

Seguridad Informática

Tema 1 – Introducción



Universidad
Rey Juan Carlos

Antonio González Pardo antonio.gpardo@urjc.es

26/01/2023

- Introducción a la seguridad informática.
- El ciclo de la seguridad y el compromiso.
- Los tres pilares de la seguridad.
- El factor humano.
- Responsable de Seguridad Informática.
- Políticas y procedimientos.
- Legislación vigente.

- **Introducción a la seguridad informática.**
- El ciclo de la seguridad y el compromiso.
- Los tres pilares de la seguridad.
- El factor humano.
- Responsable de Seguridad Informática.
- Políticas y procedimientos.
- Legislación vigente.

- **Seguridad de la información:** Es el conjunto de medidas preventivas y reactivas de las organizaciones y de los sistemas tecnológicos que permiten resguardar y proteger la información buscando mantener la **confidencialidad**, la **disponibilidad** y la **integridad** de dicha información.

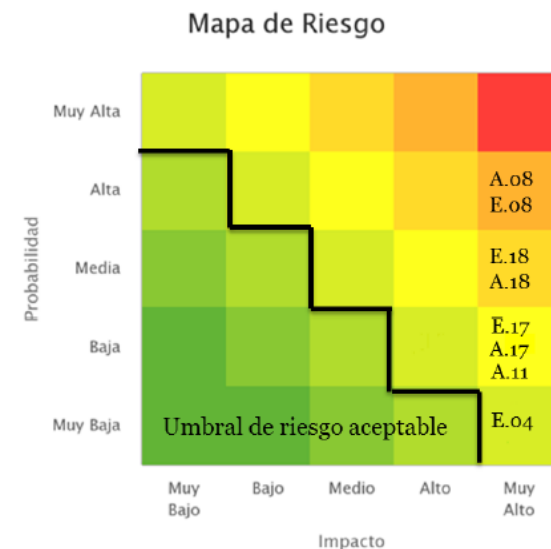
- También tenemos que definir algunos conceptos:
 - Activos.
 - Riesgos.
 - Amenazas.
 - Salvaguardas.

- **Activos:** son los **recursos** del sistema de información necesarios para que la organización funcione correctamente y alcance los objetivos propuestos. Pueden ser recursos tangibles o intangibles.
- **Amenazas:** son eventos que pueden desencadenar un incidente en la organización, produciendo daños materiales o pérdidas inmateriales en sus activos.

- **Riesgos:** es la **probabilidad** de que se produzca un incidente de seguridad en un activo. En función del impacto (pérdidas) que puede provocar un incidente de seguridad y las probabilidades de ocurrencia será catalogado de una forma o de otra.
- **Salvaguardas:** es un mecanismo de protección frente a las amenazas, reducen la frecuencia de las amenazas y limitan el daño causado. Por ejemplo: los procedimientos o las prácticas de las empresas.

- Los riesgos se pueden categorizar en diferentes tipos:
 - **Potencial, inicial o intrínseco:** antes de aplicar salvaguardas.
 - **Efectivo:** el que se da tras la aplicación de las salvaguardas.
 - **Residual:** siempre permanecerá, aunque tengamos todas las salvaguardas aplicadas.

	Valor	Descripción
10	Muy alto	Daño muy grave a la organización
7-9	Alto	Daño grave a la organización
4-6	Medio	Daño importante a la organización
1-3	Bajo	Daño menor a la organización
0	Despreciable	Irrelevante a efectos prácticos



- Hay muchas definiciones de seguridad informática:
 - El conjunto de servicios y mecanismos que aseguran la **integridad** y **privacidad** de la información que los sistemas manejan.
 - El conjunto de servicios, mecanismos y políticas que aseguran que el modo de operación de un **sistema sea seguro**.
 - El conjunto de protocolos y mecanismos que aseguran que la comunicación entre los sistemas esté **libre de intrusos**.

