Seminarios Web sobre Seguridad de la Información

eclap

Junta de Castilla y León

Ciberseguridad práctica en la Administración de la Comunidad de Castilla y León

Objetivos

"Introducir a cualquier empleado público en la seguridad de la información, la ciberseguridad y el conocimiento de la Política de Seguridad de la Información y Protección de datos (PSIPD) y la conformidad legal frente al Esquema Nacional de Seguridad"

Índice del seminario

- ¿Qué es la seguridad de la información y por qué es importante? Clasificación de la Información
- Política de Seguridad. Normas y condiciones de uso
- Organización de la Seguridad en la ACCyL
- Responsabilidad del usuario en la protección de activos esenciales
- Identificación de incidentes, actividades o comportamientos sospechosos
- Uso seguro de internet y correo electrónico
- Gestión de información sensible y/o de carácter personal
- Protección de soportes de información
- Protección de dispositivos móviles y su información
- Buenas prácticas en el teletrabajo

¿Qué es la seguridad de la información?

"La Seguridad de la Información son el conjunto de medidas preventivas y reactivas de las organizaciones y los sistemas tecnológicos que permiten resguardar la información buscando mantener la confidencialidad, integridad y disponibilidad de los datos"

No se debe confundir seguridad informática

La seguridad 100% no existe

No es un aspecto dependiente únicamente del área de Informática sino que depende de todos y cada uno de los miembros de la organización

¿Qué es la seguridad de la información?

Junta de Castilla y León

¿Por qué es tan importante la Seguridad de la Información?

Un ciberataque sincronizado afecta al INE y a ministerios como Justicia, Economía o Educación

IMPORTANTE

Debido a un posible ciberataque, se han interrumpido las comunicaciones con red SARA lo cual implicará la suspensión de servicios tales como
Portafirmas, Cl@ve, Geiser y Plataforma de intermediación.

NOTICIAS

Otro ciberataque contra administraciones públicas españolas

Un incendio destruye parte del centro de datos de OVH en Estrasburgo, uno de los servidores más importantes de Europa

TECNOLOGÍA

Un ciberataque tumba los servicios de varios ayuntamientos de España

El servicio en la nube ASAC ha sufrido un ciberataque que ha dejado fuera de juego a ayuntamientos como el de Oviedo y a instituciones como el Tribunal de Cuentas

NOTICIAS

Caída global en el SEPE por un ataque de Ransomware

¿Qué es la seguridad de la información?

¿Por qué es tan importante la Seguridad de la Información?

El Gobierno teme un efecto contagio en la Administración si hay un ciberataque

Crece la preocupación porque se produzca un ciberataque en nuestro país derivado del apoyo de la Unión Europea a Ucrania y que tenga un efecto dominó en la Administración

La administración pública española detuvo más de 10.000 ciberataques a servicios esenciales durante 2021

EL MINISTERIO DEL INTERIOR DEL GOBIERNO DE ESPAÑA HA HECHO PÚBLICO QUE EL PASADO AÑO NEUTRALIZÓ MÁS DE 10.000 CIBERATAQUES A SERVICIOS ESENCIALES GRACIAS A LA INTERVENCIÓN DE DIFERENTES ORGANISMOS DE PROTECCIÓN

Las Administraciones públicas toman medidas contra posibles ciberataques de hackers rusos

Se ha pedido a los funcionarios de la Seguridad Social y el SEPE que estén alerta ante posibles anomalías en sus ordenadores, que los apaguen cuando no trabajen y que vigilen correos y mensajes

¿Qué es la seguridad de la información?

Junta de Castilla y León

¿Cómo podemos clasificar la información?

Por nivel de accesibilidad

Confidencial, restringida, de uso interno, pública…

Por utilidad y funcionalidad

Usuarios, recursos humanos, beneficiarios, empresas, proveedores…

Por el impacto que tendría un robo, borrado o pérdida

Consecuencias legales, económicas, de no continuidad, de la propia imagen…

¿Qué es la seguridad de la información?

¿Cómo podemos clasificar la información?

Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad

Deroga 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

¿Qué es la seguridad de la información?

Junta de Castilla y León

¿Cómo podemos clasificar la información?

Para categorizar el sistema nos basamos en el Anexo I del ENS que nos indica que debemos valorar el impacto que tendría sobre la organización un incidentes si afectase a la seguridad de la información tratada o de los servicios prestados para

- Alcanzar los objetivos
- Proteger los activos a su cargo
- Garantizar la conformidad con el ordenamiento jurídico

¿Cómo hacemos esta valoración?

Confidencialidad ***Integridad*** ***Disponibilidad***

Trazabilidad ***Autenticidad***

¿Qué es la seguridad de la información?

Junta de Castilla y León

¿Cómo podemos clasificar la información?

Básico | **Medio** | **Alto**

BAJO: las consecuencias de un incidentes de seguridad tienen un perjuicio limitado sobre las funciones de la organización, activos o sobre los individuos afectados

Reducción de forma apreciable de la capacidad de la organización para desarrollar funciones y competencias, daño menor en los activos de la organización, incumplimiento formal de una ley o regulación, perjuicio menor a un individuo u otros similares

MEDIO: las consecuencias de un incidentes de seguridad tienen un perjuicio grave sobre las funciones de la organización, activos o sobre los individuos afectados

Reducción de forma significativa de la capacidad de la organización para desarrollar funciones y competencias, daño significativo en los activos de la organización, incumplimiento material de una ley o regulación, perjuicio significativo a un individuo u otros similares

ALTO: las consecuencias de un incidentes de seguridad tienen un perjuicio muy grave sobre las funciones de la organización, activos o sobre los individuos afectados

Anulación efectiva de la capacidad de la organización para desarrollar funciones y competencias, daño muy grave o irreparable en los activos de la organización, incumplimiento grave de una ley o regulación, perjuicio grave a un individuo u otros similares

¿Qué es la seguridad de la información?

Junta de Castilla y León

¿Cómo podemos clasificar la información?

Básico

Medio

Alto

Un sistema tendrá una categorización dependiendo del alcance que tengan alguna de sus dimensiones de seguridad

(en base a Criterios de Clasificación)

Política de Seguridad. Normas y Condiciones de Uso

Junta de Castilla y León

Decreto 22/2021
Política de Seguridad de la Información y Protección de Datos (**PSIPD**)

Boletín Oficial de Castilla y León BOCYL

Núm. 192 Lunes, 4 de octubre de 2021 Pág. 47003

I. COMUNIDAD DE CASTILLA Y LEÓN

A. DISPOSICIONES GENERALES

CONSEJERÍA DE ECONOMÍA Y HACIENDA

DECRETO 22/2021, de 30 de septiembre, por el que se aprueba la política de seguridad de la información y protección de datos de la Administración de la Comunidad de Castilla y León.

La Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, establece, en su artículo 13, el derecho de los ciudadanos a la protección y confidencialidad de sus datos y a la seguridad de los mismos cuando figuren en los ficheros, sistemas y aplicaciones de las Administraciones Públicas.

Política de Seguridad. Normas y Condiciones de Uso

Junta de Castilla y León

¿Por qué se necesitaba una nueva Política?

ENS

Ley 39/2015

Ley 40/2015

GDPR

LOPDGDD

Estrategia de Ciberseguridad Europea

Junta de Castilla y León

Ámbito de Aplicación

De aplicación a **todos los sistemas de información y a todas las actividades de tratamiento de datos personales de los que sean responsables los órganos de la Administración General de la Comunidad de Castilla y León, así como a sus organismos autónomos y entes públicos de derecho privado cuando ejerzan potestades administrativas**, sin perjuicio de que dichos organismos puedan aprobar su propia PSIPD.

La **obligación se extiende a todo el personal** que acceda a los sistemas de información y la información de ACCyL independientemente de la naturaleza de la relación con la Administración.

PSIPD **afectará a toda la información**, con independencia el medio en que sea tratada y de su soporte.

Debe ser conocida por todo el personal y afecta a toda la información independientemente del soporte.

Junta de Castilla y León

Principios Fundamentales de la PSIPD

Principio de alcance estratégico

Principio de seguridad integral

Principio del ciclo completo y seguridad por defecto

Principio de gestión de riesgos

Principio de proporcionalidad

Principio de responsabilidad diferenciada

Principio de responsabilidad proactiva

Principio de legitimación en el tratamiento de datos personales

Principio de licitud, lealtad y transparencia

Principio de limitación de la finalidad

Principio de minimización de datos

Principios de integridad y calidad

Principio de limitación del plazo de conservación

Principio de confidencialidad

Principio de profesionalidad

Principio de prevención, disponibilidad y recuperación

Principio de revisión periódica: las medidas de seguridad

Principio de exactitud

Junta de Castilla y León

Ámbito de Aplicación

De aplicación a **todos los sistemas de información y a todas las actividades de tratamiento de datos personales de los que sean responsables los órganos de la Administración General de la Comunidad de Castilla y León, así como a sus organismos autónomos y entes públicos de derecho privado cuando ejerzan potestades administrativas**, sin perjuicio de que dichos organismos puedan aprobar su propia PSIPD.

La **obligación se extiende a todo el personal** que acceda a los sistemas de información y la información de ACCyL independientemente de la naturaleza de la relación con la Administración.

PSIPD afectará a toda la información, con independencia el medio en que sea tratada y de su soporte.

Debe ser conocida por todo el personal y afecta a toda la información independientemente del soporte.

