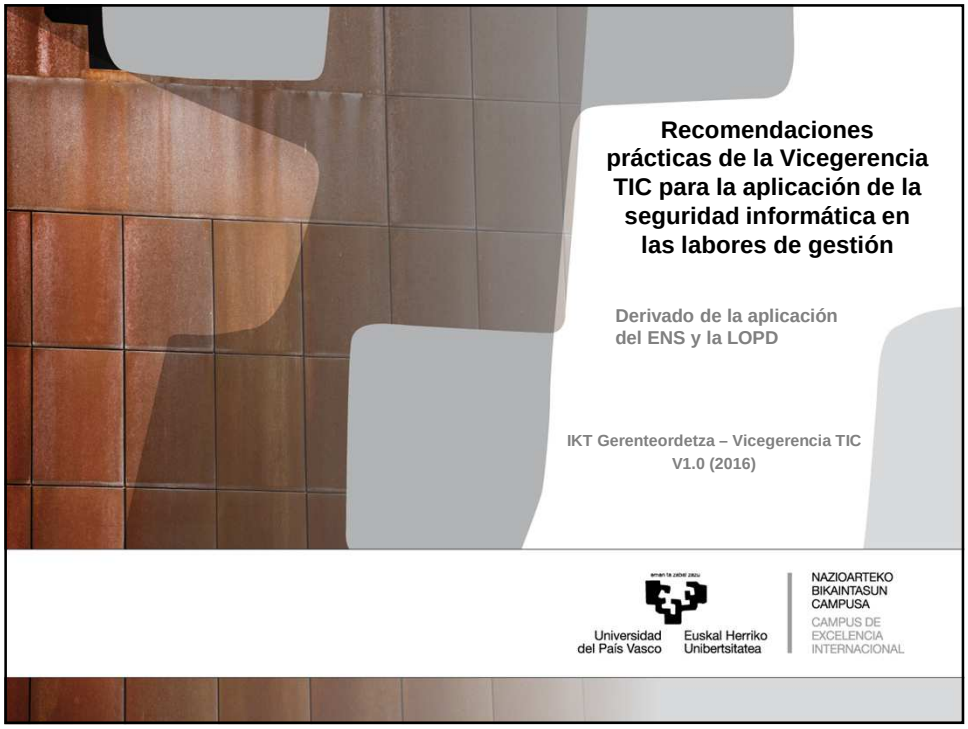


Recomendaciones prácticas de la Vicegerencia TIC para la aplicación de la seguridad informática en las labores de gestión

Derivado de la aplicación del ENS y la LOPD

IKT Gerenteordetza – Vicegerencia TIC
V1.0 (2016)

Universidad del País Vasco Euskal Herriko Unibertsitatea

NAZIOARTEKO BIKAINTASUN CAMPUSA
CAMPUS DE EXCELENCIA INTERNACIONAL

índice

Índice

- Introducción
- Gestión de la Seguridad
- Aplicación de la seguridad
  - Protección de la información
  - Protección de los soportes
  - Protección del puesto de trabajo
  - Protección de los dispositivos móviles
- Conclusiones

Definiciones

- **Seguridad:**
  - Exención de todo peligro, daño o riesgo (RAE).
- **Información:**
  - Conocimientos que permiten ampliar o precisar los que se poseen sobre una materia determinada (RAE).
  - Conjunto organizado de datos procesados, que constituyen un mensaje que cambia el estado de conocimiento del sujeto o sistema que recibe dicho mensaje (Wikipedia).
- **Seguridad de la Información:**
  - Es la capacidad para resistir, con un determinado nivel de confianza, los accidentes o acciones ilícitas o malintencionadas que comprometan la disponibilidad, autenticidad, trazabilidad, integridad y/o confidencialidad de la información.

Definiciones – Dimensiones de la Seguridad

- **Disponibilidad:**
  - Aseguramiento de que las personas usuarias autorizadas tienen acceso cuando lo requieran a la información y sus activos asociados (ENS)
- **Integridad:**
  - Garantía de la exactitud y completitud de la información y los métodos de su procesamiento (ENS)
- **Confidencialidad:**
  - Aseguramiento de que la información es accesible sólo para aquellos autorizados a tener acceso (ENS).
- **Autenticidad**:
  - Aseguramiento de la identidad u origen (ENS).
- **Trazabilidad**:
  - Aseguramiento de que en todo momento se podrá determinar quién hizo qué y en qué momento (ENS).

5

Medidas de seguridad

- **Diferentes ámbitos de actuación:**
  - Organizativo
    - Roles y responsabilidades
  - Normativo
    - Obligaciones
  - Operativo
    - Procedimientos
      - Generales / técnicos
  - Contractual
    - Condiciones (aplicable a cualquiera de los ámbitos anteriores)
    - Limitación de responsabilidades
  - Tecnológico
    - Garantizar cumplimiento de las anteriores
    - Físico / lógico
      - No documentales

6

Esquema Nacional de Seguridad

- **Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica**
- **Real Decreto 951/2015, de 23 de octubre, de modificación del Real Decreto 3/2010**
- **Objetivos:**
  - **Crear las condiciones necesarias de confianza en el uso de los medios electrónicos**
    - **Medidas para garantizar la seguridad de los sistemas, los datos, las comunicaciones y los servicios electrónicos.**
  - **Permitir a los ciudadanos y a las administraciones públicas, el ejercicio de derechos y el cumplimiento de deberes a través de estos medios**
- **Aplica a:**
  - **Servicios electrónicos**
  - **Medios electrónicos**
  - **Información tratada por dichos servicios y/o medios**

7

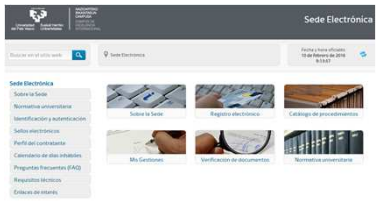
Esquema Nacional de Seguridad

- **Define las exigencias que debe cumplir un organismo público en materia de seguridad de la información**
  - **Establece los principios básicos a ser tenidos en cuenta en las decisiones en materia de seguridad.**
  - **Determina los requisitos mínimos que se deben respetar para permitan una protección adecuada de la información.**
  - **Define un mecanismo para lograr el cumplimiento de los principios básicos y requisitos mínimos**
    - **Adoptar medidas de seguridad proporcionadas a la naturaleza de la información, los sistemas y los servicios a proteger.**
  - **Incorpora un catálogo de medidas de seguridad a aplicar**
    - **Organizativas**
    - **Operacionales**
    - **Tecnológicas**

8

Casos de ejemplo de aplicación del ENS

- Sede electrónica
  - Portal
  - Registro electrónico de entrada
  - Mis gestiones
  - …
- Servicios al PAS / Prestados por el PAS
  - GAUR
  - EHUDoku
  - Portal del Empleado
  - …
- Medios utilizados para la prestación de servicios
  - Puesto de trabajo
  - PC
  - Servidores
  - Comunicaciones



Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal

Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999

Objetivos:

- Garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor e intimidad personal y familiar.
- Hacer frente a los riesgos que para los derechos de la personalidad pueden suponer el acopio y tratamiento de datos de carácter personal.

