Breve Guía de Ciberseguridad para Partidos Políticos

ÍNDICE

Mayo de 2023

1. INTRODUCCIÓN

En el marco del Plan Integral de Cultura de Seguridad Nacional, y con base en la Orden PCM/1030/2020 de 30 de octubre, por la que se publica el procedimiento de actuación contra la desinformación aprobado por el Consejo de Seguridad Nacional, se creó un grupo de colaboración público-privada, con la finalidad de aportar propuestas que puedan contribuir a la lucha contra la desinformación.

Entre las recomendaciones planteadas en el bloque dedicado a procesos electorales se contiene una dirigida a las autoridades competentes, "para que elaboren una guía de ciberseguridad para partidos políticos", señalándose en el propio documento que dicha tarea será encomendada al CCN.

Consecuentemente, la presente guía se ha elaborado en desarrollo de la citada previsión, con la finalidad de ser un instrumento útil en la consecución de la ciberseguridad de sistemas y redes informáticas como un factor de garantía en la lucha contra la desinformación en el ámbito electoral, dada la trascendencia que los partidos políticos tienen en nuestro sistema electoral.

El artículo 6 de la Constitución Española establece que "Los partidos políticos expresan el pluralismo político, concurren a la formación y manifestación de la voluntad popular y son instrumento fundamental para la participación política. Su creación y el ejercicio de su actividad son libres dentro del respeto a la Constitución y a la ley. Su estructura interna y funcionamiento deberán ser democráticos".

Este papel crucial, y las graves consecuencias que podrían derivarse de un ataque informático a uno o varios partidos políticos en el curso de un proceso electoral, justifica que los partidos deban prepararse de la mejor manera posible para hacer frente a las amenazas híbridas y reduzcan sus vulnerabilidades en ciberseguridad.

La guía tiene una intención de esquematización de elementos básicos que los partidos políticos deberían tener en cuenta en el día a día de su propia ciberseguridad. Es un instrumento breve, conciso y enfocado, como una lista de chequeo para tener previsto qué se está cumpliendo y qué debería de cumplirse para garantizar un estándar de ciberseguridad.

En un partido político, igual que en cualquier organización, la ciberseguridad es la ecuación resultante de combinar la conducta de las personas, con la gestión de la información, la protección de los dispositivos y la salvaguarda de las redes de conectividad.

En la actualidad, la ciberseguridad ya no puede entenderse únicamente como una cuestión tecnológica, ni infraestructural, sino como un revestimiento de protección para la propia identidad de una organización.

En efecto, la digitalización es ya una cualidad inherente a la información, y un partido político es, en esencia, una agrupación de ciudadanos que se unen para compartir y llevar a cabo un proyecto de ideas sobre el mejor modo de construir una sociedad.

Ese proyecto político de ideas se genera y acuerda en reuniones de los órganos del partido político, reuniones en las que habitualmente están presentes personas junto a una multiplicidad de dispositivos electrónicos, generalmente conectados a redes cibernéticas.

Las ideas se redactan por ordenador en **documentos digitales**, en versiones que se almacenan en dispositivos informáticos, que después se imprimen o no en papel a

través de impresoras conectadas a redes, y que se comparten, distribuyen o envían a través de sistemas de comunicación digitales en red, como el correo electrónico. Cada vez más, los clásicos documentos de texto van acompañados de contenidos en audio o vídeo.

Todos esos documentos o contenidos, que son ya **nativos digitales**, es decir, que nacen siendo tecleados en un computador informático o grabados a través de una aplicación software de vídeo o de audio, además de su almacenamiento digital en un dispositivo individual crecientemente tienen una copia, o incluso han sido originalmente creados, en un servidor de almacenamiento conectado a redes cibernéticas. Ese almacenamiento puede estar en una red local cerrada con acceso a los miembros del partido político, pero a menudo está configurado en la denominada nube, que no es más que un repositorio conectado en red, habitualmente a la red de redes, Internet.

Los contenidos digitales generados por un partido político no sólo representan la representación electrónica de las ideas de ese partido político, sino también un reflejo de sus deliberaciones internas, de sus expectativas, de sus estrategias, de sus modos de organización, de sus finanzas, de su personal y militancia: en definitiva, la vida e identidad de un partido político tienen hoy en día una representación digital nativa, desde la propia concepción del partido político como grupo social.

Además, cualquier formación política constituida en la última década o cualquiera con un siglo de historia que haya ido adaptando sus modos de organización e interacción sociales a las realidades digitales cambiantes tienen tanto su comunicación interna como la externa, expresadas a través de contenidos, dispositivos y servicios digitales conectados a redes informatizadas. Los documentos digitales circulan por las redes conectadas y comunican a emisores con receptores de esos contenidos, a políticos que quieren trasladar mensajes e ideas con la audiencia a la escucha de esas intenciones políticas. De nuevo, la realidad digital circulando a través de redes cibernéticas se impone en esa comunicación. La muestra más evidente de este universo social digitalizado que impregna a la actividad política es que no hay movimiento político que no tenga actividad, y haya diseñado estrategias comunicativas específicas, para las redes sociales digitales.

En ese universo digital en donde se vierten en contenidos y dispositivos electrónicos las ideas y el sistema de organización de los partidos políticos, y se comunican las intenciones y proyectos políticos tanto entre sus proponentes y emprendedores como entre los ejecutantes y las audiencias que vayan a estar interesadas en ellos, los dispositivos electrónicos no están solos: estos son instrumentos de información y comunicación de las personas, que son quienes los encienden y apagan, quienes los configuran, y los utilizan en una multiplicidad de funciones programadas a través de aplicaciones informáticas. La realidad cibernética es un binomio indisoluble entre dispositivos y personas que los manejan.

En esa ecuación entre personas y dispositivos, la ciberseguridad no sería necesaria si no hubiera amenazas, pero las hay.

Entre las numerosas tácticas, técnicas y procedimientos que emplean esas ciberamenazas para vulnerar y comprometer sistemas informáticos, dos sobresalen en porcentaje incontestable como las que acumulan el mayor volumen de incidentes informáticos en todo el mundo y cada año: 1) la vulneración de sistemas informáticos mediante el aprovechamiento, por parte del atacante, de fallos de software presentes esos sistemas; 2) la manipulación de la conducta del usuario de sistemas informáticos

para conducirle a realizar acciones (por ejemplo, pulsar un enlace de hipertexto) que, sin que el usuario tenga conciencia de ello, pongan en riesgo la seguridad de los sistemas informáticos. De este modo, los dos factores de debilidad más relevantes que gestionar mediante medidas de ciberseguridad en sistemas informáticos, ante la acción de ciberamenazas, son el factor humano y la integridad del software.

Las ciberamenazas que actualmente buscan vulnerar y comprometer sistemas informáticos de organizaciones como los partidos políticos son de diversa tipología estructural, conducidas por distintas motivaciones, y actúan a través de procedimientos que les confieren diferente peligrosidad, unas más alta y otras más moderada. Sin embargo, si hubiera que abstraer una característica que fuera el común denominador para la mayoría de las ciberamenazas que pueden interesar a la ciberseguridad de un partido político cabría señalar que es la **remotidad**: la posibilidad para una ciberamenaza de actuar remotamente, desde cualquier parte del mundo y en cualquier momento, para victimizar sistemas informáticos en cualquier otra localización del mundo, si se dan las condiciones tanto de capacidad y habilidad por parte de la ciberamenaza como de vulnerabilidad en el sistema atacado. Por tanto, la primera toma de conciencia a adoptar en la ciberseguridad preventiva de un partido político es que puede haber actores que, movidos por intenciones maliciosas, y localizados en cualquier parte del mundo, de repente y en función de las circunstancias que sean, pueden tener interés en enfocar ciberataques sobre los sistemas informáticos de ese partido político.

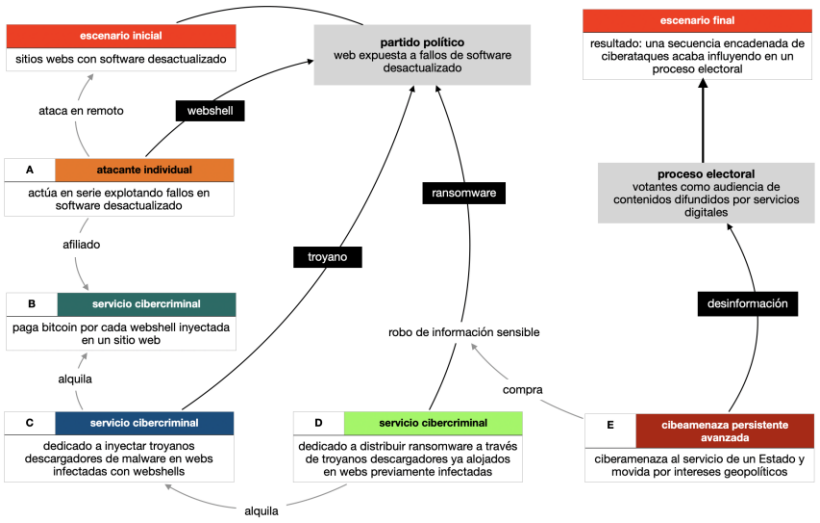
Las circunstancias, motivaciones e intereses de las ciberamenazas recorren un abanico en donde se pueden mezclar varias, pero que generalmente están recogidos en las siguientes tres categorías: ideológicas, cibercriminales de lucro, o geopolíticas. Adscritas a una o varias de esas categorías de clasificación motivacional, las ciberamenazas muestran diferentes estructuras organizativas en ecosistemas que generalmente vinculan unas estructuras a otras, y relacionan unos intereses con otros, a la manera de una cadena, mundialmente interconectada, de actividades cibernéticas maliciosas.

Como ejemplo de esa cadena (Figura 1-1): un atacante individual (A), provisto de una cierta pericia técnica, puede forzar sitios web vulnerables inyectándoles código malicioso, motivado porque es un afiliado a un servicio cibercriminal (B) que paga en divisas electrónicas a sus suscriptores por cada porción de código malicioso con el que sean capaces de infectar sitios web en cualquier parte del mundo; este primer atacante conoce que el código malicioso inyectado está conectado a una red de distribución de software dañino, pero no tiene una idea clara del propósito final de esa red. En paralelo, los gestores de esa red de distribución de software dañino la alquilan a cualquiera que pague por el servicio para diseminar, a través de ella, malware de distinto tipo y funcionalidad. Imagínese que ese primer contenido inyectado por el atacante individual es una *webshell*, código software dañino que actúa como una interfaz remota y oculta en un sitio web, y que posibilita que otro atacante utilice esa interfaz para infectar el servidor informático de esa web con cualquier virus, por ejemplo, con un troyano descargador de malware, un virus cuya función es preparar la web para recibir cualquier otra pieza de malware. Si esa *webshell* ha sido insertada por el primer atacante en la web de un partido político aprovechando que esa web exponía un fallo en su software, otro atacante con motivaciones puramente de lucro cibercriminal, puede alquilar la red cibercriminal a la que la *webshell* pertenece a otro actor cibercriminal (C) que infecta, varios sitios web alojando esa *webshell* (entre ellos, el correspondiente al partido

político), con un troyano descargador de malware que sea capaz de infectar con otro virus todas esas webs previamente comprometidas, por ejemplo con un *ransomware* manipulado por otro cuarto actor (D). Ese primer atacante que ha infectado con una *webshell* la web del partido político, junto con otras decenas de ellas, ha posibilitado que un segundo atacante, no relacionado con el primero, inserte en ella un troyano descargador, que facilitará que un tercer atacante pueda alquilar ese troyano para inocular una cepa de ransomware. Ahora la web del partido político del ejemplo, a través de la acción de tres atacantes no vinculados inicialmente entre sí, aloja tres códigos software dañinos: una interfaz remota tipo *webshell*, un troyano descargador, un ransomware. La cadena se puede incluso extender más, puesto que el operador del ransomware (D) puede robar información sensible de los sistemas informáticos del partido político y vendérselos a otra ciberamenaza (E) que ya no se conduzca por motivos cibercriminales, sino por intereses geopolíticos. Y ese cuarto operador en la cadena de ciberamenazas que actúan desde diferentes países del mundo puede considerar de su interés, del interés de los propósitos geopolíticos a los que sirva, que la información robada mediante el ransomware sea divulgada públicamente para influir en un resultado electoral. Esa información robada y publicada, puede tergiversarse a su vez mediante técnicas de desinformación, con el objetivo de torcer la percepción de partes de una comunidad de votantes. Y así tenemos como, una pieza inicial de código malicioso inyectada en una web vulnerable de entre otras tantas por parte de un atacante cuyo propósito es cobrar unos cuantos Bitcoin por vulnerar sitios web, conduce, a través de una cadena de relaciones cibercriminales, a un incidente electoral en un país.

Figura 1-1

POSIBLE ENCADENAMIENTO DE CIBERAMENAZAS



De esta manera, un ciberataque a los sistemas informáticos de un partido político, que tenga como resultado la divulgación pública de información robada de los ordenadores, teléfonos móviles o servidores informáticos comprometidos con código software dañino, siendo que esa divulgación de información se realiza durante una campaña electoral o en la propia jornada de reflexión de la población convocada a las urnas, puede tener un impacto directo y significativo en la conducta electoral del votante. Es decir, a menudo se piensa que un ciberincidente grave durante un proceso

electoral sería el derivado de un ataque informático a los sistemas de procesado de resultados electorales, o incluso a los sistemas de voto electrónico en los países donde estén implantados. Y en verdad sería grave ese tipo de incidente. Sin embargo, un ciberataque selectivamente medido y dirigido contra los sistemas informáticos de uno o varios partidos políticos, con el fin de desvelar información sensible de partidos políticos o de sus miembros, que luego sea tergiversada ante la opinión pública, puede condicionar ilegítima e ilegalmente las dinámicas democráticas.

En consecuencia, de lo que trata esta breve guía de ciberseguridad para partidos políticos es de recopilar un listado útil de sugerencias para minimizar la **superficie de exposición** de sistemas informáticos de una organización política ante las diversas tipologías de ciberataque. Aquí se da por supuesto que, minimizando las vulnerabilidades informáticas, entre las que se incluyen los fallos de software, los defectos de configuración de dispositivos informáticos o los errores de los usuarios humanos como las más comunes, los partidos políticos tendrán menos probabilidades de ser victimizados en esquemas maliciosos de desinformación dirigidos a manipular a la población española.

En cualquier caso, este recopilatorio de sugerencias de ciberseguridad para partidos políticos a modo de guía breve no pretende sustituir la necesidad de que los partidos políticos, al igual que otras organizaciones públicas y privadas provistas de infraestructuras informáticas, desarrollen sus propios Sistemas de Gestión de la Seguridad de la Información (SGSI) de manera sistemática y profesional. Tampoco es objeto de la guía agotar todos los capítulos y temas, por otra parte, inabarcables para un solo documento, propios de la ciberseguridad corporativa, sino apuntar una serie de consejos útiles y recomendaciones a tener en cuenta. El **Centro Criptológico Nacional de España** publica periódicamente un conjunto de **guías de buenas prácticas**, más específicas, que pueden servir mejor como instrumentos concretos para profundizar en el diseño, desarrollo, despliegue y aplicación de soluciones de ciberseguridad.

Entre estas guías, cabe recomendar la CCN-CERT BP/13[1], publicada en febrero de 2019 y que versa sobre procedimientos para conocer, detectar y prevenir la desinformación en el ciberespacio, con un decálogo final de recomendaciones que es interesante incorporar a las prácticas de ciberseguridad de toda organización.

[1] https://angeles.ccn-cert.cni.es/index.php/es/docman/documentos-publicos/informes-de-buenas-practicas/310-ccn-cert-bp-13-desinformacion-en-el-ciberespacio

2. PROTECCIÓN DE LA INFORMACIÓN

2.1. Sensibilidad de la información

Con independencia de que los partidos políticos en España hayan sido creados cada uno con su propia cronología, y que esa cronología se extienda por diversos períodos históricos, unos más modernos y otros más antiguos, que a su vez hayan dado origen a información almacenada en soportes analógicos, la realidad actual es que la mayor parte de la información que refleja la vida interna y externa de un partido político es nativamente digital o ha sido digitalizada: es decir, ha sido creada en un computador, una máquina informática.

La realidad digital de un partido político (sus contenidos, sus documentos con ideas políticas, estrategias, sistemas de organización, finanzas, datos personales identificativos de la militancia) está almacenada en dispositivos electrónicos que, aunque algunos estén asignados para usufructo de personas individuales, forman parte de la infraestructura del propio partido político en tanto institución societaria.

Una buena parte de esa realidad digital de los partidos políticos en forma de contenidos está definida para ser pública y, por tanto, para difundirse abiertamente también por canales digitales. Alguna de esa información digital, o de la analógica que ya ha sido digitalizada o que no lo ha sido, tiene obligación de ser pública para responder a mandatos legales de **rendición de cuentas** o de **transparencia**. Una porción significativa de esa realidad de información digital está compuesta por contenidos y documentos configurados por diferentes niveles de privacidad, de sensibilidad o de confidencialidad.

Además de la componente individual de la privacidad y de la confidencialidad sobre datos e información, el partido político mantiene un alcance propio, en tanto institución, sobre la privacidad y la confidencialidad de los contenidos. Este alcance no es sólo jurídico, derivado de la exigible protección de datos personales o de la salvaguarda de la información clasificada que emanan de la legislación vigente, sino que tiene que ver con los diferentes permisos de acceso a la información determinados en función del principio de la “necesidad de conocer”: quién debe conocer cada pieza de información en función de las responsabilidades que cada persona tenga asignada en la organización.

