ECIJA

CIBERSEGURIDAD
Marco Jurídico y Regulatorio en U.E y España

Jesús Yañez Colomo
Socio de ECIJA
jyanez@ecija.com

México 6/11/2019

Nuestro equipo

87
socios

450
profesionales

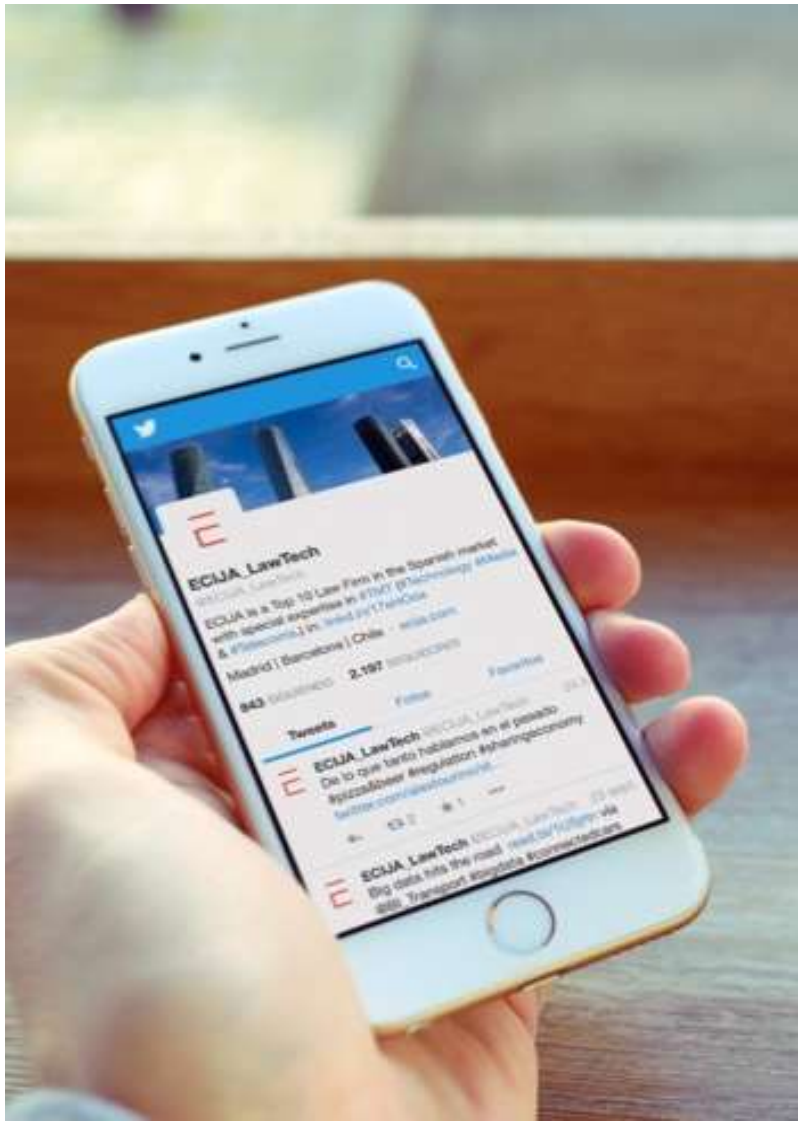
20
oficinas

12
países

ECIJA

Oficinas

ECIJA

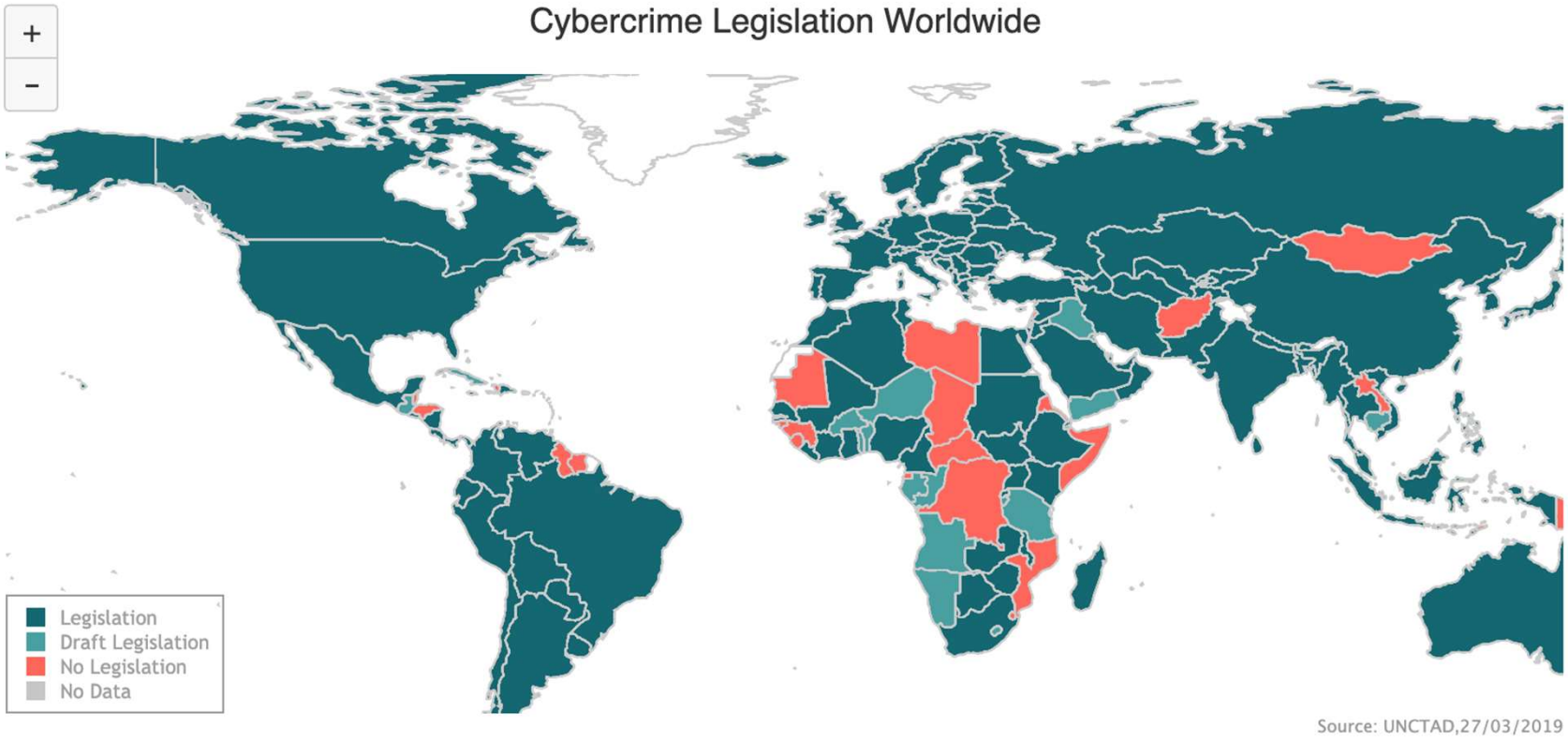


1. Normativa sobre Ciberdelitos
2. Normativa sobre Ciberseguridad
3. Medidas de Seguridad

ECIJA

Ciberdelitos

- Regular los delitos cometidos por medios electrónicos es una forma reactiva de frenar el cibercrimen.
- La gran mayoría de países han creado normas que imponen penas para cibercriminales.



- **Los delitos cometidos son los mismos delitos clásicos** (robo, estafa, falsedad documental, delitos contra la propiedad intelectual o secretos empresariales, etc…).
  Lo que ha cambiado es la forma de cometerlos

ECIJA

Convenio de Budapest

- Firmado por 67 países hasta el momento. Firmado pero no ratificado por Irlanda, Suecia y Sudáfrica.

- **México** se encuentra en trámite de adhesión en la actualidad,.

- Su principal **objetivo**, es aplicar una **política penal común** encaminada a la protección de la sociedad contra el cibercrimen, especialmente mediante la adopción de una **legislación adecuada y el fomento de la cooperación internacional.**

    - Armonización de los elementos nacionales de derecho penal de fondo de infracciones y las disposiciones conectados al área de los delitos informáticos.
    - Ajustar las normas de derecho procesal para la investigación y el enjuiciamiento de esos delitos, así como la aceptación de pruebas y evidencias en formato electrónico.