Aplica a:

- Datos de carácter personal, sea cual sea su modalidad de uso
- Soportes físicos y/o electrónicos

- **Define las exigencias que debe cumplir un organismo público en materia de protección de los datos personales**
  - Establece los principios de la protección de datos
    - Calidad de los datos
    - Deber de información y consentimiento
    - Seguridad de los datos y deber de secreto
    - Comunicación de datos (Cesiones y tratamientos por cuenta de terceros)
  - Determina los derechos básicos de los afectados (derechos ARCO: Acceso, Rectificación, Cancelación y Oposición)
  - Define las obligaciones que deben cumplir los responsables de los ficheros de datos de carácter personal
  - Establece las medidas de seguridad que se deben aplicar en el tratamiento de los datos de carácter personal.
    - Para ficheros y tratamientos automatizados (electrónicos)
    - Para ficheros y tratamientos no automatizados (en papel)
    - Con distinto nivel (Bajo/Medio/Alto) en función de los datos en cuestión
      - Datos de nivel Alto: Datos personales relativos a ideología, afiliación sindical o política, religión y creencias, origen racial, salud, vida sexual, fines policiales sin consentimiento del afectado o violencia de género

- **Casos de ejemplo de aplicación de la LOPD**
  - Datos de carácter personal tratados en la Sede electrónica
    - Mis gestiones
    - …
  - Datos de carácter personal del PAS
    - Portal del empleado
    - …
  - Datos de carácter personal tratados por el PAS
    - GAUR
    - …
  - Medios utilizados para el tratamiento de los datos personales
    - Puesto de trabajo
    - PC
    - Servidores
    - Comunicaciones

Índice

- Introducción
- Gestión de la Seguridad
- Aplicación de la seguridad
  - Protección de la información
  - Protección de los soportes
  - Protección del puesto de trabajo
  - Protección de los dispositivos móviles
- Conclusiones

13

Regulación de la Seguridad

- La universidad regula la seguridad de la información.
  - Estableciendo políticas, normas, procedimientos y guías
    - Que deben ser cumplidas y aplicadas por todas las personas.
  - Motivación:
    - Adaptar el funcionamiento de la universidad a la legislación.
    - Evitar dudas o errores de interpretación de la regulación.
    - Ayudar a las personas usuarias a que realicen su trabajo con el adecuado nivel de seguridad.
      - Pautas de actuación en el día a día.
- Política de Seguridad:
  - Conjunto de directrices que rigen la forma en que la universidad gestiona y protege la información y los servicios que considera críticos.
  - https://egoitza.ehu.eus/es/informazioaren-segurtasun-politika

- Política
- Normativa
- Procedimientos
- Guías

14

Regulación de la Seguridad

- **Normas de Seguridad:**
  - Describen:
    - El uso correcto de equipos, servicios e instalaciones.
    - Lo que se considerará uso indebido.
    - La responsabilidad del personal en caso de incumplimiento de estas normas.
      - De acuerdo con la regulación vigente.
- **Procedimientos de Seguridad:**
  - Detallan:
    - Cómo llevar a cabo las tareas habituales.
    - Quién debe hacer cada tarea.
    - Cómo identificar y reportar comportamientos anómalos.
- **Guías de Seguridad:**
  - Describen buenas formas de realizar determinadas tareas.
  - Aconsejan la mejor manera de ejecutar las actividades descritas.

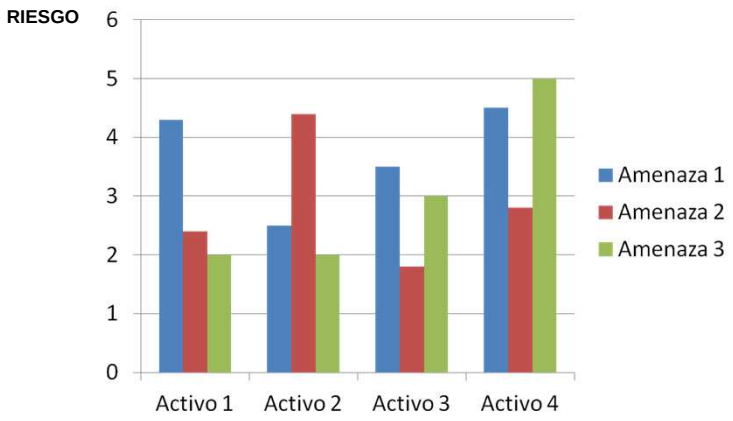
15

Gestión de los Riesgos de Seguridad

- **Objetivo: aplicar medidas de seguridad proporcionales a los riesgos.**
  - Cuando mayor sea el riesgo más seguridad será necesaria.
- **Ejemplo: Terremoto Vs Infección por Virus Informático**
  - Terremoto: Riesgo medio-bajo: muy poco probable, impacto alto (afecta a todas las personas)
  - Virus informático: Riesgo alto: bastante probable, impacto alto (si no se elimina se reproduce y acaba afectando al trabajo de todo el mundo)

