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

1 Introducción

El creciente uso de los medios electrónicos en la universidad es evidente. Este hecho no sólo es consecuencia directa del Plan Estratégico 2012-2017, sino que también pretende dar una respuesta eficaz y eficiente a la creciente regulación en materia de servicios electrónicos a la que está sujeta la UPV/EHU.

No obstante, el uso de estos medios electrónicos supone la obligación por parte de la UPV/EHU de crear las condiciones necesarias de confianza en el uso de los mismos, a través de la aplicación de medidas para garantizar la seguridad de los sistemas, los datos, las comunicaciones, y los servicios electrónicos, con el fin de permitir a la comunidad universitaria el ejercicio de derechos y el cumplimiento de deberes a través de estos medios con las garantías necesarias.

El objetivo del presente documento es el de acercar los conceptos de seguridad de la información a la labor del personal en relación a su actividad en el puesto de trabajo, presentando una serie de recomendaciones realizadas por la Vicegerencia TIC para que todo el personal pueda llevar a cabo una correcta aplicación de la seguridad informática en las labores de gestión.

Las medidas de seguridad a aplicar no dependen únicamente de la tecnología, sino que requieren que el personal que atiende los servicios y maneja los datos esté debidamente instruido y reciba la formación específica necesaria para garantizar un uso seguro de las tecnologías de la información aplicables a los sistemas y servicios de la universidad.

Por este motivo, el presente documento recoge los conceptos básicos acerca de las obligaciones legales existentes en materia de seguridad de la información y protección de datos personales y diversos consejos relativos a la aplicación práctica de las medidas de seguridad que todo el personal debería aplicar en su actividad habitual, relativas tanto al comportamiento en su puesto de trabajo como al manejo directo de la información y a la utilización de los dispositivos móviles y soportes en los que se almacena.

1.1 Conceptos básicos

El principal concepto sobre el que giran todos los demás es el de seguridad de la información. Sin embargo, es conveniente analizar ambos conceptos por separado para entender completamente su significado.

La RAE (Real Academia Española de la lengua) define el concepto de **seguridad** como la exención de todo peligro, daño o riesgo. Por lo tanto, de la propia definición de seguridad se puede deducir que el concepto de riesgo va a ser un concepto íntimamente ligado a la seguridad.

La RAE también define el concepto de **Información** como el conjunto de conocimientos que permiten ampliar o precisar los que se poseen sobre una materia determinada. Pero quizás haya otra definición alternativa más útil para nosotros, que establece que la información es un conjunto organizado de datos procesados, que constituyen un mensaje que cambia el estado de conocimiento del sujeto o sistema que recibe dicho mensaje.

Si analizamos el concepto de **dato de carácter personal**, que es cualquier información concerniente a personas físicas identificadas o identificables, es evidente que los datos de carácter personal no son más (ni menos) que un subconjunto de la información, y por lo tanto todos los conceptos aplicables a la seguridad de la información lo serán también a la seguridad de los datos de carácter personal o datos personales.

El concepto de **seguridad de la Información** se define como 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. Con esta definición podemos ver cómo ése peligro queda mucho más definido (accidentes o acciones ilícitas o malintencionadas), cómo se mantiene el concepto de riesgo (resistir con un determinado nivel de confianza) y cómo se particulariza el daño que puede sufrir la información: que se vea comprometida su disponibilidad, su integridad, su confidencialidad, su autenticidad y/o su trazabilidad.

Este concepto introduce las **5 dimensiones o características de la seguridad**:

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

Del concepto de seguridad de la información también se deriva su materialización. Si el objetivo es ser capaz de resistir frente a determinadas amenazas, la forma de resistir consistirá en aplicar medidas (de seguridad) concretas para lograr dicha resistencia.

Estas medidas de seguridad pueden ser aplicadas en ámbitos muy diferentes:

- **Organizativo**: Establecer roles y responsabilidades en torno a la aplicación de la seguridad
- **Normativo**: Definir obligaciones a cumplir por el personal que maneja la información a asegurar
- **Operativo**: Regular, mediante procedimientos, la manera de actuar de las personas para que realicen un manejo seguro de la información y de los medios, generalmente informáticos, que la procesan.
- **Contractual**: Establecer obligaciones más allá de la universidad, determinando qué condiciones deben cumplir las empresas subcontratadas y su personal, limitando las responsabilidades de la universidad al ámbito propio
- **Tecnológico**: Aplicar soluciones tecnológicas que evitan que las personas incumplan las obligaciones y procedimientos establecidos, garantizando de ese modo que su actuación es segura. Aunque muchas de estas medidas suelen ser informáticas, las medidas de carácter tecnológico también se aplican sobre la seguridad física (mediante cerraduras, tarjetas de acceso, etc.).

1.2 Legislación que regula la seguridad de la información

1.2.1 El Esquema Nacional de Seguridad

El Esquema Nacional de Seguridad, o **ENS**, lo constituyen el 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, junto con el Real Decreto 951/2015, de 23 de octubre, de modificación del Real Decreto 3/2010.