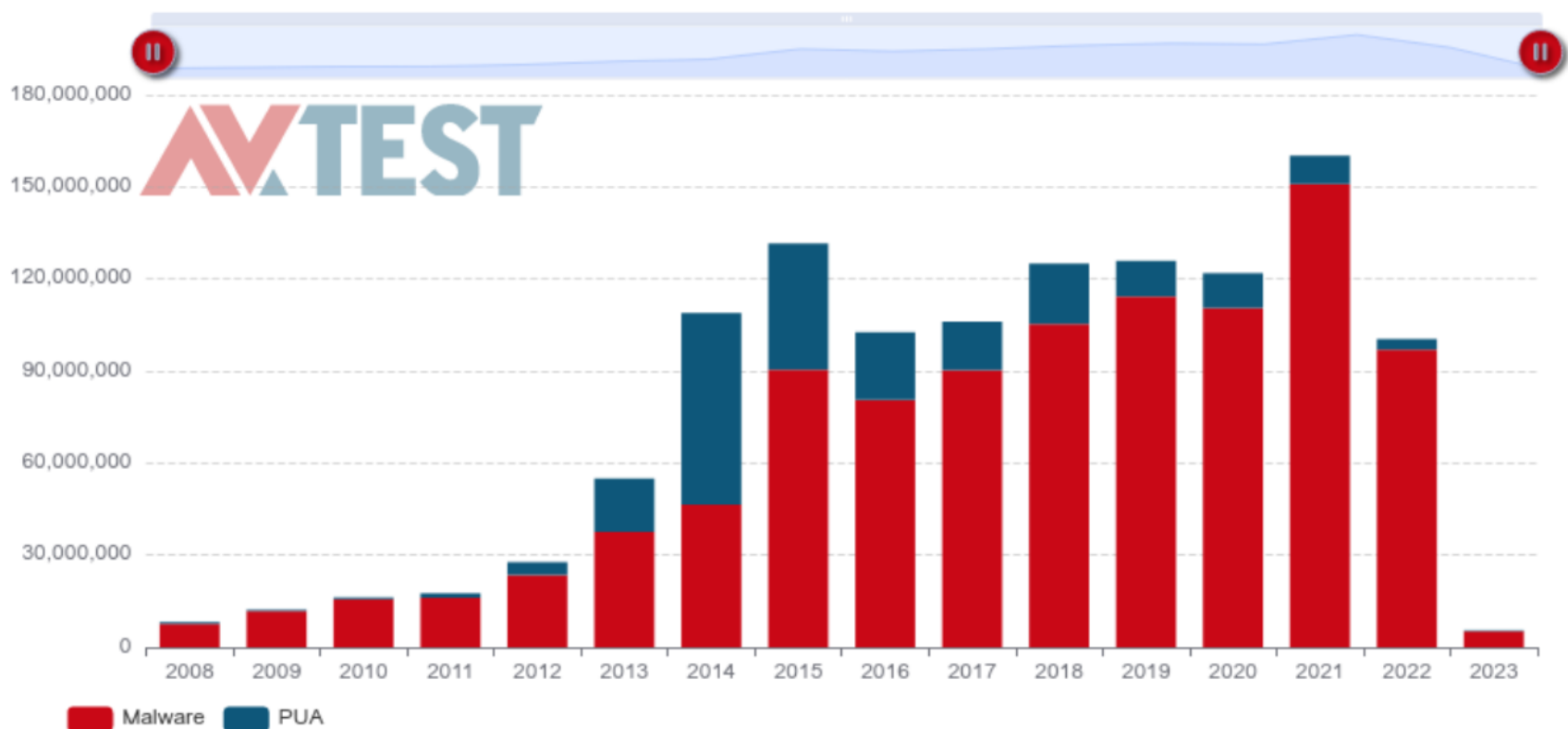
-

- Por otro lado, están creciendo de una manera considerable ciertos modelos de negocio que hacen que la seguridad sea un aspecto cada vez más importante.



- Todos estos datos son muy “golosos” para cierto tipo de personas u organizaciones.

TOTAL AMOUNT OF MALWARE AND PUA



- Un ejemplo del problema de no dar importancia a la Seguridad Informática.

El tercer ataque DDoS en Andorra sugiere que es mejor evitar irte a un lugar con un solo proveedor de Internet si eres streamer



24 Enero 2022

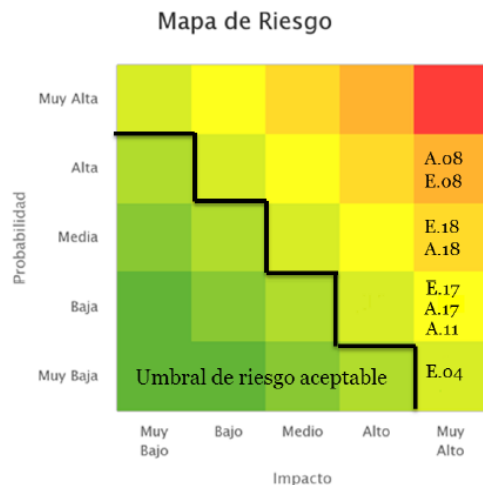
 24 Comentarios

- Introducción a la seguridad informática.
- **El ciclo de la seguridad y el compromiso.**
- Los tres pilares de la seguridad.
- El factor humano.
- Responsable de Seguridad Informática.
- Políticas y procedimientos.
- Legislación vigente.

- El ciclo de la seguridad:



- La seguridad absoluta es imposible:
 - Centrarnos en evitar todas las amenazas, o aquellas menos frecuentes, se dispara el **coste** en seguridad.
 - Pero tampoco podemos no invertir en seguridad.



- No siempre hay que basarse en temas económicos.
 - Un ejemplo son los sistemas militares.
 - Estos sistemas tienen un grado máximo de seguridad, aunque suponga disparar los costes.
- Las medidas de seguridad deben ser proporcionales a los riesgos y al valor del activo.
 - Se debe llegar a un compromiso entre nivel de seguridad, coste, funcionalidad y usabilidad.

- ¿Qué debemos proteger?
 - Datos y comunicaciones personales.
 - Propiedad intelectual de corporaciones y administraciones públicas.
 - Transacciones B2C, B2B, B2G, etc.

- Pero no sólo información y datos, sino activos informáticos y tecnológicos o incluso intangibles:
 - **Procesos y productividad.**
 - Sistemas e infraestructuras.
 - Reputación.



