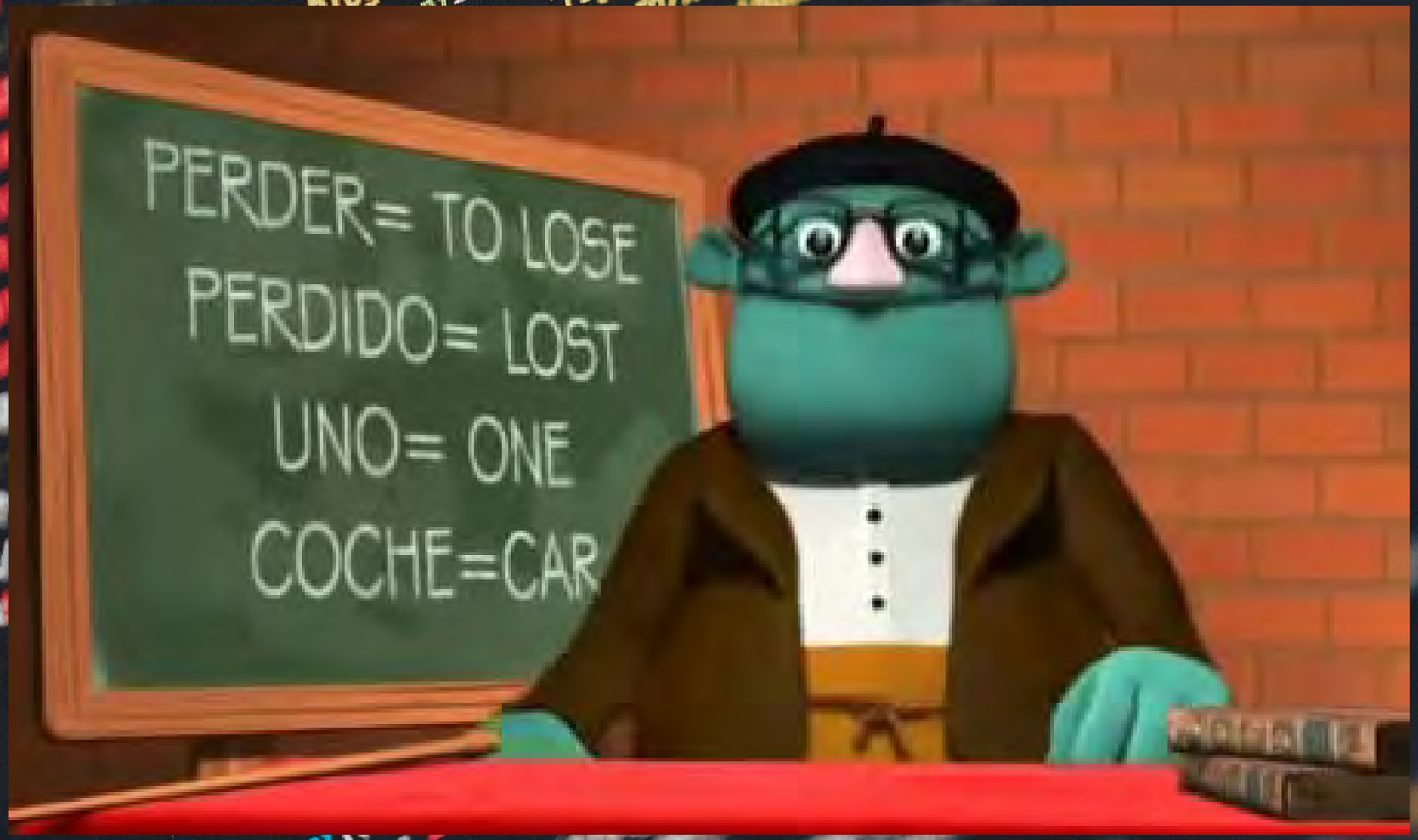
LA COMPRENSIÓN Y APLICABILIDAD DE LOS PROCESOS VERTICALES Y HORIZONTALES DE LA CIBERSEGURIDAD

Santiago G. González
Jefe de la Oficina Técnica DGP
Responsable de Ciberseguridad de GPO

Mayo de 2024

Financiado por la Unión Europea NextGenerationEU
Plan de Recuperación, Transformación y Resiliencia
España | digital 2026
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD
UNIVERSIDAD DE GRANADA


PERDER= TO LOSE
PERDIDO= LOST
UNO= ONE
COCHE=CAR

CENTRO DE PROCESO DE DATOS

PLAN DIRECTOR SEGURIDAD

Financiado por la Unión Europea NextGenerationEU
Plan de Recuperación, Transformación y Resiliencia
España | digital 2026
incibe_
UNIVERSIDAD DE GRANADA