El objetivo del Esquema Nacional de Seguridad es el de crear las condiciones necesarias de confianza en el uso de los medios electrónicos, estableciendo para ello medidas para garantizar la seguridad de los sistemas, los datos, las comunicaciones y los servicios electrónicos, con el fin de permitir a los ciudadanos y a las administraciones públicas, el ejercicio de derechos y el cumplimiento de deberes a través de estos medios.

El Esquema Nacional de Seguridad aplica a los servicios electrónicos de la universidad, a los medios electrónicos necesarios para prestarlos y a la información tratada por dichos servicios y/o medios.

El ENS define las exigencias que debe cumplir un organismo público en materia de seguridad de la información. Para ello 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 y define un mecanismo para lograr el cumplimiento de los principios básicos y requisitos mínimos, consistente en adoptar medidas de seguridad proporcionadas a la naturaleza

de la información, los sistemas y los servicios a proteger. De este modo, el Esquema Nacional de Seguridad incorpora un catálogo de medidas de seguridad a aplicar, divididas en medidas organizativas, medidas operacionales y medidas tecnológicas.

Por lo tanto, el Esquema Nacional de Seguridad se aplicará a la información tratada por los diferentes servicios de la universidad y los medios electrónicos que los soportan:

- 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, …

1.2.2 La Ley Orgánica de Protección de Datos personales

La legislación en materia de protección de datos personales lo constituyen principalmente la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal y el Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999.

Los objetivos de la legislación en materia de protección de datos personales (cualquier dato que identifique o permita identificar a una persona o esté asociado a dicha persona, como son, por ejemplo, nombre, apellidos, DNI, dirección, fecha de nacimiento, fotografía, e-mail, …) consisten en 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, así como hacer frente a los riesgos que para los derechos de la personalidad pueden suponer el acopio y tratamiento de datos de carácter personal.

La legislación en materia de protección de datos personales aplica a los datos de carácter personal, sea cual sea su modalidad de uso, tanto en soportes físicos (papel) como en soportes electrónicos.

La legislación en materia de protección de datos personales 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, deber de secreto y 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 y establece las medidas de seguridad que se deben aplicar en el tratamiento de los datos de carácter personal, tanto para información en formato electrónico como para información en papel. Estas medidas de seguridad se organizan en niveles (Bajo/Medio/Alto) en función de los datos en

cuestión, siendo los de nivel alto los que se refieren a datos de ideología, afiliación sindical, religión, creencias, origen racial, salud o vida sexual; los que contengan o se refieran a datos recabados para fines policiales sin consentimiento de las personas afectadas y aquellos que contengan datos derivados de actos de violencia de género.

Por lo tanto, la legislación en materia de protección de datos personales se aplicará a la información personal tratada por los diferentes servicios de la universidad y los medios electrónicos que los soportan:

- 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, …

De este modo, se puede comprobar cómo, independientemente de la regulación específica que aplique, la seguridad de la información acaba siendo un elemento a tener en cuenta en prácticamente cualquiera de las situaciones en las que el personal de la universidad utilice cualquier tipo de información.

2 Gestión de la seguridad

2.1 Regulación de la seguridad

La universidad regula la seguridad de la información estableciendo medidas de seguridad de carácter normativo y operativo, con el fin de adaptar el funcionamiento de la universidad a la legislación, evitar dudas o errores de interpretación de dicha legislación y ayudar a las personas usuarias a que realicen su trabajo con el adecuado nivel de seguridad, estableciendo pautas de actuación en el día a día. Estas medidas de seguridad se traducen en el desarrollo de diferentes tipos de documentos que deben ser seguidos y aplicados por las personas afectadas. Estos documentos son:

- La Política de Seguridad es un conjunto de directrices que rigen la forma en que la universidad gestiona y protege la información y los servicios que considera críticos. Puede localizarse en la siguiente URL: https://egoitza.ehu.eus/es/informazioaren-segurtasun-politika
- Las Normas de Seguridad son documentos que describen el uso correcto de equipos, servicios e instalaciones, lo que se considerará uso indebido y la responsabilidad del personal en caso de incumplimiento de estas normas, de acuerdo con la regulación vigente.
- Los Procedimientos de Seguridad son documentos que detallan cómo llevar a cabo las tareas habituales, quién debe hacer cada tarea y cómo identificar y reportar comportamientos anómalos.

- Las Guías de Seguridad son documentos que describen buenas formas de realizar determinadas tareas y aconsejan la mejor manera de ejecutar las actividades descritas.

2.2 Gestión de los riesgos de seguridad

La gestión de los riesgos es el núcleo de la gestión de la seguridad. Su objetivo es que las medidas de seguridad que se apliquen sean proporcionales a los riesgos, de modo que cuanto mayor sea el riesgo mayor seguridad será necesaria.