Política de Seguridad. Normas y Condiciones de Uso

Junta de Castilla y León

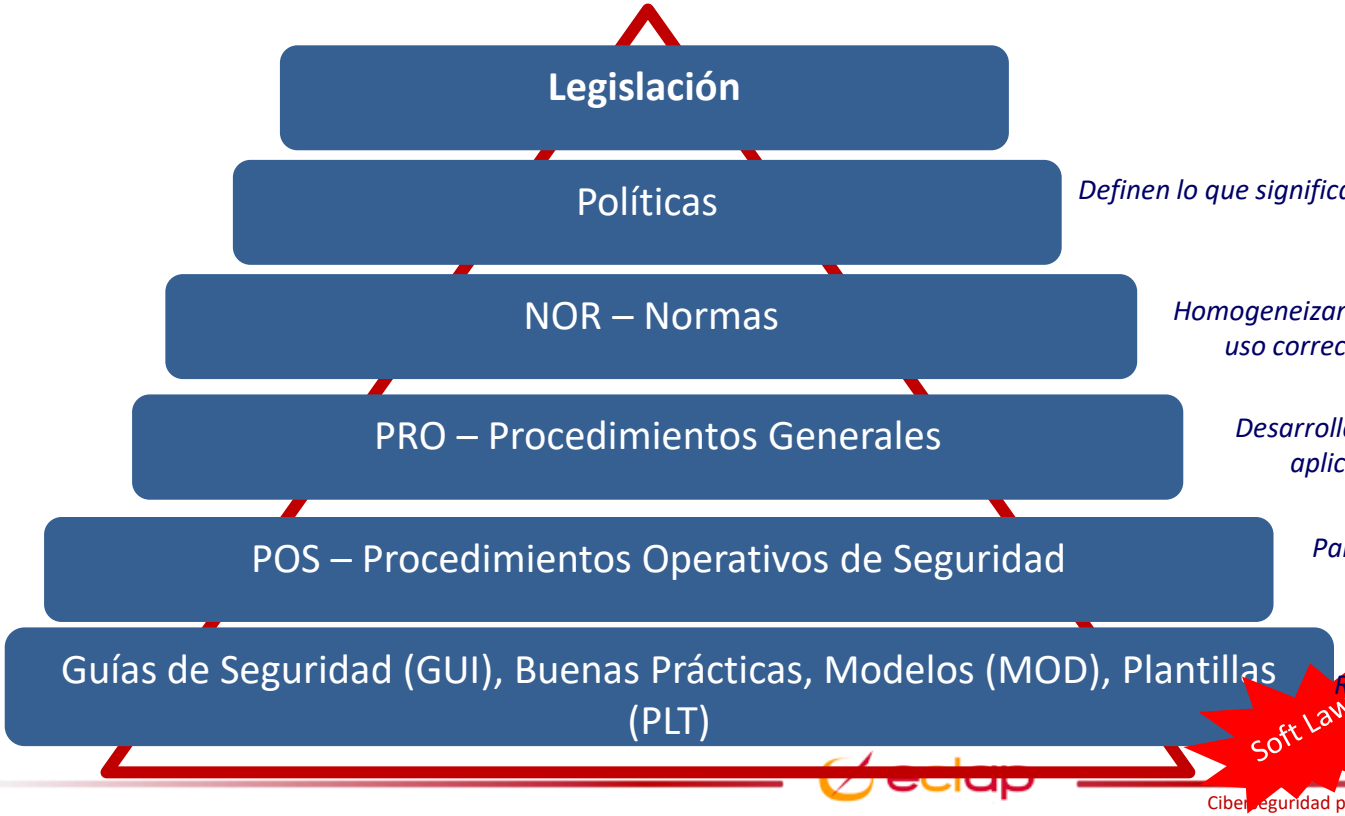
Directrices de la PSIPD

- Líneas de Defensa
- Seguridad Física
- Controles de Acceso
- Gestión de Activos de la Información
- Registro de Actividad
- Seguridad Ligada a Personas
- Gestión de Incidentes de Seguridad
- Protección de comunicaciones
- Especificaciones de seguridad
- Adquisición de productos de seguridad tecnologías de la información y comunicaciones

Política de Seguridad. Normas y Condiciones de Uso

Junta de Castilla y León

Desarrollo de la PSIPD



Definen lo que significa la Seguridad de la Información en una organización

Homogeneizan el uso de aspectos concretos, indican el uso correcto y responsabilidades. Obligatorias

Desarrollan las Normas en aspectos que sean de aplicación transversal y sea obligatorio

Para tareas concretas indicando qué hacer en cada caso paso a paso (día a día)

Recomendaciones pero que pueden tener responsabilidades

Política de Seguridad. Normas y Condiciones de Uso

Junta de Castilla y León

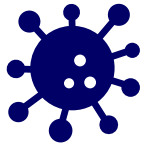
Desarrollo de la PSIPD

	Antiguo	Hasta Ahora	Nueva Estructura
Políticas		POL	POL
Normas	N	NORM	NOR
Procedimientos Generales	P	PROC	PRO
Procedimientos Operativos	T	INST	POS
Guías y otros	G	GUÍA-MODE-PLAN	GUI-MOD-PLT

Política de Seguridad. Normas y Condiciones de Uso

Junta de Castilla y León

Desarrollo de la PSIPD



Gestión de riesgos

Uso de medios digitales

Auditoría de seguridad

Notificaciones de violaciones de seguridad de los datos personales

Registro de actividades de tratamiento

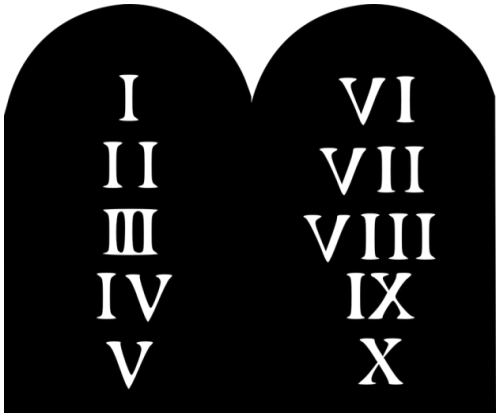
Formación y concienciación

Obligaciones del Personal

Obligaciones del Personal

El personal de la Administración de la Comunidad que tenga acceso a datos personales deberá colaborar en la implementación de la PSIPD y cumplir lo previsto en los instrumentos que la desarrollan.

Los empleados públicos cumplirán asimismo las obligaciones establecidas en la normativa de protección de datos personales y en particular las siguientes:



Política de Seguridad. Normas y Condiciones de Uso

Junta de Castilla y León

Obligaciones del Personal

Sólo accederemos a los datos personales cuando tengamos autorización y a la información que necesitamos para llevar a cabo nuestras tareas asignadas

Guardaremos deber de confidencialidad con la información que tratamos

No divulgaremos las contraseñas de acceso a los sistemas y aplicaciones informáticas que contengan datos de carácter personal

Custodiaremos con diligencia los documentos en soporte papel con datos personales e información confidencial

Solicitar las autorizaciones necesarias para grabar en dispositivos portátiles o tratar fuera de las dependencias administrativas los datos personales

No utilizar con fines diferentes a los propios del servicio los medios digitales puestos a su disposición

Organización de la Seguridad en la ACCyL

"¿Y cómo organizamos y gestionamos la Seguridad de la Información en la ACCyL?"

Organización de la Seguridad en la ACCyL

El Marco Organizativo del PSIPD estará constituido por:

- La consejería competente en materia de **seguridad de la información**, a través del centro directivo que tenga atribuida dicha materia (*Movilidad y Transformación Digital*)

  A través del centro directivo (*DG de Telecomunicaciones y Administración Digital*) que tendrá atribuida esta materia, llevará a cabo el ejercicio de facultades relativas a la seguridad de la información y de los datos personales que le atribuye la normativa.

- La consejería competente en materia de coordinación y seguimiento del cumplimiento de la normativa de **protección de datos personales**, a través del centro directivo que tenga atribuida dicha materia. (*Consejería de Presidencia*).

  A través del centro directivo que tendrá atribuida esta materia, llevará a cabo el ejercicio de facultades relativas a la seguridad de la información y de los datos personales que le atribuye la normativa.

- El **Comité de Seguridad de la Información (CSI)**. Órgano colegiado de impulso, seguimiento y coordinación interna en materia de seguridad de la información en el ámbito de la ACCyL. ***Promoverá la divulgación del PSIPD, velará por la disponibilidad de recursos necesarios, coordinará la seguridad de la información, coordina a los responsables y coopera con otras AAPPs***

Organización de la Seguridad en la ACCyL

El Marco Organizativo del PSIPD estará constituido por:

- Los **Responsables de la Información y tratamiento de datos personales**: persona titular de cada centro directivo de las diferentes consejerías, organismos autónomos o entes públicos de derecho privado serán los responsables de la información en el ámbito de sus competencias y responsables de tratamiento de datos personales (RGPD). ***Directores Generales. Velar por una adecuada gestión de la seguridad de la información, decidir sobre finalidad, uso y contenido de información, determinar niveles y medidas de seguridad aplicables, aprobar medidas técnicas y organizativas, responsabilidades de protección de datos (RAT, Encargados de Tratamiento…)***

- Los **Responsables del Servicio**: persona titular del servicio o unidad administrativa equivalente que gestione cada procedimiento o situación administrativa y en cuyo ámbito se lleve a cabo el tratamiento de la información. ***Jefes de Servicio. Determinar las características y requisitos de seguridad de los servicios en su ámbito de aplicación y mediante valoración de los servicios en la categorización.***

- Los **Responsables de la Seguridad**: titular de la secretaría general de cada consejería o de los órganos equivalentes de cada organismo autónomo o ente público de derecho privado. Debe ser siempre independiente del Responsable de Sistema. ***Promover la seguridad de la información manejada, adoptar medidas necesarias determinadas por Responsables de Información y Servicios, impulsar Normas de Seguridad de la Información, Aprobar Declaración de Aplicabilidad, determinar criterios de acceso y comunicar violaciones de seguridad, adoptar medidas de mejora, promover auditorías periódicas, validar procedimientos operativos de seguridad…***