La **sensibilidad** es una propiedad de la información definida por el grado de protección que le corresponde en función de si su conocimiento por personas ajenas a las tenedoras originales de esa información puede ocasionar un perjuicio a las personas físicas o jurídicas tenedoras originales de la información. Esa propiedad se extiende a lo largo de una gradación de mayor o menor sensibilidad. La información más sensible es aquélla cuyo conocimiento está restringido a un número definido de personas autorizadas, en el contexto de la cuales se infiere que ese conocimiento no va a suponer un perjuicio para ninguna otra persona física o jurídica, incluso que ese conocimiento implica que personas físicas o jurídicas estarán más seguras si las personas autorizadas conocen y salvaguardan la información sensible. No es tanto el contenido de una información lo que la convierte en sensible, sino el impacto negativo que podría derivarse potencialmente de su difusión fuera del círculo de personas autorizadas a conocerla.

En las Administraciones Públicas, la información está **clasificada según su nivel de sensibilidad** para el acceso diferenciado por personas con habilitación. Esa clasificación

establece distintos niveles de catalogación, que a su vez implican restricciones de acceso: desde la no-clasificación, que supone que la información no tiene restricciones de acceso adicionales a las que se puedan derivar de la necesidad de conocer su contenido por parte de personas; hasta la difusión limitada, la confidencialidad, el carácter de reservado, o el de secreto. Normativamente en España, los grados de secreto y reservado se corresponden con información protegida mediante lo dispuesto en la Ley de Secretos Oficiales, mientras los grados de confidencial y de difusión limitada abarcan informaciones sobre las que se ha dictado algún tipo de deber de protección de reserva a un número determinado y concreto de personas a las que se autoriza explícitamente a acceder a ellas.

A los partidos políticos le alcanzan las obligaciones legales de salvaguarda de la información clasificada según la legislación española de secretos oficiales siempre que sus cuadros o miembros sean destinatarios autorizados de algún tipo de información de esa naturaleza. Los partidos políticos también son sujetos obligados por las medidas de seguridad que se deriven del cumplimiento de la legislación de privacidad y de protección de datos de carácter personal. En cambio, no hay un marco regulatorio específico definido para establecer un sistema interno de clasificación, catalogación y protección de la información sensible generada o gestionada por el propio partido político al margen de los secretos oficiales y de los datos de carácter personal.

Por tanto, a efectos de implantar en un partido político un ecosistema de ciberseguridad sobre la información que es necesario proteger, cuatro son las categorías de información que debería considerarse sensible y, por tanto, ser alojada y gestionada digitalmente por **sistemas específicos de salvaguarda basados en tecnología** y en **procesos de gestión de accesos autorizados y acreditados**:

1) La información obligada por la Ley de Secretos Oficiales.
2) La información clasificada con las etiquetas de "confidencial" o de "difusión limitada".
3) La información obligada por la legislación de protección de datos de carácter personal. Es decir, cualquier tipo de datos de carácter personal o revelando aspectos de la persona de afiliados y miembros del partido político, así como de todas aquellas personas sobre las que el partido político almacena datos personales identificativos (simpatizantes, personas que contactan u otras).
4) Ciertos tipos de información interna del partido político cuya publicación no esté obligada por mandatos de transparencia o rendición de cuentas. Esta categoría de información incluiría, al menos, los siguientes objetos de información:
    a. Información de detalle sobre procesos organizativos y finanzas del partido político distinta de la necesaria para cumplir con las diversas obligaciones legales de rendición de cuentas y de transparencia.
    b. Información sobre deliberaciones internas, estrategias, planes, intenciones o conversaciones privadas con terceros del partido político que todavía no están en proceso de ser difundidas públicamente ni están obligadas legalmente por procesos de rendición de cuentas o de transparencia.
    c. Información interna sobre encuestas, acciones prospectivas, o métodos de acción que forman parte de las dinámicas de la política local, regional, nacional o internacional, y que no forman parte de las informaciones obligadas por procesos de rendición de cuentas o de transparencia.

d. Contenido de los correos electrónicos emitidos o recibidos desde cuentas operando bajo los dominios web del partido político o de sus proveedores tecnológicos. También, contenidos de correos electrónicos sobre cuestiones sensibles del partido político emitidos o recibidos desde cuentas personales alojadas en dominios web ajenos al partido político o a sus proveedores tecnológicos.
e. Información de detalle sobre los sistemas de seguridad y de ciberseguridad para la protección de las infraestructuras, las personas, los procesos o cualquier otro activo tangible e intangible del partido político.
f. Información de detalle sobre arquitecturas y sistemas tecnológicos operando en el partido político y cuya revelación no sea obligada legalmente por procesos de rendición de cuentas o de transparencia.
g. Todas las credenciales de autenticación a cualquier sistema digital o analógico con acceso protegido por contraseña u otro factor de autenticación.

Todo **el espectro de la información sensible digital o digitalizada**, desde la protegida por prescripciones legales específicas como la información clasificada o los datos de carácter personal, hasta la información interna del partido cuyo contenido se considere necesario limitar a personas autorizadas, representa **el activo más codiciado en ciberataques** que penetran dispositivos y redes informáticas de cualquier organización, partidos políticos entre ellas.

Por tanto, y puesto que es conocido que habrá un porcentaje significativo de intentos de ciberataque, conducidos por ciberamenazas avanzadas, dirigidos a acceder forzadamente a sistemas tecnológicos con el propósito de robar información sensible, la ciberseguridad de un partido político debería tener un capítulo específico dedicado a la salvaguarda de la información sensible a través de procedimientos y medios tecnológicos.

2.2. Salvaguarda de la Información

Hay dos ejes horizontales, es decir, que influirían en la definición de todos los sistemas tecnológicos desplegados, a considerar en la protección de información sensible:

1) **Cómo se cataloga y etiqueta la información** en función de sus distintos grados de sensibilidad, pudiendo ser estos, de menos a más, los siguientes:
    a. Información pública. Que no necesita protección en cuanto a su limitación de ser conocida.
    b. Información privada. Que no tiene intención ni obligación de ser conocida fuera de los miembros, simpatizantes o partes relacionadas con el partido político.
    c. Información de difusión limitada. Información privada cuyo conocimiento se considera, por las razones que fueren, que debe estar limitado a un conjunto tasado de personas específicas.
    d. Información de carácter personal. La así definida y protegida por la legislación de protección de datos de carácter personal.

e. Información confidencial. Información privada cuyo conocimiento alcanza únicamente a personas autorizadas para conocer esa información cuyo contenido, de desvelarse a no-autorizadas, podría poner en riesgo activos tangibles o intangibles de la organización.
f. Información reservada. La así clasificada por la legislación de secretos oficiales.
g. Información secreta. La así clasificada por la legislación de secretos oficiales.

2) **Cómo se diferencia a las personas** entre autorizadas y no autorizadas para el acceso a cada uno de los grados o niveles de información sensible.

Los sistemas tecnológicos de protección de la información sensible de un partido político deberían estar, por tanto, diseñados para **proteger la información frente a accesos no autorizados en función de su grado de sensibilidad**.

3. LISTA DE CHEQUEO DE LA POLITICA DE CIBERSEGURIDAD

Aunque podrían ser numerosas las variantes de diseño a aplicar en la salvaguarda de la información sensible ante ciberataques encaminados a comprometerla, se sugieren una serie de buenas prácticas que, a modo de lista de chequeo, un partido político debería tener en cuenta en la implantación de su política de ciberseguridad.

Dicha relación de buenas prácticas se vincula en las tablas que siguen con las medidas de seguridad que determina el anexo II del **Real Decreto 311/2022, de 3 de mayo, que regula el Esquema Nacional de Seguridad (ENS)**. La vinculación no pretende ser exhaustiva, sino representativa de la completa cobertura que el ENS puede llegar a aportar.

Dicho mapeo se justifica, desde un punto de vista jurídico, especialmente en cumplimiento de la Disposición adicional primera de la **Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales**, que señala "*Los responsables enumerados en el artículo 77.1 de esta ley orgánica deberán aplicar a los tratamientos de datos personales las medidas de seguridad que correspondan de las previstas en el Esquema Nacional de Seguridad, así como impulsar un grado de implementación de medidas equivalentes en las empresas o fundaciones vinculadas a los mismos sujetas al Derecho privado*".

En el referido artículo 77.1 se señala "*1. El régimen establecido en este artículo será de aplicación a los tratamientos de los que sean responsables o encargados (…) k) Los grupos parlamentarios de las Cortes Generales y las Asambleas Legislativas autonómicas, así como los grupos políticos de las Corporaciones Locales".*

3.1 GESTIONAR LA INFORMACIÓN

3.1.1 Salvaguarda de la Información Sensible

lista de chequeo 1		Salvaguarda de la Información Sensible		
nº	BUENA PRÁCTICA	PROPÓSITO	CARACTERÍSTICAS	VINCULACIÓN CON EL ENS
1.1.	Desarrollar un **Sistema de Gestión de la Seguridad de la Información** (SGSI).	El SGSI es el marco maestro de referencia para implantar todas las políticas necesarias para un sistema de ciberseguridad de la información de un partido político, al integrar las medidas de seguridad técnicas con las organizativas, logrando que se mantenga en el tiempo la eficacia y eficiencia de la ciberseguridad.	En general, un SGSI se compone de las siguientes fases recurrentes: 1) Planificación y diseño, donde se realiza una evaluación de los riesgos de seguridad de la información en una organización, así como un análisis de los controles que son necesarios para gestionar esos riesgos. 2) Implantación y puesta en operativa de los controles de gestión del riesgo. 3) Verificación periódica de la operativa de los controles y evaluación de su desempeño. 4) Introducción de los cambios consecuencia de la verificación para aumentar la eficacia y eficiencia del SGSI.	**[op.pl.2.r1.1]** Sistema de gestión, relativo a la planificación, organización y control de los recursos relativos a la seguridad de la información.
1.2.	Nombramiento de persona responsable de protección de información sensible.	Contemplado como un elemento de control dentro del SGSI, su función es supervisar el sistema de catalogación de cada pieza de información en función de su grado de sensibilidad, establecer niveles de autorización de acceso de seguridad de la información, y	Puede coincidir con la persona responsable de la seguridad de la información en el partido político, o con otra persona que desempeñe una función no incompatible. Puede responder ante un comité del partido político dedicado a definir la gradación de la sensibilidad de la información que genera y gestiona el partido.	**Artículo 13.** Organización e implantación del proceso de seguridad. **[org.1.3]** Los roles o funciones de seguridad, definiendo para cada uno los deberes y responsabilidades del cargo, así como el procedimiento para su designación y renovación.

lista de chequeo 1		Salvaguarda de la Información Sensible		
		adscribir a cada persona del partido al nivel que le corresponda en función de su necesidad de conocer la información.		
1.3.	Establecimiento de un sistema de catalogación de la información en función de su sensibilidad.	La catalogación de la sensibilidad no afecta a la información pública, sino al resto de categorías de información sensible. El objetivo es que cada miembro del partido político autorizado a conocer información tenga conciencia en todo momento del tipo de información en cuya generación está participando, de qué clasificación tiene la información a la que está accediendo, y qué permisos tiene para difundirla a otras personas autorizadas.	En el partido político, debería haber **personas habilitadas** con la función de clasificar información con una categoría de sensibilidad. Cualquier persona encargada de generar información digital o digitalizada en el partido político, debería seguir un **protocolo de consultas** para establecer si la información tiene propiedades de sensibilidad, y entonces acceder o no a ella, almacenarla y compartirla en función de los parámetros de sensibilidad. La catalogación de la sensibilidad de la información puede hacerse de varias maneras: • Con una marca en el documento y/o en el fichero. Esta marca debería ser complementaria de la **firma digital del fichero mediante criptografía** de clave pública, bien por el responsable de la custodia de la información sensible, bien por la persona autorizada a su difusión. • Sin marcado de documentos o ficheros, pero mediante su almacenamiento en repositorios protegidos en función de la clasificación determinada en el protocolo de consultas.	**Artículo 40.** Categorías de Seguridad. "*1. La categoría de seguridad de un sistema de información modulará el equilibrio entre la importancia de la información que maneja y los servicios que presta y el esfuerzo de seguridad requerido, en función de los riesgos a los que está expuesto, bajo el principio de proporcionalidad*". **Artículo 41.** Facultades. "*1. La facultad para efectuar las valoraciones a las que se refiere el artículo 40, así como, en su caso, su posterior modificación, corresponderá al responsable o responsables de la información o servicios afectados. 2. Con base en las valoraciones señaladas en el apartado anterior, la determinación de la categoría de seguridad del sistema corresponderá al responsable o responsables de la seguridad*". **[mp.info.2.2]** La política de seguridad establecerá quién es el responsable de cada información manejada por el sistema. **[mp.info.2.3]** La política de seguridad recogerá, directa o indirectamente, los criterios que, en cada organización, determinarán el nivel de seguridad requerido, dentro del marco establecido en el artículo 40 y los criterios generales señalados en el anexo I.

lista de chequeo 1		Salvaguarda de la Información Sensible		
			• Utilizando únicamente software específico, con funciones específicas de protección de información, para la generación, procesado y almacenamiento de la información sensible.	**[mp.info.2.4]** El responsable de cada información seguirá los criterios determinados en el apartado anterior para asignar a cada información el nivel de seguridad requerido, y será responsable de su documentación y aprobación formal.
1.4.	Principio de mínimo privilegio.	Cada persona autorizada sólo accede a la información que necesita conocer en el momento en que necesita conocerla.	Este principio se sustancia a través del establecimiento de categorías de autorizaciones de seguridad personales/individuales para el acceso a la información sensible.	**[op.acc.4.2]** Mínimo privilegio: los privilegios de cada entidad, usuario o proceso se reducirán al mínimo imprescindible para cumplir sus obligaciones o funciones. **[op.acc.4.3]** Necesidad de conocer y responsabilidad de compartir: los privilegios se asignarán de forma que las entidades, usuarios o procesos sólo accederán al conocimiento de aquella información requerida para cumplir sus obligaciones o funciones. La información es patrimonio de la Organización y toda aquella que resulte necesaria para el usuario estará a su disposición.
1.4.	Reglas de difusión. Protocolo de acceso y compartición.	En función del principio de mínimo privilegio, cada usuario conoce la clasificación de la información a la tiene acceso respecto de su nivel de sensibilidad. Además, debe ser consciente de que ha de cumplir unas reglas para compartir esa información sensible a la que está autorizado o autorizada a acceder. Esas reglas estarán basadas en un supuesto básico: no	La implantación de un protocolo de reglas de difusión de información sensible en un partido político tiene que desarrollarse a través de directrices procedimentales, que pueden complementarse con soluciones tecnológicas. Respecto de las directrices procedimentales, una vez el partido político ha establecido en sus estructuras internas un sistema de catalogación de la información en función de su sensibilidad, que incluya la gradación de autorizaciones a personas para acceder a los distintos niveles de información protegida, el paso siguiente es impartir al menos una jornada de sensibilización y capacitación en	**[org.3.4]** La forma en que se ha de tratar la información en consideración al nivel de seguridad que requiere, precisando cómo efectuar: a) Su control de acceso. b) Su almacenamiento. c) La realización de copias. d) El etiquetado de soportes. e) Su transmisión telemática. f) Cualquier otra actividad relacionada con dicha información. **[mp.si.1.1]** Los soportes de información (papel impreso, documentos electrónicos,

lista de chequeo 1		Salvaguarda de la Información Sensible		
		compartir etiquetada como sensible ("personal", "confidencial", "reservada" o "secreta"), ni siquiera entre personas con accesos autorizados, pues queda implícito que si esas personas han sido autorizadas a acceder a esa información ya tendrán conocimiento de ella sin que sea compartida por un usuario concreto. En cuanto a la información catalogada como de "difusión limitada", su catalogación habitualmente ya lleva explicitado con qué personas se puede compartir.	gestión de información sensible tanto a los cuadros del partido como a aquellos de sus integrantes más involucrados en el manejo de información de la institución. La capacitación de cuadros debería incluir la descripción del sistema de control de la difusión de información sensible, que puede estar basado únicamente en procedimientos, o estar apoyado en una solución tecnológica: 1) Si es procedimental, estará sustentado en etiquetar convenientemente los diferentes tipos de información sensible, y establecer instrucciones de compartición de cada tipo. 2) Si está apoyado por una solución tecnológica, el partido político habrá incorporado a sus sistemas informáticos una **herramienta de Gestión de Derechos de Información** (IRM, por sus siglas en inglés), que permite configurar diferentes niveles de protección de la información y discriminar a los diferentes usuarios del sistema en permisos de acceso, lectura, copia o compartición.	contenidos multimedia -vídeos, cursos, presentaciones- etc.) que contengan información que deba protegerse con medidas de seguridad específicas, llevarán las marcas o metadatos correspondientes que indiquen el nivel de seguridad de la información contenida de mayor calificación. **[mp.info.2]** Calificación de la información.
1.5.	Compartimentación, segmentación y securización perimetral de la información según su sensibilidad.	Una vez el partido político ha establecido un sistema de catalogación de información sensible y un protocolo de acceso y compartición de la información, asumiendo la premisa de que la mayor parte de la información actual de un	Con independencia de la arquitectura y tipología de bases de datos que el partido político haya elegido en su sistema informático de entre las variedades posibles, la segmentación de la información en función de su nivel de protección requerida (sensibilidad) implica la adopción de tres abordajes tecnológicos:	**[mp.com.1.1]** Se dispondrá de un sistema de protección perimetral que separe la red interna del exterior. Todo el tráfico deberá atravesar dicho sistema. **[mp.com.1.2]** Todos los flujos de información a través del perímetro deben estar autorizados previamente.