La gestión de los riesgos se divide en dos fases. La primera de ellas es el **análisis de los riesgos**. Para ello, en primer lugar se lleva a cabo la **identificación de los diferentes activos** que intervienen en los servicios (los propios servicios, la información, los datos personales, los medios electrónicos, las personas, etc.), y a continuación se **valora la importancia de dichos activos**, determinando cómo de grave es que ese activo "pierda" su seguridad. Dicha valoración debe ser realizada por el responsable de cada activo, puesto que es quien tiene la capacidad para evaluar adecuadamente dicha importancia.

Una vez que se han identificado y valorado los activos se **evalúan las amenazas** que afectan a cada uno de esos activos, cuantificando el "daño" (impacto) que dichas amenazas pueden provocar, con el fin de evaluar de ese modo el riesgo asociado a cada una de ellas.

La segunda fase de la gestión de los riesgos es la mitigación de los riesgos, que consiste en determinar las medidas de seguridad específicas a aplicar sobre cada activo para reducir el "daño" que cada una de las amenazas pueden provocarle, reduciendo de ese modo el riesgo hasta unos niveles que la universidad considere aceptables.

De este modo, la universidad probablemente aplicará antes medidas de seguridad frente a un virus informático, cuyo riesgo se considera alto (bastante probable y de impacto alto, puesto que si no se elimina se reproduce y acaba afectando al trabajo de todo el mundo) que frente a un terremoto, cuyo riesgo se considera medio-bajo (muy poco probable, aunque de impacto alto, puesto que afecta a todas las personas).

2.3 Gestión de incidentes de seguridad

Desafortunadamente, las medidas de seguridad no son infalibles. Ya sea porque su aplicación dependa de las personas, o ya sea porque incluso las medidas tecnológicas fallan, van a existir situaciones en las que se produzcan incidentes de seguridad, entendidos como suceso inesperado o no deseado que afecte negativamente a la seguridad de los activos (a alguna de sus dimensiones de seguridad). Estos incidentes de seguridad, en la práctica, son situaciones tales como la aparición de datos

incorrectos en una aplicación, aparición de información en lugares en los que no debería aparecer (como documentos en papel que caen en manos de quien no debería tenerlos), situaciones en las que el ordenador hace cosas “muy raras”, etc.

Como los incidentes de seguridad son inevitables, uno de los factores fundamentales de la seguridad de la información es la gestión de incidentes de seguridad, entendida como el desarrollo de planes de actuación para atender a los incidentes de seguridad que se puedan producir, y que además de resolverlos debe incorporar mecanismos de medición que permitan conocer la calidad de las medidas de seguridad y detectar tendencias antes de que se conviertan en grandes problemas.

La gestión de incidentes tiene dos pasos fundamentales que dependen de todas las personas: la detección del incidente de seguridad y su notificación. Esto supone que todo el personal es responsable de identificar cualquier tipo de situación que suponga o pueda suponer un incidente de seguridad, así como de notificarlo diligentemente tanto al CAU como al responsable del servicio o área en cuestión. A partir de ahí, serán las figuras designadas por la universidad las encargadas de llevar a cabo el tratamiento y resolución del incidente de seguridad, de acuerdo a los procedimientos previstos.

3 Aplicación de la seguridad

Aunque muchas de las medidas de seguridad vengan garantizadas por la universidad, existen muchas otras que, por ser de carácter normativo u operativo, dependen de que tanto el personal de la universidad como las personas usuarias las apliquen de manera adecuada y diligente. Por ello, a continuación se definen cada una de las medidas de seguridad que se deben tener en cuenta en las labores de gestión.

3.1 Protección de la información

Las medidas de seguridad más eficaces son las que se aplican directamente sobre la información, ya que garantizan su protección directa.

3.1.1 Clasificación de la información

La primera medida de seguridad aplicable a la información es la de su clasificación desde el punto de vista de la seguridad. Para ello habría que tener en cuenta aspectos como la valoración del propio activo de información (tal y como se ha explicado en el apartado de análisis de riesgos), considerando el impacto que supondría un incidente de seguridad que afectara a dicha información, o la naturaleza de la información, teniendo en cuenta, entre otros, los criterios legales aplicables (la LOPD si fuesen datos personales, u otros).

La clasificación de la información deriva en la aplicación de diferentes niveles, que suelen atender, habitualmente, a su confidencialidad, de modo que se habla generalmente de información pública para aquella cuya confidencialidad es nula y de información sensible o reservada si tiene algún tipo de confidencialidad, estableciéndose distintos niveles en función de dicha confidencialidad (se suelen utilizar conceptos como información de uso Interno, confidencial, restringida, etc.).

El objetivo de clasificar la información es poder aplicar medidas de seguridad proporcionales a dicha clasificación, de forma que la información menos confidencial se pueda utilizar de manera más flexible y sólo se apliquen restricciones al uso de la información cuya confidencialidad así lo requiera. De este modo, se aplicarán criterios de tratamiento de la información de acuerdo a los procedimientos que establezca la universidad para actividades como su control de acceso, su almacenamiento, la realización de copias, la utilización de soportes externos de almacenamiento, su transmisión telemática, etc.