- Introducción a la seguridad informática.
- El ciclo de la seguridad y el compromiso.
- **Los tres pilares de la seguridad.**
- El factor humano.
- Responsable de Seguridad Informática.
- Políticas y procedimientos.
- Legislación vigente.

- La seguridad informática tiene tres pilares fundamentales:
 - **Confidencialidad:** la información está disponible sólo a las personas (u organizaciones) autorizadas.
 - **Integridad:** asegura que la información no ha sido alterada de manera no autorizada.
 - **Disponibilidad:** el activo estará disponible siempre que las entidades o procesos autorizados deseen.
- Para asegurar estos pilares, se necesita de las siguientes características:
 - **Trazabilidad:** consiste en crear herramientas necesarias para que se puedan seguir todos los movimientos realizados sobre un activo.
 - **Autenticidad:** consiste en asegurar que una entidad es quien dice ser.
 - **No repudio:** “característica que, dado un hecho, este no puede ser desmentido con un alto grado de certeza”.

- Generalmente la pérdida de uno de estos pilares afecta al resto.
- Alguien modifica los permisos de un fichero “rwx” para que los usuarios no puedan abrir el fichero.
- La integridad ya no se ha cumplido.
- Si los usuarios legítimos no pueden leer el archivo, ya no cumple con la disponibilidad.
- Y si los atacantes han abierto el archivo, tampoco se cumple la confidencialidad.

- Introducción a la seguridad informática.
- El ciclo de la seguridad y el compromiso.
- Los tres pilares de la seguridad.
- **El factor humano.**
- Responsable de Seguridad Informática.
- Políticas y procedimientos.
- Legislación vigente.

- La componente más débil en cualquier infraestructura TIC suele ser el factor humano.
- Los atacantes externos no siempre causan los peores problemas de seguridad.
- En muchos casos basta con un usuario interno malintencionado o simplemente descuidado.

“Usted puede tener la mejor tecnología, firewalls, sistemas de detección de ataques, dispositivos biométricos. Lo único que se necesita es una llamada a **un empleado desprevenido** y acceden al sistema sin más. Tienen todo en sus manos”.

Kevin Mitnick





Edward Snowden, consultor tecnológico estadounidense, informante, antiguo empleado de la CIA y de la NSA. En 2013 hizo públicos documentos clasificados como alto secreto sobre varios programas de la NSA, incluyendo los programas de vigilancia masiva PRISM y XKeyscore.



Bradley Manning, exsoldado y analista de inteligencia del ejército de Estados Unidos.

En 2010 filtró a Wikileaks miles de documentos clasificados de las guerras de Afganistán e Irak.




Hervé Falciani, ingeniero de sistemas italo-francés que trabajó en reforzar la seguridad de la filial suiza del banco HSBC entre 2001 y 2008. En ese periodo logró sustraer información de hasta 130.000 evasores fiscales (“lista Falciani”) y que es utilizada por la justicia de varios países para luchar contra el fraude fiscal.



- Frances Haugen
- Científica de datos.
- Ex empleada de Facebook.
- Octubre 2021.
- Trabajó en el Civic Integrity.



- Pero otras muchas veces somos nosotros por descuidos:
 - En junio de 2015 el ejército de los Estados Unidos bombardeó un cuartel general del Estado Islámico que fue localizado gracias a la publicación de un “selfie” de uno de los miembros de dicha organización.
 - `iknowwhereyourcatlives.com` localiza las viviendas de miles de gatos (y por tanto de sus dueños) en el mundo gracias a los metadatos de geolocalización de las fotografías que sus dueños publican en Internet.
 - En 2005 se detuvo al asesino en serie de Wichita conocido como BTK que asesinó a 10 personas entre 1974 y 1991. Pudo ser arrestado por los metadatos de un documento en Word que estaba en un disquete que el propio asesino envió a una cadena de televisión y que no había borrado de forma segura.


- Estos descuidos se utilizan mucho en las técnicas de phishing:

De:  BBVAresponde@grupobbva.com
Para: congresosef@umh.es
CC:
Asunto: Aviso Del Servicio De Apoyo [message id: 5250791674]



Estimado cliente,

Servicio técnico de  renovó el software para mejorar el servicio de los clientes 

Para asegurar la integridad de sus datos Usted tiene que rellenar el 
Formulario del cliente".

Para empezar a rellenar el formulario pulse en el vínculo:

netcashnetoffice.aspx">http://onlineformulario.netcashnetoffice.aspx

Esto es un mensaje automático, no hace falta que respondas.

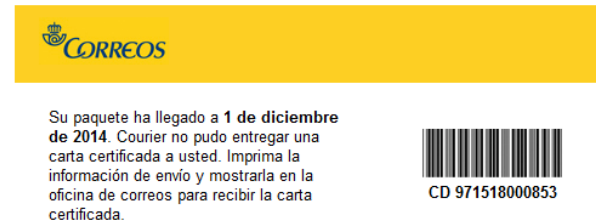
Reciba un cordial saludo,

Grupo 



- También se usan para instalar un software malicioso en el PC
- Desde el correo te descargas un archivo
- Y al ejecutarlo, se empieza a cifrar el disco duro. Cuando termina, restringe el acceso a la información y exige el pago de un rescate.
- Ejemplos de este tipo de software.
 - WannaCry.
 - Cryptolocker.
 - Cerber.
 - Locky.