lista de chequeo 1		Salvaguarda de la Información Sensible		
		partido político es nativamente digital, la adecuada protección de esa información sugiere diseñar e implantar un sistema para almacenar y segmentar la información en función de su sensibilidad, siguiendo el paradigma de que a mayor sensibilidad mayor aislamiento en el almacenamiento, mayor capa de protección en el acceso, y mayor restricción en las autorizaciones.	1) **Creación de subredes** para conectar en ellas los equipos tecnológicos (por ejemplo, servidores) alojando las bases de datos almacenando diferentes tipos de información sensible. Por ejemplo, puede establecerse una subred a la que se encuentren conectados los equipos con las bases de datos que tiene que cumplir la legislación sobre protección de datos de carácter personal, y otra subred con bases de datos de información privada y de difusión limitada. Las subredes dedicadas a proteger información con las clasificaciones oficiales de "confidencial", "reservado" o "secreto" deben articularse como **Zonas de Acceso Restringido** (ZAR) según la orientación OR-ASIP-01-02.04 de la Oficina Nacional de Seguridad del Centro Nacional de Inteligencia de España. Estas ZAR, además del concepto de **Bases de Datos No-Conectadas** a redes alojadas en dispositivos aislados en lo que toca a seguridad digital, están diseñadas y protegidas por entornos específicos de seguridad perimetral y local específicos en el plano de la seguridad física. 2) **Protección perimetral de las subredes** con soluciones tipo cortafuegos a nivel de red y a nivel de aplicación (por ejemplo, en este último caso, para proteger los servidores de correo electrónico).	**[mp.com.4.1]** El tráfico por la red se segregará para que cada equipo solamente tenga acceso a la información que necesita. **[mp.com.3.1]** En comunicaciones con puntos exteriores al dominio propio de seguridad, se asegurará la autenticidad del otro extremo del canal de comunicación antes de intercambiar información.
1.6.	Cifrado de información sensible.	En principio, y salvo que concurran vulnerabilidades, errores de configuración o fallos	Hay numerosas soluciones comerciales para el cifrado normalizado de información digital, desde las propiamente embebidas en los sistemas	**[mp.si.2]** Criptografía. Esta medida se aplica, en particular, a todos los dispositivos removibles cuando salen de un área

lista de chequeo 1		Salvaguarda de la Información Sensible		
		humanos, la encriptación de la información mediante algoritmos robustos de cifrado es una solución eficaz para protegerla contra su acceso indebido. Por definición, pues, la recomendación sobre la información digital sensible, con independencia de la arquitectura tecnológica que aloje su almacenamiento, de las reglas que protejan su acceso, y de los protocolos que regulen su difusión, es que esté cifrada en su almacenamiento y sea cifrada en su compartición.	operativos, pasando por las aplicaciones software específicamente desarrolladas para el encriptado de información. Cualquiera de las soluciones por las que se opte, tres son los elementos que se sugiere sean capaces de desplegar: 1) **Cifrado de la información sensible almacenada en bases de datos**. Con independencia de la naturaleza de la base de datos y del nivel de la información sensible, el cifrado de la información almacenada garantiza que, aunque un atacante llegue a penetrar el sistema donde está alojada la base de datos y logre acceso a la base de datos, será incapaz de leer la información encriptada si previamente no se ha apropiado de la clave de descifrado. 2) Cifrado de los canales de acceso a la información a través del uso de **Redes Privadas Virtuales** (VPN) para entrar en subredes privilegiadas. 3) **Cifrado desde origen a destino**. Además de la encriptación de la información almacenada en bases de datos de información sensible, está recomendado que los usuarios que envían y reciben información sensible de los partidos políticos la encripten antes de compartirla, y la desencripten cuando la reciben de otro usuario. Esta recomendación implica que los usuarios tengan instaladas en sus dispositivos aplicaciones software de cifrado-descifrado de información basadas en **criptografía asimétrica de clave pública**.	controlada. Se entenderán por dispositivos removibles, los CD, DVD, discos extraíbles, pendrives, memorias USB u otros de naturaleza análoga. **[mp.si.2.1]** Se usarán mecanismos criptográficos que garanticen la confidencialidad y la integridad de la información contenida [en los soportes y dispositivos removibles]. **[mp.eq.3.r1.1]** Se protegerá el dispositivo portátil mediante cifrado del disco duro cuando el nivel de confidencialidad de la información almacenada en el mismo sea de nivel MEDIO. **[mp.com.2.1]** Se emplearán redes privadas virtuales cifradas cuando la comunicación discurra por redes fuera del propio dominio de seguridad.

lista de chequeo 1		Salvaguarda de la Información Sensible		
1.7.	Copias de respaldo de la información sensible.	Una medida de seguridad intrínseca a la protección de la información sensible viene de la mano de mantener actualizada y asegurada una copia de respaldo de esa información. La copia de respaldo garantiza la integridad de la información sensible en casos de borrado o destrucción intencionada (por ejemplo, mediante un *ransomware*) o accidental del todo o de partes de esa información. La manera de garantizar que, aunque una acción intencionada o accidental, dañara permanentemente los sistemas software y/o hardware de un partido político, la información sensible podría recuperarse, es que las copias de respaldo sean **almacenadas y gestionadas en alojamientos tecnológicos independientes** de la tecnología administrativa principal del partido político.	Los parámetros por los que debería regirse un sistema de copia de respaldo de información sensible que garantice la seguridad, la integridad, y la resiliencia de la información son: 1) **Implicación tanto de la organización como de los usuarios**. No sólo el departamento tecnológico del partido político debería estar involucrado en la gestión y mantenimiento de las operaciones de copia de respaldo de la información almacenada en bases de datos o alojamientos comunes, sino que debería implantarse un conjunto de reglas internas, que puede articularse a través de avisos personalizados a los dispositivos individuales de los usuarios, para que los usuarios individuales realicen copias de respaldo mediante procedimientos seguros del contenido de los dispositivos corporativos que tiene bajo usufructo. 2) **Sistematización periódica de la copia**. Arbitrando herramientas tecnológicas que automaticen procedimientos de copia continuada de forma que permita al partido político disponer de un estado, almacenado y asegurado contra borrado y/o destrucción, lo más actualizado posible, de su información sensible. 3) **Cifrado de canales, contenidos y repositorios finales**. Proteger mediante tecnología criptográfica los canales mediante los que se transmite la copia de respaldo, así como la integridad y el acceso de la	**[mp.info.6.1]** Se realizarán copias de seguridad que permitan recuperar datos perdidos, accidental o intencionadamente. La periodicidad y los plazos de retención de estas copias de seguridad se determinarán en la normativa interna de la organización relativa a copias de seguridad. **[mp.info.6.2]** Los procedimientos de respaldo establecidos indicarán: a) Frecuencia de las copias. b) Requisitos de almacenamiento en el propio lugar. c) Requisitos de almacenamiento en otros lugares. d) d) Controles para el acceso autorizado a las copias de respaldo. **[mp.info.6.r1.1]** Los procedimientos de copia de seguridad y restauración deben probarse regularmente. Su frecuencia dependerá de la criticidad de los datos y del impacto que cause la falta de disponibilidad. **[mp.info.6.r2.1]** Al menos, una de las copias de seguridad se almacenará de forma separada en lugar diferente, de tal manera que un incidente no pueda afectar tanto al repositorio original como a la copia simultáneamente.

lista de chequeo 1		Salvaguarda de la Información Sensible		
			información sensible almacenada en su repositorio correspondiente. 4) Almacenamiento final alojado en **sistemas aislados de la red pública y protegido mediante accesos privilegiados y cifrado robusto**. En la medida en que la copia de seguridad involucre información protegida por zonas ZAR, la copia de seguridad debe igualmente alojarse en una zona ZAR.	
1.8.	Legislación de protección de datos de carácter personal.	Cualquiera que sea el sistema implantado en un partido político para proteger la información sensible, tiene que incorporar los procedimientos y tecnologías necesarios para dar cumplimiento a las prescripciones que, como sujeto obligado, vienen derivadas de la Ley Orgánica de Protección de Datos Personales y Garantía de Derechos Digitales, así como de cualquier legislación sobre protección de datos de carácter personal.	La legislación sobre protección de datos de carácter personal contiene provisiones específicas sobre tratamiento, almacenamiento, protección, acceso, y compartición del dato de carácter personal que son de obligado cumplimiento. A partir de esas provisiones, en lo que tienen que ver con la consideración de los datos de carácter personal como información sensible, se recomienda, al menos: 1) El almacenamiento cifrado de los datos de carácter personal. 2) La protección de bases de datos contiendo datos de carácter personal en subredes segmentadas provistas de seguridad digital perimetral. 3) El establecimiento de una política de accesos específica, tecnológicamente definida por accesos criptográficos (certificados digitales y/o VPN) y	**[mp.info.1.1]** Cuando el sistema trate datos personales, el responsable de seguridad recogerá los requisitos de protección de datos que sean fijados por el responsable o por el encargado del tratamiento, contando con el asesoramiento del DPD, y que sean necesarios implementar en los sistemas de acuerdo a la naturaleza, alcance, contexto y fines del mismo, así como de los riesgos para los derechos y libertades de acuerdo a lo establecido en los artículos 24 y 32 del RGPD, y de acuerdo a la evaluación de impacto en la protección de datos, si se ha llevado a cabo. Debe recordarse la Disposición adicional primera de la LOPD-GDD que determina emplear las medidas de seguridad del ENS para proteger la información de carácter personal. Asimismo, cabe recordar que un partido político puede tratar categorías especiales de datos, según los determina el artículo 9 de la LOPD-GDD y el artículo 9 del

lista de chequeo 1		Salvaguarda de la Información Sensible		
			autenticaciones multifactor para usuarios autorizados.	RGPD, en cuánto así se consideran las 'opiniones políticas' de afiliados y simpatizantes. **[op.exp.7]** Gestión de incidentes. **[op.exp.7.2]** La gestión de incidentes que afecten a datos personales tendrá en cuenta lo dispuesto en el Reglamento General de Protección de Datos; la Ley Orgánica 3/2018, de 5 de diciembre, en especial su disposición adicional primera, así como el resto de normativa de aplicación, sin perjuicio de los requisitos establecidos en este real decreto.

3.2 PROTOCOLOS DE ACCESO A LA INFORMACIÓN

3.2.1 Establecimiento de protocolos corporativos de accesos y contraseñas

Puesto que los partidos políticos, como cualquier otra organización informatizada, son actualmente indisociables de una indudable realidad corporativa involucrada en la generación, almacenamiento, gestión, distribución y comunicación de contenidos digitales de diferente grado de sensibilidad (una gradación en la "necesidad de conocer"), el acceso a esa gradación de información debería estar regulado por una política institucional o corporativa.

La sensibilidad de la información es inherente a y queda definida por la protección de su contenido en lo que tenga de accesible por personas o dispositivos gestionados por personas. Por tanto, al final, aparte de por el etiquetado que cada pieza de información lleve en sí mismo en función de las restricciones a su conocimiento por parte de personas, la sensibilidad de la información se articula por los accesos que se autorizan para ser conocida.

En un partido político, la política corporativa de accesos a la información se basaría en el ya mencionado **principio de mínimo privilegio**, que se sustancia en que cualquier usuario tiene concedido los permisos que son mínimamente indispensables para conocer la información que debe conocer por la responsabilidad, función, mandato u obligación que ese usuario desempeña institucionalmente en el partido político. Según este principio, nadie debería tener permisos para acceder a información que no sea indispensable que conozca, todo ello en función de cada momento y circunstancia. Esos permisos, además, serían graduados en función de las conductas que están autorizadas para cada pieza de información: por ejemplo, es posible que una persona tenga permisos de acceso para consultar una determinada información en un momento concreto, pero no en otro; o que otra persona tenga derecho de consulta, pero no de descarga ni de copia; o que un usuario tenga derecho de descarga de un documento, pero no de compartición. Una política institucional de accesos a información debería contemplar esos dos ejes paramétricos:

1) qué información está cada usuario autorizado a acceder;

2) qué le está permitido hacer y qué no con esa información que está autorizado a acceder.

A partir del sistema tecnológico de creación, procesamiento y almacenamiento de la información sensible, y los protocolos definidos para su gestión, el partido político debería diseñar e implantar una política de control de accesos a la información que asegure que cada usuario accede únicamente a la información que debe conocer, en el momento en que la debe conocer, y con los permisos de uso que está autorizado a tener.

lista de chequeo 2		Política de Control de Accesos a la Información		
nº	BUENA PRÁCTICA	PROPÓSITO	CARACTERÍSTICAS	VINCULACIÓN CON EL ENS
2.1.	Diseño de una arquitectura de control de accesos basada en el principio de **confianza cero**.	El planteamiento de una arquitectura de control de accesos es asumir que la infraestructura informática de un partido político tiene una multiplicidad de componentes (dispositivos, servidores, servicios digitales), cada uno de los cuales está dotado de diferente nivel de protección, y la mayoría está conectados a algún tipo de red informática, ya sea restringida, local o pública. A esa heterogeneidad de componentes electrónicos e informáticos se conectarán de manera continuada tanto personas como otros dispositivos. Asegurar el sistema y minimizar los riesgos de uso no autorizado, o de vulneración forzada de cualquier dispositivo o servicio dentro del sistema, requiere, asumir una conciencia institucional de regulación de los accesos para establecer distintos niveles de autorización tanto para personas conectando con dispositivos electrónicos, como para dispositivos conectados entre sí. La idea de la confianza cero consiste en asumir que habrá personas externas al partido político y con intenciones maliciosas que planificarán e intentarán acciones de penetración forzada de servicios digitales, dispositivos, o servidores para, sin autorización para ello, acceder a información sensible almacenada en los sistemas informático del partido político y/o	La arquitectura de control de accesos puede desarrollarse a través de varias combinaciones de posibilidades, entre ellas los: 1) Sistemas de acceso mediante Inicios de Sesión Únicos (SSO), que enrutan al usuario a los servicios y servidores a los que tiene acceso en función de su credencial de autenticación. 2) Sistemas de accesos múltiples federados a través de estándares de identificación como el OpenID. 3) Sistemas de accesos múltiples con distintos protocolos y formas de autenticación.	**[op.acc.4.1]** Todo acceso estará prohibido, salvo autorización expresa. **[op.acc.1.r1.2]** Los datos de identificación serán utilizados por el sistema para determinar los privilegios del usuario conforme a los requisitos de control de acceso establecidos en la documentación de seguridad. **[op.acc.1.r1.3]** Se asegurará la existencia de una lista actualizada de usuarios autorizados y mantenida por el administrador del sistema/de la seguridad del sistema.

lista de chequeo 2		Política de Control de Accesos a la Información		
		comprometer el normal funcionamiento de esos sistemas. Puesto que se asume esta posibilidad, los protocolos de control de accesos se basarían en que no se confía en ningún dispositivo ni en ninguna persona que pretenda realizar una conexión a cualquier punto del sistema informático del partido político sin seguir los procedimientos de acreditación habilitados para ser autorizado. Por tanto, si no es un dispositivo o una persona de confianza (acreditada y autenticada por el sistema), se los bloquea y se emite una alerta de seguridad al departamento responsable de la seguridad de la información en el partido político.		
2.2.	Establecimiento de un sistema de autorizaciones personales de accesos basado en el principio de **mínimo privilegio**.	En cualquiera de las elecciones adoptadas sobre un modelo de arquitectura de control de accesos en el sistema informático de un partido político, de las cuales varias pueden convivir varios modelos en un mismo sistema, el principio rector es que exista una **gradación de autenticaciones para los usuarios en función de las autorizaciones individuales** que cada uno tenga de acceso a la información, o a los dispositivos, servidores y servicios, bajo gobernanza del partido político. Si la arquitectura informática del control de accesos debería estar regida por la confianza cero, la concesión de autorizaciones de acceso para usuarios individuales debería fundarse en el mínimo privilegio: cada usuario sólo accede	Los protocolos de autorizaciones de accesos deberían otorgar a los usuarios del sistema informático del partido político credenciales de autenticación para identificarse ante los distintos dispositivos, servidores, subsistemas o servicios digitales, conectados a cualquier red, atendiendo a los siguientes parámetros: 1) Las credenciales de autenticación son entidades de doble sentido: acreditan al usuario ante una puerta, pero al mismo tiempo la puerta debe de estar configurada para identificar unívocamente al usuario.	**[op.acc.1.3]** Cada entidad (entidad, usuario o proceso) que accede al sistema, contará con un identificador singular que permita conocer el destinatario de los mismos y los derechos de acceso que recibe, así como las acciones realizadas por cada entidad. **[op.acc.6]** mecanismo de autenticación (usuarios de la organización)

lista de chequeo 2		Política de Control de Accesos a la Información		
		a la información, los dispositivos, servidores y servicios digitales que sean necesarios para que cumpla la función que ese usuario tenga asignada en el partido político, a ninguna pieza de información más de las que tenga necesidad de conocer ni a ninguna menos.	2) La autenticación de usuarios tiene una forma o diseño tecnológico, que puede ser unidimensional o multidimensional, entre las siguientes formas: i. Tarjeta hardware que mediante cualquier tecnología (chip, NFC u otra) utiliza una clave criptográfica para acceder a otro dispositivo hardware. ii. Lectura biométrica, mediante un dispositivo que digitalice una característica biofísica del usuario y la acredite ante un dispositivo hardware de lectura de esa digitalización. iii. Contraseñas tecleadas, o introducidas de otra manera, en una interfaz tecnológica. iv. Certificados criptográficos (por ejemplo, TLS) expedidos al individuo. Por encima de cualquiera de las modalidades que se opte de	

			protocolo de autorizaciones de acceso, una capa de protección recomendada para el acceso digital de personas a cualquier punto del ecosistema informático de un partido político es la **autenticación multifactor**, es decir, que en la identificación ante el sistema tecnológico el usuario tenga que aportar varios factores de autenticación distintos entre sí: una contraseña, una tarjeta y un certificado TLS; una contraseña y la validación del acceso mediante un SMS a su teléfono móvil; o una interfaz biométrica y un SMS, entre los ejemplos posibles. La autenticación multifactor previene que, si un atacante ha logrado robar la contraseña de acceso de un usuario a un servicio o dispositivo, la autenticación de ese atacante sea posible al carecer del resto de factores de autenticación. Los procedimientos y las tecnologías de un sistema de autorizaciones personales de accesos no deberían ir desligados, sino que tendrían que incorporar intrínsecamente, la vinculación entre las credenciales de acceso y los **permisos de uso** del	