ÍNDICE

La ciberseguridad como un desarrollo horizontal en el Centro de Proceso de Datos (CPD)

1.- RIESGO Y TECNOLOGÍA

PRINCIPIOS FUNDAMENTALES

1. **Identificar**.
    a. No podemos proteger lo que no sabemos que tenemos.
2. **Proteger**
    a. Se debe Proteger todo aquellos de ser susceptible de ser vulnerado.
3. **Detectar**
    a. Saber lo que está pasando en nuestra organización
4. **Responder**
    a. Saber como debemos reaccionar. Planes establecidos
5. **Recuperar**
    a. ¿Respaldamos nuestra información? ¿podemos reconstruir nuestros datos ? ¿Estamos preparados para recuperar?
6. **Lecciones aprendidas**

1.1 Cibercrisis

"Situación de baja probabilidad del ámbito de la ciberseguridad, que cuando sucede genera un gran impacto y cuyos efectos perduran en el tiempo"

Indica las etapas en que la organización se encuentra expuesta e involucrada por formar parte de la organización

[González S., 2020]

PRE-CRISIS

- **Se proporcionan los servicios habituales realizando acciones preventivas. Se potencia la anticipación.**

CRISIS

- **La organización se encuentra bajo la amenaza real como consecuencia de una vulnerabilidad. Estado inestable.**

POST-CRISIS

- **Estado en que la organización debe llevar a cabo acciones conducentes a la superación de las etapas anteriores.**

1.2 Objetivos Específicos

1. Implementación a nivel CPD en concreto, de un Plan director que venga a complementar el Plan General de Ciberseguridad del Cuerpo Nacional de Policía.
2. Crear y dotar de transversalidad a un canal de comunicaciones que haga la ciberseguridad un proceso global.
3. Obtención de altas capacidades de cohesión con tecnologías de diferentes fabricantes.
4. Garantizar la cadena de valor en fabricantes, desarrolladores y suministradores de servicio.
5. Diversificación en tecnologías de procesamiento, almacenamiento, monitoreo y recuperación.
6. Proporcionar capacidad de análisis en tiempo real y adaptabilidad a la arquitectura policial y a sus unidades.

Gobernanza CiberSeg

Guías STIC

NIS2

RD 43/2021

RDL seguridad de las redes y S.I.

TIER

ENS 2022

Esquema Nacional de Seguridad

1.3 Marco metodológico

Composición

Análisis de la situación y estado de madurez en ciberseguridad de los Sistemas TI

Afloramiento de nuevos escenarios conducentes a nuevas amenazas y por ende a nuevos riesgos

Conocer estos riesgos/amenazas junto con la valoración del nivel de tolerancia a los mismos se torna complicado. Matrices de Riesgos

La certificación TIER es un estándar que permite clasificar la fiabilidad y disponibilidad de un Data Center - Uptime Institute

Potenciación del conocimiento de las propias debilidades y comprensión de técnicas de ataques

Desarrollo de un Plan Director de Seguridad

Núcleo Marco Cybersecurity framework 1.1

[Stouffer K., 2020]
[Dondossola G., 2009]

2.- NECESIDADES Y PROYECTOS

FASES DEL PLAN DIRECTOR DE SEGURIDAD

Fase 1 SITUACIÓN REAL DE LA ORGANIZACIÓN EN MATERIA DE CIBERSEGURIDAD

Fase 2 ESTRATEGIA DE LA ORGANIZACIÓN

Fase 3 DEFINICIÓN DE PROYECTOS E INICIATIVAS

Fase 4 PRIORIZACIÓN DE LOS PROYECTOS

Fase 5 APROBACIÓN DEL PLAN DIRECTOR DE SEGURIDAD

Fase 6 PUESTA EN MARCHA

2.1 Necesidades

Implementación a nivel CPD en concreto, de un Plan Director que venga a complementar el Plan General de Ciberseguridad del Cuerpo Nacional de Policia

Directivas

NIS

Guías STIC

NIS2

RD 43/2021

RDL seguridadde las redes y S.I.