Organización de la Seguridad en la ACCyL

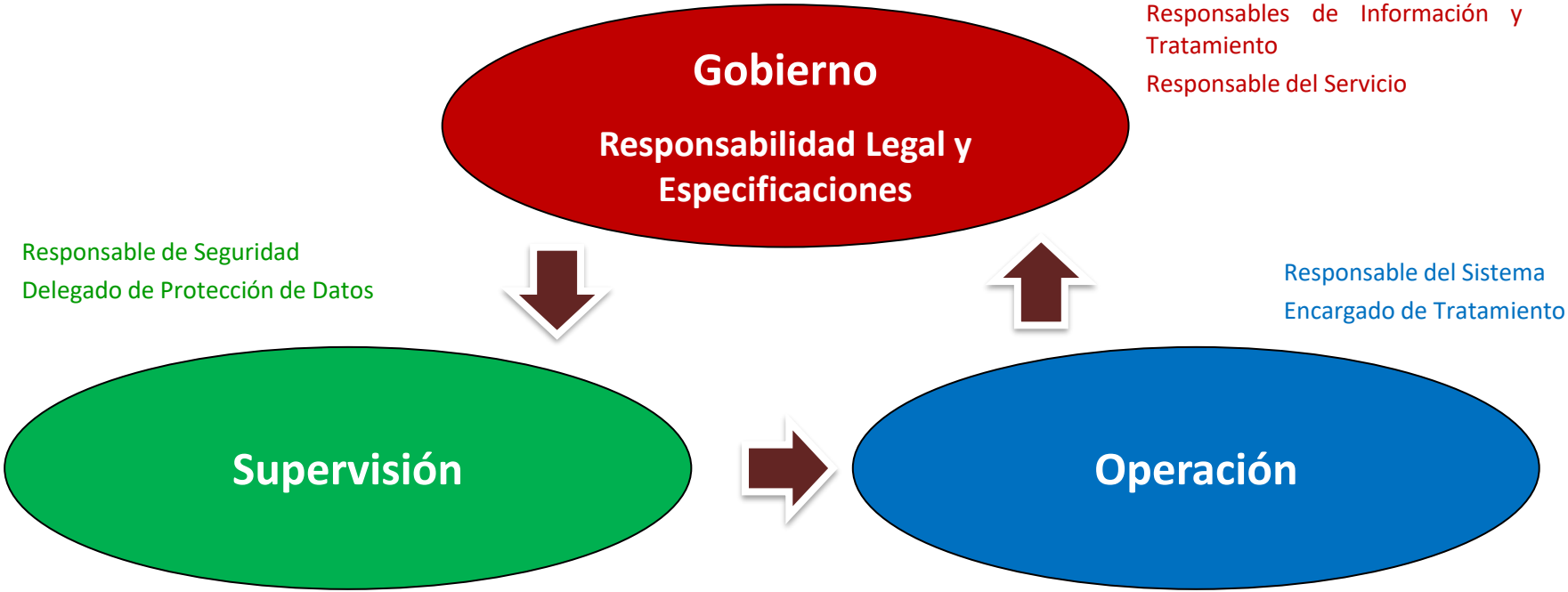
El Marco Organizativo del PSIPD estará constituido por:

- Los **Responsables del Sistema**: en cada consejería, organismo autónomo o ente público de derecho privado habrá un responsable de sistema que será la persona titular del servicio o unidad administrativa equivalente con competencias en materia de informática. *Jefe de Informática en redes, Jefe de Informática Corporativo y Jefe del Servicio de Informática de cada Consejería.* ***Implementación, gestión y mantenimiento de medidas de seguridad en los sistemas de información, informar sobre anomalías en Normas y Procedimientos, notificar incidentes de seguridad, monitorizar el estado de seguridad del sistema y proponer suspensión de tratamiento de información o prestación de servicio.***

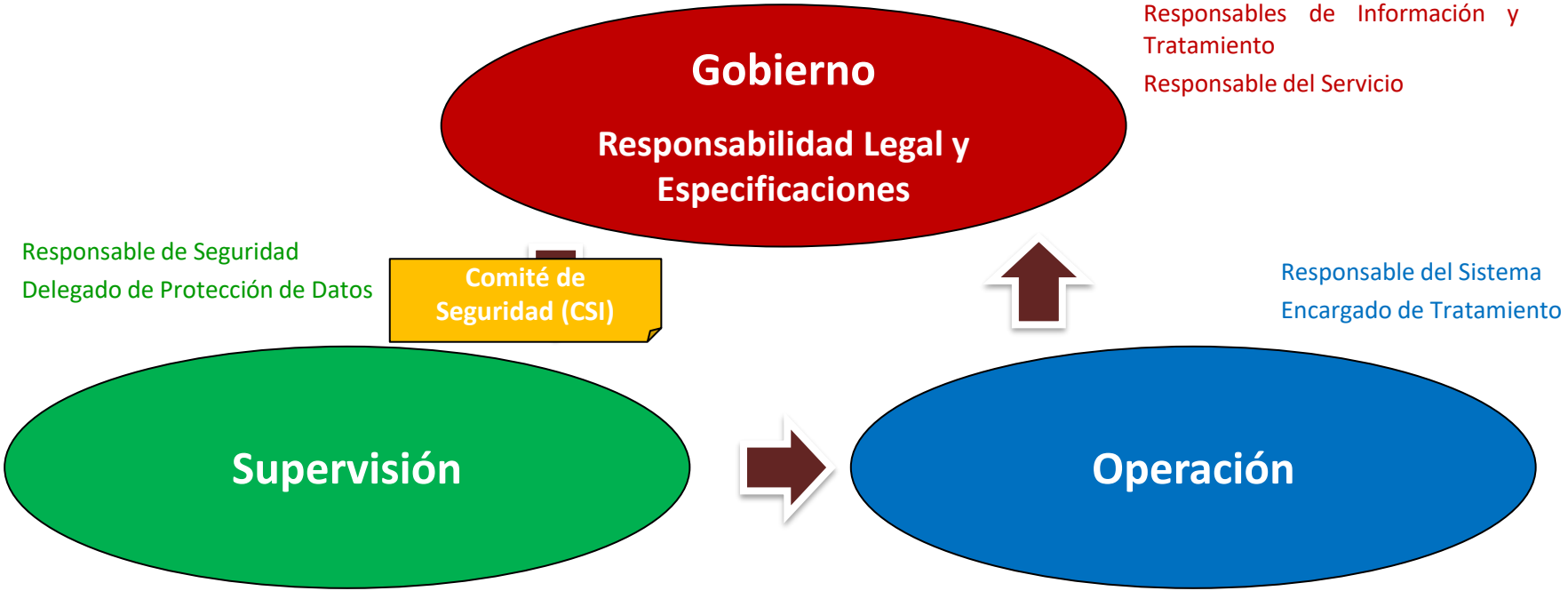
- Los **Delegados de Protección de Datos (DPO).** Debe existir un DPO en cada Consejería así como en los organismos autónomos y entes públicos de derecho privado. Puede nombrarse un DPO para cada consejería y para todas o alguna de las entidades institucionales que dependan o estén vinculadas a ella.

¿Y cómo se organizan todos estos Responsables?

Organización de la Seguridad en la ACCyL



Organización de la Seguridad en la ACCyL



Responsabilidad del usuario en la protección de activos esenciales

Junta de Castilla y León

*"**La seguridad de la información en una organización es cosa de todos** los miembros de una organización, por eso en la ACCyL se ha definido una Norma que marca las condiciones de uso de los sistemas de la información"*

Responsabilidad del usuario en la protección de activos esenciales

Junta de Castilla y León

NOR-1110 Condiciones de Uso

Orden FYM/337/2022 publicada el 20 de Abril sustituye a Orden FYM/643/2016

Es la Norma de Seguridad que describe las condiciones de uso de los sistemas de información del la ACCyL de acuerdo a lo recogido en el ENS.

Objetivo

Establecer el uso correcto de los sistemas de información, servicios e instalaciones, lo que considera uso indebido y la responsabilidad del personal respecto al cumplimiento de esta norma.

Usuario es todo el personal que, de forma permanente o eventual, preste sus servicios en ACCyL incluyéndose proveedores externos cuando sean usuarios de los sistemas de información. En el caso de estos usuarios en los pliegos de los contratos deberán contemplarse la obligación de aceptar la Norma de Condiciones de Uso.

Responsabilidad del usuario en la protección de activos esenciales

NOR-1110 Condiciones de Uso

Principios Generales

ACCyL proporcionará a los usuarios **los recursos informáticos y servicios de comunicaciones necesarios** adecuados para la realización de tareas asignadas.

Uso profesional y prohibición de usos personales o privados.

Prohibición de actividades que pretenden **comprometer, evitar o dificultar las actuaciones de protección de los sistemas de información**

Uso eficiente y seguro de los sistemas de información prohibiéndose actividades que comprometan rendimiento y seguridad

A la **finalización de la relación el usuario** devolverá todos los recursos informáticos y comunicaciones y se eliminarán las cuentas y accesos asignados.

Responsabilidad del usuario en la protección de activos esenciales

NOR-1110 Condiciones de Uso

Confidencialidad de la Información

Acceso a información necesaria para el **desempeño de las funciones** del usuarios y con autorización.

Uso de información sólo para el **cumplimiento de funciones encomendadas** garantizándose privacidad y confidencialidad. Se mantendrá aún finalizada la relación con ACCyL.

