5. Recomendaciones:

- Acceder al sitio web a través de fuentes oficiales.
- Evitar responder a mensajes enviados a través de (Correo electrónico, Telegram, Whatsapp, SMS y otros), que contengan enlaces de dudosa procedencia.
- Verificar detenidamente en la redacción y ortografía de la dirección URL, que coincidan con el sitio web oficial.
- No compartir la información con terceras personas, amigos o familiares.
- Utilizar un antivirus actualizado ya que es la primera barrera ante un ataque cibernético.

Fuentes de información	▪ Análisis propio de redes sociales y fuente abierta

Índice alfabético