lista de chequeo 2		Política de Control de Accesos a la Información		
			usuario respecto de la información que está autorizado a acceder. Esta interdependencia entre credenciales de acceso y permisos de uso puede ejecutarse tecnológicamente a través de distintas opciones, por ejemplo, mediante las ya mencionadas herramientas de **Gestión de Derechos de Información** (IRM).	
2.3.	Modelo seguro de configuración de entornos compartidos.	En todas las organizaciones con infraestructuras informáticas en donde distintas personas desarrollan labores diferentes empleando las mismas aplicaciones software, existe la concurrencia de una carga constante de usuarios operando sobre los mismos recursos. En lo que al trabajo sobre ficheros y carpetas de ficheros se refiere, la solución más extendida es desplegar entornos de trabajo compartido, en donde cada usuario lleva aparejados permisos para realizar un conjunto de operaciones tasadas sobre los entornos compartidos.	Está recomendado que el administrador de los entornos compartidos defina con claridad las reglas de compartición de ficheros, limitando la carga, por parte de usuarios, de ficheros ejecutables, de sistema o con capacidad programable para contener código ejecutable, si no han sido revisados antes por filtros de análisis de malware. Los entornos personales de cada usuario deben estar compartimentados del resto de usuarios, y dotados de acceso por autenticación individual. En los entornos donde se gestione información sensible, la autenticación individual debería realizarse por acceso multifactor.	**[op.acc.2.r1.1]** Todos los usuarios autorizados deben tener un conjunto de atributos de seguridad (privilegios) que puedan ser mantenidos individualmente. **[op.acc.2.r1.2]** Los privilegios de acceso se implementarán para restringir el tipo de acceso que un usuario puede tener (lectura, escritura, modificación, borrado, etc.). **[op.acc.6]** mecanismo de autenticación (usuarios de la organización)

lista de chequeo 2		Política de Control de Accesos a la Información		
2.4.	Protección aumentada contra accesos no autorizados y/o irregulares. Prevención de intrusiones.	Un complemento óptimo de ciberseguridad para sistemas tecnológicos que albergan y gestionan información sensible viene definido por herramientas que analizan si se están produciendo intentos de acceso no autorizado a los sistemas, o cualquier otro comportamiento irregular en el perímetro de esos sistemas que sugiera que un atacante o actor malicioso está intentando penetrarlos ilegítimamente o por la fuerza. La idea básica tras estas herramientas de análisis, detección y prevención de intrusiones es que la misma implantación de un sistema de control de accesos para los usuarios propios, debería conllevar algún mecanismo no sólo para rechazar, sino también para mantenerse alerta, sobre los intentos maliciosos o amenazantes de conectarse y acceder al sistema tecnológico que se trata de securizar.	Como paso previo a la implantación de un sistema de prevención de intrusiones, está aconsejado que en los dispositivos, servidores y servicios digitales considerados más críticos por la función que realicen en la infraestructura informática, o por su papel en la gestión de información sensible, el control de accesos esté incrementado en seguridad mediante **listas blancas** de usuarios y dispositivos autorizados a conectar con el sistema, denegándose o bloqueándose automáticamente cualquier acceso de usuarios que se identifiquen ante el sistema con un parámetro que no sea el incluido en la lista blanca. Así mismo, que los usuarios de la lista blanca tengan un proceso de autenticación reforzada con multifactor, añadiendo a las credenciales de autenticación un certificado TLS o un mecanismo adicional de validación de la identidad. En lo que se refiere concretamente a los **sistemas de prevención de intrusiones** (IPS, por sus siglas en inglés), se trata de instalar y configurar herramientas que realizan un análisis en tiempo real de los registros de conexión en los diversos	**[op.mon.1.1]** Se dispondrá de herramientas de detección o prevención de intrusiones. **[op.mon.1.r2.1]** Existirán procedimientos de respuesta a las alertas generadas por el sistema de detección o prevención de intrusiones **[op.mon.3.1]** Se dispondrá de un sistema automático de recolección de eventos de seguridad.

			protocolos software que gestionan los accesos a dispositivos, servidores y servicios corporativos conectados a redes. A partir de ese análisis, estas herramientas proporcionan a los departamentos de seguridad en la información un diagnóstico de anomalías, patrones o comportamientos sospechosos, produciendo alertas cuando sea necesario, y efectuando acciones programadas, con reglas prefijadas por los administradores del sistema, de respuesta a esos patrones de comportamiento sospechoso: por ejemplo, en los ataques por fuerza bruta o los ataques de diccionario contra una puerta digital de acceso a un servicio corporativo (p.ej. el servidor de correo electrónico), donde el atacante realiza múltiples intentos sistemáticos de inserción de usuarios y contraseñas para probar si alguno de esos intentos funciona y abre la puerta, un sistema de prevención de intrusiones detecta el comportamiento como anómalo y a la vez amenazante, y bloquea los intentos del atacante, a la vez que emite una alerta al departamento de seguridad. Existen soluciones comerciales software previstas para ser instaladas como sistemas de	

lista de chequeo 2		Política de Control de Accesos a la Información		
			prevención de intrusiones en infraestructuras tecnológicas con controles reforzados de accesos. En numerosas instalaciones de software de prevención de intrusiones se combinan o integran estas herramientas con **cortafuegos** (*firewall* en su denominación en inglés) que protegen el perímetro, por ejemplo, de un servicio digital que, debido a su participación en la gestión de información sensible, está segmentado en una subred de la infraestructura tecnológica. Los cortafuegos son soluciones software que, a través de reglas programadas, filtran conexiones sospechosas de ser maliciosas y les deniegan el acceso.	

3.2.2 Buenas prácticas para la gestión de contraseñas por usuarios

Aunque la contraseña sea un método más de entre los diversos que pueden servir como mecanismo de autenticación de personas ante dispositivos o servicios digitales, es el más extendido en uso y el más popularmente conocido. Desde acceder inicialmente al ordenador de sobremesa o el portátil, pasando por el teléfono móvil, o conectarse al correo electrónico a través de la web o una cuenta en redes sociales, las contraseñas son empleadas por un usuario medio innumerables veces a lo largo de cada día. Consiguientemente, el robo de credenciales de autenticación de usuarios ante accesos digitales conectados a redes informáticas es una de las prácticas cibercriminales más extendidas.

Las credenciales de autenticación robadas, generalmente compuestas de una denominación o código de usuario (que puede ser un alias, un nombre o una dirección de correo electrónico, entre otras) emparejada a una contraseña, son utilizadas por ciberamenazas para acceder

ilegalmente a servicios y dispositivos digitales y realizar en ellos una amplia diversidad de conductas ilícitas, desde implantar código informático dañino con fines de lucro, extorsión o sabotaje, hasta mantener el acceso forzado para ir robando información del dispositivo o servicio digital comprometido con propósitos de ciberespionaje. La compraventa de contraseñas emparejadas en credenciales de autenticación es uno de prácticas que más actividad tiene en los mercados negros cibercriminales, junto a la compraventa de números de tarjetas bancarias o credenciales de autenticación en banca online y a la compraventa de código dañino.

Por tanto, integrada en la política de control de accesos a la información, está recomendado que los partidos políticos incluyan en ella procedimientos y reglas para que los usuarios de sistemas informáticos que formen parte de la infraestructura del partido cumplan una serie de buenas prácticas en la gestión y uso de contraseñas en credenciales de autenticación de acceso a dispositivos y servicios digitales. Esos procedimientos y reglas deberían ser parametrizados por los administradores de los sistemas informáticos de manera que obliguen a los usuarios a su aplicación, e impidan a cualquier usuario continuar procesos donde las buenas prácticas sobre contraseñas no hayan sido seguidas individualmente.

lista de chequeo 3		**Uso de contraseñas**		
nº	BUENA PRÁCTICA	PROPÓSITO	CARACTERÍSTICAS	VINCULACIÓN CON EL ENS
3.1.	Crear contraseñas robustas en forma y longitud. **Obligación de la forma**.	Hay tres formas generales de que un atacante suplente la contraseña de una persona victimizada: 1) robar esa contraseña mediante cualquier procedimiento; 2) adivinarla; 3) generarla mediante procedimientos de cálculo. La forma de las contraseñas incide directamente en prevenir dos de esos métodos de ataque, la adivinación o los procedimientos de cálculo. Cuanto más **robusta** sea la forma de una contraseña,	En términos generales, la robustez de una contraseña de texto está directamente relacionada con la aleatoriedad y con la longitud de su forma: a más aleatoriedad y longitud, mayor seguridad de la contraseña. Una contraseña robusta es la que cumple las siguientes condiciones, que las políticas de control de accesos de las organizaciones políticas deberían implantar como obligación en el momento de que un usuario está generando una contraseña para establecer sus credenciales de autenticación: a) Es secreta: el usuario no las comparte con nadie y no las anota en ninguna parte para recordarlas.	**[op.acc.6.7]** Antes de autorizar el acceso, la información presentada por el sistema será la mínima imprescindible para que el usuario se autentique, evitando todo aquello que pueda, directa o indirectamente, revelar información sobre el sistema o la cuenta, sus características, su operación o su estado. **[op.acc.6.8]** El número de intentos permitidos será limitado, bloqueando la oportunidad de acceso una vez superado tal número, y requiriendo una intervención específica para reactivar la cuenta, que se describirá en la documentación. **[op.acc.6.r1.2]** Se impondrán normas de complejidad mínima y robustez frente a ataques de adivinación

lista de chequeo 3		Uso de contraseñas		
		menos probabilidad existe de que un atacante pueda adivinarla o de que, a través de potencia computacional, pueda generar una contraseña que sea igual que la del usuario al que se intenta victimizar. Es decir, una contraseña robusta es menos vulnerable a quedar comprometida en un ciberataque.	b) Tiene más de 12 caracteres. c) Los caracteres son alfanuméricos. d) Introducir caracteres especiales. e) No son palabras reconocibles. f) No son datos personales del usuario. g) A pesar de su complejidad, deberían poder recordarse. Métodos que hacen posibles contraseñas complejas que sean recordadas son los acrósticos (elegir una frase larga, quedarse con las iniciales de las palabras que componen esa frase, y éstas serán la contraseña) o las frases sin sentido, con caracteres alfanuméricos en mayúsculas y minúsculas (por ejemplo, "la b4llen4 Volaba p0r la #lmuadilla sin N3cesidad de $olares en los Zapat0S").	**[op.acc.6.r5.1]** Se registrarán los accesos con éxito y los fallidos. **[op.acc.6.r5.2]** Se informará al usuario del último acceso efectuado con su identidad. **[op.acc.6.r8.1]** Para el acceso desde o a través de zonas no controladas se requerirá un doble factor de autenticación.
3.2.	Implantar caducidad y renovación obligatorias. **Obligación de la temporalidad**.	Aunque una contraseña sea robusta en cuanto a su forma, cuanto más tiempo esté en vigor siendo utilizada rutinariamente por un usuario, mayor probabilidad es de que la contraseña, por descuido o por otras circunstancias accidentales inherentes a la	Las herramientas de administración de contraseñas del partido político deberían estar configurados para anular cualquier contraseña que no haya sido renovada en un plazo concreto de tiempo. Los plazos de tiempo más habituales para la caducidad de contraseñas son el año o, si se pretende ser más restrictivo, los seis meses.	**[op.acc.6.4]** Las credenciales se cambiarán con una periodicidad marcada por la política de seguridad de la organización. **[op.acc.6.r7.1]** Las credenciales se suspenderán tras un periodo definido de no utilización.

lista de chequeo 3		Uso de contraseñas		
		rutina, quede expuesta (por ejemplo, quede copiada en el portapapeles a la vista en la pantalla de un dispositivo) y sea divulgada.	El procedimiento de renovación de contraseña podría seguir la siguiente secuencia: 1) Una semana antes de la caducidad de la contraseña, se advierte al usuario de que su contraseña está a punto de caducar, ofreciéndole la posibilidad de cambiarla en ese momento por otra contraseña que cumpla los requisitos de forma establecidos. 2) Cuando llegue el momento de la caducidad, el procedimiento impide que el usuario se autentique hasta que actualice la contraseña.	
3.3.	Aseguramiento de las contraseñas.	De poco serviría que una contraseña fuera robusta si no se mantiene en secreto, es decir, garantizando que es únicamente el usuario que la ha creado la persona que la conoce. Una contraseña personal de un usuario individual no debe ser compartida ni publicada, y no debe ser conocida por los administradores de los sistemas informáticos en donde el usuario la utiliza como método de autenticación.	Como requisito para mantener la privacidad de las contraseñas de usuarios individuales en sistemas informáticos corporativos, las herramientas de gestión de contraseñas corporativas deben contar un **procedimiento de cifrado de la contraseña punto a punto**, desde el momento de su creación hasta su almacenamiento en un lugar seguro de la base de datos de contraseñas corporativas. Este procedimiento cifrado implica que el literal de la contraseña está protegido en cuanto se crea, sólo es visto por el usuario que la crea, y se transporta y almacena cifrado para cualquier persona distinta, incluyendo a técnicos y administradores del sistema informático. Todos los sistemas operativos actualmente empleados en sistemas informáticos de usuario ya incorporan nativamente herramientas para realizar estas funciones en los subsistemas de gestión de identidades de usuario.	**[op.acc.6.1]** Antes de proporcionar las credenciales a los usuarios, estos deberán conocer y aceptar la política de seguridad del organismo en los aspectos que les afecten. **[op.acc.6.2]** Antes de activar el mecanismo de autenticación, el usuario reconocerá que ha recibido las credenciales de acceso y que conoce y acepta las obligaciones que implica su tenencia, en particular, el deber de custodia diligente, la protección de su confidencialidad y el deber de notificación inmediata en caso de pérdida. **[op.acc.6.3]** Las credenciales estarán bajo el control exclusivo del usuario y se activarán una vez estén bajo su control efectivo. **[mp.eq.3.4]** Se evitará, en la medida de lo posible, que el dispositivo portátil contenga claves de acceso remoto a la organización que no sean imprescindibles. Se considerarán

lista de chequeo 3	Uso de contraseñas			
			En lo que tiene que ver con el usuario, el aseguramiento del carácter privado o secreto de la contraseña se logra, principalmente, **memorizando la contraseña**, sin compartirla, anotarla o divulgarla en ningún caso. Como alternativa menos segura a la memorización, aunque aceptable si se cumple una seguridad reforzada, están las herramientas software de gestión de contraseñas, los llamados “gestores de contraseñas”, que se utilizan como una caja fuerte digital para el almacenamiento de las distintas contraseñas que un usuario emplea para acceder a distintos dispositivos, sistemas, servidores o servicios corporativos. Hay disponibles diferentes soluciones comerciales de **gestores de contraseñas**. Para elegir uno de ellos, hay que asegurarse de que se trata de un software desarrollado por un fabricante conocido y acreditado que se ocupe de mantener y evolucionar el software; y que no se han reportado vulnerabilidades de seguridad continuadas y/o graves sobre esa herramienta software y, si lo han sido, que se han solventado con rapidez y eficacia por el fabricante. En cualquiera de los casos, si corporativamente se emplean gestores de contraseñas para su implementación por usuarios individuales, está recomendada su seguridad reforzada a través del procedimiento de autenticación del usuario en el gestor de contraseñas mediante el **mecanismo de factor múltiple**.	claves de acceso remoto aquellas que sean capaces de habilitar un acceso a otros equipos de la organización u otras de naturaleza análoga.

lista de chequeo 3		Uso de contraseñas		
			Está desaconsejado el almacenamiento de contraseñas en los navegadores web.	
3.4.	Selectividad de las contraseñas.	Aunque las contraseñas de autenticación en sistemas informáticos sean robustas y renovables, la utilización de una misma contraseña por parte de un usuario para autenticarse en distintos dispositivos, servidores o servicios corporativos, aunque todos ellos formen parte de la misma infraestructura informática, incrementa la debilidad de todas las credenciales de autenticación asociadas a esa contraseña. En concreto, posibilita que, si la contraseña quedara comprometida o expuesta, podrían producirse accesos no autorizados con esa contraseña a todos los dispositivos, servidores y servicios corporativos del usuario, y no sólo a uno. De hecho, una tipología de ataque llevado a cabo extensivamente por ciberamenazas es el denominado "**rellenado**" o	Al menos en dispositivos, servicios y servidores de la infraestructura informática de los partidos políticos, debe implantarse la obligación, para los usuarios, de la selectividad de cada contraseña: una contraseña distinta para cada dispositivo, servicio o servidor donde el usuario tenga credenciales de autenticación autorizadas para acceder. Puede mantenerse la misma denominación del usuario para todas las puertas digitales de la infraestructura informática del partido político a la que el usuario esté autorizado a entrar, pero para cada puerta distinta la contraseña debe de ser diferente.	**[mp.per.3]** Concienciación. Se realizarán las acciones necesarias para concienciar regularmente al personal acerca de su papel y responsabilidad para que la seguridad del sistema alcance los niveles exigidos. En particular, se recordará periódicamente: **[mp.per.3.1]** La normativa de seguridad relativa al buen uso de los equipos o sistemas y las técnicas de ingeniería social más habituales.

lista de chequeo 3		Uso de contraseñas		
		reutilización de contraseñas, que consiste en intentar autenticarse en todas las puertas de entrada visibles en Internet de una infraestructura informática con una única contraseña robada a un usuario.		
3.5.	Compartimentación de contraseñas profesionales o institucionales y personales.	Si la utilización de la misma contraseña para autenticarse en varios servicios, servidores y dispositivos informáticos corporativos supone un riesgo, que un mismo usuario utilice contraseñas idénticas en servicios digitales personales, en su entorno profesional, y en el ecosistema informático de un partido político incrementa ese riesgo, puesto que hay una multitud de servicios digitales en los que un usuario puede estar registrado por intereses personales que tengan un seguridad de accesos mínima o deficiente, con la consiguiente probabilidad de que la contraseña (esa contraseña única) quede comprometida o expuesta.	Está recomendado impartir una instrucción de cumplimiento y sensibilización para los usuarios registrados en el sistema informático de un partido político, indicándoles que eviten utilizar, en el registro de sus credenciales de autenticación en cualquier dispositivo o servicio de ese sistema informático, las mismas contraseñas que hayan elegido para otros servicios digitales que utilicen en sus actividades personales o profesionales, por ejemplo cuentas en redes sociales o en servicios de correo electrónico gratuitos.	**[org.2]** Normativa de seguridad. Se dispondrá de una serie de documentos que describan: **[org.2.1]** El uso correcto de equipos, servicios e instalaciones, así como lo que se considerará uso indebido. **[org.2.2]** La responsabilidad del personal con respecto al cumplimiento o violación de la normativa: derechos, deberes y medidas disciplinarias de acuerdo con la legislación vigente. **[mp.per.3]** Concienciación. Se realizarán las acciones necesarias para concienciar regularmente al personal acerca de su papel y responsabilidad para que la seguridad del sistema alcance los niveles exigidos. En particular, se recordará periódicamente: **[mp.per.3.1]** La normativa de seguridad relativa al buen uso de los equipos o sistemas y las técnicas de ingeniería social más habituales.