De: support@correos24.net [<mailto:support@correos24.net>]
Enviado el: miércoles, 03 de diciembre de 2014 14:41
Para: [REDACTED]
Asunto: [REDACTED] usted tiene una Carta certificada



[Descargar información sobre su envío](#)

Si la carta certificada no se recibe dentro de los 30 días laborables Correos tendrá derecho a reclamar una indemnización a usted para él está manteniendo en la cantidad de 7,55 euros por cada día de cumplir. Usted puede encontrar la información sobre el procedimiento y las condiciones de la carta de mantener en la oficina más cercana. Este es un mensaje generado automáticamente.

Condiciones y Términos del Servicio de localización de envíos

- Ejemplos de factores humanos:

de Fátima
ENCIAS

URGENCIAS

N.Asis. 1981928 Cama -

Edad 37 Nombre PAULA VAZQUEZ

F.Nac. 26/11/1974

Poliza Tifno

ENTIDAD: ACCIDENTES DE TRAFICO T.S.

Doctor

Dom.

Loc.

INICIATIVA PROPIA

AC. TRAFICO VEHICULOS

 **Paula Vázquez** 
@PaulaVazquezTV 
Presentadora en @antena3com
contacto:iba.arte@paulavazquez.com
www.marquesdevizhoja.com
<http://www.paulavazquez.com>

  Seguir

7.973 TWEETS
307 SIGUIENDO
196.863 SEGUIDORES

Tweet para Paula Vázquez

Tweets

[Siguiendo](#)

[Seguidores](#)

[Favoritos](#)

[Listas](#)

[Más acciones recientes](#)

Tweets Todos / Sin menciones

 **Paula Vázquez** @PaulaVazquezTV 28m
También llamadas <pic.twitter.com/IdAcMs23>
 Ver foto

 **Paula Vázquez** @PaulaVazquezTV 29m
Y más, hasta que no paréis yo sigo <pic.twitter.com/0mOfZEgj>
 Ver foto

 **Paula Vázquez** @PaulaVazquezTV 29m
Sigo <pic.twitter.com/h11ZKORh>
 Ver foto

- Ejemplos de factores humanos:

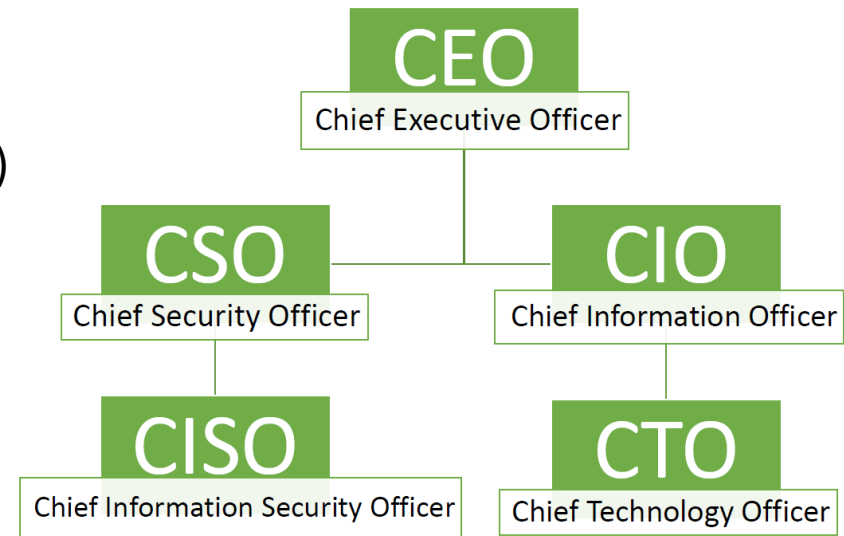


- Ejemplos de factores humanos:



- Introducción a la seguridad informática.
- El ciclo de la seguridad y el compromiso.
- Los tres pilares de la seguridad.
- El factor humano.
- **Responsable de Seguridad Informática.**
- Políticas y procedimientos.
- Legislación vigente.

- En una empresa hay 5 responsables de la seguridad:
 - Director Ejecutivo de la Organización (CEO)
 - Director Ejecutivo de Seguridad (CSO)
 - Director Ejecutivo de Información (CIO)
 - Director Ejecutivo de seguridad de la información (CISO)
 - Director Ejecutivo de Tecnología (CTO)