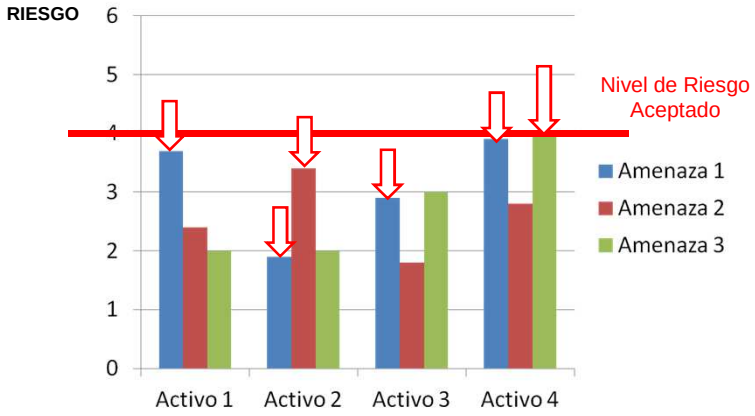
16

Análisis de riesgos:



17

Gestión de riesgos:



18

Gestión de incidentes de Seguridad

- **Incidente de seguridad:**
  - Suceso inesperado o no deseado que afecta negativamente a la seguridad de los activos (a alguna de sus dimensiones de seguridad).
  - Ej.: Datos incorrectos en la aplicación, aparece información donde no debería, el ordenador hace cosas "muy raras", etc.
- **Gestión de incidentes de seguridad:**
  - Plan de acción para atender a las incidencias que se den. Además de resolverlas debe incorporar medidas de desempeño que permitan conocer la calidad del sistema de protección y detectar tendencias antes de que se conviertan en grandes problemas (ENS).
- **Pasos de la gestión de incidentes de seguridad:**
  - Detección del incidente
  - Notificación del incidente:
    - Comunicar el incidente inmediatamente (al CAU y al responsable del servicio o área)
  - Tratamiento y resolución

19

Índice

20

Clasificación de la información

- **Se debería clasificar la información, considerando:**
  - **El impacto que supondría un incidente de seguridad que afectara a dicha información**
  - **La naturaleza de la información**
    - **De acuerdo a lo establecido legalmente (LOPD, otros).**
  - **Los posibles niveles de clasificación (confidencialidad) de la universidad:**
    - **Pública**
    - **Reservada (con distintos niveles de confidencialidad: Uso Interno, Confidencial,…).**
- **Se deberían aplicar las medidas de seguridad correspondientes a dicha clasificación.**
  - **Tratando la información de acuerdo a los procedimientos establecidos para cualquier actividad relacionada con dicha información, incluyendo:**
    - **Su control de acceso.**
    - **Su cifrado / firma electrónica.**
    - **La gestión de sus metadatos.**
    - **La realización de copias.**
    - **La eliminación de la información.**
    - **El uso de soportes / PC / Medios móviles.**

21

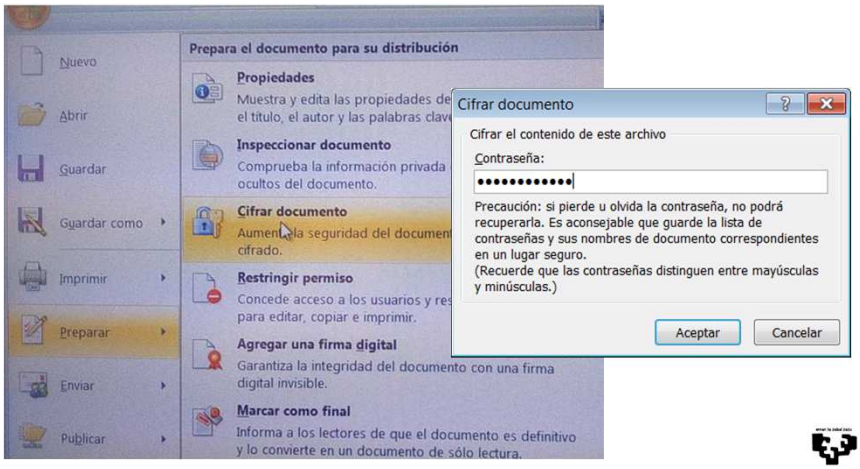
Clasificación de la información

- **Principios básicos de tratamiento de la información:**
  - **Las medidas de seguridad aplicadas por el usuario deberían ser proporcionales**
    - **A la seguridad del entorno de tratamiento de dicha información (la universidad / el exterior)**
    - **Al nivel de confidencialidad de la información**
  - **La información corporativa debe residir en los servicios corporativos**
  - **Se puede utilizar temporalmente la información corporativa en local**
    - **Protegiéndola adecuadamente, según su nivel de confidencialidad**
      - **Aplicando las medidas de protección de la información**
      - **Aplicando las medidas de protección de los soportes**
      - **Aplicando las medidas de protección del puesto de trabajo**
      - **Aplicando las medidas de protección de los dispositivos móviles**

22

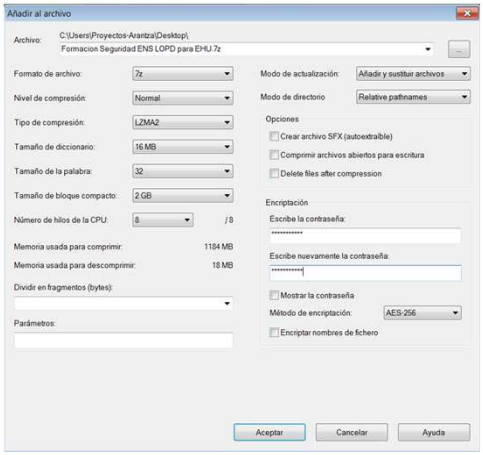
- **El cifrado de información es un proceso muy sensible y de alto riesgo**
  - Si se perdiese la contraseña o el certificado fuese revocado, no se podría recuperar NADA de la información cifrada.
- **Se cifrará toda la información de los niveles de confidencialidad más altos (y el nivel ALTO según la LOPD)**
  - Durante su almacenamiento
    - Cifrando los archivos (PDF, Office, etc.) mediante los propios programas que los utilizan, protegiéndolos con una clave.
    - Protegiendo los archivos o carpetas dentro de un ZIP con clave.
    - Cifrando carpetas completas mediante herramientas de cifrado específicas
      - En el caso de no disponer de las mismas, solicitarlas al CAU.
    - Cifrando los pen-drives, CDs, DVDs y similares en las que se graban los archivos que contienen información de dicho nivel, mediante las herramientas proporcionadas por el CAU.
    - Ejemplos:
      - Cifrado con 7-Zip(zip)
      - Microsoft Word (docx)
      - Adobe Acrobat Pro (pdf)