lista de chequeo 3		Uso de contraseñas		
3.6.	Sistema corporativo de administración de contraseñas.	Como parte de la política de seguridad de la información en un partido político, los responsables de control de accesos deberían tener implantado un sistema corporativo de administración de contraseñas que les permitiera obligar a los usuarios, por un lado, y verificar que esas obligaciones se han cumplido, por otro, respecto de los requisitos de una **contraseña robusta, temporal, selectiva y segura**. Debería arbitrarse un mecanismo para que, cuando un usuario nuevo llega a registrarse por primera vez en un servicio, servidor o sistema informático del partido político, tenga acceso y conozca todos los detalles de las políticas de control de accesos dentro de la ciberseguridad del partido político.	La administración de contraseñas debe impedir el registro de usuarios en sistemas, servidores y servicios corporativos con contraseñas que: a) Tengan una longitud menor de 12 caracteres. El sistema debería estar preparado para computar contraseñas hasta, al menos, 64 caracteres. b) Sean iguales o similares a una lista negra de contraseñas predefinidas por el administrador, y compuesta por las contraseñas más sencillas, las más conocidas, las fácilmente adivinables, o de las que el administrador tenga constancia que han sido divulgadas. c) Sean repetidas por haberlas utilizado antes el mismo usuario, o sean combinaciones literales de ellas. d) Estén caducadas por haber sido utilizadas más allá del límite marcado por la obligación de temporalidad. El sistema de verificación podría ofrecer al usuario preguntas de control para el recordatorio de la contraseña si la ha olvidado. Así mismo, y como parte de los protocolos de control de accesos, el sistema de verificación debe impedir que un usuario se autentique después de 3 intentos fallidos de introducir la contraseña: en tal	**[op.acc.5.r1.2]** Se impondrán normas de complejidad mínima y robustez frente a ataques de adivinación **[op.acc.6.r6.1]** Se definirán aquellos puntos en los que el sistema requerirá una renovación de la autenticación del usuario, mediante identificación singular, no bastando con la sesión establecida. **[mp.per.3]** Concienciación. Se realizarán las acciones necesarias para concienciar regularmente al personal acerca de su papel y responsabilidad para que la seguridad del sistema alcance los niveles exigidos. En particular, se recordará periódicamente: **[mp.per.3.1]** La normativa de seguridad relativa al buen uso de los equipos o sistemas y las técnicas de ingeniería social más habituales.

lista de chequeo 3	Uso de contraseñas			
			caso, aplica el bloqueo del usuario y una alerta al administrador del sistema, para evaluar la naturaleza del escenario (si se trata de un usuario o usuaria que ha olvidado su contraseña, o de intentos ilegítimos de acceso). Los usuarios administradores no deberían seguir esta directriz del bloqueo, para evitar situaciones que deriven en una denegación de servicio. Además, los administradores deberían disponer de herramientas de prueba y descifrado de las contraseñas, aplicados diariamente a todas las nuevas contraseñas generadas para comprobar si son resistentes a ataques por fuerza bruta (intentos informáticos de "adivinación" de la contraseña). Las contraseñas que no pasen esta prueba deben anularse, bloqueándose el registro del usuario hasta que ingrese una contraseña compatible con la política de ciberseguridad de la institución. Se recomienda establecer preguntas de verificación para el reseteo de contraseñas. En su caso, se recomienda un servicio que permita enviar al usuario un correo con un enlace para resetear la contraseña.	

3.3. PROTECCIÓN DE DISPOSITIVOS MÓVILES

Como en toda política de ciberseguridad que se implante en una organización, en este caso respecto del sistema informático de un partido político, en paralelo a cuestiones procedimentales y orgánicas son las directivas dirigidas a los usuarios y los programas de concienciación y capacitación del personal los ejes sobre los que se asentará una cultura organizativa sólida de ciberseguridad. Sin estos ejes, probablemente **la fortaleza del factor tecnológico se verá erosionada por la debilidad del factor humano**, y esa vulnerabilidad será la primera a explotar por las ciberamenazas.

Una buena parte del trabajo de sensibilización en ciberseguridad de los usuarios de sistemas informáticos, que preparará el camino para la adopción de una cultura tanto personal como corporativa de autoprotección en ciberseguridad, pasa por una adecuada **toma de conciencia sobre las interfaces tecnológicas**, sobre los dispositivos con los que un usuario está continuamente interactuando con la realidad digital. De estos dispositivos, son los equipos móviles, sobre todo los denominados teléfonos inteligentes, que habitualmente acompañan a una persona casi todas las horas de sus días, los que están actuando de verdaderos conectores continuados entre el mundo analógico y el digital a través de la persona.

Los actuales terminales de telefonía móviles hace tiempo que dejaron de ser única o principalmente teléfonos y, de hecho, en la vida habitual de muchos usuarios la función tradicional de telefonía a través de voz ha pasado a ser secundaria respecto de otras que el dispositivo tecnológico que incluye un teléfono está programado para desempeñar. Ahora, esos dispositivos son máquinas portátiles de computación que realizan una amplia variedad de funciones para ejercer de interfaz continuada de interacción entre una persona y una compleja infraestructura de servicios digitales.

Un usuario de un partido político provisto de un terminal informático portátil que incluya entre sus funciones la telefonía móvil, ya forme parte ese terminal del inventario del partido político como no, está interactuando mediante ese dispositivo tanto con sistemas informáticos propios del partido político como ajenos, todo ello en paralelo y al mismo tiempo, a través de diversos procedimientos de conexión y autenticación. En el supuesto más general de la mayoría de los usuarios, ese terminal está continuamente conectado a infraestructuras informáticas remotas a través de redes digitales.

Por tanto, la protección de los dispositivos móviles es un capítulo primordial de las políticas de ciberseguridad de una organización, y así debe ser objeto de provisiones específicas en el marco de la ciberseguridad de un partido político. Las dimensiones de riesgo asociadas a los dispositivos portátiles son variadas y proceden de la multifuncionalidad de esos aparatos, puesto que:

- Son almacenes de información. Si el dispositivo se pierde o es robado, expone esa información a terceros, en una medida que depende de si esa información está o no protegida con medidas adicionales.
- Son herramientas de comunicación que permiten al usuario entablar conversaciones de audio, videollamadas, o intercambiar mensajes en texto o multimedia a través de aplicaciones software. En la práctica totalidad de las ocasiones, esas comunicaciones se producen a través de la infraestructura de proveedores de servicios digitales y de telecomunicaciones que son externos a los partidos políticos. Las interacciones comunicacionales a través de dispositivos móviles implican generalmente que los mismos dispositivos son utilizados para cuestiones personales, profesionales e institucionales, con los riesgos (por ejemplo, la comisión de errores por parte del usuario) que podrían derivarse del uso de los distintos tipos de información almacenada.
- Son sistemas de geolocalización, que permiten a los proveedores de servicios digitales y de telecomunicaciones, en virtud de los contratos de servicio y de los términos y condiciones legales de uso del dispositivo, establecer un sistema de seguimiento y almacenamientos permanentes, presente e histórico, de la posición del dispositivo en el espacio y en el tiempo. Puesto que esos dispositivos son actualmente una compañía quasi-constante del usuario individual, el geoposicionamiento del dispositivo implica el geoposicionamiento del individuo.
- Son agendas personales digitales, donde constan un porcentaje significativo de relaciones personales, profesionales e institucionales provistas de sus datos identificativos personales en las aplicaciones software para la gestión de contactos personales. Las aplicaciones de calendario de muchos usuarios y usuarias contienen un diario de las actividades llevadas a cabo por la persona.
- Son diarios de vida personal y profesional a través de las aplicaciones de mensajería instantánea, de las aplicaciones de correo electrónico, y de las aplicaciones de redes sociales digitales, mediante las cuales se comparten continuamente contenidos tanto personales como profesionales e institucionales.
- Crecientemente, los dispositivos móviles son instrumentos de gestión de activos financieros, como interfaces con cuentas bancarias o diversos sistemas de pago digital.

Siendo así, la ciberseguridad de un partido político debería dotarse con medidas que supervisen y controlen cada uno de esos planos de riesgo potencial a través de provisiones específicas.

lista de chequeo 4		Control de dispositivos móviles		
nº	BUENA PRÁCTICA	PROPÓSITO	CARACTERÍSTICAS	VINCULACIÓN CON EL ENS
4.1.	Control de la ubicación física.	Todos los computadores informáticos portátiles de usuario, tabletas y teléfonos, con anecdóticas excepciones, disponen de dispositivos hardware y herramientas software para geolocalizar continuamente el dispositivo. Esa geolocalización implica, entre otras posibilidades, la situación del terminal informático en una trayectoria específica de antenas o repetidores de telefonía móvil, y también los servicios de geolocalización que una cantidad prácticamente completa de aplicaciones software instalada, sobre todo en teléfonos inteligentes, incorpora en los permisos que son otorgados por el usuario en el momento de instalar esas aplicaciones. Muchas de esas aplicaciones software incluso dejan de funcionar apropiadamente si el permiso de geolocalización es desactivado por el usuario. La geolocalización continuada y permanente de un dispositivo computacional que, como el teléfono portátil, está físicamente posicionado junto a su usuario,	En términos generales, para otorgar al usuario el máximo control posible de la información de geolocalización que proporciona a terceras partes, está recomendado que el usuario desactive la geolocalización de todas las aplicaciones software y dispositivos en la medida en que la desactivación de la función de geolocalización no impida la funcionalidad de aplicaciones o dispositivos que sean necesarios en cada momento para el usuario. Alternativamente, el usuario puede aprender a desactivar y activar la geolocalización a conveniencia en aplicaciones software dependiendo de si las está utilizando y necesita la geolocalización como una función necesaria de esa utilización, o no lo está haciendo, en cuyo caso la geolocalización puede estar desactivada.	**[op.exp.2.2]** Se aplicará la regla de «mínima funcionalidad», es decir: a) El sistema debe proporcionar la funcionalidad mínima imprescindible para que la organización alcance sus objetivos. b) No proporcionará funciones injustificadas (de operación, administración o auditoría) al objeto de reducir al mínimo su perímetro de exposición, eliminándose o desactivándose aquellas funciones que sean innecesarias o inadecuadas al fin que se persigue. **[op.exp.2.3]** Se aplicará la regla de «seguridad por defecto», es decir: a) Las medidas de seguridad serán respetuosas con el usuario y protegerán a éste, salvo que se exponga conscientemente a un riesgo. b) Para reducir la seguridad, el usuario tendrá que realizar acciones conscientes. c) El uso natural, en los casos que el usuario no ha consultado el manual, será un uso seguro.

lista de chequeo 4		Control de dispositivos móviles		
		supone que terceras partes (aquéllas a las que el usuario ha concedido permiso legal, vía aceptación de condiciones de servicio, para recibir datos de geolocalización) disponen de información cartográfica sobre movimientos del sujeto prácticamente en todos los momentos de su vida personal, profesional y de ocio. Con independencia de que esa información deba ser utilizada por esas terceras partes cumpliendo la legislación vigente, y con los contratos de prestación de servicios suscritos por el usuario con cada aplicación software y con la nueva activación de un dispositivo, las personas involucradas en actividad política deberían ser, al menos, conscientes de que esa geolocalización permanente se está produciendo.		
4.2.	Control del acceso al dispositivo.	Aunque dispositivos informáticos portátiles formen parte de la infraestructura tecnológica de un partido político, cuando están dedicados al usufructo por una persona individual debido a la función que esta persona desempeña, es esa persona	En dispositivos informáticos y teléfonos móviles portátiles que admiten una contraseña de autenticación o **PIN con formato alfanumérico**, se recomienda utilizarlo en detrimento del PIN de cuatro dígitos, siguiendo las mismas directrices que la contraseña: que sea un código de longitud mayor de 12 caracteres, que combine letras, números y caracteres especiales, y que no	**[mp.eq.2.1]** El puesto de trabajo se bloqueará al cabo de un tiempo prudencial de inactividad, requiriendo una nueva autenticación del usuario para reanudar la actividad en curso. **[op.acc.5.r1.2]** Se impondrán normas de complejidad mínima y robustez frente a ataques de adivinación.

lista de chequeo 4		Control de dispositivos móviles		
		individual la que habitualmente configura y controla el mecanismo de acceso inicial al dispositivo. Ese control de accesos se aplica en la mayoría de los casos a través de un número de identificación personal (PIN), que puede ser un código alfanumérico, complementado o no con un factor biométrico de autenticación (huella dactilar o reconocimiento facial), en algunos casos mínimos utilizándose otros mecanismos adicionales como tokens de hardware o tarjetas con chips. El control de accesos al dispositivo es la primera barrera para acceder al contenido del dispositivo, con posibilidad de conocerlo y/o manipularlo, incluso de gestionar elementos de la identidad del usuario.	represente datos personales o palabras con alto potencial de ser adivinadas. En los dispositivos cuya autenticación de acceso inicial se realiza mediante movimientos o geometrías del dedo en una pantalla táctil, se recomienda complementar ese procedimiento con un segundo factor de autenticación, debido a la mayor probabilidad de que esos movimientos sean vistos y replicados por terceras personas. Adicionalmente, se sugiere que, una vez un dispositivo portátil está encendido y funcionando, se aplique de manera sistemática el **bloqueo de actividad en pantalla** mediante acceso por PIN y/o biometría. Este bloqueo debería configurarse en cualquier caso para que entrara automáticamente en funcionamiento tras un período breve de inactividad, que debería procurarse que fuera configurado al mínimo, o siempre que el usuario haya pulsado la función de apagar pantalla.	**[op.acc.6.r2.1]** Se requerirá un segundo factor tal como «algo que se tiene», es decir, un dispositivo, una contraseña de un solo uso (OTP, en inglés) como complemento a la contraseña de usuario, o «algo que se es».
4.3.	Control de privacidad en superficie.	Con independencia de los mecanismos de regulación de la privacidad que deberían configurarse en aplicaciones software o servicios digitales accesibles desde un dispositivo portátil, la mayoría de los equipos informáticos móviles tienen posibilidad de configurar **notificaciones en pantalla** para el	Como mecanismo de control de la privacidad evitando la exposición de información significativa en la pantalla de los dispositivos, se recomienda desactivar todas las notificaciones de aplicaciones software en la pantalla del dispositivo, al menos cuando la pantalla está en modo bloqueado.	**[mp.eq.2.1]** El puesto de trabajo se bloqueará al cabo de un tiempo prudencial de inactividad, requiriendo una nueva autenticación del usuario para reanudar la actividad en curso. **[op.exp.2.2]** Se aplicará la regla de «mínima funcionalidad», es decir: a) El sistema debe proporcionar la funcionalidad mínima imprescindible para que la organización alcance sus objetivos.

lista de chequeo 4		Control de dispositivos móviles		
		usuario procedentes de aplicaciones software instaladas en el dispositivo. A menudo, esas notificaciones se exponen en la pantalla del dispositivo incluso estando bloqueado con código de acceso, de manera que se hace posible que, en determinadas circunstancias, personas ajenas con línea de visión sobre la pantalla del dispositivo accedan puntualmente a la información contenida en esas notificaciones, alguna de las cuales podría ser información personal identificativa o información sensible.		
4.4.	Control de instalación de aplicaciones software.	Numerosos de los vectores de diseminación de malware dirigido a infectar dispositivos informáticos portátiles consisten en inocular virus o código informático malicioso en ficheros que se descargan de Internet simulando ser apps que ofertan distintas funciones al usuario. Las tácticas de muchas ciberamenazas pasan por infectar apps con código dañino, sabedores de que la instalación de apps, sobre todo en teléfonos móviles, es una conducta habitual de la mayoría de	Una buena práctica en ciberseguridad consiste en **centralizar en el departamento tecnológico correspondiente de partido político todas las instalaciones y actualizaciones de software** con destino a máquinas que formen parte de la infraestructura informática del partido, incluidos todos los dispositivos otorgados en usufructo a cualquier usuario. En esa línea, debería implantarse una instrucción de ciberseguridad corporativa, con su correspondiente articulación tecnológica, que impida la descarga, desde Internet o desde cualquier otra red, e instalación de cualquier	**[op.exp.6.r3.1]** Solamente se podrán ejecutar aquellas aplicaciones previamente autorizadas. Se implementará una lista blanca para impedir la ejecución de aplicaciones no autorizadas. **[op.exp.4.3]** El mantenimiento solo podrá realizarse por personal debidamente autorizado. **[org.2]** Normativa de seguridad. Se dispondrá de una serie de documentos que describan: **[org.2.1]** El uso correcto de equipos, servicios e instalaciones, así como lo que se considerará uso indebido.