    - Establecimiento de un régimen rápido y eficaz de la cooperación internacional. Prevé la creación de una red de 24/7 para garantizar una asistencia rápida entre las Partes Colaboradoras

- **Delitos definidos:** acceso ilícito, interceptación ilícita, ataque a la integridad de datos, ataques a la integridad del sistema, abuso de los dispositivos, falsificación informática, fraude informático, los delitos relacionados con la pornografía infantil y los delitos relacionados con infracciones de la propiedad intelectual y de los derechos afines.

- **Protocolos posteriores que complementan el convenio:**
    - Xenofobia y racismo a través de sistemas informáticos. Ya aprobado.
    - En la actualidad 8 protocolos adicionales en preparación. El más inminente dedicado a las pruebas y evidencias en formato electrónico.

- **Principales programas actuales auspiciados por el Consejo de Europa en relación al Convenio de Budapest:**
    - Cybercrime Programme Office of the Council of Europe (C-PROC): Soporte.
    - Octopus: Conferencias.

ECIJA

España

- Delitos regulados en el **Código Penal** (Ley Orgánica 10/1995, de 23 de noviembre=.

- **La tipificación de los delitos es similar a la de los delitos clásicos** (robo, estafa, falsedad documental, delitos contra la propiedad intelectual o secretos empresariales, etc…). **Lo que ha cambiado es la forma de cometer estas acciones a través de medios digitales.**

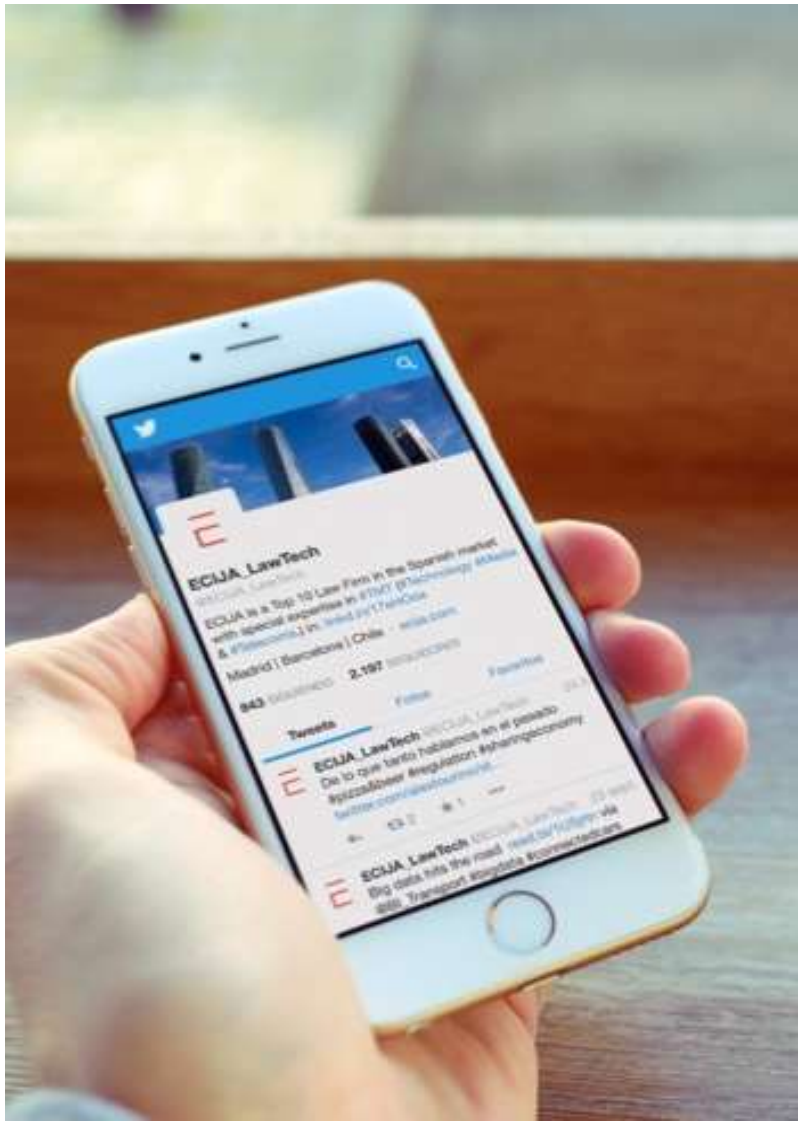
- Los **más habituales** en España son (datos del Observatorio Español de Delitos Informáticos – OEDI)

