“MÉS SEGURS” EN LA XARXA DE LA GENERALITAT

Carmen Serrano Durbá

SUBDIRECTORA GENERAL DE CIBERSEGURIDAD

DGTIC

GENERALITAT VALENCIANA

En las noticias recientemente:

- **¿Cómo?**
  - Origen: ordenador de un policía local
  - Posible robo de credenciales o correo de phishing
- **¿Quien?**
  - LockBit
- **Impacto**
  - Rescate: 5M $
  - 4.000 equipos parados + servidores
  - Ayuntamiento fuera de servicio por tiempo indefinido (mínimo 1 mes). Tareas de contención y recuperación.
  - Posible afectación de datos (confidencialidad de los datos exfiltrados, integridad de los datos cifrados)

DGTIC

En las noticias recientemente:

GENERALITAT VALENCIANA

LA VANGUARDIA

CIBERCRIMEN

El hospital Clínic sufrió un ciberataque exterior "sofisticado" y no puede usar el sistema informático

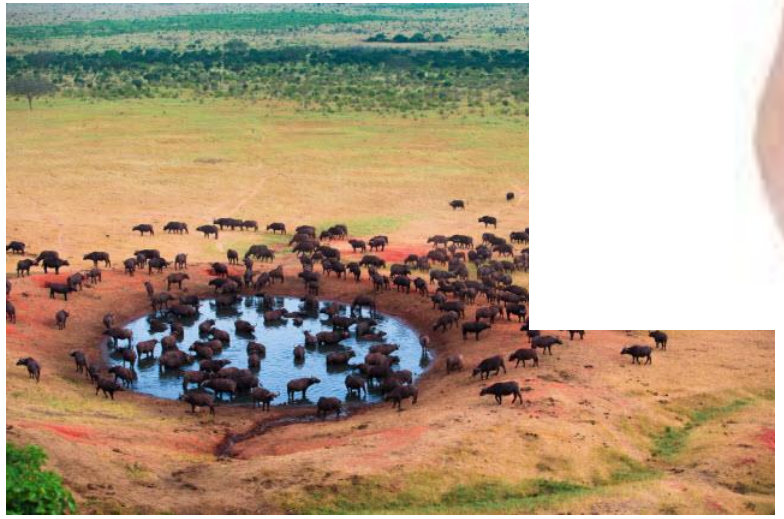
- El centro ha desprogramado este lunes 150 operaciones, ha cancelado 3.000 visitas y ha aplazado las sesiones de radioterapia oncológica
- Los piratas informáticos, Ransom House, no han solicitado rescate y la Generalitat afirma que no va a pagar

- **¿Cómo?**
  - Origen: robo de credenciales acceso remoto
- **¿Quien?**
  - Ransom House
- **Impacto**
  - Rescate: 4,5M $
  - Hospital fuera de servicio. Tareas de contención y recuperación.
  - Publicación de datos meses después en varias entregas: Datos de pacientes, trabajadores, colaboradores y proveedores fuera de control(confidencialidad de los datos exfiltrados, integridad de los datos cifrados)
- **Riesgo**
  - Posible uso para estafa, suplantación de identidad o fraude
  - Los datos médicos se comercializan a las aseguradoras privadas
  - Impacto en contratos, …

DGTIC

GENERALITAT VALENCIANA

¿Cómo han conseguido acceso a los sistemas?



DGTIC

Ransomware

GENERALITAT VALENCIANA

DGTIC

GENERALITAT VALENCIANA

¿Cómo funciona un ransomware?

* También pueden ser otros links de Internet en los que se descarguen los archivos maliciosos al hacer clic.

** Llamado Command and Control (C&C)

Fuente: Carbon Black Threat Report 2016

statista

DGTIC

GENERALITAT VALENCIANA

Cuando esto ocurre…Nos enfrentamos a un gran problema

- ✓ ¿Quién es el Responsable?
- ✓ ¿Cómo actuamos?
- ✓ ¿A qué nos enfrentamos?
- ✓ ¿Cómo lo contamos?
- ✓ ¿Cuánto va a durar?

DGTIC

GENERALITAT VALENCIANA

Tenemos obligaciones legales:

- ✓ **Notificar al CERT de referencia: CCN-CERT (inmediata) → A través de nuestro CERT CSIRT-CV**

  artículo 33.2. Sin perjuicio de lo establecido en el artículo 19.4 del Real Decreto-ley 12/2018, de 7 de septiembre, las entidades del sector público notificarán al CCN aquellos incidentes que tengan un impacto significativo en la seguridad de los sistemas de información concernidos, de acuerdo con la correspondiente Instrucción Técnica de Seguridad.

- ✓ **Notificar a la Agencia Española de Protección de Datos (72 horas)**

  El artículo 33 del RGPD impone a los responsables de un tratamiento de datos personales la obligación de notificar a la autoridad de control competente las brechas de datos personales cuando sea probable que constituyan un riesgo para los derechos y libertades de las personas.

- ✓ **Denunciar a la Policía el Delito**

- ✓ **Notificaciones afectados (conforme al artículo 34 del RGPD)**

  1. Cuando sea probable que la violación de la seguridad de los datos personales entrañe un alto riesgo para los derechos y libertades de las personas físicas, el responsable del tratamiento la comunicará al interesado sin dilación indebida.

  2. La comunicación al interesado contemplada en el apartado 1 del presente artículo describirá en un lenguaje claro y sencillo la naturaleza de la violación de la seguridad de los datos personales y contendrá como mínimo la información y las medidas a que se refiere el artículo 33, apartado 3, letras b), c) y d).