Evitar almacenar información sensible o confidencial en medios desatendidos o dejar visible y accesible esta información sin atención.

Cumplimiento de normativa de protección de datos personales.

NOR-1110 Condiciones de Uso

Incidentes de Seguridad

Cuando un usuario detecte cualquier anomalía o incidente de seguridad que pueda comprometer el buen uso y funcionamiento de los sistemas de información de la ACCyL deberá informar inmediatamente por los cauces establecidos a su **Centro de Atención a Usuarios** o a los centros de servicios especializados que se habiliten.

Los **incidentes de seguridad que afecten a datos de carácter personal** serán comunicados, por el Responsable del Tratamiento, a la Agencia Española de Protección de Datos, siempre que dichos incidentes puedan causar daños o perjuicios a las personas. Si además estos daños son graves, la brecha o incidente de seguridad deberá ser comunicada asimismo al interesado.

Junta de Castilla y León

NOR-1110 Condiciones de Uso

Uso de Recursos Informáticos y de comunicaciones

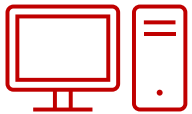
Responsabilidad de custodia por parte del usuario de los recursos informáticos y las comunicaciones. El uso será eficiente y los usuarios deberán:

- Mantener **puesto de trabajo despejado**
- Activar el **salvapantallas** si está disponible
- **Bloqueo de sesión de usuario** en el dispositivo o apagado del dispositivo en ausencias prolongadas
- **Verificar la ausencia de virus** en ficheros en soportes extraíbles autorizados y adjuntos de mails
- **Evitar almacenamiento de información relevante en disco local**. Uso de redes de trabajo compartido
- **Intercambio de ficheros de trabajo** a través de unidades de red adecuadas siempre que sea posible
- Uso de **impresoras de red y fotocopiadora**s compartidas asegurando la documentación enviada al dispositivo y permaneciendo el menor tiempo posible en estas.
- El **uso de dispositivos particulares** está condicionado a la autorización de ACCyL.
- Los **ceses de usuarios o cambio de funciones** deberán ser comunicados inmediatamente por Jefe de Unidad a través del CAU.

Responsabilidad del usuario en la protección de activos esenciales

Junta de Castilla y León

NOR-1110 Condiciones de Uso



Instalación y configuración de recursos informáticos y comunicaciones

Las unidades competentes serán las que definirán la configuración de los diferentes recursos informáticos y de comunicaciones, la utilización de periféricos así como la instalación de software de equipos que se conecten a redes internas.

Los **usuarios no dispondrán de permisos de administración** de equipos salvo la autorización de las unidades.

Sólo el personal autorizado puede instalar o desinstalar software y hardware. Prohibido alterar componentes lógicos y físicos de los recursos informáticos y de comunicación.

Se prohíbe el uso de aplicaciones o herramientas para la descarga o intercambio de archivos salvo los autorizados por JCYL.

Responsabilidad del usuario en la protección de activos esenciales

Junta de Castilla y León

NOR-1110 Condiciones de Uso

Dispositivos móviles

Usuario adoptará medidas para **evitar la pérdida, robo o uso inadecuado**.

En caso de **extravío o robo del dispositivo, de funcionamiento anómalo o de incidente** que pueda afectar a la seguridad de la información se informará inmediatamente al CAU.

El dispositivo móvil **se devolverá** cuando se modifiquen las circunstancias profesionales que originaron su asignación.

Autenticación y Acceso

Por regla general cada usuario tendrá **una única cuenta, personal e intransferible con identificador + contraseña**. Sólo usuarios con privilegios especiales podrán tener más de una cuenta con perfiles diferentes

Los usuarios deben **custodiar convenientemente sus credenciales y está prohibido el uso de credenciales ajenas**, cesión de propias o mecanismos cuyo objeto sea suplantar la identidad. No puede utilizarse credenciales para registrarse en servicios no relacionados con las funciones del puesto de trabajo

Responsabilidad del usuario en la protección de activos esenciales

Junta de Castilla y León

NOR-1110 Condiciones de Uso

Acceso a terceras personas

Personal ajeno de ACCyL **accederá sólo con autorización previa** del Responsable del Sistema de Información.

Deberán **cumplir esta Norma de Condiciones de Uso** y resto de normativa y procedimientos de seguridad.

Acceso remoto

Previamente autorizado en función de las necesidades del usuario y teniendo en cuenta:

- Utilización de **conexiones de red de confianza** evitando redes abiertas
- **Vigilancia de equipos** para evitar accesos no deseados o robos
- Limitación de uso del acceso remoto al **mínimo privilegio imprescindible**. En caso de ausencia bloqueo de puesto o fin de acceso remoto.
- Se mantendrá el **equipo actualizado**

Responsabilidad del usuario en la protección de activos esenciales

Junta de Castilla y León

NOR-1110 Condiciones de Uso

Salidas de Información

Prohibida la salida al exterior de información que no esté categorizada como pública en cualquier soporte no autorizado por Responsable de Información.

Cifrado en los casos que el nivel lo requiera o adopción de otras medidas de seguridad.

No autorizado el uso de USB, CD/DVD… Si se dispone de autorización el usuario es responsable de su salvaguarda. La pérdida con información pública no será notificada como incidencia.

Los **soportes que vayan a ser reutilizados o causen baja** deberán ser previamente tratados para eliminar la información que puedan contener.

No se considera salida de información al exterior el almacenamiento cloud autorizado por ACCyL y esté gestionado por las unidades competentes para la prestación de servicios corporativos de informática y comunicaciones.

Junta de Castilla y León

NOR-1110 Condiciones de Uso

Acceso a internet y herramientas de colaboración

Autorización previa y sólo a través de medios y comunicaciones puestos a disposición por ACCyL. Se podrá restringir el acceso a determinadas páginas web.

Se podrán asignar **perfiles de acceso y restringir acceso** a algunas páginas web.

Sólo acceso a internet mediante **navegadores autorizados y configurados por ACCyL** en los puestos de usuario.

Prohibido el acceso a conexiones de internet con **contenidos ilegales, ofensivos o atentatorios** contra la dignidad humana así como a aquellos que puedan comprometer la seguridad.

Prohibido la descarga o compartición de contenidos que vulneren la legislación.

El **uso de cualquier dispositivo de comunicaciones con el acceso alternativo a internet** contará con previa asignación y autorización.

Junta de Castilla y León

NOR-1110 Condiciones de Uso

Uso de correo corporativo

Las unidades competentes para la prestación de servicios corporativos de informática y comunicaciones suministrarán a cada usuario una **dirección de correo individual asociada a la cuenta de usuario**.

Cada usuario es **responsable de sus correo electrónico y las actividades realizadas** con el mismo.

Sólo podrán utilizarse **clientes de correo electrónico autorizados por ACCyL**.

Se debe **evitar el envío de correos con adjuntos de gran tamaño o el envío de correos masivos así como el uso abusivo** (correo ofensivo, cadenas de correos…)

Prohibido el envío de correos con información sensible o confidencial sin proteger.

Prohibido el reenvío automático de correo corporativo a cuentas externas así como leer, interceptar, borrar, enviar, copiar… el contenido de los correos de otros usuarios.

Responsabilidad del usuario en la protección de activos esenciales

Junta de Castilla y León

NOR-1110 Condiciones de Uso

Monitorización

Por razones de seguridad y operatividad habrá posibilidad de **monitorización, registro y análisis que permitan detectar incidencias** que puedan suponer un problema para el funcionamiento de los servicios o poner en riesgo la seguridad y protección de la información.

Formación y concienciación

Se deberá asistir a los **cursos de formación en materia de seguridad** que se consideren necesarios en función de recursos informáticos y comunicaciones puestos a su disposición.

Responsabilidades y Medidas cautelares extraordinarias

Las responsabilidad de incumplimiento así como cualquier actuación irregular, ilícita o ilegal detectada por ACCyL será exigida de acuerdo con lo previsto en el **régimen disciplinario** de los empleados públicos o de conformidad con lo previsto en materia de ordenamiento civil y penal.
Si el incumplimiento supone un **riesgo manifiesto y grave para la seguridad y eficiencia** de los sistemas de información de la ACCyL así como para la confidencialidad, integridad y disponibilidad de la información se podrán adoptar medidas cautelares adecuadas.

Junta de Castilla y León

¿Qué es un incidente de seguridad?

"Un incidente de seguridad en un sistema de información es cualquier situación o eventualidad en la que pueda verse amenazada la información y pueda, en consecuencia, dar lugar a una degradación o pérdida de su confidencialidad, integridad, disponibilidad, autenticidad o trazabilidad"

Identificación de incidentes, actividades o comportamientos sospechosos

¿Qué NO es un incidente de seguridad?

Medidas de mitigación sin necesidad de notificar incidente de seguridad	
Se recibe un correo marcado como [SPAM] o [POSIBLE SPAM], redactado con una gramática muy burda, en un idioma extranjero, al que no se contesta, ni se pincha en ningún enlace.	Eliminar y bloquear remitente.
Se reciben correos sospechosos de un remitente conocido.	Informar a remitente de los mismos
Se ha perdido o destruido un dispositivo cifrado con datos de los que hay copia.	Informar responsable de tratamiento. Restaurar la información de la copia de seguridad.
El antivirus indica que ha realizado una serie de tareas que no requieren atención.	Reiniciar equipo si se indica.
Fallo en una aplicación	Generar petición de aplicación, no de seguridad

¿Qué SÍ es un incidente de seguridad?