    - Acceso e interceptación ilícita: Descubrimiento o revelación de secretos, acceso ilegal informático, otros relativos al mercado o a los consumidores. Hasta 2 años de prisión.
    - Amenazas y coacciones a grupos étnicos, religiosos, autoridades, personajes públicos. Hasta 5 años de prisión.
    - Delitos contra el honor: calumnias e injurias. Hasta 2 años de prisión.
    - Actos delictivos contra la propiedad intelectual/industrial. Hasta 4 años de prisión.
    - Delitos sexuales Exhibicionismo, provocación, acoso o abuso sexual, corrupción de menores/incapacitados, pornografía de menores. Hasta 9 años de prisión
    - Falsificación informática. De identidad, de moneda, posesión de los materiales y herramientas necesarias para falsificar. Hasta 3 años de prisión.
    - Fraude informático. Estafas principalmente en ámbito bancario. Hasta 6 años de prisión.
    - Interferencia en datos y sistema. Ataques informáticos como tal. Hasta 2 años de prisión.

- **RESPONSABILIDAD DE LA PERSONA JURÍDICA (EMPRESA) EN ESPAÑA:**

    - Las personas jurídicas SÍ pueden ser responsables penalmente en España.
    - Puede haber **responsabilidad para los administradores** de las entidades cuando de manera negligente no ejerzan sus funciones. Existen sanciones impuestas por el Banco de España a administradores por la toma de decisiones contrarias a la normativa del sector financiero (no implementar las medidas de seguridad necesarias),

ECIJA



1. Normativa sobre Ciberdelitos
2. Normativa sobre Ciberseguridad
3. Medidas de Seguridad

ECIJA

	P.DATOS	SEGURIDAD INFORMACIÓN	ENTIDADES FINANCIERAS
EUROPA	RGPD enisa European Network and Information Security Agency	NIS enisa European Network and Information Security Agency	R.PSD2 EBA EUROPEAN BANKING AUTHORITY EUROPEAN CENTRAL BANK
ESPAÑA	aepd agencia española protección datos	CCN-CERT incibe-cert_ ens Esquema Nacional de Seguridad	BANCO DE ESPAÑA

ESQUEMA CERTIFICABLE EUROPEO 2020

ESQUEMA CERTIFICABLE ENISA 2020

ECIJA

DIRECTIVA NIS

Directiva de seguridad de las redes y sistemas de información 6 de julio de 2016. Ha comenzado a aplicarse en 2018

Directiva NIS

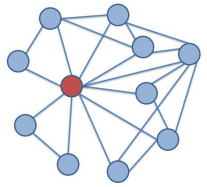
Niveles desiguales de protección de los consumidores y las empresas en la UE

→ Seguridad de las redes y sistemas de información de la Unión

Operadores de servicios esenciales y los proveedores de servicios digitales

1 Establece un marco común de seguridad (evita la normativa nacional)

2 Notificar los incidentes → efecto perturbador,



Creación de una **red de cooperación**

3 Implementar medidas de seguridad suficientes. Marco certificable (2020)

ECIJA

¿A QUIÉN VAN DIRIGIDAS LAS MEDIDAS NIS?

Infraestructuras Críticas y Esenciales (Públicas y Privadas)

- Administración
- Instalaciones del Espacio
- Industria Química y Nuclear
- Agua
- Centrales y Redes de energía
- Sistema de Salud
- Transportes (aeropuertos, puertos, ferrocarril, etc);
- **Sistema Financiero y Tributario**
- Distribución de Alimentación

Proveedores de Servicios Digitales

Más de 50 trabajadores o 10 millones €

- Buscadores
- Proveedores de sistemas en la nube
- Mercados en línea que ofrezcan productos o servicios de terceros

LA IMPORTANCIA DE LA CERTIFICACIÓN

Aunque el 95% de las empresas en la UE no pueden considerarse infraestructuras críticas, esenciales, o proveedores de servicios digitales, la UE ha creado un **sistema de certificación**, de modo que se espera que las entidades que se certifiquen aún no estando obligadas, serán reconocidas y recompensadas por el propio mercado. De este modo Europa va a contar con:

1. Sello de Privacidad
2. sello de Ciberseguridad

ECIJA

RÉGIMEN SANCIONADOR EN EUROPA

NIS

Sanciones entre 100.000 € y 1Millón € (**21.500.000 MXN**)

por infracciones graves y muy graves graves. Además las sanciones podrán ser publicadas (pérdida de imagen).

RGPD

Hasta 20 millones de € (**426.500.000 MXN**) o el 4% de la facturación global anual.