En cualquier caso, se deberían considerar una serie de principios básicos relacionados con el tratamiento de la información, como son que las medidas de seguridad aplicadas por la persona usuaria deberían ser proporcionadas, y tener en cuenta, tanto la seguridad del entorno de tratamiento de dicha información (considerando que la universidad siempre será un entorno más confiable que el exterior, donde habrá que ser más estrictos en la aplicación de las medidas de seguridad) como el nivel de confidencialidad de la información, teniendo en cuenta siempre que la información corporativa debería residir en los servicios corporativos, aunque se pueda utilizar temporalmente la información corporativa en local. No obstante, para dicho tratamiento temporal habrá que tener en cuenta las medidas de protección de la información, de los soportes, del puesto de trabajo y/o de los dispositivos móviles contenidas a continuación.

3.1.2 Cifrado

El cifrado de la información es un mecanismo de seguridad potente, pero también es necesario tener en cuenta que es un proceso muy sensible y de alto riesgo, ya que si se perdiese la contraseña o el certificado con el que ha sido cifrada la información fuese revocado, no se podría recuperar nada de la información cifrada. Por lo tanto, el cifrado debería ser un mecanismo de seguridad a utilizar exclusivamente con la información de los niveles de confidencialidad más altos, así como con la información de nivel Alto según la LOPD.

La manera de aplicar el cifrado durante el almacenamiento de la información es diversa, en función del ámbito al que se aplique:

- Cifrando los archivos mediante las herramientas propias de los programas (PDF, Office, etc.), así como carpetas completas mediante herramientas de

cifrado específicas. En el caso de no disponer de las mismas, puede abrir una solicitud en el CAU.

- Cifrando los pen-drives, CDs, DVDs y similares en las que se graban los archivos que contienen información de dicho nivel, mediante herramientas de cifrado específicas. En cualquier caso, siempre se puede optar por cifrar los archivos contenidos en estos medios, en vez de los propios medios. En el caso de no disponer de herramientas de cifrado, puede abrir una solicitud en el CAU.

También se debe considerar la aplicación del cifrado durante la transmisión de la información. Los mecanismos de cifrado también son diversos en función del ámbito de aplicación:

- Cifrando los archivos adjuntos en los correos electrónicos que contienen dicha información, y transfiriendo la información al adjunto si fuese el contenido a cifrar (y comunicando la contraseña de cifrado por un medio alternativo al correo electrónico).
- Utilizando VPNs para acceder desde el exterior de la universidad a sistemas y/o servicios que contienen información que requiere transmisión cifrada.

Así mismo, las personas deberían asegurarse de que los servicios web que contienen la información del nivel de confidencialidad más alto son servicios cifrados, es decir, servicios https. Para ello, la persona usuaria simplemente tendrá que verificar que en la barra de direcciones del navegador aparece un candado.

3.1.3 Firma electrónica

La firma electrónica es una medida de seguridad que se utiliza para garantizar la autenticidad del origen y la integridad de la información.

Los casos de uso más habituales en la universidad serían la firma electrónica de los documentos PDF que lo requieran utilizando el certificado corporativo (integrado en la tarjeta universitaria), así como la firma electrónica de las actuaciones administrativas que lo requieran (tramitación electrónica/registro electrónico), utilizando también en este caso el certificado corporativo.

El uso de la firma electrónica también sirve para verificar la autenticidad del origen y la integridad de la información, verificando que los documentos electrónicos que lo requieran han sido firmados de forma válida, en las propiedades de seguridad del documento PDF.

Un caso específico relacionado con la firma electrónica es la impresión de documentos electrónicos firmados electrónicamente. Es importante tener en cuenta que estos documentos impresos no tienen validez salvo que tenga CSV (Código Seguro de Verificación), que es un código formado por un conjunto de dígitos que identifican de

forma única a un documento electrónico oficial, impreso en todas y cada una de las páginas del documento. Dicho CSV sirve para contrastar la autenticidad e integridad de un documento impreso originalmente electrónico y la validez de la firma, y se lleva a cabo introduciendo dicho código en el apartado correspondiente de la sede electrónica del emisor del documento y verificando que el documento electrónico que se visualiza es el documento que estamos verificando.

3.1.4 Metadatos

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, que 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.

De acuerdo con este planteamiento se debería aplicar un proceso de limpieza de documentos, en el que se retire 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.

3.1.5 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. Sin embargo, son las personas usuarias las que deberían realizar copias de seguridad de aquella información almacenada localmente en sus equipos, ya que esa información no es salvaguardada por la universidad.

Para realizar las copias de seguridad de la información almacenada localmente se deberían utilizar soportes externos (Pen-drive USB, CD, DVD, etc.). Estas copias deberían disfrutar, al menos, del mismo nivel de seguridad que los datos originales.