Incidente	Resolución	Categoría petición Seguridad
Correo basura, spam	Eliminar y opcionalmente bloquear remitente. Si se ha respondido adjuntando datos o se ha accedido a un enlace o fichero adjunto, generar petición.	Correo spam o publicitario
Correo suplantación, phishing	Eliminar y opcionalmente bloquear remitente. Si se ha respondido adjuntando datos o se ha accedido a un enlace o fichero adjunto, generar petición.	Correos sospechosos o sondeo de información. Phishing
Nuestros contactos nos informan de envíos propios de correos sin ser conscientes de los mismos	Notificar a remitente de la situación y de la precaución en dichos correos. Generar petición.	Código dañino o malicioso, malware
Visualización del propio correo en lista pública externa ACCyL	Eliminar el correo corporativo del servicio ajeno no laboral con brecha de seguridad. Generar petición.	Política de seguridad. Incumplimiento de normativa.
El dispositivo de puesto de usuario se comporta de forma errática Aparecen elementos que no se han instalado de forma consciente	Generar petición.	Código dañino o malicioso, malware.
Se cifran archivos y documentos en el equipo o unidad de red	Desconectar cable de red del equipo, y desactivar red inalámbrica en su caso. Generar petición.	Código dañino o malicioso, malware.
Pérdida o robo de dispositivo no cifrado con datos personales o confidenciales Fuga o brecha de datos personales en un sistema de la ACCyL	Notificar al responsable del tratamiento y al Delegado de Protección de Datos. Generar petición.	Compromiso de información. Acceso no autorizado o fuga de información. Mal uso de sistemas de información
Préstamo entre empleados o uso de credenciales ajenas	Modificar clave, no prestar ni usar cuenta de terceros. Generar petición	Suplantación identidad. Intento de fraude o uso de recursos no autorizados.
Imposibilidad de actualización de antimalware, antivirus	Reiniciar equipo. Si no se actualiza, generar petición.	Antivirus o sistema no actualizado, vulnerable.

Junta de Castilla y León

¿Cómo se detectan los incidentes?

Automatizadamente

A través de herramientas o recursos informáticos como Servicios de Alerta Temprana (sondas SAT-SARA, SAT-INET, SAT-ICS).

Notificación de Usuarios

Como usuarios podemos detectar incidentes que pueden estar ocurriendo y puede haber diferentes aspectos que nos hagan detectar estos incidentes:

- **Pérdida o robo** de un dispositivo no cifrado con datos personales
- **Notificación de terceros** (compañeros, usuarios, proveedores…) de que han recibido algún mail no enviado por nosotros.
- **Correos sospechosos** solicitando información a los que se ha respondido o se ha introducido información (phishing)

Junta de Castilla y León

¿Cómo se detectan los incidentes?

Notificación de Usuarios

- **Comportamientos erráticos del equipo** como
  - Aparición de mensajes, pop-ups, mucha publicidad, barras de tareas o extensiones en navegador
  - Falsos antivirus, falsas aplicaciones de soportes técnicos
  - Bloqueo o reinicio del equipo o comportamientos no habituales
  - Lentitud del ordenador. tarda mucho en arrancar o el disco duro trabaja sin cesar
  - Aplicaciones que no funcionan o ejecución de otras sin permisos
  - Demasiado correo basura
  - Desaparición de archivos

- Se **cifran archivos y documentos**. Probablemente sea un ramsonware por lo que deberemos
  - Desconectar inmediatamente el cable de red y desactivar la red inalámbrica
  - Generar petición en ASISTA3

- Adware / Spyware
- Troyanos
- Botnet
- Gusanos
- Minería o criptominado
- Ramsonware

Identificación de incidentes, actividades o comportamientos sospechosos

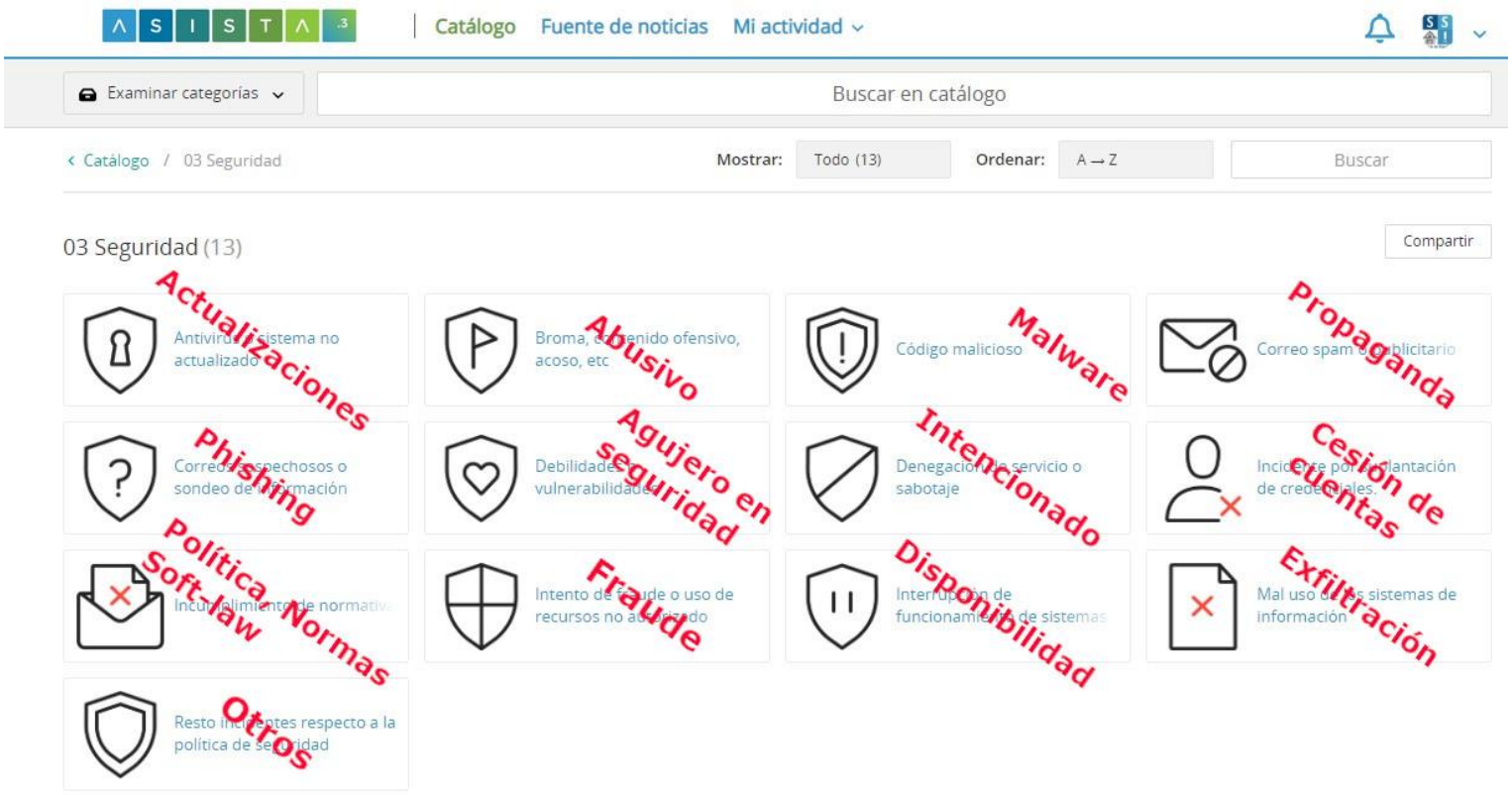
¿Y si detecto estos síntomas?

¿Cómo debo actuar?

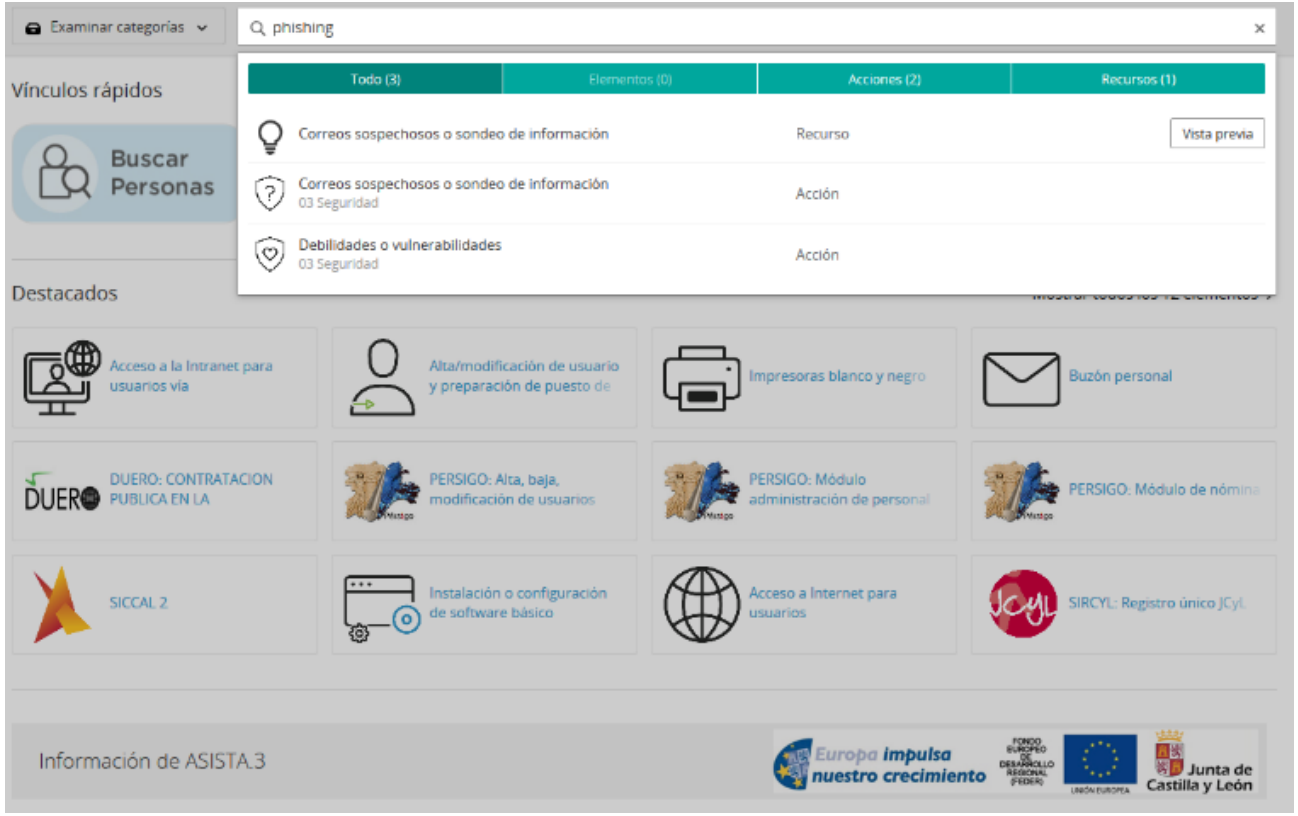
¿A quién se lo notifico y por qué medios