lista de chequeo 4		Control de dispositivos móviles		
		usuarios de dispositivos informáticos. Siendo como son las aplicaciones software (apps) un objeto de deseo por parte de las ciberamenazas, los partidos políticos, como cualquier otra organización provista de una infraestructura informática, debería incluir en su política de ciberseguridad corporativa un control exhaustivo de las instalaciones de software en los terminales informáticos utilizados por personas en calidad de usufructuarios o de usuarios finales.	fichero ejecutable o de sistema en los sistemas operativos más habituales, Windows y sus variantes móviles, macOS y sus variantes móviles, cualquier distribución de Linux, o Android. La implantación tecnológica de esta directiva debería hacerse por **bloqueo directo de cualquier descarga, para todos los usuarios ajenos al departamento responsable**, de los formatos de fichero más relacionados con ejecutables de sistema operativo. Se recomienda que todas las aplicaciones instaladas en los dispositivos de los usuarios se realicen desde un market de aplicaciones confiable tanto en caso de Android (Play Store) como iOS (App Store). Evitar que el dispositivo permita instalar aplicaciones directamente desde el fichero instalador (IPA y APK) tanto desde la interfaz gráfica como vía depuración USB. En resumen, **ningún usuario**, por sí mismo y sin el concurso del departamento técnico responsable, debería tener permiso para instalar software en una máquina que sea parte de la infraestructura informática de un partido político.	**[org.2.2]** La responsabilidad del personal con respecto al cumplimiento o violación de la normativa: derechos, deberes y medidas disciplinarias de acuerdo con la legislación vigente.
4.5.	Control reforzado de aplicaciones software que gestionan información sensible.	La política general de control de accesos definida por un partido político para los dispositivos, servidores y servicios de su infraestructura informática debería suplementarse granulando permisos específicos para usuarios	Las aplicaciones software por las que circule información catalogada con algún nivel de sensibilidad en la política de ciberseguridad corporativa de un partido político, y que estén instaladas en cualquier dispositivo móvil de la infraestructura informática del partido, deberían estar provistas de un **sistema propio de**	**[op.acc.6.r6.1]** Se definirán aquellos puntos en los que el sistema requerirá una renovación de la autenticación del usuario, mediante identificación singular, no bastando con la sesión establecida. **[mp.sw.2]** Aceptación y puesta en servicio. **[mp.sw.2.1]** Se comprobará que:

lista de chequeo 4		Control de dispositivos móviles		
		concretos sobre aplicaciones software específicas que manejen información sensible. Esta granularidad de accesos debería ser guardar coherencia y dependencia con los niveles de autorización para acceso a información sensible.	**autenticación de acceso** para usuarios autorizados, a través de un protocolo de **acreditación multifactor**. Adicionalmente, se sugiere desactivar el acceso a estas aplicaciones software de otras aplicaciones instaladas en el mismo dispositivo cuya interdependencia no sea necesaria para su funcionamiento, especialmente las aplicaciones de geolocalización, de reconocimiento por voz, o cualquier servicio no jerárquicamente dependiente y conectado a Internet.	a) Se cumplen los criterios de aceptación en materia de seguridad. b) No se deteriora la seguridad de otros componentes del servicio. **[op.acc.6.r2.1]** Se requerirá un segundo factor tal como «algo que se tiene», es decir, un dispositivo, una contraseña de un solo uso (OTP, en inglés) como complemento a la contraseña de usuario, o «algo que se es».
4.6.	Control de la disponibilidad y conectividad.	Los usuarios de dispositivos electrónicos deben tomar conciencia de los distintos estados de disponibilidad de sus aparatos portátiles. Cuando un teléfono está fuera de línea (modo avión) tiene suspendidas sus funciones de línea telefónica y, si el usuario lo define así, también su conectividad por línea inalámbrica, pero no otros servicios informáticos, como la comunicación de la geolocalización. Incluso hay aplicaciones software diseñadas para estar operativas con las líneas inalámbrica y telefónica desactivadas.	Está recomendado que las reuniones físicas donde se maneje información con clasificación de seguridad protegida por legislación de secretos oficiales estén libres de dispositivos electrónicos que no hayan sido previamente acreditados para el almacenamiento de ese tipo de información. Se sugiere a los partidos políticos dispone de sobres portátiles diseñados como jaulas de Faraday en donde introducir los dispositivos electrónicos en este tipo de reuniones. En otros escenarios donde no apliquen los preceptos de la legislación de secretos oficiales, si se pretende garantizar la confidencialidad total del escenario, se recomienda evitar introducir un dispositivo electrónico o aislarlo en una jaula de Faraday. Por otro lado, se recomienda mantener **desactivadas por defecto las conexiones vía**	**[mp.eq.3.3]** Cuando un dispositivo portátil se conecte remotamente a través de redes que no están bajo el estricto control de la organización, el ámbito de operación del servidor limitará la información y los servicios accesibles a los mínimos imprescindibles, requiriendo autorización previa de los responsables de la información y los servicios afectados. Este punto es de aplicación a conexiones a través de internet y otras redes que no sean de confianza. **[mp.eq.3.4]** Se evitará, en la medida de lo posible, que el dispositivo portátil contenga claves de acceso remoto a la organización que no sean imprescindibles. Se considerarán claves de acceso remoto aquellas que sean capaces de habilitar un acceso a otros equipos de la organización u otras de naturaleza análoga.

lista de chequeo 4		Control de dispositivos móviles		
			Bluetooth, Airdrop o similares de todos los dispositivos electrónicos, activándolas exclusivamente para comunicaciones donde sean necesarias y desactivándolas cuando hayan dejado de serlo.	
4.7.	Seguridad del correo electrónico.	Los servicios de correo electrónico representan uno de los canales primordiales, sino el principal, a través de los cuales se transmite información digital en las organizaciones. Además de los accesos a través de web o de clientes software instalados en computadores, los teléfonos móviles suelen ser habituales dispositivos de gestión y uso del correo electrónico. En ese sentido, el correo electrónico a través de dispositivos informáticos portátiles debe ser objeto de medidas específicas de seguridad que garanticen su uso eficiente a la par que se minimizan al máximo tres posibilidades: 1) que sea utilizado como canal de inoculación de malware; 2) que sea un medio de fuga de información sensible, ya porque su acceso ha sido comprometido mediante un ciberataque, ya por errores humanos	Como medida general de prevención de errores humanos en el envío y respuesta de mensajes, allá donde pueda ser aplicado sin crear disfuncionalidades, se recomienda que **no convivan cuentas de correo electrónico de uso personal con cuentas de correo institucionales** en el mismo cliente de correo electrónico del mismo dispositivo corporativo asignado a un usuario. Incluida en la política de ciberseguridad corporativa debería estar la **concienciación y capacitación a usuarios para distinguir indicadores de sospecha de correos electrónicos maliciosos**, con contenidos no deseados, o con hipervínculos o ficheros adjuntos que podrían conducir o incluir código malicioso para la descarga de malware. La instrucción a los usuarios debería incluir la prevención de alertar a los servicios de ciberseguridad corporativa de la recepción de cualquier correo electrónico sospechoso. Igualmente, a modo preventivo ante el esquema criminal denominado “comprometimiento del correo de negocios o corporativo” (business email compromiso), los usuarios deberían seguir la	**[mp.s.1]** Protección del correo electrónico. El correo electrónico se protegerá frente a las amenazas que le son propias, actuando del siguiente modo: **[mp.s.1.1]** La información distribuida por medio de correo electrónico se protegerá, tanto en el cuerpo de los mensajes como en los anexos. **[mp.s.1.2]** Se protegerá la información de encaminamiento de mensajes y establecimiento de conexiones. Se protegerá a la organización frente a problemas que se materializan por medio del correo electrónico, en concreto: **[mp.s.1.3]** Correo no solicitado, en su expresión inglesa «spam». **[mp.s.1.4]** Código dañino, constituidos por virus, gusanos, troyanos, espías, u otros de naturaleza análoga. **[mp.s.1.5]** Código móvil de tipo micro aplicación, en su expresión inglesa «applet». Se establecerán normas de uso del correo electrónico para el personal. Estas normas de uso contendrán: **[mp.s.1.6]** Limitaciones al uso como soporte de comunicaciones privadas.

lista de chequeo 4		Control de dispositivos móviles		
			directiva de la **doble verificación** cuando reciban correos electrónicos solicitándoles información sensible sobre el partido político, sus miembros o sus actividades, o pidiéndoles aportaciones económicas o de otra naturaleza, principalmente si esos correos provienen de orígenes conocidos o de confianza. Ese origen puede haber sido falsificado por un atacante, y la doble verificación implica que la persona que lo recibe lo verifica por otro canal (por ejemplo, una llamada telefónica) con la persona que lo envía. Un modo adicional de introducir más seguridad respecto del origen de mensajes de correo electrónico, es que los usuarios de cuentas de correo electrónico corporativas **firmen electrónicamente** todos sus mensajes mediante un mecanismo de firma electrónica instalado corporativamente. Está recomendado que, de modo sistemático, las **comunicaciones por correo electrónico** entre los diversos usuarios operando desde una cuenta de correo electrónico corporativa de un partido político, **estén cifradas** a través del mismo software cliente instalado por los servicios de ciberseguridad corporativa en esos dispositivos. Respecto de los accesos al correo electrónico corporativo a través de dispositivos móviles, aplican las mismas recomendaciones en cuanto al uso de contraseñas que las definidas para la política institucional de control de accesos. En	**[mp.s.1.7]** Actividades de concienciación y formación relativas al uso del correo electrónico. **[op.acc.6]** Mecanismo de autenticación (usuarios de la organización). **Refuerzo R8**-Doble factor para acceso desde o a través de zonas no controladas. Se denomina «zona controlada» aquella que no es de acceso público, requiriéndose que el usuario, antes de tener acceso al equipo, se haya autenticado previamente de alguna forma (control de acceso a las instalaciones), diferente del mecanismo de autenticación lógica frente al sistema. Un ejemplo de zona no controlada es Internet. **[op.acc.6.r8.1]** Para el acceso desde o a través de zonas no controladas se requerirá un doble factor de autenticación.

lista de chequeo 4		Control de dispositivos móviles		
			conexiones móviles a servidores de correo electrónico a través de interfaces tipo web (**webmail**), se recomienda habilitar **segundos factores de autenticación** para los accesos.	
4.8.	Prevención en la descarga de ficheros.	Aunque no se trate de la intención de un usuario de descargar aplicaciones software de Internet, otro tipo de ficheros con otros formatos o, aparentemente, otros contenidos distintos de las aplicaciones software, pueden ser dañinos para un dispositivo informático, pues pueden incorporar código malicioso o malware. Incluso cuando se trate de ficheros de aparente uso común, como los formatos PDF, pueden haber sido manipulados por un atacante para hacerlos parecer PDF cuando en realidad son ficheros ejecutables del sistema operativo cargados con código software dañino.	Como norma general, debería instruirse a los usuarios para aplicar una prevención reforzada y evitar la descarga de ficheros en las siguientes circunstancias: 1) Si los ficheros provienen de pulsar un hipervínculo recibido por correo electrónico, mensaje en redes sociales, SMS, MMS o red P2P de un origen desconocido o sobre el que el usuario no haya aplicado el mecanismo de doble verificación de origen. 2) Si la descarga es solicitada por una web que el usuario ha visitado y de la cual no tiene conocimiento previo acreditado de que es un origen seguro. 3) Si la descarga es solicitada por una web al que el usuario ha sido redirigido automáticamente tras visitar un sitio web previo. 4) Si el fichero solicita descargarse y/o ejecutarse mediante un mensaje que aparece, de repente, en una ventana emergente en la pantalla del dispositivo solicitando autorizar la descarga.	**[org.2]** Normativa de seguridad. Se dispondrá de una serie de documentos que describan: **[org.2.1]** El uso correcto de equipos, servicios e instalaciones, así como lo que se considerará uso indebido. **[org.2.2]** La responsabilidad del personal con respecto al cumplimiento o violación de la normativa: derechos, deberes y medidas disciplinarias de acuerdo con la legislación vigente.

lista de chequeo 4		Control de dispositivos móviles		
4.9.	Prevención reforzada en entornos de teletrabajo.	El uso de dispositivos móviles tanto para mantener reuniones virtuales de trabajo, como para ejecutar tareas de teletrabajo es ya una condición infraestructural de todo tipo de organizaciones. El uso de software a través de dispositivos electrónicos en entornos de trabajo requiere de los usuarios prestar atención a nuevos elementos, como la protección de la privacidad, y a nuevas configuraciones de las ciberamenazas.	Respecto a las políticas de ciberseguridad corporativa, se aconseja establecer **provisiones específicas para la protección de información en situaciones de movilidad y teletrabajo,** que incluyan un análisis incrementado de la integridad y seguridad de los dispositivos corporativos que hayan pasado por situaciones de movilidad en entornos de seguridad deficiente o desconocida. Buenas prácticas de ciberseguridad en el uso de dispositivos móviles en escenarios de teletrabajo o trabajo en remoto son las siguientes: 1) No conectar dispositivos móviles corporativos a redes inalámbricas externas al partido político para recibir o transmitir información sensible o para conectarse en remoto a servicios o servidores corporativos que no estén amparados por protección reforzada multifactor. 2) Utilizar comunicaciones cifradas punto a punto en comunicaciones en las que no haya otra forma de conectividad que no sea registrar el dispositivo móvil en una red inalámbrica externa a las redes habituales de confianza. 3) Sólo permitir la conexión remota a sistemas informáticos corporativos que manejen información sensible a través de soluciones de escritorio virtual (VDI). En los demás casos que no involucren acceso a sistemas sensibles, habilitar soluciones de escritorio remoto (MSTSC).	**[mp.com.2]** Protección de la confidencialidad. **[mp.com.2.1]** Se emplearán redes privadas virtuales cifradas cuando la comunicación discurra por redes fuera del propio dominio de seguridad. **[mp.com.3]** Protección de la integridad y de la autenticidad. **[mp.com.3.1]** En comunicaciones con puntos exteriores al dominio propio de seguridad, se asegurará la autenticidad del otro extremo del canal de comunicación antes de intercambiar información. **[mp.com.3.2]** Se prevendrán ataques activos garantizando que al ser detectados se activarán los procedimientos previstos de tratamiento del incidente. Se considerarán ataques activos: a) La alteración de la información en tránsito. b) La inyección de información espuria. c) El secuestro de la sesión por una tercera parte. [mp.eq.4] Otros dispositivos conectados a la red. **[mp.eq.4.1]** Los dispositivos presentes en el sistema deberán contar con una configuración de seguridad adecuada de manera que se garantice el control del flujo definido de entrada y salida de la información. **[mp.eq.4.2]** Los dispositivos presentes en la red que dispongan de algún tipo de almacenamiento temporal o permanente de información proporcionarán la funcionalidad

lista de chequeo 4		Control de dispositivos móviles		
			4) En accesos remotos directos a sistemas corporativos no amparados por soluciones VDI o MSTSC, implantar restricciones de IP de origen, múltiple factor de autenticación de usuarios, listas de acceso en finalizador de túnel para garantizar enrutamiento únicamente a los servicios que permiten conexión. 5) Dotar a todos los dispositivos móviles corporativos trabajando en remoto sobre redes corporativas de protecciones antimalware y cortafuego, en ambos casos manteniendo el software actualizado. 6) En comunicaciones remotas por vídeo y voz entre dispositivos corporativos, emplear únicamente software y procedimientos contemplados en el SGSI del partido político. 7) En videollamadas en entornos corporativos, los usuarios deben prestar atención a no desvelar información personal identificativa que no sea la estrictamente requerida por el protocolo de la llamada. 8) Por lo demás, en reuniones virtuales, tanto los terminales de sala de reuniones, como los terminales virtuales o las infraestructuras de comunicación, deberían ajustarse a lo recomendado en la Guía de Buenas Prácticas BP/18 del Centro Criptológico Nacional.	necesaria para eliminar información de soportes de información.

lista de chequeo 4		Control de dispositivos móviles		
4.10.	Copias de seguridad en dispositivos móviles.	Al igual que en los servidores y computadores de escritorio corporativos, en los dispositivos portátiles aplican las mismas recomendaciones de copia de seguridad. La diferencia es que, en estos últimos, al menos respecto de parte del contenido que está almacenado en el dispositivo y no en soluciones de almacenamiento en línea, es el usuario del dispositivo el que suele llevar a cabo el procedimiento de copia de seguridad.	Ya sea porque la copia de seguridad de computadores portátiles o teléfonos inteligentes del partido político adjudicados para uso de personas individuales, sea una tarea desarrollada por un departamento concreto o por el propio usuario, está recomendado: 1) Que las copias de seguridad sean periódicas, y en lo posible automatizadas, sobre el contenido almacenado en el dispositivo. 2) Ya sea que las copias se hagan en dispositivos hardware de almacenamiento externo o en dispositivo en línea, en cualquier caso, los repositorios deben estar provistos de su propio control de accesos con el nivel de seguridad correspondiente al del propio usuario, y su contenido debe almacenarse cifrado, y también transmitirse cifrado si la copia se realiza hacia un repositorio en línea.	**[mp.info.6.1]** Se realizarán copias de seguridad que permitan recuperar datos perdidos, accidental o intencionadamente. La periodicidad y los plazos de retención de estas copias de seguridad se determinarán en la normativa interna de la organización relativa a copias de seguridad. En relación a las copias en soportes personales, tipo pen-drives: **[mp.si.3.1]** Se aplicará la debida diligencia y control a los soportes de información que permanecen bajo la responsabilidad de la organización, garantizando el control de acceso con medidas físicas. **[mp.si.4]** Transporte. **[mp.si.4.3]** Se utilizarán los medios de protección criptográfica correspondientes al mayor nivel de seguridad de la información contenida. **[mp.per.3]** Concienciación. En particular, se recordará periódicamente: **[mp.per.3.1]** La normativa de seguridad relativa al buen uso de los equipos o sistemas y las técnicas de ingeniería social más habituales.
4.11.	Aplicaciones antimalware para dispositivos móviles.	Los dispositivos móviles del partido político, teléfonos inteligentes u ordenadores portátiles deben estar provistos del mismo software antimalware y de protección de terminal que el resto de los sistemas informáticos corporativos,	Con independencia de la solución software antimalware y de protección de terminal elegida, ésta debería proporcionar, al menos, las siguientes funciones: 1) Escaneo de ficheros antes de descargarse en el dispositivo.	**[op.exp.6.1]** Se dispondrá de mecanismos de prevención y reacción frente a código dañino, incluyendo el correspondiente mantenimiento de acuerdo a las recomendaciones del fabricante. **[op.exp.6.2]** Se instalará software de protección frente a código dañino en todos los

lista de chequeo 4		Control de dispositivos móviles		
		añadiendo las soluciones de movilidad que sean preceptivas.	2) Escaneo perimetral de correos electrónicos. 3) Control de firmas digitales y de la integridad de ficheros. 4) Búsqueda de anomalías en ficheros y procesos a través de métodos heurísticos.	equipos: puestos de usuario, servidores y elementos perimetrales. **[op.exp.6.5]** El software de detección de código dañino instalado en los puestos de usuario deberá estar configurado de forma adecuada e implementará protección en tiempo real de acuerdo a las recomendaciones del fabricante.