Para ello, para garantizar la protección de la copia de seguridad (backup), se debería, al menos, comprimir y cifrar dicha información (ZIP). Además, también será necesario que las personas usuarias verifiquen regularmente que dichas copias de seguridad sean recuperables, comprobando que dichos soportes externos y su contenido es legible por un ordenador.

Lo recomendable, como alternativa a las copias de seguridad de la información local, sería optar por trasladar dicha información local a los servicios corporativos de almacenamiento (gorde, gordetalde, EHUDoku, -teniendo en cuenta que tanto gordetalde como EHUDoku son medios compartidos-, etc.).

3.1.6 Eliminación de la información

La información corporativa almacenada en local debería ser considerada de carácter temporal, y por tanto ser eliminada una vez que finalice dicho uso temporal. No obstante, esta información debería ser conservada en los repositorios y/o servicios corporativos antes de su eliminación en local.

Toda la información corporativa almacenada en local debería ser borrada, y además se deberían eliminar de forma segura sus copias en soportes externos, bien destruyendo las copias temporales impresas en papel o bien formateando a bajo nivel (o destruyendo si no es formateable) los soportes en los que haya copias electrónicas, de acuerdo a lo indicado en el apartado correspondiente.

3.2 Protección de los soportes

En este apartado se consideran los soportes electrónicos externos de información, también conocidos como medios 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, cuyas medidas de seguridad se definen en el apartado correspondiente.

Todos los soportes externos de información deberían estar identificados (etiquetados) de forma que se indique el máximo nivel de seguridad de la información contenida, pero sin revelar su contenido. El significado de dicha identificación o etiqueta debería ser interpretable de algún modo por las personas usuarias, aunque dicha interpretación no tendría por qué ser directa mediante simple inspección visual, sino que también podría ser necesaria alguna utilidad o referencia que lo explique.

Las personas usuarias deberían aplicar la debida diligencia y control a los soportes de información que permanezcan bajo su responsabilidad, aplicando al menos las siguientes precauciones:

- Respetar las condiciones del fabricante respecto a temperatura, humedad y otros agresores medioambientales.
- Garantizar que sólo puede acceder físicamente a ellos el personal autorizado.
- Registrar los envíos y/o recepciones de dichos soportes y quién autoriza dicho movimiento.
- Cifrar el contenido de acuerdo a lo indicado en el apartado correspondiente.

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 del soporte) y notificar el correspondiente incidente de seguridad si dicha verificación falla. En este caso, la contraseña de cifrado debería ser comunicada al destinatario del envío por un medio alternativo al del propio envío.

Si se reciben soportes de información, las personas usuarias deberían asegurarse de que la recepción estaba prevista y verificar el origen, adoptando todas las cautelas necesarias en caso contrario. Además deberán registrar la entrada y el transportista que entrega el soporte, cotejar la recepción con el envío asociado y notificar el correspondiente incidente de seguridad si dicho cotejo falla.

Por último, 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.

3.3 Protección del puesto de trabajo

Uno de los principales focos sobre el que aplicar medidas de seguridad es el puesto de trabajo, ya que es tanto el entorno en el que se llevan a cabo la mayoría de las operaciones de tratamiento de la información como el que permite aplicar la mayor cantidad de medidas de seguridad, dada la capacidad que ofrece el ordenador personal para aplicar medidas de seguridad tecnológicas.

3.3.1 Puesto de trabajo

El puesto de trabajo, entendido como el espacio físico de trabajo (mesa y ordenador) debería permanecer despejado, sin más información ni soportes encima de la mesa que los requeridos para la actividad que se está realizando en cada momento, de modo que se minimice el riesgo de que cualquier persona no autorizada pueda acceder a información a la que no debería tener acceso.

Por ello, toda la información reservada (aquella que no sea pública) no debería ser accesible cuando no se esté utilizando. Por lo tanto, la documentación en papel se

debería guardar en lugar cerrado cuando no se esté utilizando, y la pantalla del ordenador no debería mostrar información reservada cuando no esté siendo utilizada.

3.3.2 Ordenador corporativo

Los ordenadores deberían estar operativos en todo momento. Para tratar de mantener esta premisa se intentan minimizar los riesgos de que se puedan producir alteraciones en los ordenadores personales que puedan dañar dicha capacidad.

Por ello, ninguna persona usuaria debería disponer de permisos de administración del equipo, con el fin de evitar que ningún tipo de actuación incorrecta, 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.

Además, es necesario tener en cuenta que el uso del ordenador corporativo, así como de todos los medios electrónicos corporativos ligados a él (correo electrónico, navegación, etc.) deberían ser de uso exclusivamente profesional, y por tanto no se deberían utilizar para fines particulares, ya que esta utilización puede incrementar significativamente el riesgo, puesto que dicho uso sería mucho más incontrolado. Además, es importante tener en cuenta que siempre que se utilizan estos medios electrónicos corporativos el uso que se hace de los mismos está siempre ligado a la identidad de la universidad (se navega desde la universidad, el correo electrónico está asociado al dominio de la universidad, etc.), de modo que cualquier actividad que se lleve a cabo es entendida siempre como una actividad de la universidad.