- **Entorno web ASISTA.3**. En primer lugar, se podrá comunicar mediante el enlace a **ASISTA.3** https://asista.jcyl.es/ durante las 24 horas del día. Seleccionar la categoría **SEGURIDAD**.
- **Asistencia telefónica**: 6116 (interno) y 983 41 94 80 (público y externo). Se presta atención continua durante la jornada de trabajo: de lunes a jueves de 8:00 a 19:00, viernes de 8:00 a 15:00.
- **Usuarios externos**: forma de contacto a través del **012**
- **Interfaz técnico web**: Se trata de una sección sólo para técnicos.

Identificación de incidentes, actividades o comportamientos sospechosos

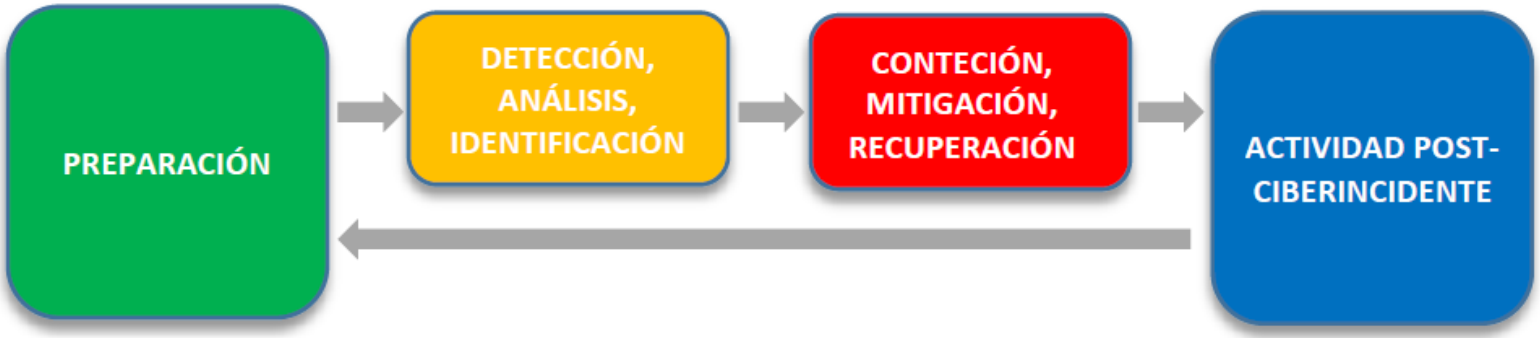


Identificación de incidentes, actividades o comportamientos sospechosos



Junta de Castilla y León

¿Y cómo se responde ante ciberincidentes?



Ciclo de vida de la Respuesta a Ciberincidentes

Junta de Castilla y León

Consejos para prevenir brechas de seguridad y fugas de datos

- Las **credenciales corporativas no se usarán en otros servicios no laborales** y finalizaremos sesión al acabar.
- **Contraseñas diferentes** en diferentes sitios o servicios
- Uso de **VPN** en dispositivos portátiles.
- Habilita doble factor de autenticación (**2FA**) si se permite
- **Elimina regularmente la información obsoleta** si no se debe conservar. Comprueba periódicamente unidades locales y de red.
- **No uses la dirección de ACCyL como correo alternativo** a otros servicios no laborales.
- Se **monitorizan listas públicas de internet desde ACCyL** con el fin conocer que direcciones corporativas pueden tener más afectación posterior de spam o phising

Uso seguro de internet y del correo electrónico

Internet

Correo Electrónico

Junta de Castilla y León

Normas de uso del correo electrónico

Correo Electrónico

- Se deberán utilizar los **clientes de correo autoriza**dos y junto a los mensajes pueden transmitirse ficheros adjuntos a excepción de ejecutables y ficheros de código y scripts.
- Las **direcciones de correo de ACCyL son de ámbito labor**al y para uso profesional únicamente.
- La **cuenta de correo identificativa es individual y el usuario es responsable de las actividades realizadas**. El acceso externo mediante dispositivo móvil deberá ser autorizado.
- Correos colaborativos tendrán protección adecuada y sus miembros estarán identificados.
- Se deberá tener una protección y **credenciales suficientemente seguras y robustas.**
- Se permite recepción y envío de información sensible o confidencial con mecanismos de protección adecuadas (**cifrado**)
- **Evitar almacenamiento excesivo de correos** y cumplimiento de periodos de retención

Junta de Castilla y León

Normas de uso del correo electrónico

Correo Electrónico

➢ Cuando envío un Correo Electrónico

Antes de enviar un correo electrónico, **verifica los destinatarios** para comprobar que son los adecuados y mantén ocultas (CCO) aquellas direcciones que no implicadas directamente

➢ Cuando recibo un Correo Electrónico

Si recibes un mail, asegúrate de la **identidad del remitente** antes de abrir el mensaje

Elimina sin responder los correos spam, suplantación de identidad, sospechosos e ignora enlaces fuera de lo habitual o adjuntos sospechosos

➢ La **configuración del correo electrónico** se hará siempre primando seguridad y protección en la apertura

Junta de Castilla y León

Normas de uso del correo electrónico

Correo Electrónico

➢ Usos Prohibidos

Suscripción y comunicación de correo electrónico corporativo a **servicios no relacionados con la actividad profesional**

Prohibido redirigir cuentas corporativas de correo a correos externos de ACCyL salvo por autorización expresa

Queda **prohibido interceptar, leer, borrar, enviar, copiar o modificar el contenido de los mensajes** de correo electrónico de otros usuarios. Se prohíbe en especial la suplantación de identidad tanto en el envío como en la gestión de mensajes de correo electrónico.

Prohibida la conexión a servidores de correo no corporativos

Prohibida la utilización de herramientas o sistemas que intenten ocultar la identidad del emisor

Prohibido el uso abusivo de correo electrónico, envíos masivos, exceso de adjuntos, envío de malware, contenidos ofensivos o propagación de cadenas de correos.

Junta de Castilla y León

Cuidado con la Ingeniería Social

Correo Electrónico

¿Qué es el la Ingeniería Social?

Conjunto de técnicas que usan los cibercriminales para engañar a los usuarios incautos para que les envíen datos confidenciales, infecten sus computadoras con malware o abran enlaces a sitios infectados.

Este tipo de engaños pueden venir por **diferentes medios** como el correo electrónico, páginas web de internet, redes sociales, SMS, llamadas falsas…

La ingeniería social busca **engañar al usuario** de forma que una vez consigue la confianza del usuario lo manipula para que revele la información que necesita, instale un determinado software…

Existen diferentes ataques de ingeniería social que debemos conocer para poder prevenirlos. La mejor defensa ante los ataques de ingeniería social es el **conocimiento y la educación para poder identificar estos ataques** o sospechar ante cierta información recibida.

Junta de Castilla y León

Cuidado con la Ingeniería Social

Correo Electrónico

- *Phishing* 
- *Spear Phishing* 
- *Smishing* 
- *Falso Soporte Técnico* 

Fraude del CEO

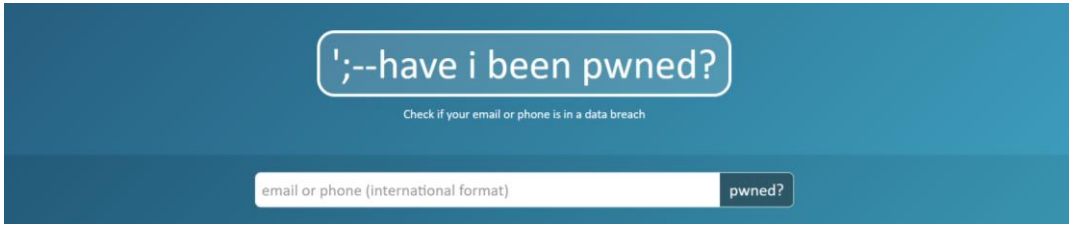
Fraude de RRHH

Ataques suplantación proveedores

Junta de Castilla y León

Gestión de Filtraciones HIPB

Correo Electrónico



Junta de Castilla y León

Normas de navegación web

Internet

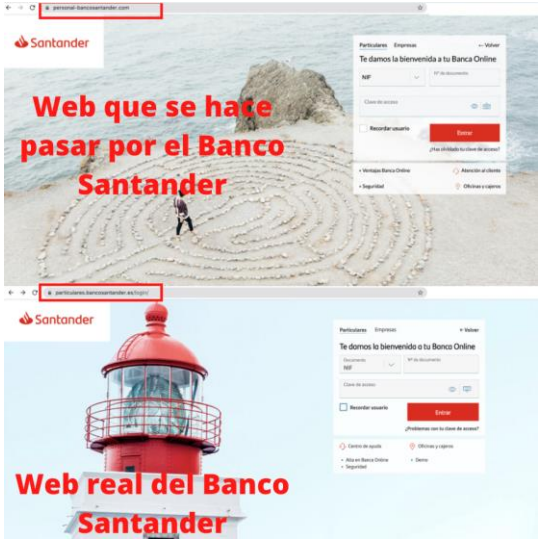
- Se podrán definir **diferentes perfiles de navegación we**b teniendo acceso los usuarios a destinos concretos y requiriendo autorización el resto.
- Habrá **destinos no autorizados** por considerarse peligrosos o no relacionados con ACCyL.
- Desde el respeto a la intimidad y protección de datos del usuario, se podrá **acceder a la navegación web con riesgos de seguridad** con el fin de garantizar integridad y continuidad de prestación de servicios públicos.