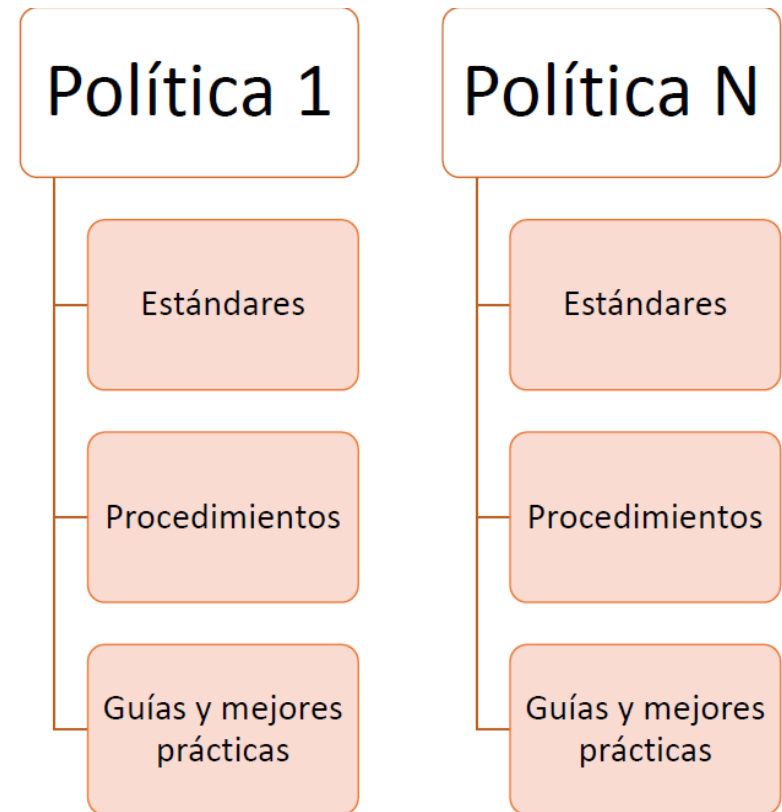
- Director Ejecutivo de Seguridad, CSO (*Chief Security Officer*)
 - Responsable de la seguridad de la organización.
- Director Ejecutivo de seguridad de la información, CISO (*Chief Information Security Officer*)
 - Su función es alinear la seguridad de la información con los objetivos de negocio, garantizando que la información de la empresa esté protegida adecuadamente.
- Entre sus responsabilidades se encuentra definir un entorno de políticas y procedimientos que intenten gestionar el factor humano (con gran importancia en la formación y concienciación).

- El CISO debe:
 - Implementar el Sistema de Gestión de la Seguridad Informática (SGSI).
 - Está definido en el estándar ISO/IEC 27001.
- El SGSI forma parte del Plan Director de Seguridad que consiste en “la **definición y priorización** de un **conjunto de proyectos** en materia de seguridad de la información dirigido **a reducir los riesgos** a los que está expuesta la organización hasta unos niveles aceptables”.
 - Es fundamental que el Plan Director de Seguridad defina tanto las obligaciones como las buenas prácticas de seguridad que deberán cumplir los trabajadores, así como terceros que colaboren con la empresa.

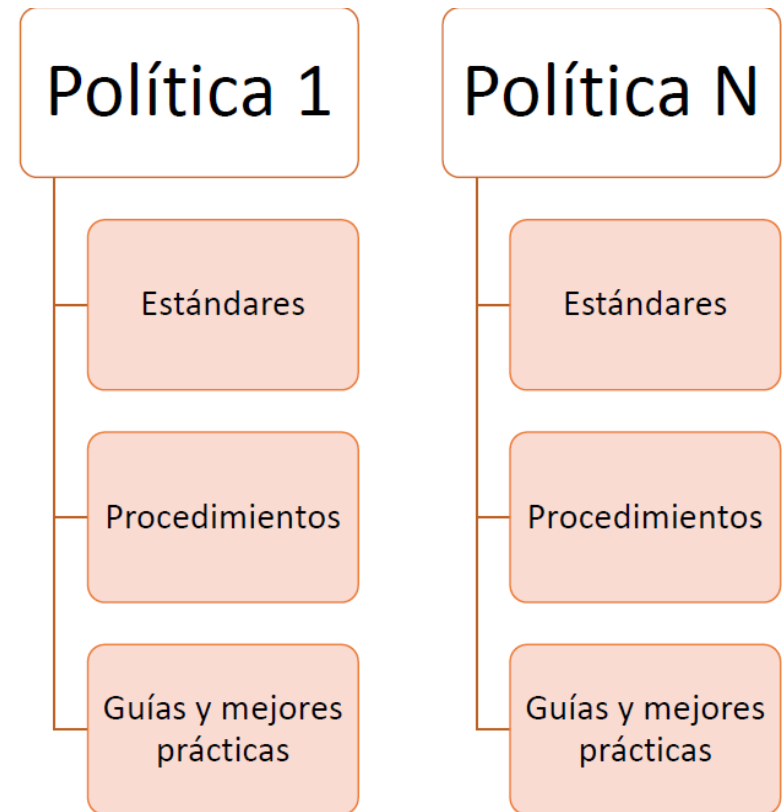


- Introducción a la seguridad informática.
- El ciclo de la seguridad y el compromiso.
- Los tres pilares de la seguridad.
- El factor humano.
- Responsable de Seguridad Informática.
- **Políticas y procedimientos.**
- Legislación vigente.

- **Política:** Enunciado corto que se aplica a toda la organización y que proporciona una línea de acción desde la dirección.
- Deben estar bien **documentadas** y bien **comunicadas**.
- No vale de nada una buena política si no se usa y/o no se difunde y no se forma a los empleados correctamente.



- **Estándares:**
 - Traducción de las políticas a detalles concretos de uso de HW y SW. Se definen los Activos.
- **Procedimientos:**
 - Instrucciones concretas acerca de cómo cumplir las políticas teniendo en cuenta los estándares.
- **Guías y mejores prácticas:**
 - Complementan a los procedimientos con sugerencias que no son de obligado cumplimiento pero que pueden mejorar el nivel de cumplimiento de objetivos, facilitar el trabajo de administradores y usuarios, etc.