En caso de incidencia que perjudique gravemente a los titulares de los datos, deberá comunicarse a los titulares de los datos (pérdida de imagen)

ECIJA

NORMATIVA ESPECÍFICA DEL SISTEMA FINANCIERO Y FINTECH

Normativa PCI (TARJETAS)

Pago tarjetas de crédito

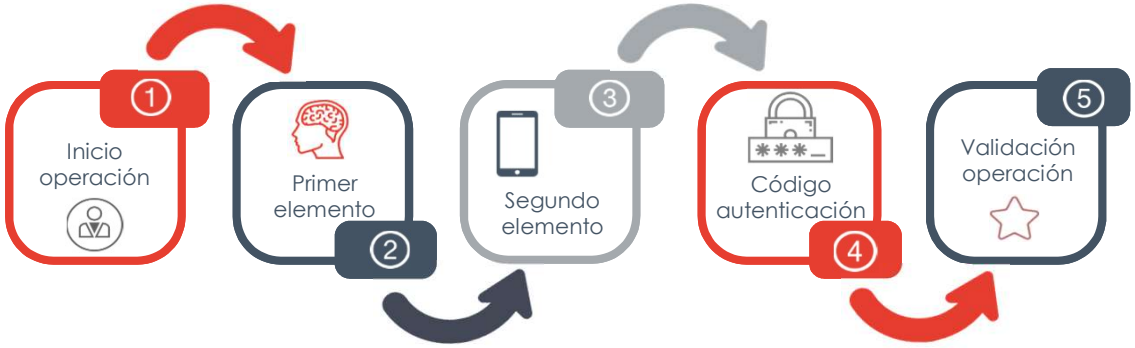
Referencia de requisitos técnicos y operativos para proteger los datos de los titulares de tarjetas.

PCI DSS aplican a todas las entidades que participan en el procesamiento de tarjetas de pago (comerciantes, procesadores, adquirientes, entidades emisoras y proveedores de servicios…)

Normativa PSD2 (MEDIOS DE PAGO)

La PSD2 exige (sin sanciones hasta diciembre de 2020) unos requisitos reforzados de seguridad (SCA) que exige la autenticación de dos o más factores de estos 3 posibles.

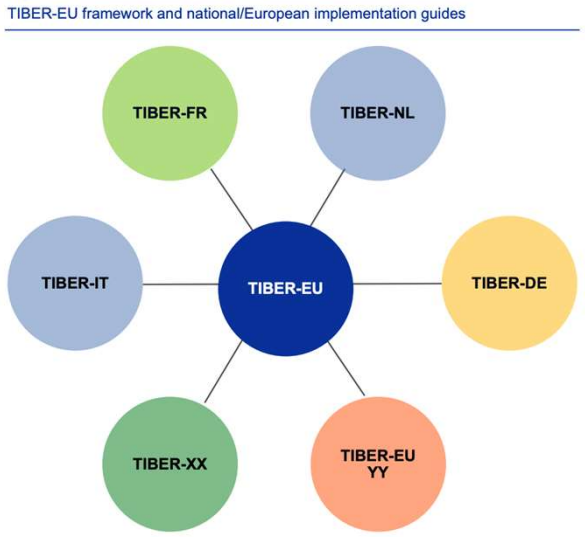
- Conocimiento. Algo que conoce el usuario (una contraseña)
- Posesión. Algo que posee el usuario (un móvil, una llave de memoria)
- Inherencia. Algo que es inherente al usuario (biometría. Huella/Voz)



BANCO CENTRAL EUROPEO:

Sigue las directrices del Comité de Pagos e Infraestructuras de Mercado (**CPMI**) y la Organización Internacional de Comisiones de Valores (**IOSCO**), así como del **G7**.
8 puntos fundamentales:

1. Estrategia y Marco Común en materia de ciberseguridad para las entidades financieras
2. Gobernanza de la ciberseguridad como algo necesario
3. Basada en análisis de riesgos y establecimiento de controles
4. Monitorización constante
5. Respuesta ante brechas gestionadas: contener y mitigar el riesgo
6. Recuperación y Resiliencia
7. Compartir información sobre incidentes entre las entidades
8. Formación continua



TIBER-EU. Threat Intelligence Based Ethical Redteaming

LAS ENTIDADES FINANCIERAS SERÁN ANALIZADAS POR EL BANCO CENTRAL EUROPEO

CROE. Cyber Resilience Oversight Expectations

GUÍAS ESPECÍFICAS QUE TOMAN LO MEJOR DE NIST, COBIT, ISO 27001

ECIJA

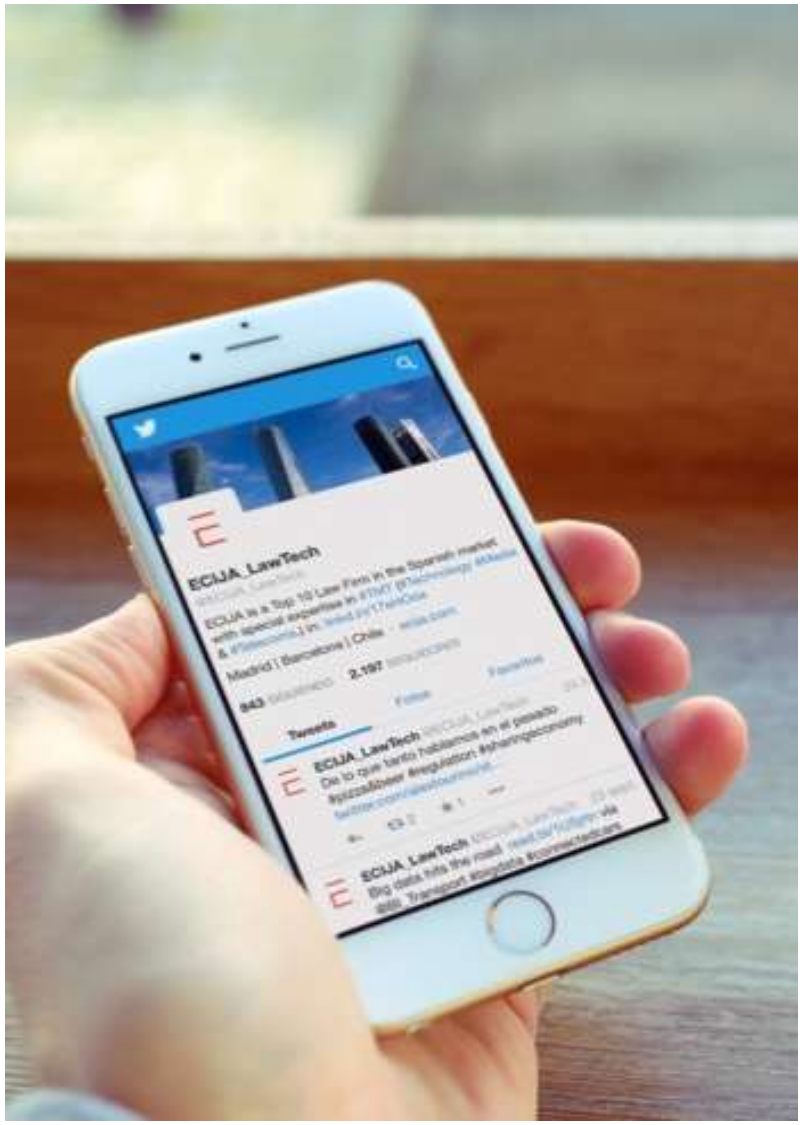
Otras propuestas internaciones recientes