3.3.3 Identificación de personas usuarias

Cada persona debería estar identificada unívocamente, mediante la correspondiente credencial (también conocido como identificador de persona usuaria), ante los sistemas de información de la universidad, de forma que en todo momento se pueda saber qué persona recibe cada identificador y qué derechos de acceso recibe, y también sea posible saber quién ha hecho algo y qué es lo que ha hecho.

Por este motivo, las credenciales de acceso siempre deben estar bajo el control exclusivo de la persona usuaria y sólo se activarán una vez que lo estén. Ninguna persona debe utilizar nunca las credenciales de acceso de otra (información personal que no se puede transferir ni prestar).

3.3.3.1 Mecanismos de autenticación y control de acceso

Una vez que la persona usuaria haya recibido las credenciales de acceso debe ser consciente de que su tenencia conlleva una serie de responsabilidades:

- 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 de la universidad:

- **Cuenta/Contraseña corporativa**: Es un sistema de autenticación cuya robustez se basa en la fortaleza de la contraseña (en la política de contraseñas aplicada).
- **Tarjeta corporativa + PIN**: Es un sistema de autenticación más robusto, hacia el que la universidad debería ir en un futuro.
- **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.).

Los sistemas de información deberían estar preparados para que durante el proceso de autenticación la información revelada a quien intenta acceder sea la mínima imprescindible, motivo por el cual no se debería indicar nunca si el parámetro incorrecto es el identificador de persona usuaria (cuenta) o la contraseña, de modo que un posible atacante no pueda saber si la cuenta o contraseña que está utilizando es correcta.

Con el fin de evitar ataques de fuerza bruta (introducción repetida de contraseñas diferentes para tratar de dar con la contraseña correcta), el número de intentos permitidos será limitado, bloqueando la oportunidad de acceso una vez efectuados un cierto número de fallos consecutivos.

Además, los sistemas de información mostrarán a la persona usuaria sus obligaciones durante el proceso de acceso y autenticación, con el fin de que sea consciente de las implicaciones de acceder a dichos sistemas.

3.3.3.2 Uso de contraseñas de autenticación

Las contraseñas deberían ser **memorizadas**, no siendo aconsejable registrarlas o apuntarlas en ningún sitio, puesto que este proceder implica un riesgo evidente de que cualquiera que acceda al lugar en el que han sido registradas pueda conocerlas. Si se opta por anotar las contraseñas en un medio electrónico, esta anotación debería estar en un fichero cifrado y, en cualquier caso, almacenadas en un lugar seguro.

La persona usuaria debería **cambiar la contraseña** la primera vez que se conecte, y también siempre que la contraseña haya sido suministrada por un administrador o sistema, con el fin de que sólo la persona usuaria conozca dicha contraseña. Además, la contraseña se debería cambiar ante cualquier sospecha de que otras personas puedan ser conocedoras de la misma.

La contraseña **no se debería comunicar nunca a nadie** (ni siquiera a superiores, compañeros o personal de los servicios informáticos) bajo ninguna circunstancia.

3.3.3.3 Política de contraseñas

Con el fin de que las contraseñas no sean fácilmente adivinables ni puedan ser vulneradas por mecanismos automatizados diseñados a tal efecto se debería seguir la siguiente política de contraseñas:

- **Longitud mínima**:
  - Debería tener una longitud mínima de 8 caracteres.
- **Compleja**:
  - Debería contener caracteres de al menos 3 de los siguientes 4 tipos:
    - Números
    - Mayúsculas
    - Minúsculas
    - Caracteres especiales: * . + $ & # @ - ! % ^ ; ( ) { } [ ] < > ? /_
  - No debería tener caracteres en blanco.
- **No predecible**:
  - No debería estar formada únicamente por palabras de diccionario u otras fácilmente predecibles o asociables a la persona usuaria (nombres, direcciones, matrículas, etc.)
  - Nunca se debería utilizar el identificador de la cuenta de la persona usuaria, el nombre o los apellidos como contraseña o parte de la misma.
- **Renovada frecuentemente**:
  - Las contraseñas se deberían modificar con una periodicidad máxima de seis (6) meses.
  - No se deberían reutilizar las últimas diez (10) contraseñas utilizadas.

3.3.4 Bloqueo del ordenador

El ordenador debería bloquearse al cabo de un tiempo prudencial de inactividad. Este bloqueo debería ser, al menos, automático, tal y como sucede en los equipos corporativos tras un cierto tiempo de inactividad. No obstante, las personas usuarias siempre deberían bloquearlo manualmente cuando van a ausentarse del puesto de trabajo. Este bloqueo manual se puede realizar pulsando las teclas <Windows>+<L> simultáneamente o retirando la tarjeta corporativa, siempre que se haya utilizado para iniciar sesión en un equipo corporativo.