- **Cifrado de docx con Microsoft Word:**
  - Botón Office → Preparar → Cifrar documento → Introducir contraseña de cifrado



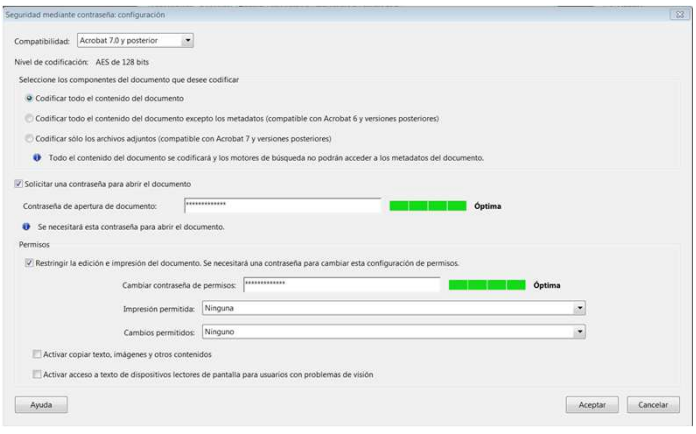
Cifrado de zip con 7-Zip:

- Clic derecho sobre el archivo → 7-Zip → Añadir al archivo → Introducir contraseña en el apartado "Encriptacion"



Cifrado de pdf con Adobe Acrobat Pro:

- Archivo → Propiedades → Seguridad Sistema de Seguridad → Seleccionar Seguridad mediante contraseña



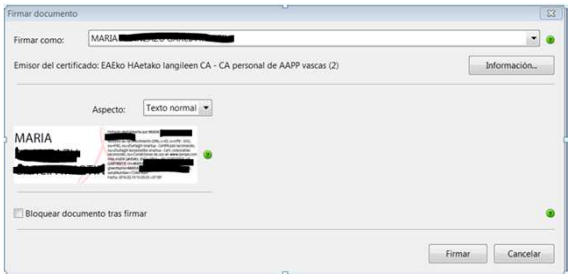
Protección de la información

- **Se cifrará toda la información de los niveles de confidencialidad más altos (y el nivel ALTO según la LOPD):**
  - **Durante la comunicación:**
    - **Cifrando los archivos adjuntos en los correos electrónicos que contienen dicha información.**
      - **Transfiriendo la información al adjunto si fuera necesario.**
      - **Comunicando la contraseña de cifrado por un medio alternativo.**
    - **Utilizando VPNs para acceder desde el exterior de la universidad a sistemas y/o servicios que contienen información de dicho nivel (según se indica en el apartado correspondiente).**
- **Las personas deberían asegurarse de que los servicios web que contienen la información del nivel de confidencialidad más alto son servicios https (verificando el "candado" de la barra de direcciones del navegador).**

27

Firma electrónica

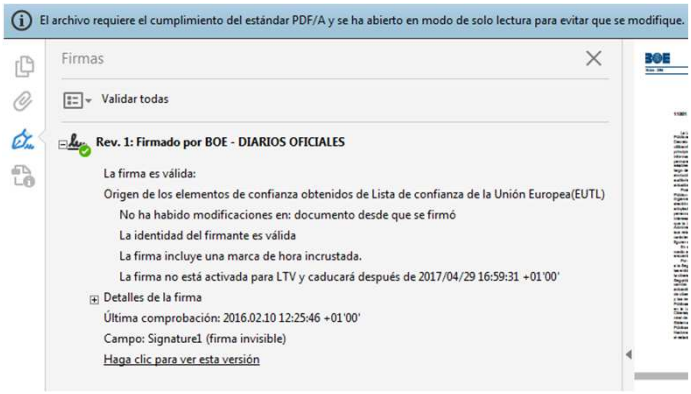
- **Se empleará la firma electrónica para garantizar la autenticidad del origen y la integridad de la información:**
  - **Firmando las actuaciones administrativas que lo requieran con el certificado corporativo (tramitación electrónica / registro electrónico)**
  - **Firmando los documentos PDF que lo requieran (siempre que el programa esté correctamente configurado y personalizado) con el certificado corporativo (integrado en la tarjeta universitaria)**
    - **Ver → Rellenar y Firmar → Colocar firma → Arrastrar nuevo rectángulo de firma → Seleccionar certificado a utilizar → Firmar**



28

Firma electrónica

- **Se verificará la autenticidad del origen y la integridad de la información verificando su firma electrónica:**
  - **Verificando que los documentos electrónicos que lo requieran han sido firmados de forma válida**



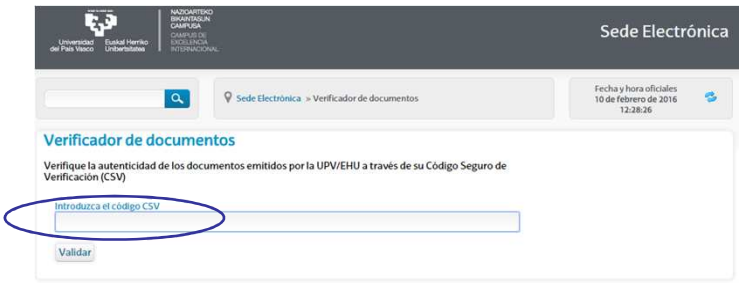
29

Firma electrónica

- **Impresión de documentos firmados:**
  - **No tiene validez, salvo que tenga CSV (Código Seguro de Verificación)**
    - **CSV es un código formado por un conjunto de dígitos que identifican de forma única a un documento electrónico oficial.**
      - **Lo generan automáticamente la sede electrónica y herramientas relacionadas.**
      - **Aparece impreso en todas y cada una de las páginas del documento.**
    - **Sirve para contrastar la autenticidad e integridad de un documento impreso originalmente electrónico y la validez de la firma.**

30

- **Verificación de documentos CSV:**
  - En la sede electrónica del organismo que ha generado el documento



- **Los metadatos son datos que definen o describen características de los ficheros, y se generan de forma automática y sin control por parte de las personas usuarias. Son, por ejemplo:**
  - Fecha y hora de creación del archivo
  - La ubicación geográfica de dónde fue creado el archivo
  - El nombre del equipo informático y/o su dirección IP
  - Los nombres de las personas, sistemas y/u organizaciones que hayan participado en la edición del documento y los comentarios que insertaron
- **Los metadatos pueden revelar más información de lo deseable sobre las personas o sobre la propia institución.**
  - Dicha información puede ser utilizada para realizar ataques, sobre todo si el documento se difunde ampliamente, como cuando se ofrece al público en un servidor web u otro tipo de repositorio de información.
  - Por ello, es necesario minimizar dicha información.