DGTIC

GENERALITAT VALENCIANA

Y muuuucho trabajo:

Tareas técnicas

- **Contención:** aislamiento infraestructura
- Evaluación del **impacto incidente**
- Evaluación de las **copias de seguridad** para la recuperación y pruebas restauración
- Búsqueda de **evidencias** para investigación y forense
- **Planificación de la recuperación** del servicio con las máximas garantías de seguridad:
    - Creación de una **red limpia**
    - Plan **reinstalación y despliegue** nueva infraestructura: Sistema virtualización, DA, formateo e instalación equipos usuarios
    - Recuperación copias seguridad
    - Creación usuarios y reparto credenciales
    - Configuración electrónica red
    - **Auditoría nueva instalación**

Tareas administrativas

- **Gabinete Crisis**: coordinación y decisión en situaciones de emergencia formado por responsables políticos y personal técnico asesor.
    - **Medidas administrativas**: suspensión de plazos de tramitaciones, firma en papel…
    - **Medidas organizativas**: nuevas formas de organización interna para funcionamiento en contingencia.
    - **Medidas comunicativas**: determina los flujos de comunicación interna y las líneas generales de la comunicación externa.
- Información al equipo de gobierno.
- Información a la oposición.
- **Rueda de prensa / Nota de prensa**: información a la ciudadanía.
- **Reunión con representantes sindicales**.
- **Denuncia a la Policía Nacional**.
- **Notificación a la Agencia Española de Protección de Datos**.

Tiempo de recuperación Sistemas:

- ✓ **99% servicios recuperados** (incluyendo todos los fundamentales y básicos) aprox. 1 mes

- Recuperando los sistemas
- Atendiendo a los usuarios en contexto de crisis

Abril 2020

	Lu	Ma	Mi	Ju	Vi	Sá	Do
14			1	2	3	4	5
15	6	7	8	9 Jueves Santo	10 Viernes Santo	11	12 Domingo de Pascua
16	13 Lunes de Pascua	14	15	16	17	18	19
17	20	21	22	23	24	25	26
18	27	28	29	30			

Mayo 2020

	Lu	Ma	Mi	Ju	Vi	Sá	Do
18					1 Fiesta del Trabajo	2	3
19	4	5	6	7	8	9	10
20	11	12	13	14	15	16	17
21	18	19	20	21	22	23	24
22	25	26	27	28	29	30	31

DGTIC

GENERALITAT VALENCIANA

Agencia Española de Protección de Datos: Brecha de Seguridad

- **Notificación** brecha en menos de 72 horas
- Notificaciones adicionales en circunstancias relevantes
  - Cuando se publica la información en la dark web.
  - Ampliación de información sobre tipos de datos exfiltrados.
- **Requerimiento de información de la AEPD (plazo 15 días)**
  - Solicita información sobre datos sustraídos y acciones emprendidas
- **Informe** :
  - Cronología de hechos y actuaciones.
  - Causas posibles de la brecha.
  - Información sustraída y análisis.
  - Información sobre las fechas de exposición de los datos sustraídos.
  - Medidas de seguridad previas a la brecha.
- **Resolución de Archivo de Actuaciones** : si consideran demostrada la existencia de medidas de seguridad previas y la actuación diligente en el incidente

DGTIC

GENERALITAT VALENCIANA

Tratamiento de la información y riesgos asociados

✓ Depende de:

- La **categoría de los datos** exfiltrados: Datos sensibles/ Datos personales
- **Tipo de datos**: Base de datos /Ficheros / información no estructurada
- **Volumen** de datos

✓ Nuestro ejemplo:

- Procedentes de las **carpetas de red**
- Todo **tipo de ficheros** (pdf, imágenes, ofimáticos)
- **Imposible tratamiento automático**
- **Contenido**: Todo tipo de datos personales. La mayoría categoría básica (incluidos categorías especiales)

- ✓ **Clasificación manual** de cada fichero
- ✓ **Análisis de las categorías de datos**
- ✓ **Evaluación de los riesgos** de cada tipología de datos
- ✓ **Recomendaciones tratamiento** del riesgo
- ✓ **Vigilancia digital** en fuentes abiertas: monitorizar posibles ventas de datos

DGTIC

GENERALITAT VALENCIANA

Análisis de Riesgos de la brecha

RIESGO: Posibles delitos que se podrían cometer utilizando la información exfiltrada, principalmente relacionados con contratación de servicios o compra de bienes.

RECOMENDACIONES GENERALES PARA TRATAMIENTO RIESGOS:

1. **Comunicaciones individualizadas**.
2. **Emisión de un documento-certificado en el que el organismo** confirme el hecho
3. Presentación de **denuncias individualizadas**
4. **Comunicación con las entidades emisoras con aportación de las denuncias para:**
   - Cuentas bancarias: Entidades bancarias
   - Tarjetas sanitarias SIP: Conselleria de sanidad
   - Tarjetas inspección técnica: DGT
5. **Puesta a disposición de la persona afectada de asistencia jurídica** para soporte en caso uso fraudulento.