TIER

ENS 2022

Esquema Nacional de Seguridad

2.2 Proyectos

www.policia.es

Portal del ciudadano

2.3 Proyectos

Fuente: www.policia.es

- PROMETEO (Evolución de SIDENPOL)
- D.N.I. / Pasaporte
- INVESTIGA
- ORION
- OVD (Oficina Virtual de Denuncias)
- @FirmaFederada
- MAPOL
- DNI en el Móvil - DnieExpress
- iZeta - AXON Commander

2.4. Estadísticas

- **Sistemas Windows**
  - 300 máquinas virtuales
  - 60 máquinas físicas
- **Sistemas Linux**
  - 250 Máquinas Virtuales
  - 50 máquinas físicas
- **Sistemas Solaris**
  - 285 máquina virtuales Sparc
  - 70 máquinas físicas
- **Bases de datos**
  - 750 Bases de datos (Pro-Prepro-Des)
- **Almacenamiento**
  - 20 Peta-bytes (estático)
  - 2 Peta-byte (distribuido)

3.- PROVEEDORES T.I.C.

PROVEEDORES DE TECNOLOGÍAS

Adaptadas a los tiempos actuales

1. **Integridad, confidencialidad y disponibilidad**
2. **Tipos de normativa aplicable a cada entorno**
3. **Enfoques referentes a la seguridad**
   a. **Cadena de valor**
   b. **Alineación de las tecnologías con los objetivos**
   c. **Continuidad de negocio**
   d. **Capacidad de resiliencia**

TECNOLOGÍAS

POLICÍA NACIONAL

RED HAT OPENSHIFT Container Platform

kubernetes

KVM

Red Hat Enterprise Linux

openstack CLOUD SOFTWARE

Microsoft Hyper-V

Windows Server 2022

BUGBUSTERS

vmware ORACLE VIRTUALIZATION

SUSE

docker

4.- ESTRATEGIA Y CIUDADANÍA.

Adecuación al ENS

Fuente : CCN-CERT

4.1- CIUDADANÍA.

CIUDADANÍA

Aportes a la ciudadanía

1. Programa Colectivos de Ciudadanos
2. Comercio Seguro
3. Seguridad en la vivienda
4. Consejos para prevenir determinadas estafas
5. Secuestros virtuales
6. Ocupaciones ilegales
7. Plan Mayor-Seguridad
8. Plan Turismo Seguro
9. Plan Director para la Convivencia y Mejora de la Seguridad en los Centros Educativos y sus Entornos
10. Delitos de Odio

www.policia.es

SÍGUENOS...

https://twitter.com/policia

https://www.facebook.com/PoliciaNacional

https://www.youtube.com/user/Policia

https://www.instagram.com/policianacional/?hl=es

https://telegram.im/@policianacional

https://www.pscp.tv/policia/1mnxeaXrOpYxX

https://www.tiktok.com/@policia

https://c1b3rwallacademy.usal.es/2022-2023/

https://www.linkedin.com

4.2- CIUDADANÍA.

POLICÍA NACIONAL

AUMENTA LA INVERSIÓN EN PROTECCIÓN

La administración regional sufre unos 60 ciberataques de alta intensidad cada mes

La ciberseguridad es una cuestión cada vez más relevante en la sociedad actual, y la Comunidad de Mu
decidido invertir 2
es de euros al año
zarla y hacer frente a los ataques que se produzc

Los ciberataques contra la administración pública aumentaron un 455% en 2022

El auge del teletrabajo, el impulso a la digitalización y la proliferación de las redes sociales han afectado.

- EE. UU. desmantela una red internacional de secuestro de datos en internet

IALIZADA 27/1/2023 A LAS 18:11

El ciberataque al SEPE se produjo tras caducar un contrato de mantenimiento informático

Pese a que la documentación detalla que el contrato expiró el 28 de febrero sin ninguna opción de prórroga, Trabajo asegura que las empresas prolongaron sus servicios sin mayor coste hasta adjudicar una licitación

Sitios web de puertos españoles sufrieron ciberataques simultáneos

Estos ataques, que han afectado a importantes sitios web portuarios, han dejado al descubierto la vulnerabilidad de los sistemas digitales en el ámbito estatal

a CAV registra 6086 delitos informáticos en el primer trimestre de 2023, un 22 % que el año anterior

Publicado: 06/06/2023 12:51 (UTC+2)
Última actualización: 06/06/2023 13:57 (UTC+2)

5364 (un 19 % más) fueron ciberestafas, 279 falsificaciones de identidad (un 37 % más), ción de secretos (un 15 % más), 44 amenazas o coacciones (un 4 % menos), 25 delitos un 108 % más) y los otros 11 fueron ciberataques (un 83 % más).