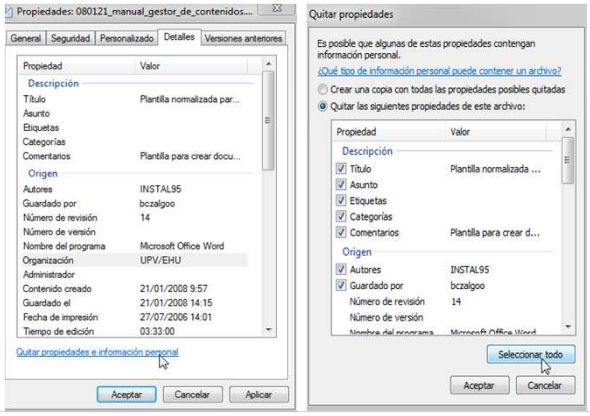
Documentos y metadatos

- Se debería aplicar un proceso de limpieza de documentos, en el que se retirará toda la información adicional contenida en campos ocultos, meta-datos, comentarios o revisiones anteriores
  - Salvo cuando dicha información sea pertinente para el receptor.
- El procedimiento de limpieza de documentos será diferente en función del tipo de archivo y la aplicación asociada. Por ejemplo:
  - Eliminar metadatos en Windows 7
  - Eliminar metadatos ocultos en Microsoft Office
  - Eliminar metadatos en Adobe Acrobat Pro

33

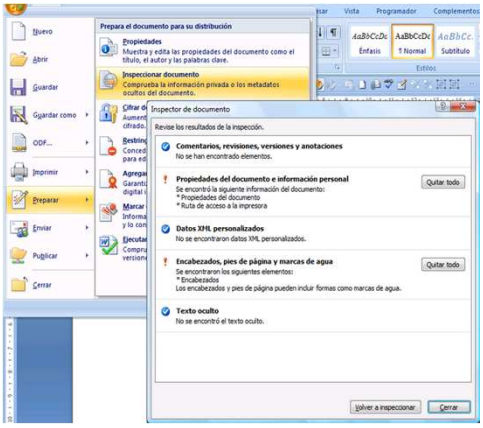
Documentos y metadatos

- Eliminar los metadatos (Windows 7):
  - En Propiedades del Archivo (click derecho) → Detalles → Quitar propiedades e Información Personal → Seleccionar "Quitar las siguientes propiedades de este archivo"
  - Opción 1: "Seleccionar todo" → Aceptar
  - Opción 2: Seleccionar las propiedades que deseen eliminar → Aceptar



34

- **Eliminar metadatos ocultos en docx (Microsoft Office 2007 o superior):**
  - **Botón Office→ Preparar → Seleccionar "Inspeccionar documento"**
  - **Pulsar en "Inspeccionar" → Seleccionar los metadatos que deseen eliminar → Pulsar en "Quitar todo" en el apartado correspondiente**



- **Eliminar metadatos en PDF (Adobe Acrobat Pro):**
  - **En Archivo → Propiedades → Pestaña Descripción → Borrar los metadatos deseados → Pulsar Metadatos adicionales → Borrar los metadatos deseados**

Copias de Seguridad

- La universidad realiza regularmente copias de seguridad de los servicios corporativos, que permiten recuperar datos perdidos, accidental o intencionadamente con una antigüedad determinada.
- Las personas usuarias deberían realizar copias de seguridad de aquella información almacenada localmente en sus equipos.
  - Realizando copias de seguridad en soportes externos (Pen-drive USB, CD, DVD, etc.).
- Estas copias deberían disfrutar, al menos, del mismo nivel de seguridad que los datos originales.
  - Para garantizar la protección de la copia de seguridad (backup), se debería, al menos, comprimir y cifrar dicha información (ZIP).
  - Será necesario verificar que las copias de seguridad sean recuperables.
- Lo recomendable sería trasladar dicha información local a los servicios corporativos de almacenamiento (gorde, gordetalde, EHUDoku, etc.).
  - Ojo! Hay medios, como gordetalde y EHUDoku, que son compartidos

37

Eliminación de la información

- Toda la información y/o documentación de carácter corporativo debería ser conservada en los repositorios y/o servicios corporativos antes de su eliminación en local (en el puesto de trabajo) .
- La información corporativa almacenada en local debería ser considerada de carácter temporal, y por tanto ser eliminada una vez que finalice dicho uso temporal.
- Los mecanismos de eliminación pueden ser:
  - Borrando la información en local.
  - Formateando a bajo nivel (o destruyendo si no es formateable) los soportes en los que haya copias electrónicas almacenadas (ver apartado correspondiente).
  - Destruyendo las copias temporales impresas en papel.

38

Índice

- Introducción
- Gestión de la Seguridad
- Aplicación de la seguridad
  - Protección de la información
  - Protección de los soportes
  - Protección del puesto de trabajo
  - Protección de los dispositivos móviles
- Conclusiones

39

Soportes externos de información

- **Se considerarán soportes externos de información a todos los dispositivos removibles (Pen-Drives USB, CDs, DVDs u otros de naturaleza análoga).**
  - No se consideran soportes externos de información los teléfonos móviles, smartphones, tabletas y similares, que se enmarcan en la categoría de dispositivos móviles (ver apartado correspondiente).
- **Todos los soportes externos de información se identificarán de forma que se indique el máximo nivel de seguridad de la información contenida, pero sin revelar su contenido.**
  - Las personas usuarias deberían poder entender el significado de las identificaciones
    - Mediante alguna utilidad o referencia que lo explique
    - Mediante simple inspección visual

40

Soportes externos de información

- **Las personas usuarias deberían aplicar la debida diligencia y control a los soportes de información que permanezcan bajo su responsabilidad:**
  - Garantizando que se respetan las condiciones del fabricante respecto a temperatura, humedad y otros agresores medioambientales.
  - Garantizando que sólo puede acceder físicamente a ellos el personal autorizado.
  - Registrando los envíos y/o recepciones de dichos soportes y quién autoriza dicho movimiento.
  - Cifrando el contenido.
- **Si se realizan envíos de soportes de información, las personas usuarias deberían:**
  - Registrar la salida y el transportista que recibe el soporte.
  - Cotejar el envío con la recepción asociada (verificar la recepción).
  - Notificar un incidente de seguridad si el cotejo falla.