- Estonia
- Israel
- Corea
- Australia
- Canadá
- Hong Kong
- Tailandia
- Uruguay
- Colombia
- México
- Chile
- Brasil (entidades financieras)
- Perú

Elementos Comunes

- Todas las normativas tienden a garantizar:
  - Confidencialidad
  - Integridad
  - Disponibilidad
  - Resiliencia
- En todos los casos, el establecimiento de medidas se realiza en función al **RIESGO**

ECIJA

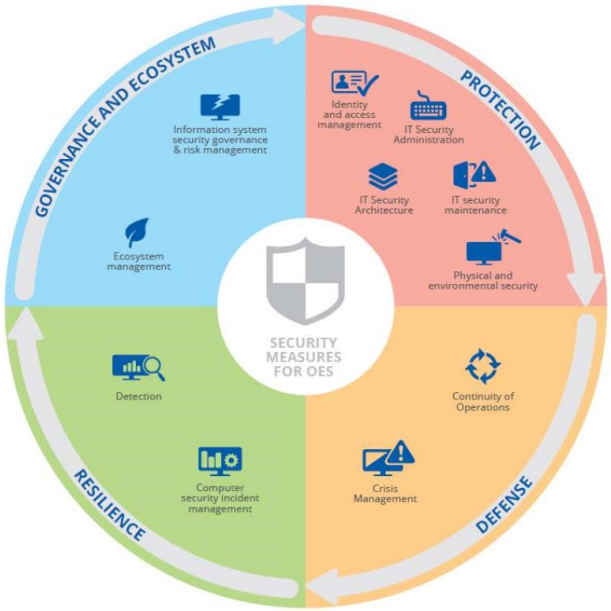


1. Normativa sobre Ciberdelitos
2. Normativa sobre Ciberseguridad
3. Medidas de Seguridad

ECIJA

SISTEMAS DE GESTIÓN: ESTÁNDARES INTERNACIONALES

ISO 27001-2 · enisa · NIST National Institute of Standards and Technology U.S. Department of Commerce



1. PROCEDIMIENTOS DOCUMENTADOS Y TESTADOS
2. MEDIDAS DE PROTECCIÓN FÍSICA
3. GESTIÓN DE SOPORTES – DISPOSITIVOS (CIFRADO)
4. CONTROL DE ACCESOS LÓGICOS
5. REGISTROS DE ACCESOS (TRAZABILIDAD)
6. DISPONIBILIDAD – CONTINUIDAD DE NEGOCIO
7. GESTIÓN DE INCIDENCIAS
8. SEGURIDAD EN LAS COMUNICACIONES (CIFRADO)
9. AUDITORÍA DE SEGURIDAD DE SISTEMAS - PENTESTING
10. GESTIÓN DE LAS VULNERABILIDADES TÉCNICAS
11. SEGURIDAD EN LOS ENTORNOS DE DESARROLLO Y PRUEBA
12. SEUDONIMIZACIÓN - DISOCIACIÓN EN BASE DE DATOS CUANDO EXISTAN DATOS PERSONALES

ECIJA

ARQUITECTURA DE SISTEMAS. ELEMENTOS VULNERABLES

Servidor físico (HOST)
Bios actualizada?
Firmware actualizado?
Disponibilidad?

S.O (HOST)
S.O HOST actualizado?
Usuarios
ADMINISTRADORES

S.O Servidores Virtuales
-Discos Virtuales-
S.O virtualizado actualizado?
Usuarios S.O virtualizado
ADMINISTRADORES S.O. Virtualizado
ADMINISTRTADORES Sistema virtualización

Aplicación
Aplicación actualizada?
Usuarios
ADMINISTRADORES

Base de Datos
Distintos entornos?
Base de datos actualizada?
Usuarios
ADMINISTRADORES

Rack
Firmware cabina actualizado?
Medidas físicas CPD?

S.O ordenador / teléfono / tablet actualizado?
Almacenamiento cifrado?
Usuarios
ADMINISTRADORES

Firewall - Comms
Firmware actualizado?
Reglas correctas aplicadas?

Internet
Datos cifrados?

Cloud
ESPECIAL ANTENCION
PARA ENTIDADES FINANCIERAS

ECIJA

DC1: MEDIDAS DE PROTECCIÓN Y CONTROL DE ACCESO FÍSICO

- MEDIDAS DE SEGURIDAD FÍSICAS: Extintores, Cámaras, Redundancia eléctrica
- SISTEMA DE CONTROL DE ACCESO FÍSICO A CPD: Cierre, biometría, videovigilancia
- REGISTRO DE ACCESOS A CPD: Internos y externos
- REVISIÓN REGISTRO DE ACCESOS
- PLAZO DE ALMACENAMIENTO QUE CUBRA PERIODOS DE RESPONSABILIDAD