Junta de Castilla y León

Buenas prácticas de navegación web

Internet

- Siempre debemos comprobar **qué página web estamos visitando**. A través de phishing y otras técnicas nos intentarán engañar y llevarnos a webs que se hacen pasar por organismos y engañarnos
- Mantener navegador actualizado para evitar exploits al visitar webs
- Fijarnos siempre en la **URL de la web** que visitamos y que sea HTTPS
- Revisa periódicamente **plugins, extensiones y seguridad del navegador**
- **Evita guardar contraseñas en el navegador** cuanto te da la opción de recordar contraseña
- Cuidado con las **WIFI abiertas**
- No olvidemos **cerrar sesión** si hemos entrado en un sitio que nos ha requerido registro



Gestión de información sensible y/o carácter personal

“La adecuada gestión de la información sensible y de los datos de carácter personal se han convertido en un aspecto fundamental para cualquier tipo de organización y también para la ACCyL”

Gestión de información sensible y/o carácter personal

- **Como usuarios debemos cumplir en todo momento con las legislaciones en materia de protección de datos (RGPD y LOPDGDD)**
- Análisis de **Legitimación**
- **Información** adecuada a los usuarios en la recogida de los datos personales
- Procedimientos de **Ejercicio de los Derechos**
- **Medidas de Seguridad** en el tratamiento de los datos personales
- **Datos de Categoría Especial**
- **Encargados de Tratamiento** y Corresponsables de Tratamiento
- Comunicación de **violaciones de seguridad**
- Contacto con **el Delegado de Protección de Datos**
- Evaluaciones de Impacto (**EIPD**), Transferencias Internacionales(**TID**)…

Gestión de información sensible y/o carácter personal

- Política de **Mínimo privilegio (*NOR-1050*).** Nivel de difusión de la documentación de seguridad a las personas que lo necesiten.
- Seguridad desde el diseño y por defecto (*Privacy by Design / Security by Design*)
- Etiquetado de la información y los **documentos de seguridad** siguiendo un protocolo internacional ***Traffic Light Protocol (TLP)***
  - **TLP RED**: información limitada a personas concretas y tiene impacto en privacidad, reputación y operaciones. Receptores no deben compartir información.
  - **TLP AMBER**: información distribuida de forma limitada pero supone un riesgo. Receptores sólo pueden compartir con miembros de su organización.
  - **TLP GREEN**: información útil para todas las organizaciones que participan y terceros. Se puede compartir con organizaciones afiliadas y miembros del mismo sector. (Ej. Normas y Procedimientos Generales)
  - **TLP WHITE**: no supone riesgos de mal uso dentro de las reglas de difusión de información pública. Se puede compartir sin restricciones. (Ej. PSIPD)

Código	Cuándo utilizarlo	Cómo compartirlo	Color	Fondo
TLP:RED	Se debe utilizar TLP:RED cuando la información está limitada a personas concretas, y podría tener impacto en la privacidad, reputación u operaciones si es mal utilizada.	Los receptores no deben compartir información designada como TLP:RED con ningún tercero fuera del ámbito donde fue expuesta originalmente.	#ff0033	#000000
TLP:AMBER	Se debe utilizar TLP:AMBER cuando la información requiere ser distribuida de forma limitada, pero supone un riesgo para la privacidad, reputación u operaciones si es compartida fuera de la organización.	Los receptores pueden compartir información indicada como TLP:AMBER únicamente con miembros de su propia organización que necesitan conocerla, y con clientes, proveedores o asociados que necesitan conocerla para protegerse a sí mismos o evitar daños. El emisor puede especificar restricciones adicionales para compartir esta información.	#ffc000	#000000
TLP:GREEN	Se debe utilizar TLP:GREEN cuando la información es útil para todas las organizaciones que participan, así como con terceros de la comunidad o el sector.	Los receptores pueden compartir la información indicada como TLP:GREEN con organizaciones afiliadas o miembros del mismo sector, pero nunca a través de canales públicos.	#33ff00	#000000
TLP:WHITE	Se debe utilizar TLP:WHITE cuando la información no supone ningún riesgo de mal uso, dentro de las reglas y procedimientos establecidos para su difusión pública.	La información TLP:WHITE puede ser distribuida sin restricciones, sujeta a controles de Copyright.	#ffffff	#000000

TLP:GREEN

Gestión de información sensible y/o carácter personal

Junta de Castilla y León

Categorización de la Información de ACCyL

- Se establecerá **una categorización de la información de ACCyL** para clasificar cada uno de los activos de información en base a las categorías del Anexo I del ENS y las legislaciones de protección de datos.

- ¿Qué niveles concretos existirán? Serán independientes de TLP y se determinan en base al impacto que tendría la materialización de una amenaza sobre los activos de información de ACCyL.

SECRETA: La información de la ACCyL que precise del **más alto grado de protección de seguridad** debe recibir la categoría de secreta. Su revelación o utilización no autorizada puede dar lugar a una amenaza o a un perjuicio extremadamente grave para los intereses de la ACCyL, como poner en peligro la vida de los ciudadanos, alterar el orden público o el manejo de información de otras organizaciones que requieran el más alto grado de protección.

CONFIDENCIAL: Es la categoría que se asigna a la información que precisa de un **alto grado de protección**. Su revelación o utilización no autorizada pueda dar lugar a una amenaza o a un perjuicio grave para los intereses de la ACCyL, como poner en peligro la seguridad de los ciudadanos, la seguridad de la infraestructuras críticas, revelar información estratégica de la organización o el manejo de información de otras organizaciones que requieran un alto grado de protección.

INTERNA: En esta categoría, la información precisa **medidas de protección leves para fortalecer su seguridad**, debido a que es información que sólo deben conocer las personas de la ACCyL y no se encuentra clasificada en ninguna de las categorías anteriores. Su divulgación no autorizada, pérdida o destrucción de esta información puede causar un perjuicio para los intereses de la ACCyL en relación al funcionamiento de los servicios públicos prestados por la ACCyL.

PUBLICA: Cualquier información de la ACCyL no comprendida en las categorías anteriores y que **no precise de medidas especiales de protección**. Se considerará información pública toda aquella información de uso general y público dentro y fuera de la Junta de Castilla y León. La divulgación o pérdida o destrucción de esta información no generará ningún impacto para la organización.

Protección de soportes de información

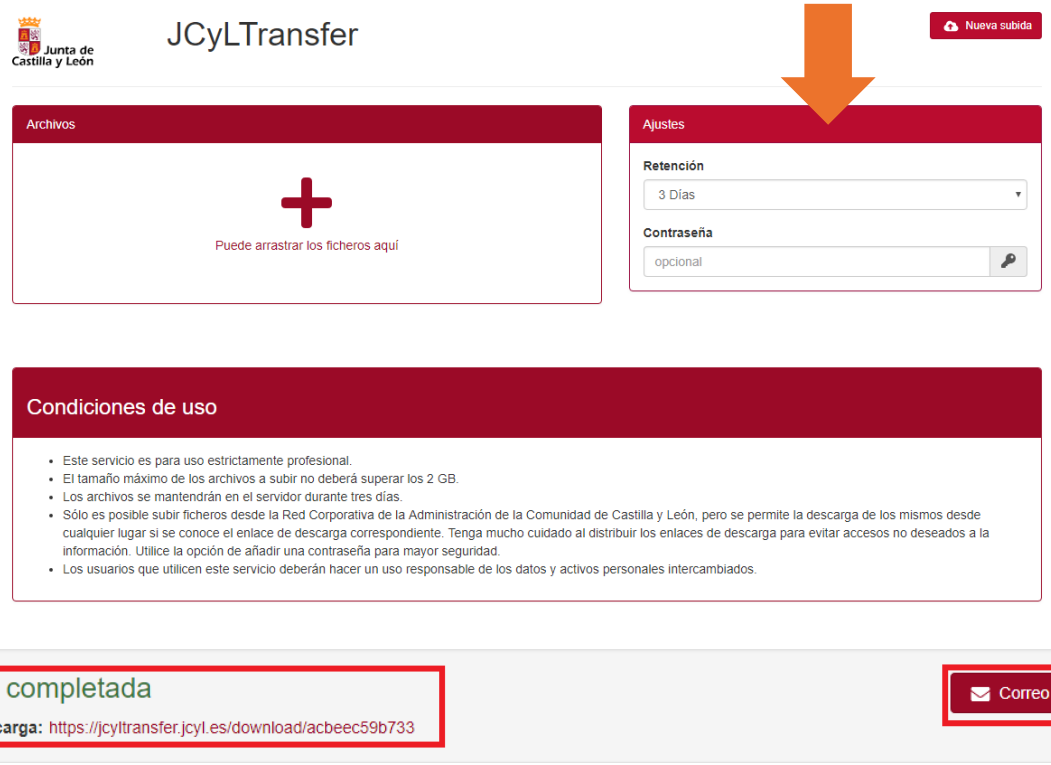
“Debemos evitar en la medida de lo posible la utilización de dispositivos extraíbles para manejar información ya que son un riesgo para la seguridad de los sistemas y de la propia información”

Junta de Castilla y León

Normas en el uso de soportes

- No debemos conectar dispositivos sospechosos a nuestros equipos ya que pueden ser un riesgo. En caso de tener que conectarlos utilizaremos el antivirus sobre ese dispositivo.
- Si necesitamos enviar información de gran tamaño, podemos utilizar **JCYL Transfer**
- Los soportes etiquetados no deben revelar el contenido pero sí el nivel de seguridad
- Si debemos utilizar los mismos, este dispositivo deberá ser cifrado o la información que contenga deberá ser cifrada (recomendable para todos y obligatorio para información de nivel medio y alto del ENS)
- Una vez cumplido su objetivo deberemos borrar la información de forma segura (Ccleaner, Eraser… y otras herramientas pueden ser utilizadas).