Tratamiento Riesgos de la brecha

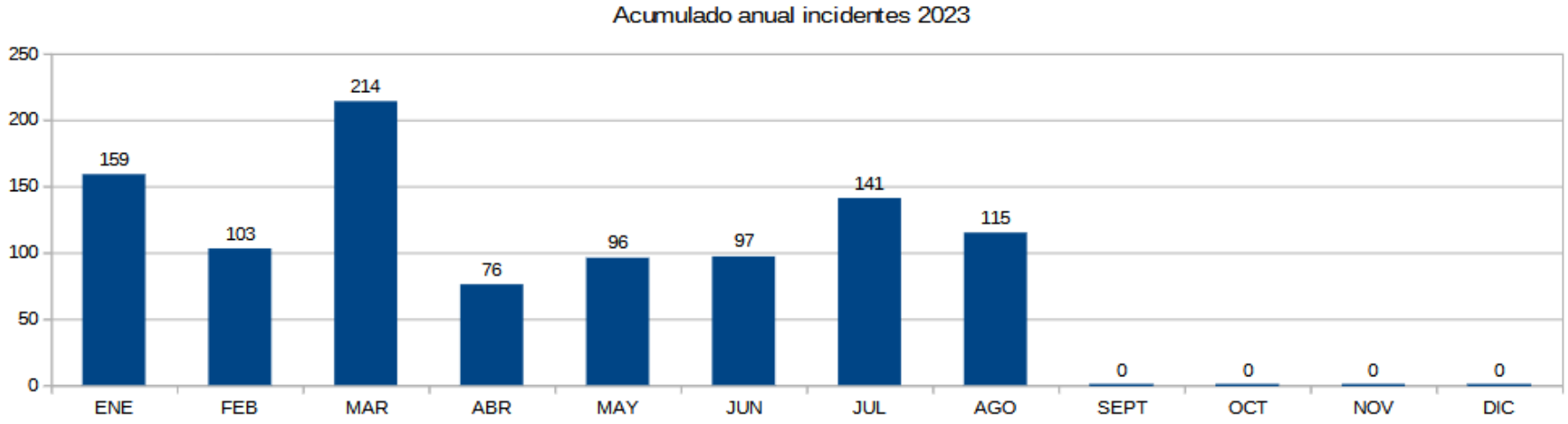
- Tratamiento datos para **comunicación individualizada** a las personas afectadas:
  - Priorizando **colectivos especialmente vulnerables**
  - Colectivos **acotados y perfectamente individualizados** (empleados, usuarios,…)
  - **Acciones protección** derechos y libertades que pudieran verse afectadas

- Tratamiento de datos para la **comunicación general (art 34.3 c) RGPD)**
  - **Bases de datos de afectados**
  - **Información genérica** en la web: Trámite **solicitud información**
  - **Procedimiento de gestión de consultas**
  - **Dificultad de integración de datos** de los afectados (1 persona puede tener datos afectados en distintos expedientes/servicios municipales)

DGTIC

GENERALITAT VALENCIANA

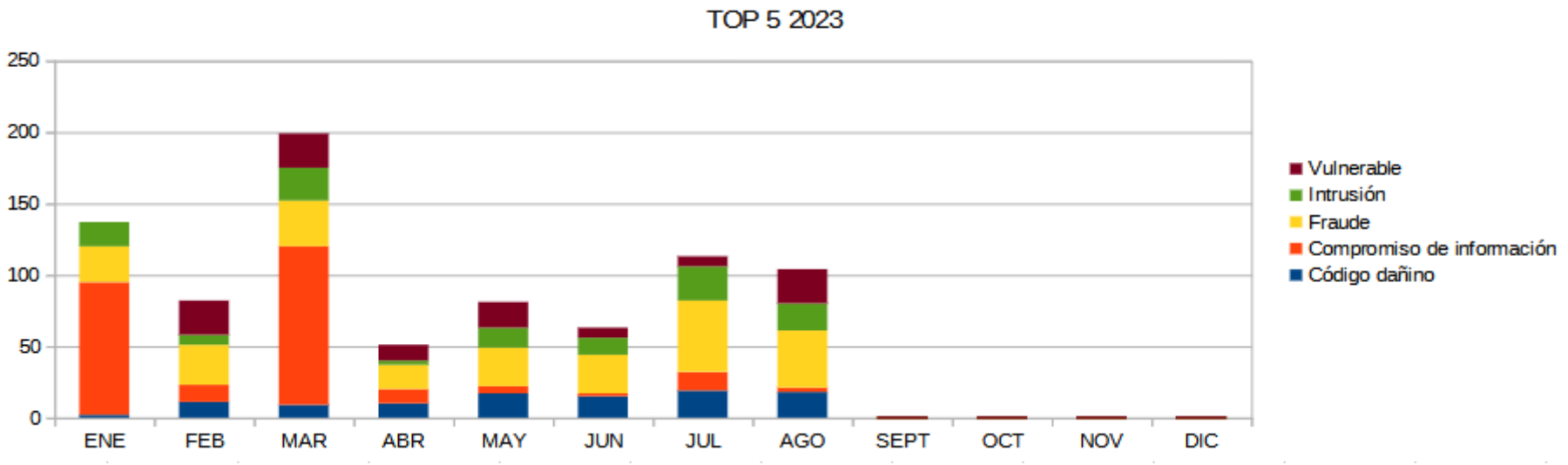
Evolución incidentes GVA:



DGTIC

GENERALITAT VALENCIANA

Incidentes GVA por tipo:

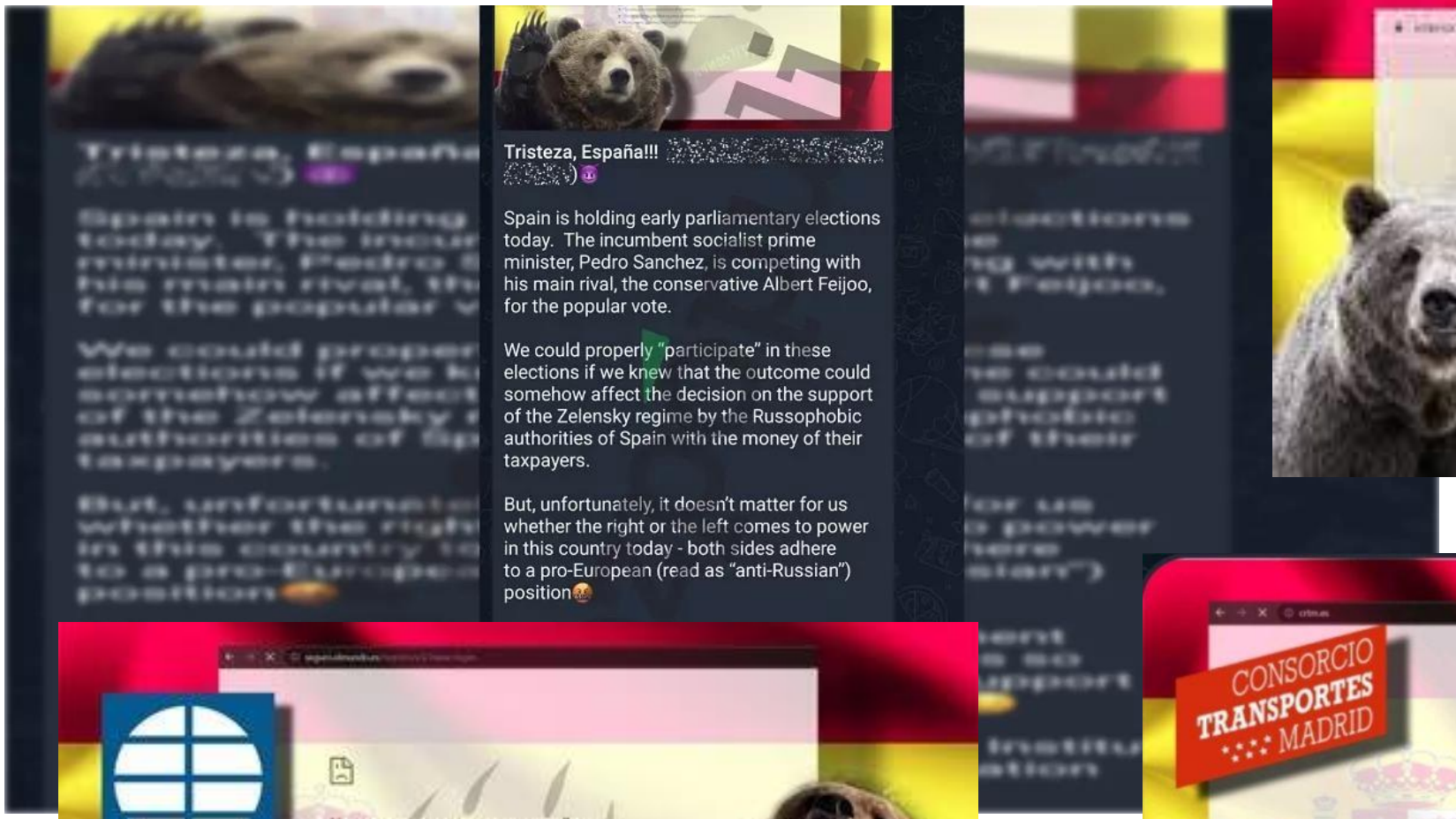


DGTIC

GENERALITAT VALENCIANA

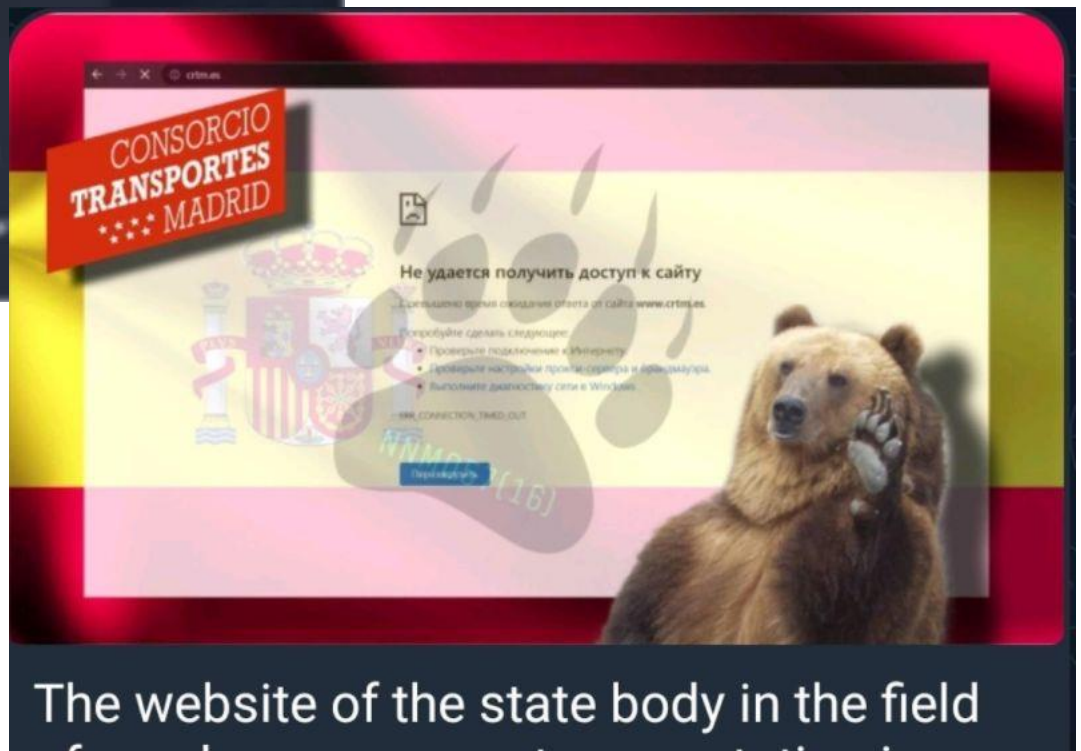
Campañas ataques continuados

- Banca
- Gobiernos y Administraciones Públicas
- Sistemas de Transporte: aeropuertos, ferrocarril, puertos