3.4. PROTECCIÓN DE SERVICIOS Y SERVIDORES CONECTADOS A INTERNET

Aunque la infraestructura informática de un partido político pueda disponer de computadores y otros dispositivos tecnológicos que actúan desconectados de las redes, por ejemplo, los dedicados a almacenamiento y gestión de información con clasificación de seguridad, en la actualidad una infraestructura informática es una infraestructura conectada a través de redes, también estas redes definidas y gestionadas por hardware y software.

Esta red que da forma a la infraestructura informática conectada tiene, en realidad, una topología de red de redes, pues son diferentes configuraciones de redes locales, que aglutinan dispositivos que se vinculan entre sí, las que se conectan formando una malla establecida en Internet.

La realidad de una infraestructura informática conectada implica que los partidos políticos deben definir sus políticas de ciberseguridad sobre un ecosistema con un número creciente y cambiante de puertas digitales que se orientan hacia el exterior de la propia infraestructura, donde otros dispositivos y personas ajenas a la infraestructura informática de la organización llamarán para realizar conexiones, por ejemplo, a los servidores web públicos.

En este formato de redes, cualquier organización, como un partido político, puede adoptar diversas decisiones sobre la arquitectura de red y de servicios, servidores y dispositivos conectados a esa red. Las decisiones sobre la topología de red implicarán a su vez opciones de ciberseguridad, muchas de las cuales dependen de las opciones de hardware y software que se adopten, y que no cabe que sean definidas a priori.

Entre las decisiones a adoptar por una organización respecto de su **topología de redes** y que determinarán qué opciones de ciberseguridad son las más eficientes están, sin pretensiones de exhaustividad, las siguientes:

- **Segmentación** de servidores, servicios y sitios web, incluyendo:
    - El tipo de subredes donde se alojarán.
    - Qué dispositivos y servicios estarán conectados, qué otros compartimentados en subredes de accesos restringidos, y qué otros desconectados.
    - Qué porción de las redes involucrarán la conexión de servicios y servidores virtualizados y radicados en la nube (*cloud*), y cómo convivirán, en términos de topología de red, con dispositivos, servidores y servicios radicados en hardware y software en infraestructuras propias (los denominados *on-premise*).
- Control de accesos definido como **red de accesos**, incluyendo:

- La definición de protocolos de acceso a redes y subredes.
- La introducción de accesos a perímetro, previos al acceso a dispositivos y servicios, o zonas de acceso restringido.

En cualquiera de las opciones de topología de redes la ciberseguridad de redes es una condición horizontal sobre la que caben varias recomendaciones generales, aplicables a cualquier decisión sobre arquitectura informática.

lista de chequeo 5		Ciberseguridad de redes informáticas		
nº	BUENA PRÁCTICA	PROPÓSITO	CARACTERÍSTICAS	VINCULACIÓN CON EL ENS
5.1.	Redes de **confianza cero**.	Cualquiera que sea el diseño de la arquitectura de red de una organización, en lo relativo a ciberseguridad debería definirse como de confianza cero. El modelo de confianza se define sobre el supuesto de que ninguna conexión que llegue a dispositivos, servicios y servidores alojados en subredes y redes corporativas desde el exterior de la infraestructura propia es, a priori, confiable, es decir, que esas conexiones deben acreditar su confiabilidad autenticándose apropiadamente en el punto de la red donde haya llamado a una puerta digital de la	El paradigma de la confianza cero implica establecer cada red, subred y servidor, servicio o dispositivo conectados a ella mediante tres requisitos: 1) **Microsegmentación**, haciendo cada subred del mínimo tamaño funcional posible para limitar los daños a otras subredes caso de que una de ellas fuera comprometida en un ciberataque. 2) **Protección perimetral** de cada subred, con su propio control de accesos. 3) Tras el control perimetral, **control de accesos**, siempre que sea posible mediante **autenticación multifactor**, en cada dispositivo, servidor o servicio digital.	**[mp.com.4]** Separación de flujos de información en la red. La segmentación acota el acceso a la información y, consiguientemente, la propagación de los incidentes de seguridad, que quedan restringidos al entorno donde ocurren. Cuando la transmisión de información por la red se restringe a ciertos segmentos, se acota el acceso a la información y los incidentes de seguridad quedan encapsulados en su segmento. Requisitos. Los flujos de información se separarán en segmentos de forma que: **[mp.com.4.1]** El tráfico por la red se segregará para que cada equipo solamente tenga acceso a la información que necesita. **[mp.com.4.2**] Si se emplean comunicaciones inalámbricas, será en un segmento separado. Refuerzo R4-Puntos de interconexión. **[mp.com.4.r4.1]** Control de entrada de los usuarios que llegan a cada segmento y control de entrada y salida de la información disponible en cada segmento.

lista de chequeo 5		Ciberseguridad de redes informáticas		
		infraestructura informática que se está protegiendo.		**[mp.com.4.r4.2]** El punto de interconexión estará particularmente asegurado, mantenido y monitorizado.
5.2.	Principio de **mínimo privilegio**.	El principio de mínimo privilegio es una condición de los modelos de confianza cero. Al igual que en la buena práctica 1.4. establecida para la seguridad de la información sensible, este principio se basa en que, a cada subred, y dispositivo, servicio o servidor dentro de cada subred, sólo tienen concedida autorización de acceso las personas que deben utilizar en cada momento uno de esos elementos conectados a la red de la infraestructura informática a proteger.	Establecimiento de una gradación de autorizaciones de conexión a servicios y dispositivos conectados, sustanciadas a través del supuesto de la necesidad de acceso que cada usuario debería tener a los servicios digitales de una organización en función del papel que juega en esa organización. puesto que la infraestructura informática de una organización no es más que una de las maneras que esa organización tiene de representarse a sí misma. La gestión de accesos en un modelo de mínimo privilegio en red debería reforzarse con los siguientes elementos: 1) Establecimiento de **listas de autenticación y denegación**, sobre todo en dispositivos y servicios esenciales o que gestiones información sensible. 2) Establecimiento de un mecanismo de **control de accesos no autorizados**, con protocolos de denegación de accesos fallidos y emisión de alertas de seguridad ante accesos sospechosos. 3) Establecimiento de un **mecanismo de monitorización y análisis de conexiones**,	**[op.acc.2.1]** Los recursos del sistema se protegerán con algún mecanismo que impida su utilización, salvo a las entidades que disfruten de derechos de acceso suficientes. **[op.acc.4.1]** Todo acceso estará prohibido, salvo autorización expresa. **[op.acc.4.2]** Mínimo privilegio: los privilegios de cada entidad, usuario o proceso se reducirán al mínimo imprescindible para cumplir sus obligaciones o funciones. **[op.acc.4.3]** Necesidad de conocer y responsabilidad de compartir: los privilegios se asignarán de forma que las entidades, usuarios o procesos sólo accederán al conocimiento de aquella información requerida para cumplir sus obligaciones o funciones. La información es patrimonio del organismo y toda aquella que resulte necesaria para el usuario estará a su disposición. **[op.acc.4.4]** Capacidad de autorizar: Exclusivamente el personal con competencia para ello podrá conceder, alterar o anular la autorización de acceso a los recursos, conforme a los criterios establecidos por su responsable. Los permisos de acceso se revisarán de forma periódica. **[op.acc.4.5]** Se establecerá una política específica de acceso remoto, requiriéndose autorización expresa. [**op.exp.8.1]** Se generará un registro de auditoría, que incluirá, al menos, el identificador del usuario o entidad asociado al evento, fecha y hora, sobre qué información se realiza el evento, tipo de evento y el

lista de chequeo 5		Ciberseguridad de redes informáticas		
			que sirva para detectar anomalías de tráfico que anticipen situaciones de ciberamenazas.	resultado del evento (fallo o éxito), según la política de seguridad y los procedimientos asociados a la misma. **Refuerzo R5**-Revisión automática y correlación de eventos. **[op.exp.8.r5.1]** El sistema deberá implementar herramientas para analizar y revisar la actividad del sistema y la información de auditoría, en búsqueda de comprometimientos de la seguridad posibles o reales. **[op.exp.8.r5.2]** Se dispondrá de un sistema automático de recolección de registros, correlación de eventos y respuesta automática ante los mismos.
5.3.	Política corporativa de actualización de software.	Aparte de los dispositivos hardware, con la creciente virtualización de servicios y dispositivos digitales las redes informáticas son, sobre todo, complejos conglomerados de software, que no sólo tiene entidad propia en cada pieza de software desarrollada para accionar funciones de servicios concretos, sino que, especialmente en lo referente a redes, se trata de soluciones de software que deben conectarse, interactuar, integrarse con otras soluciones de software, la mayor parte de las veces unas y otras programadas por fabricantes distintos.	La medida central a adoptar, en el contexto del SGSI, es implantar una política corporativa de actualización de software. Esta política debería tomar en consideración numerosos asuntos, algunos de los cuales son: 1) Determinación de **qué software debe ser instalado** en infraestructura informática del partido político para cumplir con las funciones necesarias que se piden a esa infraestructura. 2) A partir del software instalado, determinar qué **aplicaciones software son críticas o esenciales**, y requieren por tanto una ciberseguridad reforzada. 3) Fijar una **programación planificada de actualizaciones de software**, teniendo en	**[op.exp.4]** Mantenimiento y actualizaciones de seguridad. Para mantener el equipamiento físico y lógico que constituye el sistema, se aplicará lo siguiente: **[op.exp.4.1]** Se atenderá a las especificaciones de los fabricantes en lo relativo a instalación y mantenimiento de los sistemas, lo que incluirá un seguimiento continuo de los anuncios de defectos. **[op.exp.4.2]** Se dispondrá de un procedimiento para analizar, priorizar y determinar cuándo aplicar las actualizaciones de seguridad, parches, mejoras y nuevas versiones. La priorización tendrá en cuenta la variación del riesgo en función de la implantación o no de la actualización. **[op.exp.4.3]** El mantenimiento solo podrá realizarse por personal debidamente autorizado. **Refuerzo R1**-Pruebas en preproducción **[op.exp.4.r1.1]** Antes de poner en producción una nueva versión o una versión parcheada, se

lista de chequeo 5		Ciberseguridad de redes informáticas		
		Desde el punto de vista de la ciberseguridad, la complejidad de este conglomerado de software hace que no sólo haya que estar pendiente de asegurar que no existen líneas de código informático debilitadas a través de la cuales se pueda filtrar una ciberamenaza, sino los puntos de intersección y contacto entre distintos desarrollos de software tampoco dejan grietas que representen un riesgo. Muchas de estas grietas o debilidades en el código informático se corrigen continuamente en actualizaciones de software distribuidas por los fabricantes, ya sea porque se ha descubierto una vulnerabilidad en ese código que lo hace susceptible de ser atacado, ya sea porque se ha definido una manera de que ese código sea todavía más seguro. Al tratarse de muchas soluciones de software distintas conviviendo en las mismas redes informáticas, a menudo actualizaciones de un software no son compatibles con la versión de otra solución de	cuenta dependencias, interdependencias y criticidades de cada solución de software. Esta planificación debería identificar interactuaciones de actualizaciones y parches con software crítico y prevenir disfuncionalidades. 4) Desplegar un **entorno de pruebas de actualizaciones de software**, provisto de herramientas de diagnóstico de funcionalidad e interfuncionalidad de actualizaciones, con verificación de ficheros fuente de actualizaciones. 5) Vinculado al entorno de pruebas, implantar un **mecanismo de protección de contenidos instalados** contra actualizaciones defectuosas o fallidas, que incluya la reversión de cambios operados sobre el software ya instalado. 6) Al igual que está recomendado con los dispositivos móviles, y siguiendo la directiva de una autoridad centralizada para las actualizaciones de software, **bloquear en todos los dispositivos de usuario cualquier instalación de software accionada por un usuario individual**.	comprobará en un entorno de prueba controlado y consistente en configuración al entorno de producción, que la nueva instalación funciona correctamente y no disminuye la eficacia de las funciones necesarias para el trabajo diario. **[op.exp.6.r3.1]** Solamente se podrán ejecutar aquellas aplicaciones previamente autorizadas. Se implementará una lista blanca para impedir la ejecución de aplicaciones no autorizadas.

lista de chequeo 5		Ciberseguridad de redes informáticas		
		software con la que tiene que conectar, y la decisión de actualización tiene que esperar a que todo el software involucrado tenga el mismo nivel de madurez; o una actualización debe hacerse modificando a su vez otras soluciones de software. Estos escenarios de actualizaciones de versiones de software que influyen en la funcionalidad de otras soluciones de software puede exponer riesgos de ciberseguridad y, por ello, las actualizaciones de software en una infraestructura informática de un partido político deben estar centralizadas en un departamento responsable y planificadas con una visión de SGSI.		
5.4.	Auditoría continuada de vulnerabilidades.	Las actualizaciones de software nacieron para que versiones instaladas recibieran mejoras desarrolladas del software para incrementar su eficiencia y funcionalidad. Sin embargo, actualmente las actualizaciones de software tienen en su esencia una elevada componente de parches de seguridad para atajar vulnerabilidades o fallos de	La auditoría de vulnerabilidades en sistemas informáticos conectados descansa en dos pilares: 1) El establecimiento de un **sistema de alertas sobre vulnerabilidades** reportadas y parches de seguridad disponibles para cada una de las distintas soluciones de software instalado. Este sistema de alertas debe estar alimentado por el flujo de información continuada procedente tanto	**[op.mon.3]** Vigilancia. **Refuerzo R2**-Análisis dinámico. **[op.mon.3.r2.1]** Se dispondrá de soluciones de vigilancia que permitan determinar la superficie de exposición con relación a vulnerabilidades y deficiencias de configuración. **Refuerzo R6**-Inspecciones de seguridad. Periódicamente, o tras incidentes que hayan desvelado vulnerabilidades del sistema nuevas o subestimadas, se realizarán las siguientes inspecciones:

lista de chequeo 5		Ciberseguridad de redes informáticas		
		código que pueden implicar su explotación por parte de ciberamenazas con propósitos de comprometer sistemas informáticos. Por tanto, un elemento indispensable de la protección de redes informáticas, asociado a las políticas de actualización de software, es someter las soluciones software instaladas a continuas auditorías y pruebas para la detección y corrección de vulnerabilidades de código que puedan presentar riesgos de ciberseguridad.	de los distintos fabricantes, como de las empresas e investigadores de ciberseguridad, así como los diversos centros de respuesta a incidentes de ciberseguridad de gobiernos e instituciones. 2) La configuración de un **procedimiento activo de búsqueda de vulnerabilidades y fallos de seguridad en los sistemas conectados**. Este procedimiento está normalmente articulado a través de ejercicios de ciberataque y penetración forzada simulados de los sistemas propios buscando intencionadamente puntos de debilidad en redes y servicios y dispositivos conectados, con el fin de resolverlos proactivamente.	**[op.mon.3.r6.1]** Verificación de configuración. **[op.mon.3.r6.2]** Análisis de vulnerabilidades. **[op.mon.3.r6.3]** Pruebas de penetración.
5.5.	Aplicaciones antimalware para redes informáticas.	Al igual que 4.11. para la ciberseguridad de dispositivos móviles, dispositivos móviles cuya característica esencial es estar conectados a redes en su movilidad, el software que define y gestiona las redes informáticas también deben estar provistos de software antimalware y de protección perimetral.	Con independencia de la solución software antimalware para redes y de las soluciones cortafuegos elegidas, deberían proporcionar, al menos, las siguientes funciones: 1) Bloqueo de conexiones desde direcciones IP marcadas como fuentes de actividad maliciosa. 2) Bloqueo de usuarios desprovistos de credenciales de paso.	**[op.mon.1.1]** Se dispondrá de herramientas de detección o prevención de intrusiones. **[mp.com.1.1]** Se dispondrá de un sistema de protección perimetral que separe la red interna del exterior. Todo el tráfico deberá atravesar dicho sistema. **[mp.com.1.2]** Todos los flujos de información a través del perímetro deben estar autorizados previamente. **[op.mon.3]** Vigilancia. **Refuerzo R3**-Ciberamenazas avanzadas. **[op.mon.3.r3.1]** Se dispondrá de sistemas para detección de amenazas avanzadas y comportamientos anómalos.

lista de chequeo 5		Ciberseguridad de redes informáticas		
			3) Filtrado de tráfico de red para detectar anomalías y bloquear actividades sospechosas. 3) Filtrado de ficheros y bloqueo de aquellos que presenten características de peligrosidad programadas en el filtro, como los ficheros conocidos por transportar código dañino. El filtrado de contenidos puede incluir tecnología de inspección profunda de paquetes de datos (DPI, por sus siglas en inglés). 4) Filtrado de contenidos marcados como sospechosos o que sean indicadores de actividad sospechosa como el *phishing* o el *spam*. 5) Control de firmas digitales y de la integridad de ficheros.	**[op.mon.3.r3.2]** Se dispondrá de sistemas para la detección de amenazas persistentes avanzadas (*Advanced Persistent Threat, APT*) mediante la detección de anomalías significativas en el tráfico de la red.

3.5. CIBERSEGURIDAD EN REDES SOCIALES

Las redes sociales con estructuras interpersonales propias de la naturaleza del ser humano como ser social. En el momento en que se constituyen grupos de individuos que comparten lazos sociales personales o vínculos de interés hacia cualquier dominio económico, religioso, político, de ocio o de otro tipo, ya está configurada una red social. Por tanto, la relación social de los seres humanos en red existe desde que el ser humano se comunica e interactúa con otros.