En cualquiera de los casos, la persona usuaria siempre tendrá que autenticarse de nuevo para reanudar la actividad en curso.

En caso de ausencias prolongadas del puesto de trabajo se recomienda apagar el ordenador, ya que una sesión iniciada en el equipo, aunque esté bloqueado, siempre es más vulnerable, ya que puede tener sesiones de actividad iniciadas (navegación, aplicaciones, etc.).

3.3.5 Antivirus

Todos los ordenadores personales deberían disponer de mecanismos de prevención y reacción frente a código dañino (comúnmente conocidos como antivirus). Los equipos corporativos incluyen dicho antivirus, activado por defecto.

Este software anti-malware (antivirus) siempre debería cumplir dos premisas básicas: estar siempre habilitado y disponer de un patrón de firmas de virus actualizado. En caso contrario la persona usuaria no estaría protegida frente a los últimos virus que hayan aparecido.

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.

3.3.6 Firewall del ordenador personal

El ordenador personal también debería disponer de mecanismos de protección frente a ataques de red (conocidos como firewall o cortafuegos). Los equipos corporativos también lo incluyen activado por defecto.

La utilización del firewall debería cumplir dos premisas fundamentales: estar siempre habilitado y que la persona usuaria nunca evada la configuración por defecto. En línea con esta premisa, 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.

3.3.7 Correo electrónico, SPAM y phishing

La Universidad ha establecido una serie de normas básicas de uso del correo electrónico por parte del personal:

https://www.euskadi.eus/r47-bopvapps/es/bopv2/datos/2015/03/1501146a.shtml

No obstante, más allá de las citadas normas se debería prestar atención a algunos aspectos adicionales en materia de seguridad, como son los siguientes:

- El buzón de correo personal proporcionado por la universidad siempre se debería considerar intransferible.
- Se debería 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, siempre se debería 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.

A la hora de enviar un correo electrónico se debería prestar especial atención a los destinatarios, verificando que están correctamente escritos y que son los destinatarios correctos (ya que funciones como la de auto-completar pueden provocar envíos a destinatarios incorrectos y por lo tanto desvelar información a destinatarios no previstos si no se presta la suficiente atención), y al nivel de confidencialidad de la información enviada y, sobre todo, reenviada, ya que el correo puede contener información de un tercero que no debería ser conocida por el destinario final. Además, siempre se debería limitar, en la medida de lo posible, el envío de información de los niveles de confidencialidad más altos por correo electrónico, cifrando dicha información si fuera necesario.

También existen ciertas prácticas que deberían ser evitadas, como son las siguientes:

- Participar en la propagación de cartas encadenadas o participar en esquemas piramidales o temas similares.
- Enviar o contestar mensajes que puedan introducir malware o implicar riesgos o problemas en los sistemas y herramientas informáticas y tecnológicas de la universidad.
- Hacer clic en enlaces sospechosos.
- Ejecutar archivos adjuntos sospechosos.

3.3.8 Uso de servicios web, internet y redes sociales

Existen una serie de recomendaciones y buenas prácticas que se deberían seguir, en la medida de lo posible, en el uso de internet, servicios web y redes sociales, como son las siguientes:

- Comprobar la seguridad y autenticidad de la página visitada (HTTPS).
- Utilizar los niveles de seguridad del navegador.
- Limitar, si es posible, el uso de cookies durante la navegación.
- Eliminar la información privada (historial, cookies, contraseñas, etc.) o navegar en modo InPrivate (Internet Explorer) / Privado (Firefox) / Incognito (Chrome).

- 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.

Además, en el uso de internet, servicios web y redes sociales existen diversas actuaciones que deberían evitarse, como pueden ser:

- 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.
- Publicar cualquier tipo de información perteneciente a la universidad 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 universidad o ajenos a ella.
- Hacer clic en enlaces sospechosos.

En relación específicamente al uso de redes sociales se deberían considerar, de manera adicional, dos criterios generales, como son los de limitar la cantidad de información proporcionada y, sobre todo, "Pensar antes de publicar", ya que la huella digital es prácticamente imposible de eliminar, y cualquier publicación se convierte prácticamente en permanente.

3.4 Protección de los dispositivos móviles

Los dispositivos móviles requieren de la aplicación de medidas de seguridad adicionales, ya que existen determinados riesgos inherentes a dicha movilidad que deben ser tratados expresamente.

3.4.1 Acceso remoto y VPN

Las soluciones VPN (Virtual Private Network) proporcionadas por la universidad aportan confidencialidad (cifrado) e integridad en la comunicación, así como autenticidad de la identidad de la persona usuaria. Dicho servicio se explica en la siguiente URL:

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 debería realizar mediante el uso de las herramientas de

VPN dispuestas por la universidad. Debería estar prohibido, 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 deberían tener que llevar a cabo el mismo proceso de autenticación que el aplicado en la red de la universidad. Por lo tanto, el acceso remoto por VPN no debería suponer la concesión de privilegios de acceso adicionales.