Tristeza, España!!!
Spain is holding early parliamentary elections today. The incumbent socialist prime minister, Pedro Sanchez, is competing with his main rival, the conservative Albert Feijoo, for the popular vote.
We could properly "participate" in these elections if we knew that the outcome could somehow affect the decision on the support of the Zelensky regime by the Russophobic authorities of Spain with the money of their taxpayers.
But, unfortunately, it doesn't matter for us whether the right or the left comes to power in this country today - both sides adhere to a pro-European (read as "anti-Russian") position


GOBIERNO DE ESPAÑA
MINISTERIO DEL INTERIOR


Не удается получить доступ к сайту


CONSORCIO
TRANSPORTES
MADRID
Не удается получить доступ к сайту
The website of the state body in the field

Refuerzo de medidas de seguridad

El CCN-CERT, a raíz del inicio de la guerra de Ucrania, estableció 5 tipos de escenarios en función del nivel de alerta de materialización de ciberamenazas. La aplicación de unas u otras medidas de seguridad depende de la situación de alerta establecida y el objetivo es articular una respuesta efectiva y garantizar una mejor protección y defensa del sector público.

A lo largo de este tiempo, se han implementado diferentes medidas en función del nivel de alerta decretado. Las principales son:

- Apagado de ordenadores sin utilizar, incluido Educación y Justicia.
- Despliegue del 2FA para el acceso a la nube de Microsoft.
- Mejoras en los sistemas de detección de CSIRT-CV
- Eliminación de permisos de administración de los usuarios del dominio Generalitat.
- Revisión y validación de la política de aplicación de parches de seguridad y corrección de vulnerabilidades.
- Revisión de la segmentación de redes.
- Revisión de la política de copias de seguridad y su almacenamiento. Adopción de nuevas estrategias.
- Implantación de nuevas medidas de protección de correo electrónico: activación de políticas de mejora de la seguridad del correo electrónico (SPF y DKIM).
- Revisión de los niveles de rigurosidad del antivirus. Preparación de distintos niveles.

Además de las medadas implantadas

- ✓ Política de Contraseñas
- ✓ Protección equipo: Antivirus, conf. Seguridad
- ✓ Protección navegación
- ✓ Protección comunicaciones
- ✓ Protección servidores y web
- ✓ Protección aplicaciones
- ✓ Refuerzo sistemas acceso
- ✓ Formación y Concienciación a las personas
- ✓ Establecimiento normas uso seguro

rticipación usuari

estos

- ➢ Usar contraseñas complicadas /caducan
- ➢ No instalar aplicaciones ni dispositivos
- ➢ Navegación web limitada
- ➢ No usar aplicaciones no corporativas
- ➢ Protección de USB
- ➢ No usar plataformas de alojamiento/correo externas
- ➢ No usar correo externo
- ➢ Usar certificados y VPN
- ➢ No usar equipos domésticos
- ➢ **MFA. Autenticación en dos pasos**

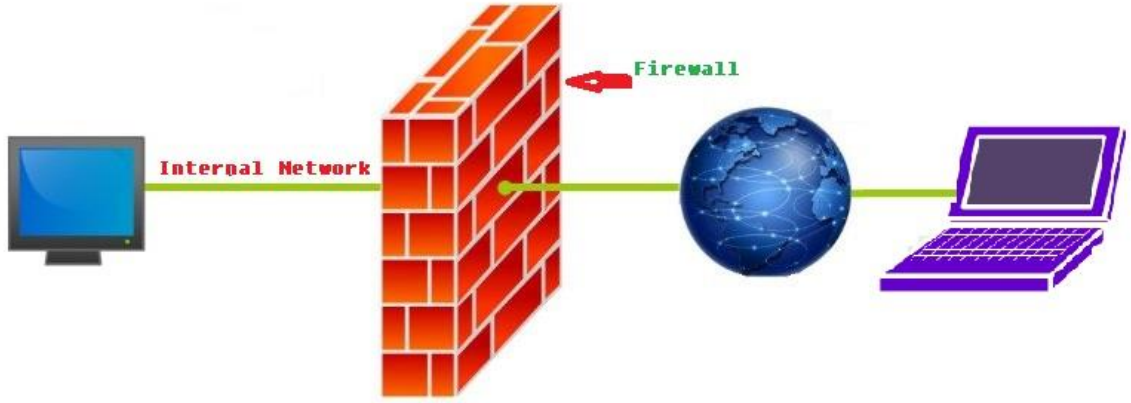
DGTIC

GENERALITAT VALENCIANA

Herramientas de protección y defensa

Cortafuegos	Sistemas de Detección y Prevención de Intrusiones con herramientas avanzadas de detección	Antivirus correo	Antivirus/EDR equipos

Configuraciones de Seguridad equipos	Herramientas de seguridad en M365	Sistemas de protección comunicaciones: Cifrado, VPN



DGTIC

GENERALITAT VALENCIANA

Monitorización, detección y respuesta

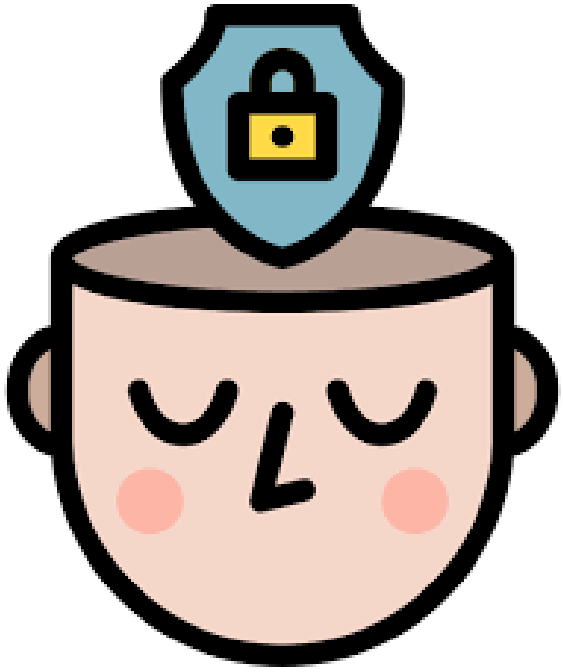
CSIRT-CV
Centre Seguretat TIC
de la Comunitat Valenciana