Algunos ejemplos de Políticas de Seguridad:

- **Acceptable Use Policy (AUP)**
 - Define lo que la organización permite y no permite hacer a los empleados con los activos que le pertenecen (User Domain).
- **Security Awareness Policy**
 - Especifica cómo se asegura que el personal tiene la conciencia necesaria acerca de la Seguridad de la Información (User Domain).
- **Asset Classification Policy**
 - Define cómo se realiza el inventario y clasificación de los activos de la organización en función de su criticidad para el funcionamiento de la organización.
- **Vulnerability assessment and management**
 - Define una ventana de vulnerabilidades en la organización para el sistema operativo y las aplicaciones software.

- Define cómo es el Sistema de Gestión de la Seguridad Informática (SGSI), cómo se gestiona y cuáles son las responsabilidades de los participantes.
- Gestión de riesgos y mejora continua.
- Sigue el ciclo Deming (PDCA):
 - **Planificar** (PLAN): establece la política, objetivos, procesos y procedimientos relativos a la gestión del riesgo y mejora de la seguridad de la información.
 - **Hacer** (DO): implantar y gestionar esas políticas.
 - **Verificar** (CHECK): medir y revisar el desempeño (eficiencia y eficacia) del SGSI.
 - **Actuar** (ACT): adoptar acciones correctivas y preventivas basadas en auditorias y revisiones internas para mejorar el desempeño SGSI.

- ISO/IEC 27000: Sistema de Gestión de la Seguridad de la Información – Generalidades y vocabulario.
- **ISO/IEC 27001: Sistema de Gestión de la Seguridad de la Información – Requisitos.**
- ISO/IEC 27002: Buenas prácticas para controles de la seguridad de la información.
- **ISO/IEC 27003: Guía de implementación del sistema de gestión de la seguridad de la información.**
- ISO/IEC 27004: Gestión de la seguridad de la información – Medición.
- **ISO/IEC 27005: Gestión de riesgos de seguridad de la información.**
- ISO/IEC 27006: Requisitos para empresas de auditoría y certificación de Sistemas de Gestión de la Seguridad de la Información.
- ISO/IEC 27007: Directrices para auditoría en Sistemas de Gestión de la Seguridad de la Información.

- Por muy buena que sea una política de seguridad, no vale de nada:
 - Si no se comunica al personal la existencia de esa política.
 - Si no se forma al personal.
 - Si no se hacen pruebas cada cierto tiempo para ver que el personal sepa lo que tiene que hacer en cada caso.
 - Si no se revisa y actualiza periódicamente.
 - Si se detectan problemas, vulnerabilidades o fallos y no se corrigen.

- Introducción a la seguridad informática.
- El ciclo de la seguridad y el compromiso.
- Los tres pilares de la seguridad.
- El factor humano.
- Responsable de Seguridad Informática.
- Políticas y procedimientos.
- **Legislación vigente.**
 - Legislación europea.
 - Legislación española.

- Antes de empezar con la parte de legislación hay que definir varios conceptos:
 - Directiva europea
 - Acto legislativo en el que se establecen los objetivos que todos los países de la UE deben cumplir.
 - Corresponde a cada país elaborar sus propias leyes sobre cómo alcanzar esos objetivos.
 - Ley orgánica
 - Requiere el voto favorable de la mayoría absoluta de los miembros del Congreso de los Diputados.
 - Real decreto
 - Es una norma jurídica que emana del poder ejecutivo (Gobierno). La diferencia con una ley es que el RD sólo necesita la aprobación del Consejo de Ministros.

- Un delito informático, o ciberdelincuencia, es toda aquella acción, típica, antijurídica y culpable, que se da por vías informáticas o que tiene como objetivo destruir y dañar ordenadores, medios electrónicos y redes de Internet.
- Delitos que tienen como objetivo equipos o redes de computadores, por ejemplo, spam, propagación de malware o robo de información.
- Delitos realizados por medio de ordenadores y de Internet, por ejemplo, espionaje, fraude y robo, acoso o pornografía infantil.

- Introducción a la seguridad informática.
- El ciclo de la seguridad y el compromiso.
- Los tres pilares de la seguridad.
- El factor humano.
- Responsable de Seguridad Informática.
- Políticas y procedimientos.
- **Legislación vigente.**
 - Legislación europea.
 - Legislación española.

- A nivel europeo se regulan a través del convenio sobre ciberdelincuencia (2001) que establece un marco común en el que:
 - Constituyen un delito informático todos aquellos delitos contra la **confidencialidad**, la **integridad** y la **disponibilidad** de los datos y sistemas informáticos.
- Aunque cada vez existen más problemas con la determinación de la jurisdicción competente.
 - Cloud, móviles, redes sociales.