41

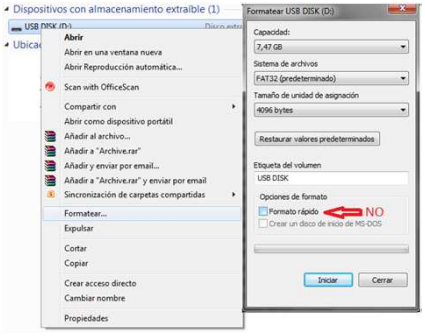
Soportes externos de información

- **Si se reciben soportes de información, las personas usuarias deberían:**
  - Asegurarse de que la recepción estaba prevista y verificar la fuente.
    - Adoptar todas las cautelas necesarias en caso contrario.
  - Registrar la entrada y el transportista que entrega el soporte.
  - Cotejar la recepción con el envío asociado.
  - Notificar un incidente de seguridad si el cotejo falla.
- **Los medios de cifrado a aplicar serán los definidos en el apartado de protección de la información.**
  - La contraseña de cifrado debería ser comunicada al destinatario del envío por un medio alternativo.

42

Soportes externos de información

- Las personas usuarias deberían formatear a bajo nivel los soportes que vayan a ser reutilizados para almacenar otra información o vayan a ser liberados a otra organización.



- En cualquier otro caso, los soportes deberían ser destruidos.
  - También deberían ser destruidos en caso de que exista un procedimiento específico que así lo estipule.

Índice

Puesto de trabajo

- **Los puestos de trabajo deberían permanecer despejados, sin más información ni soportes encima de la mesa que los requeridos para la actividad que se está realizando en cada momento.**
- **La información reservada no será accesible cuando no se esté utilizando.**
  - **La documentación en papel se guardará en lugar cerrado cuando no se esté utilizando.**
  - **La pantalla no debería mostrar información reservada cuando no esté siendo utilizada.**

45

Ordenador corporativo

- **Los ordenadores deben estar preparados para dar servicio en todo momento.**
  - **Para ello, ninguna persona usuaria podrá disponer de permisos de administración del equipo, con el fin de evitar que ningún tipo de actuación, malware o funcionamiento anómalo pueda afectar gravemente a dicha operatividad.**
  - **Del mismo modo, ninguna persona usuaria debería instalar ningún software no autorizado, para evitar que pueda afectar al funcionamiento o rendimiento del equipo.**
- **El uso del ordenador y los medios electrónicos corporativos (e-mail, navegación, etc.) debería ser exclusivamente profesional.**
  - **Su uso para fines particulares puede incrementar significativamente el riesgo.**
  - **La actividad de las personas usuarias está asociada a la universidad**

46

Identificación de personas usuarias

- **Cada persona estará identificada unívocamente, mediante la correspondiente credencial, ante los sistemas de información de la universidad, de forma que:**
  - **Se pueda saber qué persona recibe cada identificador y qué derechos de acceso recibe.**
  - **Se pueda saber quién ha hecho algo y qué ha hecho.**
- **Las credenciales de acceso estarán bajo el control exclusivo de la persona usuaria y sólo se activarán una vez que lo estén.**
  - **Ninguna persona podrá utilizar las credenciales de acceso de otra.**

47

Mecanismos de autenticación y control de acceso

- **La persona usuaria reconocerá que ha recibido las credenciales de acceso y que conoce y acepta las obligaciones que implica su tenencia:**
  - **Deber de custodia diligente**
  - **Protección de su confidencialidad**
  - **Información inmediata en caso de pérdida.**
- **Se podrán utilizar diferentes medios de autenticación para el acceso a los sistemas de información:**
  - **Cuenta/Contraseña corporativa**
    - **Es un sistema de autenticación cuya robustez se basa en la fortaleza de la contraseña (política de contraseñas aplicada).**
  - **Tarjeta corporativa + PIN**
    - **Es un sistema de autenticación más robusto, hacia el que la universidad debería ir en un futuro.**

48

Mecanismos de autenticación y control de acceso

- **Se podrán utilizar diferentes medios de autenticación para el acceso a los sistemas de información:**
  - **Otros medios de autenticación**
    - **Se prevé la utilización, en un futuro, de otros medios de autenticación avanzados (contraseñas de un solo uso, tarjetas de barcos, etc.).**
- **La información revelada a quien intenta acceder será la mínima imprescindible.**
- **El número de intentos permitidos será limitado, bloqueando la oportunidad de acceso una vez efectuados un cierto número de fallos consecutivos.**
- **El sistema informará a la persona usuaria de sus obligaciones durante el proceso de acceso y autenticación.**

49

Uso de contraseñas de autenticación

- **Las contraseñas deberían memorizarse.**
  - **Si se opta por almacenarlas en un medio electrónico, las contraseñas deberían estar anotadas en un fichero cifrado**
  - **Siempre deberían estar almacenadas en un lugar seguro.**
- **La persona usuaria debe cambiar la contraseña la primera vez que se conecte y siempre que la contraseña haya sido suministrada por un administrador o sistema.**
- **La contraseña se debe cambiar ante cualquier sospecha de que otras personas puedan ser conocedoras de la misma.**
- **La contraseña no se comunicará a nadie (ni siquiera a superiores, compañeros o personal de los servicios informáticos) bajo ninguna circunstancia.**

50

Política de contraseñas

- Longitud mínima 8 caracteres
- Deberían contener caracteres de al menos 3 de los siguientes 4 tipos:
  - Numérico
  - Mayúsculas
  - Minúsculas
  - Caracteres especiales: * . + $ & # @ - ! % ^ ; ( ) { } [ ] < > ? /_
- No podrá tener caracteres en blanco.
- No podrá estar formada únicamente por palabras de diccionario u otras fácilmente predecibles o asociables a la persona usuaria (nombres, direcciones, matrículas, etc.)