ATAQUES INFORMÁTICOS >

El Ministerio de Trabajo sufre un ciberataque, tres meses después de ser 'hackeado' el SEPE

El organismo trabaja con el Centro Criptológico Nacional para determinar el origen y el impacto. Informa que ha sido un 'ransomware', que el SEPE no está afectado y que no les han pedido ningún rescate

Detenido Alcas hood' de los 'hackers españoles, por crear un Google de datos para mafias criminales

José Luis Huertas, de 19 años, que suplantó a Paolo Vasile y expidió él mismo carnets de conducir auténticos tras entrar en la DGT, había entrado ahora en las bases de la CGPJ, donde su guardan todos los pleitos de España

ESPAÑA / CIBERSE

Una banda de hackers afines al Kremlin lanza un ciberataque contra puertos en España

ESPAÑA

Ciberataque al Poder Judicial: rastrean el móvil del segundo hacker por sus operaciones con 'criptos'

El segundo detenido por el robo masivo de datos a medio millón de españoles ha vuelto a comparecer en la Audiencia Nacional para dar cuenta del movimiento con criptomonedas procedente de la venta de estos datos

- El juez envía a prisión a un colaborador del hacker que robó datos de medio millón de españoles

INICIO / INCIBE / Sala de prensa / Los incidentes de ciberseguridad de 2023, gestionados por INCIBE, aumentan en un 24% respecto al año anterior

Los incidentes de ciberseguridad de 2023, gestionados por INCIBE, aumentan en un 24% respecto al año anterior

24/04/2024

Más de 7.000 incidentes están relacionados con contenido abusivo, como pornografía infantil, delitos de odio o ciberacoso.

Balance Ciberseguridad 2023 INCIBE

Financiado por la Unión Europea NextGenerationEU

Plan de Recuperación, Transformación y Resiliencia

España | digital 2026

incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD

UNIVERSIDAD DE GRANADA

ÚLTIMOS CIBERATAQUES 2024 ESPAÑA

Enero 2024: Un hacker interrumpe el servicio en Orange

Enero 2024: El Ayuntamiento de Calvià (Mallorca) sufre un ataque de ransomware

Enero 2024: Web falsa de la cadena de perfumerías Douglas

Enero 2024: Ataque a un Concello gallego

Marzo 2024: FIATC Seguros confirma una filtración de datos

Marzo 2024: Las Fuerzas Armadas también están en el punto de mira

Abril 2024: Un ataque que afecta al transporte público de Guadalajara

Abril 2024: La consultora tecnológica Ayesa también es puesta a prueba

Abril 2024: El Confidencial tiene que responder a un hackeo

Enlace a las noticias

CIBERATAQUES EN GRANADA

06 de octubre de 2023:

Investigan posibles ciberataques rusos contra webs públicas de Granada durante la Cumbre europea

Enlace a las noticias

10 de julio de 2023:

“El 70% de los ciberataques en Granada se producen en pequeñas empresas (Javier Delgado, director comercial de Sinergia Ciberseguridad y profesor de la Universidad de Granada)

Enlace a las noticias

28 enero 2021:

La UGR denuncia ante el CNI un ataque cibernético masivo en plenos exámenes on line

Enlace a las noticias

5. - CONCLUSIONES.

1. **Definición de un punto de partida PDS**
2. **Establecimiento del estado real de los sistemas**
3. **Inventario de activos y análisis de riesgos**
    a. **Establecidas las etapas del Plan Director de Seguridad**
4. **Definición de proyectos enfocados a la mejora d la ciberseguridad y ciberresiliencia.**
    a. **Demandados por la propia institución.**
    b. **Demandados por la ciudadanía.**
5. **Estrategia operacional.**
6. **Concienciación / Implicación de la alta dirección**

Financiado por la Unión Europea
NextGenerationEU

GOBIERNO DE ESPAÑA
MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA

Plan de Recuperación, Transformación y Resiliencia

España | digital 2026

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD

UNIVERSIDAD DE GRANADA

SI CREES QUE LA TECNOLOGÍA PUEDE SOLVENTAR TUS PROBLEMAS DE SEGURIDAD, ENTONCES NO ENTIENDES LOS PROBLEMAS Y NO ENTIENDES DE TECNOLOGÍA.

Bruce Schneier

- DNI
65430C
FIRMA)

Firmado digitalmente por SANTIAGO GONZALEZ GONZALEZ - DNI 03465430C (FIRMA)
Nombre de reconocimiento (DN): c=ES, o=MINISTERIO DEL INTERIOR, ou=CERTIFICADO ELECTRONICO DE EMPLEADO PUBLICO, ou=AMBITO DEL CUERPO NACIONAL DE POLICIA, serialNumber=IDCES-03465430C, sn=GONZALEZ GONZALEZ - DNI 03465430C, givenName=SANTIAGO, cn=SANTIAGO GONZALEZ GONZALEZ - DNI 03465430C (FIRMA)
Fecha: 2024.05.14 12:55:49 +02'00'