3.4.2 Ordenadores portátiles

La persona responsable de cada equipo portátil debería estar identificada. Estas personas usuarias deberían mantener precauciones específicas frente a las posibilidades de pérdida o robo de estos equipos. En caso de que se produjeran pérdidas o sustracciones de estos equipos se debería informar al CAU y al responsable correspondiente de forma inmediata, ya que pueden contener información sensible (cuyo nivel de confidencialidad sea elevado), 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 ordenador portátil contenga credenciales de acceso remoto a la universidad, entendiendo por 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.

Además, debido a las mayores posibilidades de pérdida o robo de información, se debería prestar especial atención a todas las medidas de seguridad aplicables al ordenador personal, y en particular a las relativas al 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.

3.4.3 Teléfonos móviles

Para el uso seguro de teléfonos móviles, tabletas y dispositivos similares se deberían utilizar todas las medidas de seguridad propias de este tipo de dispositivos, con el fin de proteger adecuadamente la información contenida en ellos (cuyo nivel de confidencialidad pueda ser elevado):

- Control de acceso al dispositivo: PIN, Patrón, Huella o similar, ocultando la visualización del patrón en caso de que se use este método.
- Cifrado

Otra de las recomendaciones de seguridad básicas para el uso de teléfonos móviles y similares es la de limitar el uso de información sensible. Además, habría que aplicar todas las medidas de seguridad definidas para los ordenadores portátiles que fuese posible.

En el caso de los dispositivos móviles corporativos es fundamental notificar su pérdida o robo, así como gestionar su avería o rotura a través del CAU de la Vicegerencia TIC.

En el caso de que se utilice el móvil personal para tareas corporativas (BYOD, Bring Your Own Device) también habría que aplicar las mismas medidas establecidas para los móviles corporativos, y notificar igualmente su pérdida o robo. Sin embargo, en este caso sería conveniente aplicar medidas de seguridad adicionales, como son diferenciar lo personal de lo corporativo, separándolo y aislándolo siempre que sea posible, y evitar compartir información corporativa con servicios de Internet (google, iTunes, etc.).

3.4.4 WiFis públicas o redes de terceros

La única red WiFi que se debería considerar segura es la red WiFi de la universidad (eduroam). Más allá de dicha red, es importante tener siempre en cuenta que las **WiFis públicas** (sin contraseña –abiertas– o aquellas cuya contraseña sea compartida –incluyendo, por tanto, EHU-wGuest–) son un entorno totalmente **inseguro**, ya que cualquiera se puede conectar y por tanto cualquiera puede espiar las conexiones de cualquiera. Por lo tanto, es fundamental tomar precauciones si se utilizan WiFis públicas o redes de terceros.

Las principales precauciones adicionales a adoptar si se usan WiFis públicas o redes de terceros son las siguientes:

- No acceder a información sensible (reservada, privada)
- Utilizar sólo servicios seguros si hay que acceder a información sensible (servicios https y/o VPN para acceder a los servicios de la universidad)
- Evitar que otras personas vean cómo se introducen las contraseñas
- Reforzar la aplicación de las medidas de seguridad de los dispositivos móviles, con especial atención a la renovación frecuente los mecanismos de control de acceso al dispositivo

4 Conclusiones

La seguridad es cuestión de todos. La universidad tiene que garantizar la aplicación de las medidas de seguridad necesarias, pero siempre van a existir medidas de seguridad que dependen de las personas. Además, en seguridad siempre se utiliza el símil de que una cadena es tan fuerte como su eslabón más débil, y si hablamos de seguridad

de la información es necesario reconocer que las personas somos ése eslabón más débil, ya que muchas veces incumplimos las medidas de seguridad definidas, por múltiples motivos (a veces por desconocimiento, otras por imprudencia, muchas por pereza, algunas por inconstancia y otras incluso hasta por desidia).

No podemos olvidar que los problemas de seguridad afectan a todos. Las personas se ven afectadas y comprometidas, la universidad ve dañados sus activos, y las consecuencias las acaba pagando toda la sociedad. Por lo tanto, velar por la seguridad debe ser cosa de todos.

Por todo ello, es importante ser consciente de cuáles son las medidas de seguridad que se deben aplicar, y tener claro que en caso de duda en temas de seguridad el sentido común suele ser una de las principales herramientas para discernir el comportamiento correcto. La máxima “Piensa mal y acertarás” suele ser una herramienta eficaz a la hora de identificar las prácticas de seguridad a seguir y a evitar. En caso de duda siempre se podrá recurrir tanto al CAU como al responsable del área o servicio, pero lo que siempre habrá que tener claro es que, en caso de sospecha de algún tipo de problema de seguridad, lo fundamental será notificarlo, cuando antes y aportando la mayor información posible, tanto al CAU como al responsable.

En definitiva, es necesario recordar siempre lo siguiente: Tanto la seguridad como la buena imagen de la universidad también dependen de ti.