DGTIC

GENERALITAT VALENCIANA

La medida más importante

Los usuarios/as



Concienciación

DGTIC

GENERALITAT VALENCIANA

[DGTIC Informa] Gràcies pel teu compromís amb la Ciberseguretat

Estimat company / Estimada companya:

Ens posem en contacte amb tu per a **agrair-te el teu compromís amb les noves mesures de ciberseguretat** dutes a terme, en l'últim any, per la Direcció General de Tecnologies de la Informació i les Comunicacions (DGTIC). Som conscients que, en alguns casos, la seua implementació ha suposat un gran esforç d'adaptació per al personal de la Generalitat, per la qual cosa **valorem la teua comprensió, adaptació i col·laboració** per al continu funcionament del servei públic en la Comunitat Valenciana.

Les mesures de seguretat estan fent efecte i s'han implementat amb èxit gràcies a la teua imprescindible ajuda. Entre tots, **estem aconseguint protegir l'organització, així com les dades de la ciutadania** que custodia l'Administració.

En ciberseguretat, ni un pas arrere

Com hauràs pogut comprovar, s'han establit **diverses mesures** relacionades amb la protecció del correu electrònic corporatiu, l'increment de la rigorositat de l'antivirus, la instal·lació del doble factor d'autenticació, el canvi obligatori de contrasenyes, l'apagat diari dels equips, la limitació de la instal·lació d'aplicacions i la priorització de pegats de seguretat i correcció de vulnerabilitats. També s'han adoptat **altres mesures no visibles**, com l'elaboració de pautes

Reactivació de la campanya "Més Segurs"

Comunicación Ciberseguridad

En sintonía con estas acciones y con el objetivo de promocionar la cultura de la ciberseguridad y las buenas prácticas en el uso de las nuevas tecnologías en la Generalitat, CSIRT-CV va a reactivar la campaña de concienciación "**Més Segurs"**.

Además, la DGTIC va a aprovechar el anuncio de la campaña para **agradecer a los usuarios y usuarias finales los esfuerzos de adaptación y colaboración** durante la implementación de las medidas de mejora de la ciberseguridad en la Generalitat.

DGTIC

GENERALITAT VALENCIANA

¿Como podemos participar?

Manténte alerta

DGTIC

GENERALITAT VALENCIANA

Estando alertas

DGTIC

GENERALITAT VALENCIANA

Cuéntanoslo

DGTIC

GENERALITAT VALENCIANA

En caso de incidente:

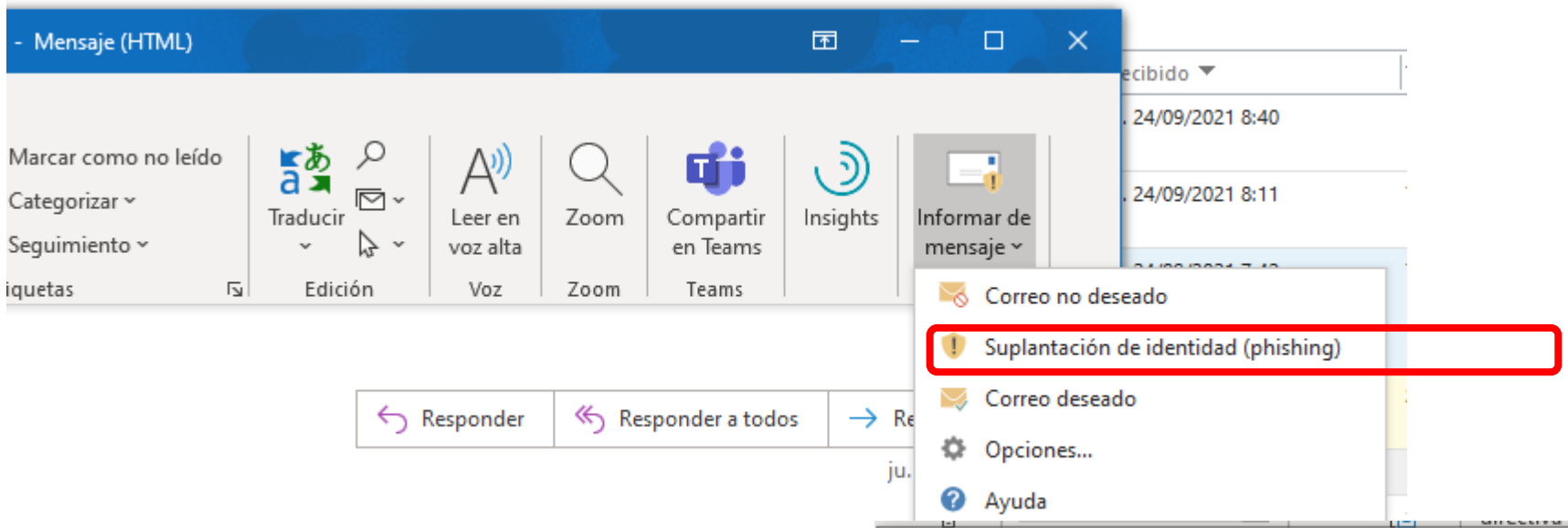
- Reportarlo a csirtcv@gva.es para poder conocer el alcance del ataque y cuantificarlo adecuadamente.