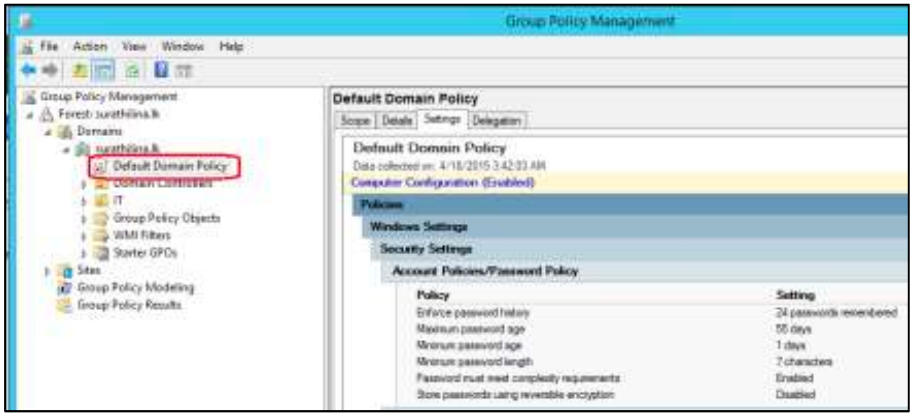
DC2: GESTIÓN DE SOPORTES

- INVENTARIO ACTUALIZADO DE ACTIVOS: HARDWARE Y SOFTWARE
- SALIDAS Y ENTRADAS DE SOPORTES GESTIONADA Y REGISTRADAS (AUTORIZACIONES)
- BRING YOUR OWN DEVICE CON MEDIDAS DE SEGURIDAD IMPLEMENTADAS DE CIFRADO
- ENCRIPTADO DE SOPORTES, INCLUIDOS DISPOSITIVOS MOVILES, Y PORTÁTILES
- DESTRUCCIÓN/BORRADO SEGURO DE SOPORTES

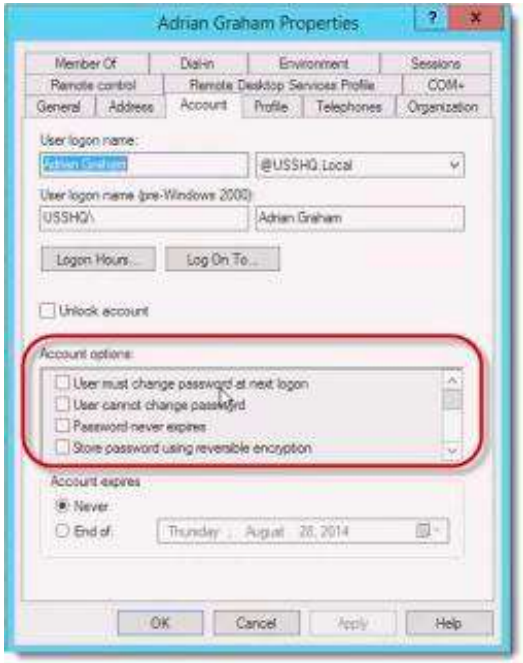
DC3: ACCESOS LÓGICOS

- LISTADO DE USUARIOS Y ADMINISTRADORESAUTORIZADOS ACTUALIZADO
- SEGREGACIÓN DE FUNCIONES DE USUARIOS (ROLES) Y ADMINISTRADORES
- SEGREGACIÓN DE FUNCIONES DE ADMINISTRADORES (ROLES)
- IDENTIFICACIÓN Y AUTENTICACIÓN INDIVIDUAL DE USUARIOS (GESTOR DE USUARIOS)
- CADUCIDAD DE PASSWORD / DOBLE FACTOR
- SEGURIDAD DE PASSWORD: COMPLEJIDAD HABILITADA
- BLOQUEO AUTOMÁTICO DE ACCESOS POR FALTA DE USO
- BLOQUEO DE CUENTA TRAS INTENTOS FALLIDOS
- CONTRASEÑAS RECORDADAS
- OBLIGACION CAMBIO DE CONTRASEÑA TRAS PRIMER ACCESO
- ALMACENAMIENTO ENCRIPTADO DE CONTRASEÑAS
- FICHEROS TEMPORALES CONTROLADOS

DC3: ACCESOS LÓGICOS



Ejemplo gestión de usuarios en Windows Server 2012

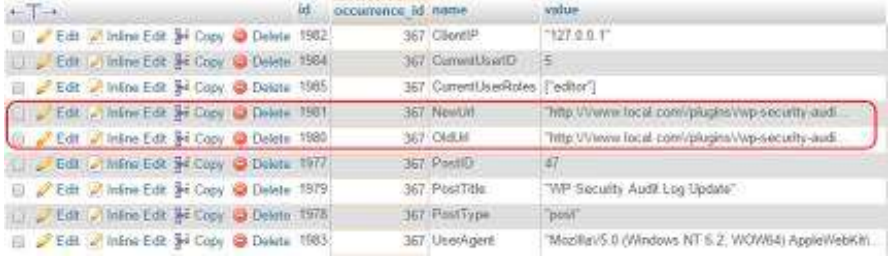


Ojo con las excepciones en directivos y administradores

ECIJA

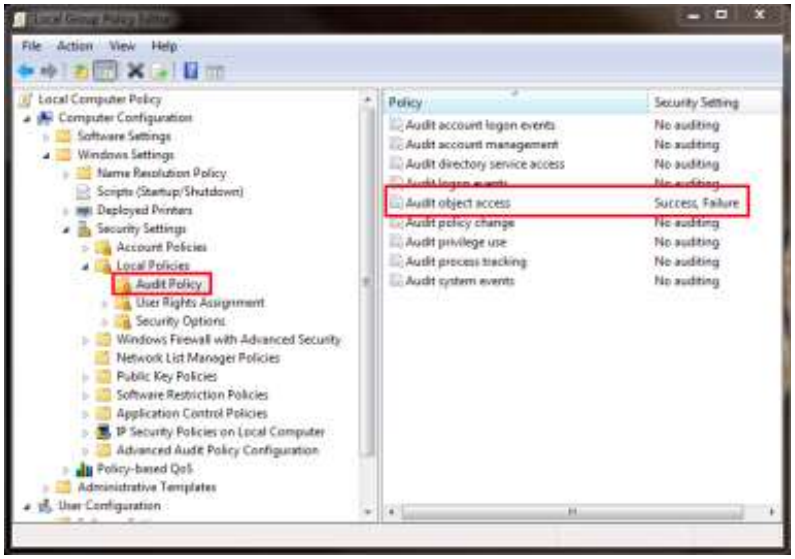
DC4: REGISTRO DE ACCESOS A LOS DATOS

- REGISTRO ACCESOS LÓGICOS
- REGISTRO DE FECHA Y HORA



	id	occurrence_id	name	value
Edit Inline Edit Copy Delete	1982	367	ClientIP	"127.0.0.1"
Edit Inline Edit Copy Delete	1984	367	CurrentUserID	5
Edit Inline Edit Copy Delete	1985	367	CurrentUserRoles	["editor"]
Edit Inline Edit Copy Delete	1981	367	NewUrl	"http://www.local.com/plugins/wp-security-audi...
Edit Inline Edit Copy Delete	1980	367	OldUrl	"http://www.local.com/plugins/wp-security-audi...
Edit Inline Edit Copy Delete	1977	367	PostID	47
Edit Inline Edit Copy Delete	1979	367	PostTitle	"WP Security Audit Log Update"
Edit Inline Edit Copy Delete	1978	367	PostType	"post"
Edit Inline Edit Copy Delete	1983	367	UserAgent	"Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit...