51

Política de contraseñas

- No está permitido el uso del identificador de la cuenta de la persona usuaria, nombre o apellidos como contraseña o parte de la misma.
- Las contraseñas se deberían modificar antes de que transcurran seis (6) meses.
  - El tiempo de uso de una contraseña es un factor fundamental para que pueda ser descubierta.
- No se deberían reutilizar las últimas diez (10) contraseñas utilizadas.

52

Bloqueo del ordenador

- El ordenador debe bloquearse al cabo de un tiempo prudencial de inactividad.
  - Las personas usuarias siempre podrán bloquearlo manualmente pulsando las teclas <Windows>+<L> simultáneamente.
    - Fundamental en caso de ausencia del puesto de trabajo.
  - Los equipos corporativos también disponen de bloqueo automático por inactividad.
    - Si se emplea la tarjeta corporativa para iniciar sesión, el equipo corporativo también se podrá bloquear manualmente retirándola.
  - La persona usuaria debería autenticarse de nuevo para reanudar la actividad en curso.
- Se recomienda apagar el ordenador ante ausencias prolongadas
  - Una sesión iniciada en el equipo siempre es más vulnerable.

53

Antivirus

- El PC debería disponer de mecanismos de prevención y reacción frente a código dañino (comúnmente conocidos como antivirus).
  - Los equipos corporativos lo incluyen activado por defecto.
- El software anti-malware (antivirus) debería cumplir las siguientes premisas:
  - SIEMPRE debería estar habilitado
  - El patrón de firmas de virus debería estar actualizado
- Cualquier aviso del software antivirus relativo a una detección pero no eliminación de malware debería ser reportado diligentemente al CAU, de acuerdo a los procedimientos establecidos por la universidad.

54

Firewall del puesto de trabajo

- El PC debería disponer de mecanismos de protección frente a ataques de red (firewall o cortafuegos).
  - Los equipos corporativos lo incluyen activado por defecto.
- El firewall debería cumplir las siguientes premisas:
  - SIEMPRE debería estar habilitado.
  - NUNCA se podrá evadir la configuración por defecto.
- No debería estar permitido que a través de Internet alguien se pueda conectar al equipo
  - Salvo que sea una necesidad justificada y se obtenga el permiso correspondiente.
- Cualquier aviso sospechoso del firewall debería ser reportado diligentemente al CAU, de acuerdo a los procedimientos establecidos por la universidad.

55

E-mail, SPAM y Phishing

- Existen normas de uso del correo electrónico por parte del personal:
  - https://www.euskadi.eus/r47-bopvapps/es/bopv2/datos/2015/03/1501146a.shtml
- Además de las normas establecidas, se debería prestar atención a aspectos como:
  - El buzón de correo personal proporcionado por la UPV/EHU se considerará intransferible.
  - Se debe evitar introducir la dirección de correo en foros o listas de correo de Internet, salvo si es necesario y con proveedores de confianza, ya que muchos ataques se sirven de estas direcciones
  - Si no se conoce el remitente de un correo, y/o el asunto del mismo es extraño, se recomienda encarecidamente borrar el mensaje sin abrirlo (o situarlo en cuarentena hasta disponer de más datos), especialmente si contiene ficheros adjuntos y ejecutables.
  - Notificar al remitente la recepción de un correo electrónico recibido por error, y eliminarlo.

56

E-mail, SPAM y Phishing

- **Presta especial atención a los destinatarios**
  - Verifica que están correctamente escritos
  - Verifica que son los destinatarios correctos (cuidado con auto-completar)
  - Ten en cuenta el nivel de confidencialidad de la información enviada y sobre todo reenviada, limitando en la medida de lo posible el envío de información de los niveles de confidencialidad más altos
- **Además de las normas establecidas, se debería evitar:**
  - Participar en la propagación de cartas encadenadas o participar en esquemas piramidales o temas similares.
  - Hacer clic en enlaces sospechosos.
  - Ejecutar archivos adjuntos sospechosos.
  - Enviar o contestar mensajes que puedan introducir malware o implicar riesgos o problemas en los sistemas y herramientas informáticas y tecnológicas de la UPV/EHU.

57

Uso de servicios web, internet y redes sociales

- **En el uso de internet, servicios web y redes sociales se debería evitar:**
  - Acceder a sitios web relacionados con actividades ilegales.
  - Acceder a sitios de "hacking" o sitios reconocidos como inseguros, los cuales puedan poner en riesgo la integridad y confidencialidad de la información.
  - Descargar desde Internet cualquier material (incluyendo software) protegido bajo leyes de derecho de propiedad sin la correspondiente autorización o licencia de derecho de uso.
  - Hacer clic en enlaces sospechosos.
  - Publicar cualquier tipo de información perteneciente a la UPV/EHU o en nombre de ésta sin la autorización correspondiente
  - Obtener o intentar obtener acceso no autorizado sobre equipos, servicios, aplicaciones, datos o infraestructuras de la UPV/EHU o ajenos a ella.

58

Uso de servicios web, internet y redes sociales

- **En el uso de internet, servicios web y redes sociales se deberían seguir, en la medida de lo posible, las siguientes buenas prácticas:**
  - **Comprobar la seguridad y autenticidad de la página visitada (HTTPS).**
  - **Utilizar los niveles de seguridad del navegador.**
  - **Limitar el uso de navegación con cookies, si es posible.**
  - **Eliminar la información privada (historial, cookies, contraseñas, etc.) o navegar en modo InPrivate / Privado / Incognito**
  - **Limitar y vigilar la ejecución de Applets y Scripts.**
  - **No visitar páginas no fiables o sospechosas.**
  - **No descargar código o programas no confiables.**
  - **No instalar complementos desconocidos.**

59

Uso de servicios web, internet y redes sociales

- **Además, en el uso de redes sociales, se deberían considerar las siguientes buenas prácticas:**
  - **Limitar la cantidad de información proporcionada**
  - **"Pensar antes de publicar"**
    - **Cualquier publicación se convierte en permanente**
    - **La huella digital es prácticamente imposible de eliminar**

60

Índice

- Introducción
- Gestión de la Seguridad
- Aplicación de la seguridad
  - Protección de la información
  - Protección de los soportes
  - Protección del puesto de trabajo
  - Protección de los dispositivos móviles
- Conclusiones

Acceso Remoto y VPN

- Las soluciones VPN (Virtual Private Network) proporcionadas por la universidad aportan confidencialidad (cifrado) e integridad en la comunicación y autenticidad de la identidad de la persona usuaria.
  - http://www.ehu.eus/es/web/ikt-tic/vpn
- El acceso remoto de las personas usuarias, realizado desde fuera de las propias instalaciones de la universidad a través de redes de terceros (Internet), a servicios no expuestos en Internet, sólo se podrá realizar mediante el uso de las herramientas de VPN dispuestas por la universidad.
  - Se prohíbe, por tanto, el uso de herramientas alternativas de acceso y/o control remoto de los sistemas de la universidad.
- Una vez establecida la conexión VPN, las personas usuarias tendrán que llevar a cabo el mismo proceso de autenticación que el aplicado en la red de la universidad.
  - El acceso remoto por VPN no supondrá, por tanto, la concesión de privilegios de acceso adicionales.