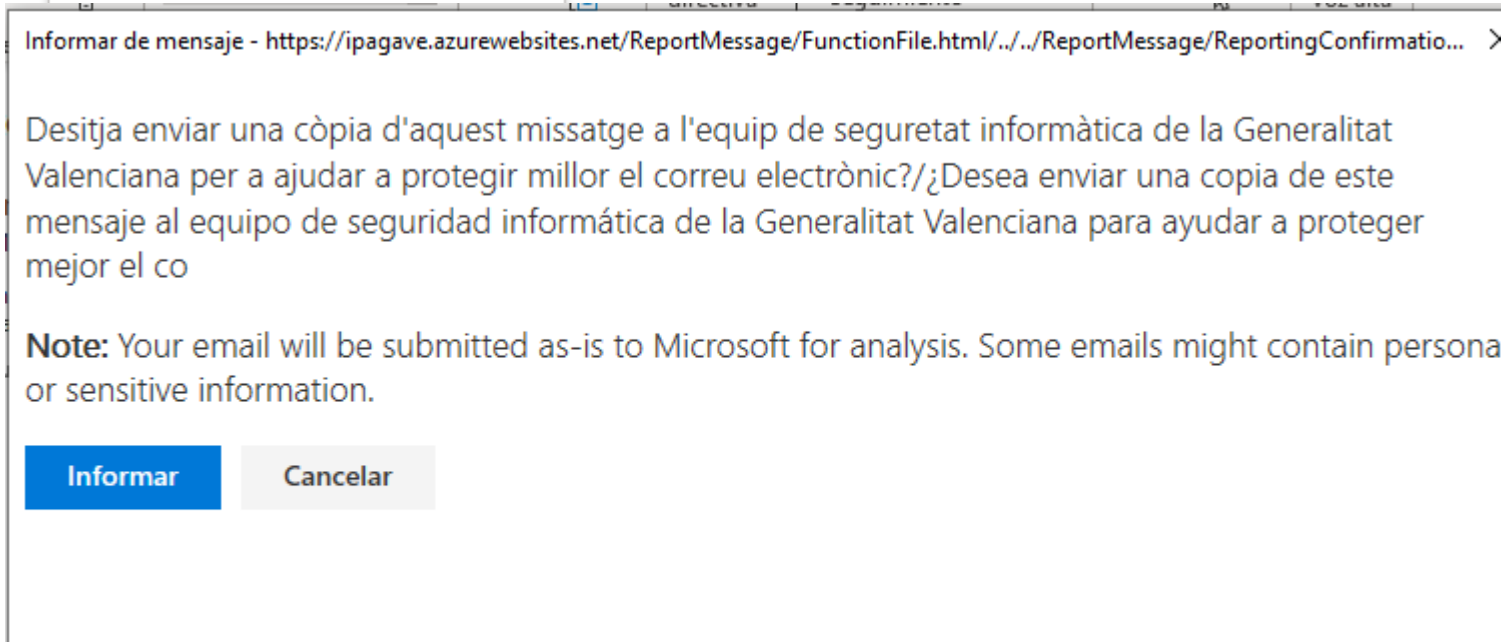
- Contactar con Servicio de Atención al Usuario CAU-TIC

963 866011 (si estás en Justicia)
963 985309 (si estás en Centros Educativos)
963 985300 (resto del Consell)

- Correos de Phishing:

Informar de Phishing





Desde CSIRT-CV:

- Se bloquean los enlaces
- Se bloquean los mensajes del remitente

DGTIC

https://concienciat.gva.es/infografias/

GENERALITAT VALENCIANA

DGTIC

GENERALITAT VALENCIANA

Fórmate

DGTIC

GENERALITAT VALENCIANA

Adquirir buenos hábitos de Ciberseguridad

- Cursos IVAP:

	Curso	Horas	Tipo
1	CURSO CIBERSEGURIDAD EMPLEADOS GVA	15	Autoformativo
2	SEGURIDAD EN DISPOSITIVOS MÓVILES	15	Telepresencial
3	SEGURIDAD Y BUENAS PRÁCTICAS EN EL USO DE LOS SISTEMAS DE INFORMACIÓN (NIVEL I)	30	Telepresencial
4	SEGURIDAD PRÁCTICA EN EL USO DE INTERNET Y LAS TIC	20	On line
5	SEGURIDAD Y BUENAS PRÁCTICAS EN EL USO DE LOS SISTEMAS DE INFORMACIÓN (NIVEL II)	20	Telepresencial
6	BUENAS PRÁCTICAS Y USO SEGURO DE LAS TECNOLOGÍAS DE LA INFORMACIÓN EN LA GENERALITAT	25	On line
7	SEGURIDAD PARA INFORMÁTICOS	15	Telepresencial

Apuntes IVAP: https://ivap.gva.es/es/apunts-ivap

DGTIC

Píldoras formativas

GENERALITAT VALENCIANA

GENERALITAT VALENCIANA
IVAP
Institut Valencià d'Administració Pública

Conselleria de Justicia, Interior y Administración Púb

Buscar Val / C

Carpeta ciudadan

ÁREAS TEMÁTICAS

- ASUNTOS EUROPEOS
- CONTRATACIÓN
- INTEGRIDAD INSTITUCIONAL, TRANSPARENCIA Y BUEN GOBIERNO
- JURÍDICO-PROCEDIMENTAL
- SEGURIDAD Y SALUD LABORAL
- **TECNOLOGÍA DE LA INFORMACIÓN Y COMUNICACIÓN**