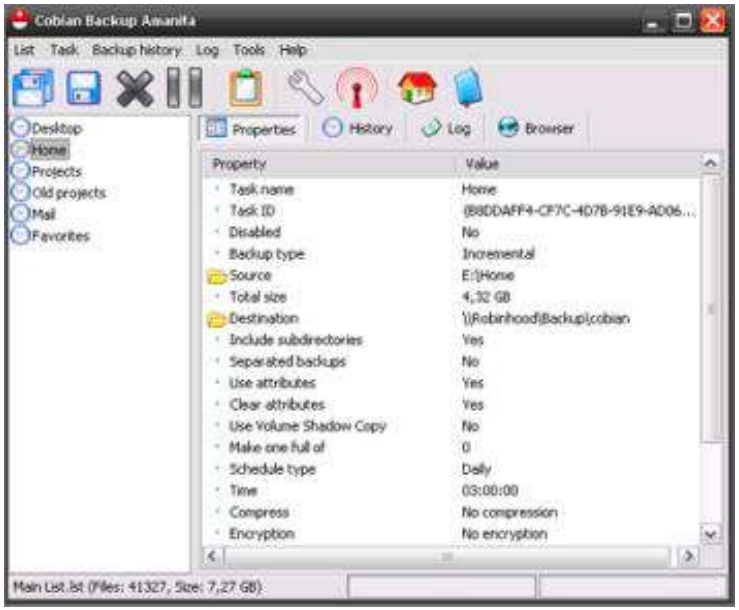
- REGISTRO DE ACCIÓN REALIZADA (CAMPO CONCRETO O AUDITORÍA DE OBJETOS)



- PLAZO DE CONSERVACIÓN DEL REGISTRO DE ACCESO: LO SUFICIENTE PARA CUBRIR PERIODOS DE RESPONSABILIDAD
- REVISIÓN DE REGISTROS DE ACCESO

DC5: COPIA DE SEGURIDAD

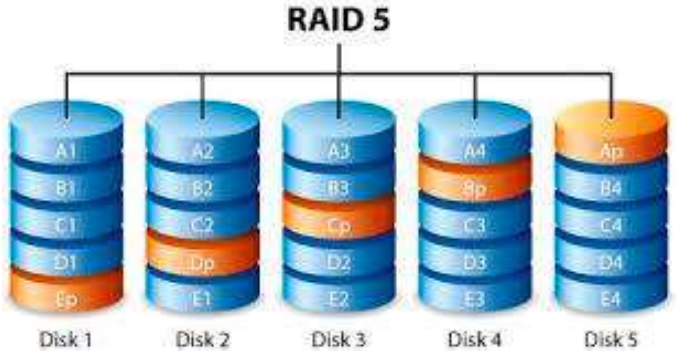
- EXISTENCIA DE COPIA DE SEGURIDAD
- PERIODICIDAD BACKUP
- LUGAR DE CONSERVACIÓN
- VERIFICACIÓN DE BACKUP
- PRUEBAS DE RESTAURACIÓN DE TODOS LOS SISTEMAS
- ENCRIPTADO DE COPIAS DE SEGURIDAD



DC6: RESILIENCIA Y CONTINUIDAD DE NEGOCIO

- PROCEDIMIENTOS DEFINIDOS
- PRUEBAS DE LOS PROCEDIMIENTOS REALIZADAS
- SISTEMA RAID DE DISCOS?
- ELEMENTOS REDUNDADOS? HARDWARE, RED, COMMS, ELECTRICIDAD
- SISTEMAS DE ALIMENTACIÓN ININTERRUMPIDA?