Ordenadores portátiles

- Las personas deberían mantener precauciones frente a las posibilidades de pérdida o robo de estos equipos.
- Los responsables de cada equipo portátil estarán identificados.
- Se debería informar al CAU y al responsable correspondiente de pérdidas o sustracciones de estos equipos, de forma inmediata.
  - Indicando expresamente si el portátil sustraído contenía ficheros con información de nivel ALTO según la LOPD.
- Se debería evitar, en la medida de lo posible, que el equipo portátil contenga credenciales de acceso remoto a la universidad.
  - Se considerarán credenciales de acceso remoto aquellas que sean capaces de habilitar un acceso a otros equipos de la universidad, como las contraseñas de conexión VPN, contraseñas de acceso a servicios de la universidad u otras de naturaleza análoga.

63

Ordenadores portátiles

- Debido al aumento de posibilidades de pérdida o robo de información, se prestará especial atención a todas las medidas de seguridad aplicables al ordenador personal:
  - Backup de la información
  - Cifrado de la información de los niveles de confidencialidad más altos (y los datos personales de nivel ALTO según la LOPD).
  - Política de contraseñas
  - Antivirus
  - Firewall
  - VPN y acceso remoto

64

Teléfonos móviles y BYOD

- **Habrá que utilizar todas las medidas de seguridad propias de los teléfonos móviles, tabletas y dispositivos similares**
  - **PIN / Patrón / Huella / …**
    - **Ocultando la visualización del patrón en caso de que se use este método**
  - **Cifrado**
- **Habrá que aplicar todas las medidas de seguridad definidas para los ordenadores portátiles que sea posible**
- **Se debería limitar el uso de información sensible con estos dispositivos**
- **Si el móvil es corporativo**
  - **Notificar su pérdida o robo**
  - **Su avería o rotura debe ser gestionada por el CAU**

65

Teléfonos móviles y BYOD

- **Si utilizas tu móvil personal para tareas corporativas (BYOD, Bring Your Own Device)**
  - **Aplica las mismas medidas establecidas para los móviles corporativos**
  - **Diferencia lo personal de lo corporativo**
    - **Sepáralo y aíslalo siempre que sea posible**
    - **Evita compartir información corporativa con servicios de Internet (google, iTunes, etc.).**
  - **Notifica su pérdida o robo**

66

Wifis públicas o redes de terceros

- Las WiFis públicas son un entorno totalmente INSEGURO
  - Cualquiera se puede conectar
  - Cualquiera puede espiar las conexiones de cualquiera
    - Aunque haga falta clave (todo el que está conectado la tiene)
  - En la universidad sólo EDUROAM (no así EHU-wGuest) se debe considerar WiFi segura, ya que además cifra las comunicaciones
- Toma precauciones al utilizar las WiFis públicas o redes de terceros
  - No accedas a información sensible (reservada, privada)
  - Si tienes que acceder a información sensible utiliza sólo servicios seguros
    - Servicios HTTPS / VPN para acceder a los servicios de la universidad
  - Evita que te vean introducir tus contraseñas
  - Refuerza la aplicación de las medidas de seguridad para móviles

67

Índice

- Introducción
- Gestión de la Seguridad
- Aplicación de la seguridad
  - Protección de la información
  - Protección de los soportes
  - Protección del puesto de trabajo
  - Protección de los dispositivos móviles
- Conclusiones

68

Pon en práctica lo que has aprendido

- 1. Elige un documento Word cualquiera de tu PC
- 2. Quítale todos los metadatos
- 3. Genera un pdf dentro del Word
- 4. Fírmalo con tu tarjeta corporativa con Adobe Acrobat Pro
- 5. Cífralo mediante 7zip usando una contraseña robusta
- 6. Envíalo como adjunto por e-mail a otro asistente al curso
- 7. Comunícale la contraseña por un medio diferente al e-mail anterior
- 8. ¿Has recibido un e-mail con un adjunto cifrado? Ábrelo
- 9. ¿Crees que la contraseña era robusta? Coméntalo con el remitente
- 10. ¿Está firmado? Verifica la firma
- 11. ¿Te parece un documento que se pueda publicar en la web? Crees que debe ser accesible para todo el personal de la UPV/EHU? ¿Crees que debería estar cifrado siempre? Coméntalo con el remitente

69

Conclusiones

- La seguridad depende de todas las partes
  - De la universidad
  - De las personas
- Las personas solemos ser el eslabón más débil de la seguridad
  - Por desconocimiento
  - Por imprudencia
  - Por pereza
  - Por inconstancia
  - Y hasta por desidia
- Los problemas de seguridad afectan a todos

70

Conclusiones

- En caso de duda en temas de seguridad
  - Utiliza tu sentido común
    - "Piensa mal y acertarás"
- Si tienes sospechas de que hay algún problema de seguridad:
  - NOTIFICA
    - Al CAU y a tu responsable
    - Cuanto antes
    - Aportando la mayor información posible
  - Pregunta
    - Al CAU y a tu responsable

71

Dudas y preguntas

Joseba Enjuto, Nextel S.A.

72

La seguridad de la información y la buena imagen de la Universidad también dependen de ti

IKT Gerenteordetza – Vicegerencia TIC
V1.0 (2016)

Universidad del País Vasco
Euskal Herriko Unibertsitatea

NAZIOARTEKO BIKAINTASUN CAMPUSA
CAMPUS DE EXCELENCIA INTERNACIONAL

www.ehu.es