Protección de soportes de información



Protección de dispositivos móviles y su información

“Se han convertido en un elemento indispensable en nuestra vida diaria por lo que debemos también tenerlos en cuenta de cara a la ciberseguridad”

Junta de Castilla y León

Normas de seguridad en dispositivos móviles

- Se mantendrá un **inventario de dispositivos móviles corporativos** y personas a quienes se les ha asignado el uso
- Se seguirá un **proceso de autorización** en base a requisitos y condiciones específicas del uso que serán cumplidas
- El **propietario es ACCyL** y podrá retirarse el uso en cualquier momento si se detecta uso inadecuado
- La **custodia y cuidado es responsabilidad del usuario**
- Deben utilizarse de forma eficiente y segura por lo que se adoptarán **medidas de seguridad para mantenerlo controlado y evitar pérdidas**. El transporte se hará de forma segura y se evitará la utilización en lugares públicos y el uso de conexiones inalámbricas inseguras.
- Los dispositivos móviles se **configurarán de forma segura** permitiendo actualizaciones bloqueos y borrados remotos
- Mecanismos de **cifrado** para proteger la confidencialidad

Normas de seguridad en dispositivos móviles

- En caso de **incidente**, notificación inmediata a ACCyL.
- Prohibida la manipulación sin autorización de configuraciones de seguridad y software y la desactivación de antivirus corporativo.
- **Retirada del dispositivo móvi**l en caso de cambio de puesto de trabajo o extinción de relación contractual debiendo ser comunicado inmediatamente.

¿Y los dispositivos móviles de terceros o de empleados? (BYOD)

- A nivel general **está prohibida la conexión de dispositivos móviles** de terceros está prohibida la conexión a las redes de ACCyL salvo las de cortesía para invitados y con autorización
- **Autorización de conexiones** cuando se determine y con **autorización** de los Responsables de Sistemas de Información.
- Se regirán por la **Normativa de Acceso** Remoto.

Protección de dispositivos móviles y su información

- **No dejar el dispositivo desatendido y sin desbloqueo** activado.
- Configura una **protección de acceso robusta** al activarse la pantalla (desbloqueo)
- Procura hacer uso de las opciones de **cifrado** del dispositivo
- **Actualiza las apps y sistema operativo** periódicamente y descarga las apps siempre de sitios oficiales
- Realiza **copias de seguridad periódicas y programadas**. Revisa periódicamente la información si se almacena en algún servicio cloud.
- Deshabilita los interfaces de comunicación que no se estén utilizando (datos, bluetooth, WI-FI…)
- Evita la conexión a **WiFis abiertas**

Dispositivos móviles

Por norma general, nos centraremos en los equipos informáticos como portátiles, móvil *smartphone*, *tablet*, que permiten acceder a los recursos e información de la organización. Dejamos fuera aquellos dispositivos tipo pulsera o relojes inteligentes que necesiten enlazarse con un móvil.

BYOD

Bring Your Own Device, trae tu propio dispositivo, es aquella tendencia en la cual los empleados tienen la posibilidad de llevar y utilizar sus propios dispositivos móviles para acceder a los recursos de su organización.

CYOD, COPE, COBO

CYOD, elige tu propio dispositivo personal, pero de un listado que ofrece la organización.

COPE, dispositivo propiedad de la empresa con uso personal permitido.

COBO, donde tanto el dispositivo es de la organización y su uso es profesional.

VPN

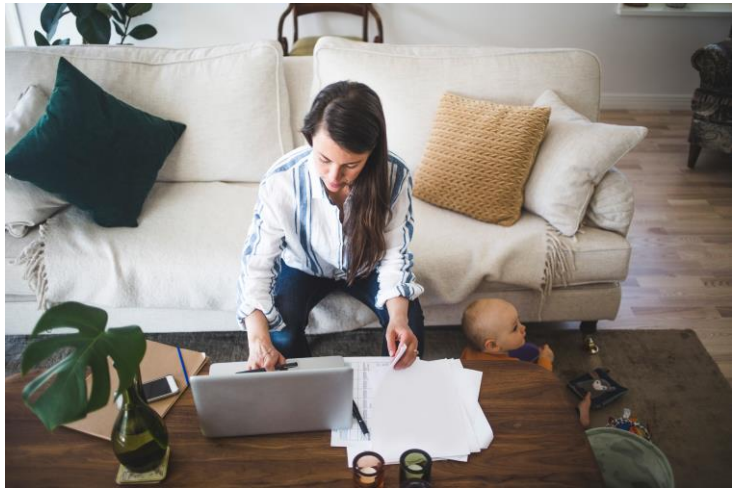
Red Privada Virtual; red lógica que existe dentro de otra red física. Circuito de red informática cifrada, dentro dev una red abierta como Internet.

Biometría

Procedimiento de autenticación basado en la medición de alguna característica física o biológica de una persona. (Ribagorda: 1997).

Buenas prácticas en teletrabajo

“La pandemia, las nuevas formas de trabajar y la necesidad de conciliación laboral han traído un auge del teletrabajo”



“Con el teletrabajo también existen nuevos riesgos debido al cambio de ubicación habitual y el cambio en el uso de los recursos que debemos gestionar”

Buenas prácticas en teletrabajo

Junta de Castilla y León

- Las personas que desarrollan su actividad en **modalidad teletrabajo** pueden:

  Utilizar sus propios equipos y dispositivos móviles (BYOD)
  Utilizar portátiles y dispositivos móviles proporcionados por su organización

¿Cuál es el principal objetivo de seguridad para quien realiza teletrabajo?

Conseguir equiparar la misma seguridad que tendríamos en nuestro puesto de trabajo habitual

Entorno de Trabajo

Seguridad en las Comunicaciones

Seguridad en los equipos

Buenas prácticas en teletrabajo

- **Entorno adecuado** para llevar a cabo el teletrabajo en el que cuidemos tanto la seguridad física y acceso son autorizados como la seguridad de los propios dispositivos y el acceso a información en papel. Elige un lugar adecuado y que también te proporcione tranquilidad.

- Procura actualizar la clave WIFI periódicamente y utiliza contraseñas robustas.

- Si estamos en un **lugar público** extremaremos las medidas de seguridad evitando conectarnos a redes públicas y no dejando equipos desatendidos.

- **Conexiones seguras a ACCyL** a través de los medios seleccionados para el acceso a la información (Acceso remoto a la Red Corporativa de JCYL). En la medida de lo posible, no trabajar en local ni guardar información en su propio equipo.

- Método de **autenticación** mediante 2FA o certificado o DNI electrónico.

- Analiza la **seguridad de tu equipo** y procura utilizarlo de forma segura:

  - Actualizando Sistema Operativo y utilizando antivirus
  - Navegación segura
  - Evitar conectar USBs en los que no tengas confianza
  - Cierra todas las sesiones abiertas en los servicios utilizados
  - Elimina habitualmente la información temporal que pudiera haber en tu equipo (papelera, descargas…)

Buenas prácticas en teletrabajo

Junta de Castilla y León

Como usuario ¿cuáles serían las buenas prácticas a seguir?

- No utilizar WIFIs públicas ni abiertas
- Actualiza la clave WIFI de tu casa frecuentemente y con contraseñas robustas
- Configura tu router/WIFI de la forma más segura posible
- Actualizaciones del sistema operativo del ordenador, programas y el antivirus
- Protección antimalware en tiempo real con análisis automatizados o periódicos, activar cortafuegos…
- Procura limitar el acceso a internet a páginas seguras y que ya hayas utilizado antes
- Evita conectar dispositivos USB en los que no tengas plena confianza y deshabilita la opción de autoejecución.
- Especial cuidado con la documentación manejada en papel ya que no estamos en el entorno laboral extremando medidas de seguridad para su custodia y destruyéndola adecuadamente.

Buenas prácticas en teletrabajo

Junta de Castilla y León

Como usuario ¿cuáles serían las buenas prácticas a seguir?

- Al terminar de trabajar, cierra todas las sesiones en los servicios que hayas utilizado.
- Elimina habitualmente la información temporal (Descargas, Papelera de Reciclaje, Mis Documentos…)
- Evita el uso de post-it con información a la vista
- Bloquea tu equipo cuando abandones el mismo
- Controla la webcam y tápala cuando no la estés utilizando
- Cuidado con la configuración de dispositivos iOT, mal configurados pueden ser un riesgo para la seguridad y la puerta de entrada a grandes amenazas

Turno de preguntas

Junta de Castilla y León

eclap