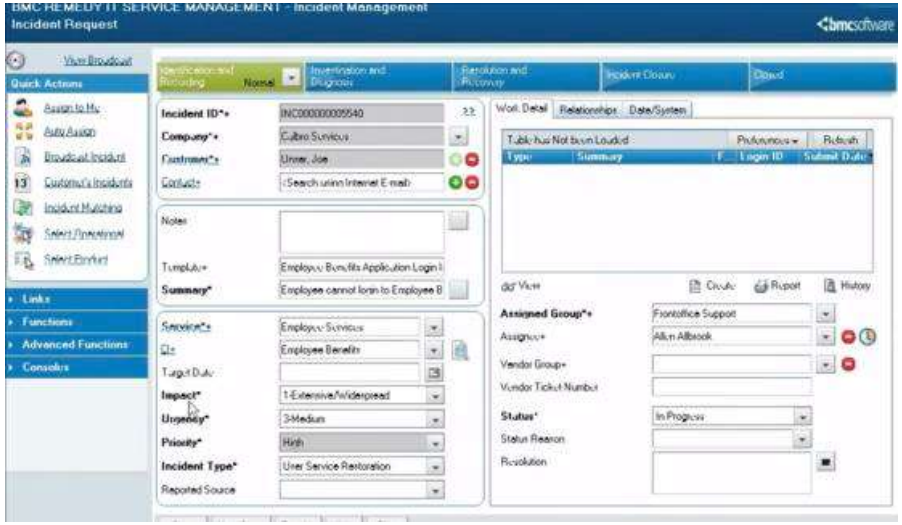
SAI



Fuente alimentación redundante

DC7: INCIDENCIAS

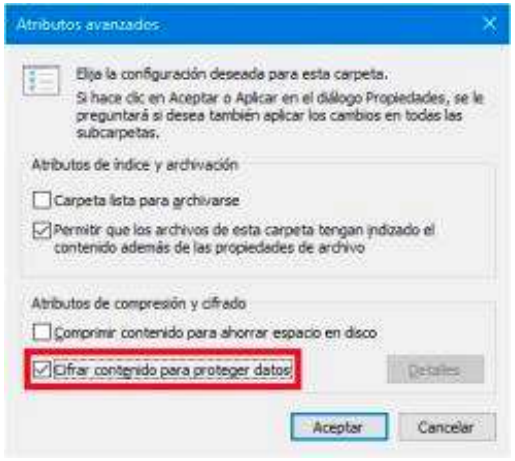
- REGISTRO Y GESTIÓN DE INCIDENCIAS
- PROCEDIMIENTO DE NOTIFICACIÓN BRECHAS SEGURIDAD
- MONITORIZACIÓN DE EVENTOS DE SEGURIDAD
- REMEDIACIÓN DE EVENTOS DE SEGURIDAD

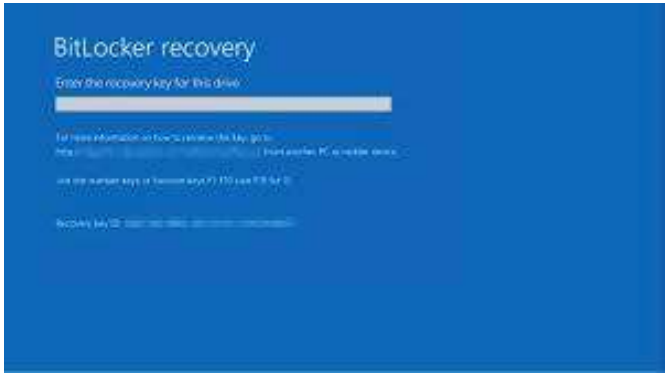


Ejemplo Herramienta gestión incidencias

DC8: COMUNICACIONES

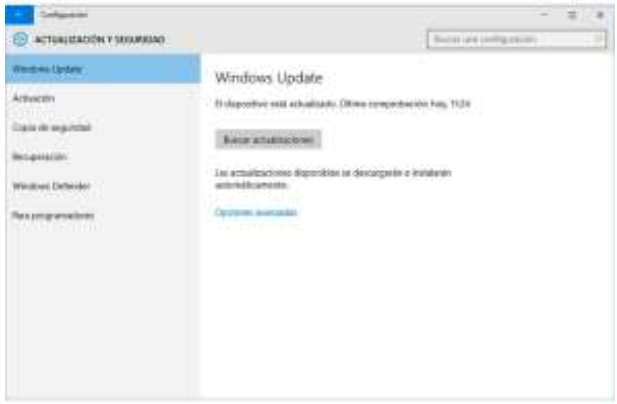
- FILTRADO DE COMUNICACIONES (FIREWALL, FILTRADO IP, IDS, ETC)
- ENCRIPTADO DE CONTENIDO
- ENCRIPTADO DE COMUNICACIONES
- METODO DE ENCRIPTADO ACTUALIZADO





DC9: VULNERABILIDADES

- AUDITORÍA PERIÓDICA DE SEGURIDAD DE SISTEMAS (PENTESTING, ETC)
- ANTIVIRUS / ANTIMALWARE
- VULNERABILIDADES GESTIONADAS (S.O - APLICACIÓN HOST Y VIRTUAL)
- PERIODICIDAD REVISIÓN PARCHEO DE S.O. (AUTOMÁTICO O GESTIONADO)
- CONTROL DE VERSIONES APLICACIONES Y BBDD (GESTIONADO)

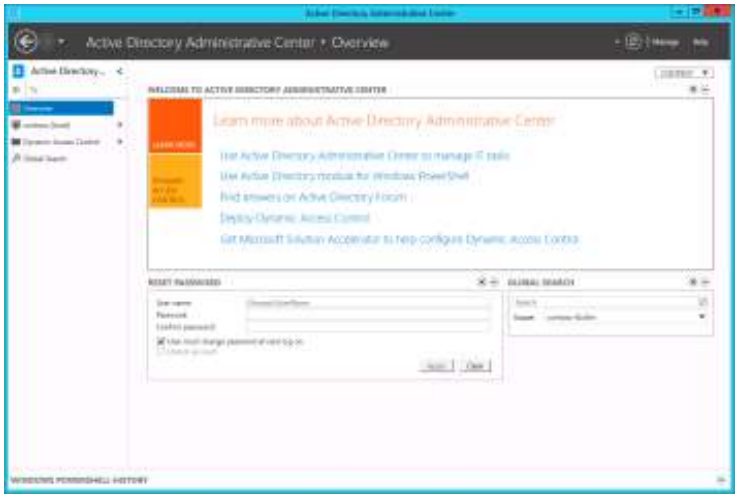


Microsoft System Center Configuration Manager

ECIJA

DC10: ENTORNOS

- ENTORNOS SEPARADOS (Desarrollo, Test, Producción)
- MISMAS MEDIDAS EN ENTORNOS CON DATOS REALES
- ADMINISTRACION EN INSTALACION DE APLICACIONES



DC11: ANONIMIZACIÓN

- SEUDONIMIZACIÓN
- ANONIMIZACIÓN

DC12: ¿OTRAS MEDIDAS DE SEGURIDAD?

- Se impide el uso de USBs externos?
- Se impide el acceso a plataformas de compartición no autorizadas?

OneDrive Dropbox wetransfer

- Hemos comprobado que no somos susceptibles de Ingeniería social?

TECNOLOGÍA • NOTICIA

773 millones de correos expuestos en una de las mayores brechas de seguridad de la historia

B.T. 17 ENE. 2019 | 13:37

ECIJA

¡Muchas gracias por vuestra atención!

Jesús Yañez

Socio IT, Privacy & Cibersecurity

jyanez@ecija.com