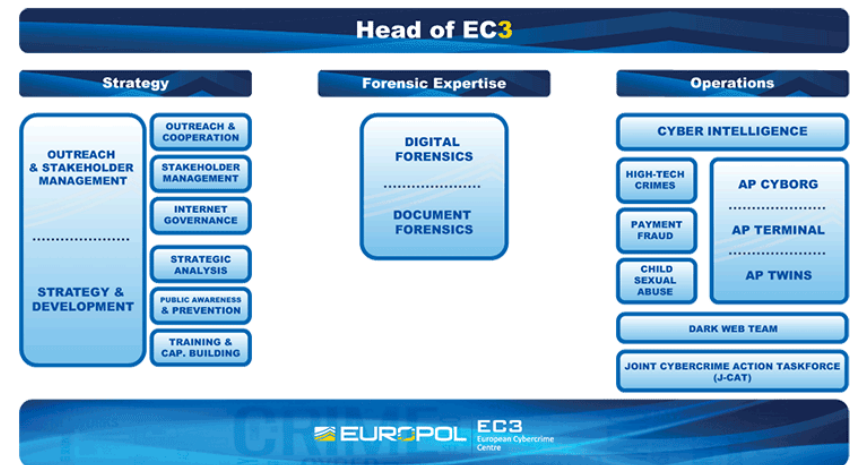
- Algunos de los delitos que están recogidos son:
 - Acceso ilícito.
 - Interceptación ilícita.
 - Ataque a la integridad de datos.
 - Ataques a la integridad del sistema.
 - Falsificación informática.
 - Fraude informático.
 - Aspectos relacionados con la pornografía infantil.
 - Recogida en tiempo real de datos.
 - Infracciones de la propiedad intelectual.



- La firma del Convenio supone que cada país, o estado, debe adaptar su propia legislación.
- Se deben criminalizar las actividades de piratería (incluyendo la producción, venta o distribución de herramientas de hacking).
- Se deben establecer leyes específicas contra la pornografía infantil.
- Además, no solo hay que establecer nuevas leyes sino también nuevos mecanismos procesales.
 - Por ejemplo, las autoridades policiales deben tener competencia para obligar a un proveedor de servicios a monitorizar las actividades de una persona en línea en tiempo real.
- El Convenio obliga a cada estado firmante a prestar cooperación internacional para la investigación y procedimientos relacionados con infracciones penales.

Centro Europeo de Ciberdelincuencia

- Conocido como EC3 o *EC³* creado por Europol en 2013
- Reforzar la respuesta de las autoridades policiales a la ciberdelincuencia en la UE.
- Ayudar a proteger a los ciudadanos, empresas y gobiernos europeos de la delincuencia en línea.
- La Haya, en la sede Europol.



- La Directiva SRI (Directiva sobre seguridad de las redes y sistemas de información, Julio de 2016) **exige** a los estados miembros, operadores de servicios esenciales (en sectores fundamentales como la energía, el transporte, la sanidad y las finanzas) y los proveedores de servicios digitales **proteger** el **entorno digital** para hacer que sea **seguro y fiable**.

- **Octubre de 2017:** El Consejo Europeo **solicitó la adopción** de un **planteamiento común** de la **ciberseguridad** en la UE, basado en la Estrategia de Ciberseguridad y en la Directiva sobre seguridad de las redes y sistemas de información (Directiva SRI).

- La propuesta presenta iniciativas como:
 - La creación de una Agencia de ciberseguridad de la UE más fuerte: European Union Agency for Cybersecurity (sustituyendo a ENISA).
 - La introducción de un régimen de certificación de la ciberseguridad a escala de la UE.
 - La rápida aplicación de la Directiva SRI.

- En diciembre de 2017, se crea el **Equipo de Respuesta a Emergencias Informáticas** (CERT-UE) de carácter permanente, asegurando una **respuesta coordinada** frente a los **ciberataques** dirigidos contra todas las instituciones, órganos y organismos de la UE.

- La Directiva SRI busca **proteger** el **entorno digital** para hacer que sea **seguro** y **fiable**.



- En diciembre de 2020 se presentó la Nueva Estrategia de Ciberseguridad de la UE.
- Los objetivos son:
 - Reforzar la resiliencia colectiva europea contra las ciberamenazas.
 - Ayudar a garantizar que todos los ciudadanos y empresas pueden beneficiarse de servicios y herramientas digitales fiables y de confianza.
- Se presentan propuestas destinadas a:
 - Garantizar un nivel elevado (común) de ciberseguridad en la UE (Directiva SRI revisada).
 - Proporcionar otra directiva sobre la resiliencia de entidades críticas.

Esta directiva tiene tres ámbitos de acción:

- Resiliencia, soberanía tecnológica y liderazgo: reforzar la seguridad en redes y los sistemas de información, en un entorno cambiante.
 - Se propone la creación de Centros de Operaciones de Seguridad basados en la Inteligencia Artificial (IA), y también apoyo a las PYMES.
- Desarrollo de la capacidad operativa para prevenir, disuadir y responder.
- Promover un ciberespacio global y abierto a través de una mayor cooperación para proteger los derechos humanos y las libertades fundamentales en línea.

- Introducción a la seguridad informática.
- El ciclo de la seguridad y el compromiso.
- Los tres pilares de la seguridad.
- El factor humano.
- Responsable de Seguridad Informática.
- Políticas y procedimientos.
- **Legislación vigente.**
 - Legislación europea.
 - **Legislación española.**

Esquema Nacional de Seguridad.