TECNOLOGÍA DE LA INFORMACIÓN Y COMUNICACIÓN

- Aprenent M365 (Iniciativa FUNCION@gva) **(Es necesario pertenecer a una conselleria de la Generalitat y tener un usuario de Microsoft 365 para acceder a estos recursos)**
- Cursos de entrenamiento para elevar tu nivel
- Guía de seguridad en el teletrabajo. CSIRT-CV
- Buenas prácticas en dispositivos móviles. CSIRT-CV
- Campaña de Whatsapp - Guía de utilización segura. CSIRT-CV
- Guía de buenas prácticas para el borrado seguro de dispósitivos móviles. CSIRT-CV
- Guía de uso seguro de Android. CSIRT-CV
- Guía de uso seguro de certificados digitales. CSIRT-CV
- Guía de uso seguro de iOS. CSIRT-CV
- Guía para identificar phising. CSIRT-CV
- Guía sobre utilización segura de Dropbox. CSIRT-CV

DGTIC

GENERALITAT VALENCIANA

Adquirir buenos hábitos de Ciberseguridad

- Cursos CSIRT-CV.

concienciaT
Una iniciativa de CSIRT-CV

https://concienciat.gva.es/

Video Interactivo: Correos phishing

Video Interactivo: Ingeniería Social

Video Interactivo: Protección de la Información

DGTIC

GENERALITAT VALENCIANA

Adquirir buenos hábitos de Ciberseguridad

✓Centro de entrenamiento digital.

Área 4: Seguridad

14. Protección de dispositivos

15. Protección de datos personales y privacidad

DGTIC

GENERALITAT VALENCIANA

Estando informados

GENERALITAT VALENCIANA

CSIRT-CV
Centre Seguretat TIC de la Comunitat Valenciana

Conselleria de Hacienda y Modelo Económico

Buscar...

Val / Cas

Está en: Centro Seguridad TIC de la Comunidad Valenciana » **Boletines**

MENÚ

- Inicio
- CSIRT-CV
- Actualidad
- **Boletines**
- Documentación
- Recursos externos
- Aplicaciones CSIRT-CV
- Contáctanos
- Hemeroteca
- RFC2350 Description

CONTÁCTANOS

¿Quieres recibir nuestros boletines? Suscríbete

Accede a nuestra hemeroteca de boletines

24/09/2021

Boletín 11/09/2021 – 24/09/2021

Nuevo boletín quincenal donde os comentamos las principales noticias relacionadas con el mundo de la ciberseguridad.Iniciamos con una noticia en la que un grupo de ciberdelincuentes han conseguido comprometer la red informática de las Naciones Unidas, con el fin de

Continuar...

10/09/2021

Boletín 28/08/2021 – 10/09/2021

Una quincena más os remitimos nuestro boletín con las principales noticias relacionadas con el mundo de la ciberseguridad.Comenzamos con la noticia relacionada con la empresa EskyFun, asociada al mundo de los videojuegos, concretamente con los juegos de rol para Android.

Continuar...

27/08/2021

Boletín 14/08/2021 – 27/08/2021

Una vez más os hacemos llegar nuestro boletín con las principales noticias relacionadas con el mundo de la ciberseguridad.Empezamos el boletín destacando una noticia relacionada con una brecha de datos que se ha producido en la Fundación de Investigación de

Continuar...

DGTIC

GENERALITAT VALENCIANA

Comparte tu conocimiento

DGTIC

GENERALITAT VALENCIANA

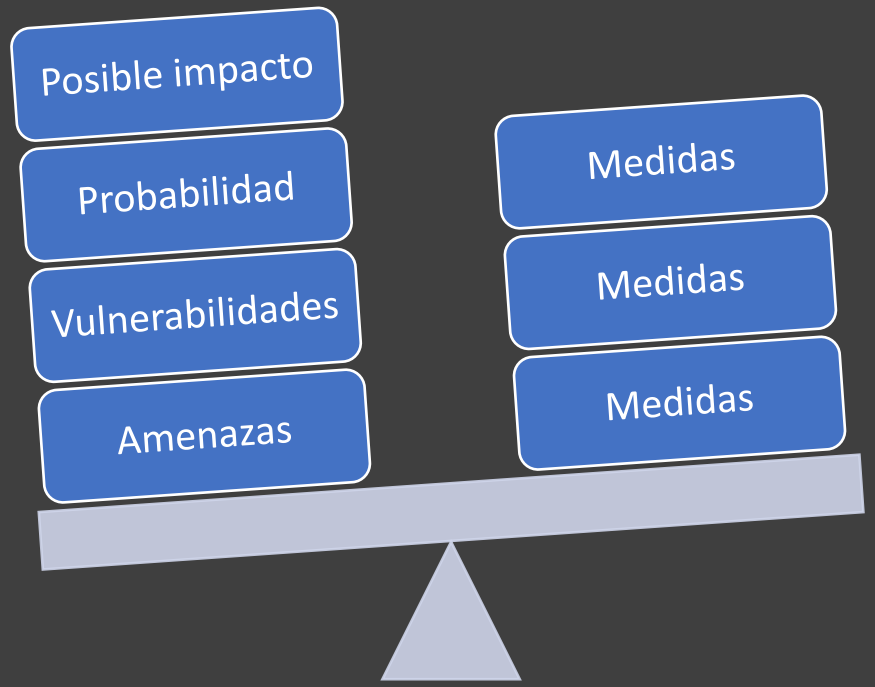
DGTIC

GENERALITAT VALENCIANA

Es cosa de todos

La seguridad Total NO EXISTE

Nivel de RIESGO Aceptable



DGTIC

GENERALITAT VALENCIANA

La colaboración de todos es necesaria para estar "Més Segurs" en la red y los sistemas de la Generalitat y así garantizar los servicios y la protección de nuestra ciudadanía.