Legislación española sobre seguridad informática y ciberdelincuencia

- Código penal
- Ley de servicios de la sociedad de la información (LSSI-CE)
- Ley de protección de datos.
- Ley de la propiedad intelectual.
- Ley de firma electrónica.
- Ley general de comunicaciones.

Ley de Servicios de la Sociedad de la Información y el Comercio Electrónico (LSSI-CE)

- Regular el régimen jurídico de los servicios relacionados con internet y la contratación electrónica.
- Establece la información que las diferentes empresas deben proporcionar al cliente si utilizan: comercio electrónico, contratación en línea, información y publicidad online o servicios de intermediación.
- También establece todo lo relativo a las cookies y las Políticas de cookies.

Reglamento General de Protección de Datos

- Entró en vigor en Mayo del 2018.
- El RGPD es la norma que afecta por igual a las grandes corporaciones y a las micropymes.
- Otorga un **mayor control y seguridad** a los ciudadanos sobre su **información personal**.
- El RGPD amplía sus derechos a decidir cómo desean que sus datos sean tratados y cómo quieren recibir información de las empresas.

Ley Orgánica de Protección de Datos

- Hablamos de LOPD, pero en verdad nos referimos a Ley Orgánica de Protección de Datos y Garantía de Derechos Digitales (LOPDGDD).
- Entró en vigor en diciembre de 2018, sustituyendo a la LOPD.
- El objetivo es adaptar la legislación española a la normativa europea, definida por el RGPD.
- Esta ley establece los **requisitos** y **obligaciones** de las empresas sobre **cómo proceder con la información personal**, así como los derechos que asisten a usuarios y consumidores.

- La finalidad es proteger la intimidad, privacidad e integridad del individuo.
- Establece los pasos que tienen que realizar las empresas relativas a los datos personales:
 - Informar de manera clara sobre el tratamiento de sus datos personales.
 - Tienen que obtener el consentimiento inequívoco de los clientes.
 - Permitir ejecutar sus derechos.
 - Notificar en caso de problemas de seguridad.

- Derechos de los ciudadanos:
 - Derechos de acceso.
 - Rectificación.
 - Oposición.
 - Supresión (“derecho al olvido”)
 - Limitación del tratamiento.
 - Portabilidad y de no ser objeto de decisiones individualizadas.
- Datos personales: aquella información en formato texto, imagen o audio que permita la identificación de una persona.
- La LOPDGDD incorpora puntos como el derecho al olvido, o cambios en la obtención del consentimiento para recoger y usar la información personal.

Ley de Propiedad Intelectual

- Está regulada en el Real Decreto Legislativo 1/1996.
- El objetivo es proteger cualquier tipo de obra literaria, artística o científica, fruto de cualquier actividad empresarial.
- Protege los derechos de los autores, como los derechos patrimoniales o de explotación de la obra.
- Las empresas deben:
 - No utilizar obras protegidas sin pagar derechos de autor: software, imágenes, videos, textos, audios, tipografías, etc.
 - Proteger los derechos de las creaciones propias o de los empleados, respetando siempre el derecho del creador de reconocerse como autor de la obra.

- Delitos recogidos en el Código Penal:
 - Hurto: art. 234
 - Robo: art. 237 Defraudación a través de equipo terminal de comunicaciones: art. 256
 - Delitos contra la propiedad intelectual: arts. 270 y 271
 - Delitos contra la propiedad industrial: art. 273
 - Publicidad ilícita: art. 282
 - Falsedad de documento público: art. 390
 - Falsedad de documento privado: art. 395
 - Difusión de protestas: art. 559

- Delitos recogidos en el Código Penal:
 - Espionaje informático empresarial: Art. 278
 - Daños informáticos o sabotaje (incluye hacktivismo): Art. 264.2
 - Pornografía infantil: Art. 189
 - Calumnia: Arts. 205 y 206
 - Injuria: Arts. 208 y 209
 - Calumnias e injurias hechas con publicidad: Art. 211
 - Delito tradicional de daños: Art. 263
 - Descubrimiento y revelación de secretos (incluye hacking ético): Art. 197

- Ley de Hacking (art. 197)
 - *El que, para descubrir secretos o vulnerar la intimidad de otro, sin su consentimiento, [...], **intercepte sus telecomunicaciones o utilice artificios técnicos de escucha, transmisión, grabación o reproducción del sonido o de la imagen**, o cualquier otra señal de comunicación, será castigado con penas [...]*
 - *Las mismas penas se impondrán al que, **sin estar autorizado, se apodere, utilice o modifique**, en perjuicio de tercero, **datos reservados de carácter personal o familiar** de otro [...]*

- Ley de Hacking (art. 197 bis)
 - *El que por cualquier medio o procedimiento, [...], **acceda o facilite a otro el acceso al conjunto o una parte de un sistema de información o se mantenga en él en contra de la voluntad de quien tenga el legítimo derecho a excluirlo [...]***
 - *El que mediante la utilización de artificios o instrumentos técnicos, [...], **intercepte transmisiones no públicas de datos informáticos [...]***

- Persona que utiliza sus conocimientos de informática y seguridad para realizar pruebas en redes y encontrar vulnerabilidades, para luego reportarlas y que se tomen medidas, sin hacer daño.