Sin embargo, la eclosión de las redes sociales como concepto global y cotidianamente pronunciado por millones de seres humanos con independencia de su geografía de residencia o de su cultura de procedencia, es inherente a la aparición y crecimiento exponencial de los intercambios sociales a través de Internet, de la web o, en definitiva, del ciberespacio.

Las redes sociales, entendidas desde la perspectiva de internet y la conectividad web, son espacios digitales destinados a comunicar personas entre sí, constituyendo una red de interacciones que traslada lo social al ciberespacio. Podría decirse que las redes sociales en el ciberespacio son el equivalente digital o virtual al conjunto de relaciones personales, laborales o sociales que habitualmente mantienen los seres humanos en su vida física. De este modo, las redes sociales también son un fenómeno que canaliza y expresa las inquietudes, intereses, opiniones y expectativas políticas de los ciudadanos y, por tanto, un espacio digital de relación entre partidos políticos, representantes de los ciudadanos, y la propia ciudadanía.

En las redes sociales en el ciberespacio se mantiene una agenda de amigos o conocidos, se conversa con ellos y se comparten intereses y aficiones; las redes sociales acaban estando configuradas para compartir social, colectivamente, experiencias digitales masivas: por ejemplo, puede acudirse a un concierto de música virtualmente a través de redes sociales, asistir a una clase universitaria que está siendo impartida en otro país distinto al de residencia física del usuario.

Las enormes posibilidades que brindan las redes sociales y su uso masivo llevan aparejados una serie de riesgos de diversa índole, tanto en el ámbito privado como el profesional.

Ante la creciente tendencia a utilizar este tipo de redes como medio para el desarrollo de ciberataques, es de vital importancia estar protegido y utilizar un entorno seguro durante su empleo.

En general, las amenazas que emplean las redes sociales como puerta de entrada para realizar ciberataques y comprometer la seguridad de los usuarios aprovechan dos tipos de vulnerabilidades implícitas a la propia “arquitectura social” de las redes:

1) **Sobreexposición de información personal**. La sobreabundancia de información personal que los usuarios difunden a través de sus perfiles en redes sociales, que constituyen una atractiva materia prima para que cibercriminales utilicen esa información con propósitos maliciosos.
2) **Autopistas de información**. La propia fluidez y apertura inherente a la comunicación en redes sociales, que las convierte en auténticas autopistas de información por las que circulan comunicaciones socialmente inocuas, pero también otro tipo de contenidos que están enlazados a varios tipos de malware. Este malware que busca estar enlazado y circular por las autopistas de información de las redes sociales tiene una amplia tipología y está diseñado para realizar todo tipo de funciones maliciosas: desde mostrar publicidad no deseada; pasando por robar información sensible o credenciales bancarias o de tarjetas de crédito de los usuarios; siguiendo por instalar ransomware que secuestre los datos de los usuarios y pida un rescate para liberarlos; o terminando por infectar ordenadores o dispositivos móviles con virus que toman el control de los aparatos y realizan fotos de los usuarios sin su autorización, envían y reciben SMS, o graban sus conversaciones. Estos tipos de malware no son específicos de las redes sociales, pero aprovechan la fluidez de comunicación social en red para difundirse y extender su infección al mayor número de usuarios posible.

Respecto de estos dos conjuntos de vulnerabilidades inherentes a las redes sociales, individuos y grupos con propósitos malintencionados o cibercriminales aplican elevadas dosis de creatividad para intentar producir un daño u obtener un beneficio ilícito mediante la utilización ilegítima de las posibilidades que ofrecen las redes sociales. Los tipos de amenazas o de utilizaciones malintencionadas de las redes sociales más habituales se inscriben en categorías como la ingeniería social, el robo de identidad, el ciberacoso, el perjuicio reputacional, la publicidad engañosa o la distribución de malware.

En lo que a ciberamenazas en redes sociales se refiere, el usuario es el “talón de Aquiles”, puesto que, aunque el software y los dispositivos hardware puedan dotarse de las últimas medidas de ciberseguridad, al final el usuario dependerá siempre de su propia consciencia de seguridad, de su propia protección, para resguardarse. Y usuarios en redes sociales hay cientos de millones globalmente, cada uno con su propia protección o desprotección individuales en su comportamiento en el ciberespacio, con independencia de que sus dispositivos estén actualizados “a la última”.

La ingeniería social pretende explotar precisamente esa debilidad potencial del componente humano en las redes sociales en vez de atacar directamente al software o al hardware para vulnerar la seguridad de un sistema, en este caso de la comunicación en redes sociales. La ingeniería social recurre a las pautas conocidas del comportamiento humano para diseñar procesos de conducta online que hagan que los usuarios realicen determinadas acciones: cliqueen contenidos que responden a sus intereses, proporcionen información en determinados contextos o compartan datos sensibles. A fin de lograr que el usuario incurra en conductas que le supondrán un peligro para su privacidad o para sus finanzas, la ingeniería

social recurrirá al engaño y a la simulación para mostrar a los usuarios escenarios que en realidad no son lo que parecen: anuncios en redes sociales que al cliquearlos conducen a la descarga de malware; avisos fraudulentos simulando provenir de entidades bancarias que conducen a formularios diseñados para robar credenciales de tarjetas de crédito; o trucos publicitarios más o menos burdos para lograr suscribir fraudulentamente al usuario a servicios SMS de tarificación especial.

De esta manera, en tanto espacios digitales donde se establecen relaciones políticas entre los partidos representativos y los ciudadanos, y realidades digitales que son instrumentadas por ciberamenazas para desarrollar actividades dañinas tanto para los partidos políticos como para la propia ciudadanía, es de sentido común que las políticas de ciberseguridad de los partidos políticos contemplen una serie de buenas prácticas con las que reducir los riesgos posibles que la presencia de los partidos políticos y de sus miembros en redes sociales puede suscitar ante las ciberamenazas.

lista de chequeo 6		Ciberseguridad de redes sociales		
nº	BUENA PRÁCTICA	PROPÓSITO	CARACTERÍSTICAS	VINCULACIÓN CON EL ENS
6.1.	Atención reforzada cuando se define una identidad en redes sociales.	Por su propia naturaleza de canales de comunicación interpersonal, las redes sociales siempre son un foco de exposición, por intención o por descuido, para datos identificativos personales. Precisamente son esos datos identificativos personales los que son necesarios proteger cuando se constituye una cuenta en redes sociales.	Un lugar permanente encabezado por la fotografía, los datos personales e información sobre los estudios, profesión, gustos, intereses, amigos y familia proporciona mucha más información de una persona que su DNI o Pasaporte y, en la mayoría de los casos, está a la vista de todo el mundo. Conviene prestar atención a cómo se define un usuario así mismo en sus perfiles en redes sociales, porque ésa será la carta de presentación de su identidad en el ciberespacio.	**[mp.per.3]** Concienciación. Se realizarán las acciones necesarias para concienciar regularmente al personal acerca de su papel y responsabilidad para que la seguridad del sistema alcance los niveles exigidos. En particular, se recordará periódicamente: **[mp.per.3.1]** La normativa de seguridad relativa al buen uso de los equipos o sistemas y las técnicas de ingeniería social más habituales.
6.2.	Atención reforzada sobre contenidos compartidos.	En las redes sociales se comparten contenidos de todo tipo permanentemente, que no sólo pueden sobre-exponer datos personales identificativos, sino también	Para evitar riesgos de sobre-exposición en redes sociales, es necesario reflexionar sobre los contenidos que se comparten. Lo que se comparte define a quien lo comparte, y cada vez más personas y empresas observan y	**[mp.per.3]** Concienciación. Se realizarán las acciones necesarias para concienciar regularmente al personal acerca de su papel y responsabilidad para que la seguridad del sistema alcance los niveles exigidos. En particular, se recordará periódicamente:

lista de chequeo 6		Ciberseguridad de redes sociales		
		ser un reflejo de opiniones, intereses, expectativas.	analizan las redes sociales para adoptar un juicio sobre otras personas.	**[mp.per.3.1]** La normativa de seguridad relativa al buen uso de los equipos o sistemas y las técnicas de ingeniería social más habituales. **[op.mon.3]** Vigilancia. **Refuerzo R4**-Observatorios digitales. – [op.mon.3.r4.1] Se dispondrá de observatorios digitales con fines de cibervigilancia dedicados a la detección y seguimiento de anomalías que pudieran representar indicadores de amenaza en contenidos digitales.
6.3.	Limitación sobre información sensible.	Las redes sociales son un canal que los partidos políticos deberían tener vetado para compartir información sensible. Adicionalmente, los usuarios de redes sociales que sean miembros de partidos políticos y, que, por tanto, tienen una exposición aumentada ante la opinión pública, reciben mucha más atención que la mayoría respecto a la información que comparten sobre su vida personal, familiar y social.	No se compartan contenidos sensibles sobre tu vida o la de otros en redes sociales: números o imágenes de documentos identificativos, números de teléfono, direcciones postales, localizaciones exactas, identificadores de vehículos, detalles exhaustivos de viaje… cuanto más contenidos de este tipo se compartan, más probabilidades hay de ser víctima de un robo de identidad, de ciberacoso o de otra conducta ilícita que utilice la propia información en perjuicio propio. Es recomendable, mantener en privado la lista de contactos y analizar bien las solicitudes de amistad de desconocidos. Adicionalmente, debería ser una limitación, además de poder ser constitutivo de una infracción legal, compartir información privada de otras personas sin su consentimiento, así	**[mp.per.3]** Concienciación. Se realizarán las acciones necesarias para concienciar regularmente al personal acerca de su papel y responsabilidad para que la seguridad del sistema alcance los niveles exigidos. En particular, se recordará periódicamente: **[mp.per.3.1]** La normativa de seguridad relativa al buen uso de los equipos o sistemas y las técnicas de ingeniería social más habituales.

lista de chequeo 6		Ciberseguridad de redes sociales		
			como contenidos que por sí mismo están tipificados como ilícitos.	
6.4.	Prevención ante lo desconocido.	El flujo de contenidos que circulan por minuto en las redes sociales escapa con claridad al control atencional que una persona puede ejercer sobre ellos. Entre esos contenidos puede encontrarse actividad maliciosa intencionada, que a menudo se oculta en lo desconocido o lo novedoso.	No se haga clic en contenidos o hipervínculos en esos contenidos sobre los que no se tenga claro su origen o propósito, aumentando la cautela ante mensajes que lleguen de identidades que no se conocen. Los contenidos desconocidos, sobre todo aquellos que cuanto más desconocidos más atractivos se nos presentan, pueden ser virus envueltos en el paquete glamuroso de lo desconocido.	**[mp.per.3]** Concienciación. Se realizarán las acciones necesarias para concienciar regularmente al personal acerca de su papel y responsabilidad para que la seguridad del sistema alcance los niveles exigidos. En particular, se recordará periódicamente: **[mp.per.3.1]** La normativa de seguridad relativa al buen uso de los equipos o sistemas y las técnicas de ingeniería social más habituales.
6.5.	Registro con contraseñas fuertes.	La protección de la autenticación en redes sociales en redes sociales debería seguir los mismos principios en cuanto a fortaleza, caducidad y selectividad de las contraseñas que la autenticación en dispositivos o en servicios y servidores corporativos conectados a redes.	Proteger el acceso a los perfiles en redes sociales con contraseñas fuertes, alfanuméricas, y que contengan una combinación pseudoaleatoria de caracteres ordinarios y especiales. Conviene renovarla periódicamente, y no utilizar la misma contraseña de una cuenta de red social en otras cuentas de redes sociales, y mucho menos en dispositivos, servicios o servidores del partido político. Cuando estén disponibles para proteger el acceso a las cuentas en redes sociales, es siempre más seguro utilizar dos factores de autenticación.	**[op.acc.6]** Mecanismo de autenticación (usuarios de la organización) **Refuerzo R1**-Contraseñas. **[op.acc.6.r1.2]** Se impondrán normas de complejidad mínima y robustez frente a ataques de adivinación. **Refuerzo R2**-Contraseña + otro factor de autenticación. **[op.acc.6.r2.1]** Se requerirá un segundo factor tal como «algo que se tiene», es decir, un dispositivo, una contraseña de un solo uso (OTP, en inglés) como complemento a la contraseña de usuario, o «algo que se es».
6.6.	Control de la geolocalización.	Muchas de las redes sociales proporcionan al usuario la posibilidad de declarar la	Controlar la geolocalización de los perfiles y de los contenidos que se transmiten a través de ellos en redes sociales, mediante la	**[mp.per.3]** Concienciación. Se realizarán las acciones necesarias para concienciar regularmente al personal acerca de su

lista de chequeo 6		Ciberseguridad de redes sociales		
		localización geográfica de los contenidos que se comparten. Esta función podría aportar a un atacante un mapa de la actividad de una persona, que podría ser objetivo así de un ciberataque selectivo.	desactivación de las funciones de geolocalización por defecto en el menú de configuración de las cuentas, haciendo uso de esa función de manera inteligente: es una función puesta al servicio del usuario, de manera que conviene emplearla sin ponerse en riesgo y pensando en cada caso si interesa que los demás tengan un mapa de la vida del usuario, o de parte de ella.	papel y responsabilidad para que la seguridad del sistema alcance los niveles exigidos. En particular, se recordará periódicamente: **[mp.per.3.1]** La normativa de seguridad relativa al buen uso de los equipos o sistemas y las técnicas de ingeniería social más habituales. **[op.exp.2]** Configuración de seguridad. Se configurarán los equipos previamente a su entrada en operación, de forma que: **[op.exp.2.2]** Se aplicará la regla de «mínima funcionalidad», es decir: a) El sistema debe proporcionar la funcionalidad mínima imprescindible para que la organización alcance sus objetivos. b) b) No proporcionará funciones injustificadas (de operación, administración o auditoría) al objeto de reducir al mínimo su perímetro de exposición, eliminándose o desactivándose aquellas funciones que sean innecesarias o inadecuadas al fin que se persigue.
6.7.	Atención reforzada en la mensajería privada.	La utilización de redes privadas de mensajería instantánea es masiva en todos los ámbitos de la vida social y personal. En esa utilización, conviven salas de mensajes de grupos familiares, profesionales, políticos e institucionales, con conversaciones privadas. Además, se produce una creciente intersección entre las	Para disminuir los riesgos de ciberseguridad en la actividad de usuarios en aplicaciones de mensajería privada, las siguientes recomendaciones son de aplicación: 1) Incrementar la atención puesta en el momento de compartir contenidos entre grupos o conversaciones distintas, o entre aplicaciones distintas (entre el correo electrónico y la mensajería instantánea, por ejemplo). Detenerse unos minutos a pensar y cerciorarse en cada momento si el contenido que se va a	**[mp.per.3]** Concienciación. Se realizarán las acciones necesarias para concienciar regularmente al personal acerca de su papel y responsabilidad para que la seguridad del sistema alcance los niveles exigidos. En particular, se recordará periódicamente: **[mp.per.3.1]** La normativa de seguridad relativa al buen uso de los equipos o sistemas y las técnicas de ingeniería social más habituales. **[org.2]** Normativa de seguridad. Se dispondrá de una serie de documentos que describan:

lista de chequeo 6		Ciberseguridad de redes sociales		
		aplicaciones de mensajería instantánea y otras aplicaciones instaladas en teléfonos inteligentes, como el correo electrónico o las aplicaciones de redes sociales.	compartir con origen en un grupo o en una conversación es adecuado para el destino de redifusión que se le pretende dar. 2) No aceptar solicitudes de adhesión a grupos de mensajería sin efectuar una doble verificación (comprobación extra por otro canal): que quien nos está proponiendo la adhesión lo está haciendo realmente, y es alguien que es conocido o que puede ser verificado. 3) Como norma general, no cliquear enlaces ni ficheros recibidos mediante mensajería privada, salvo que se haya realizado una doble verificación de la identidad e intención del remitente del mensaje. 4) No compartir información sensible por mensajería privada. Si se hace, encriptar previamente con software de cifrado, y fuera de la aplicación de mensajería, el contenido a compartir.	**[org.2.1]** El uso correcto de equipos, servicios e instalaciones, así como lo que se considerará uso indebido.

3.6. GESTIÓN DE INCIDENTES DE CIBERSEGURIDAD

Si bien la esencia de una guía de ciberseguridad reside en recomendar medidas que prevengan incidentes en la seguridad de la información y en sistemas informáticos, no es menos cierto que esas recomendaciones están basadas en la asunción de que, de otra manera, con mayor o menor profundidad y gravedad, los incidentes de ciberseguridad se producirán. Es la premisa que adopta, por el ejemplo, el modelo de confianza cero. Tal asunción permite planificar la ciberseguridad de un modo realista, aceptando que no existe un sistema informático cien por cien seguros pero que, precisamente por eso, hay que tender a que quedarse lo más cerca que sea posible de ese cien por cien.

Igual que las medidas preventivas están destinadas a anticiparse a las ciberamenazas, la aceptación estratégica de que los incidentes de ciberseguridad acaecerán en algún momento sugiere tener preparado un repertorio de procedimientos y recursos dirigidos a gestionar esos incidentes cuando lleguen. Esta preparación permitirá, en primera instancia, contener y mitigar los efectos del incidente y, en segunda, facilitar la resiliencia, la recuperación de la continuidad y operativa de los sistemas informáticos después de que hayan sido afectados por un incidente de ciberseguridad.

Un incidente informático es cualquier anomalía de hardware, software o redes que impide que un sistema, gestionado por informática, funcione con normalidad. Si ese incidente es, además, de ciberseguridad, implica que ha sido producido directa o indirectamente por la acción intencionada de uno o varios atacantes recurriendo a tácticas, técnicas y procedimientos específicos: es decir, que el incidente ha sido producido por una ciberamenaza.

Aunque las aproximaciones a la contención, mitigación, resolución y recuperación de sistemas informáticos afectados por incidentes de ciberseguridad puedan ser variadas e implementadas de maneras distintas, cabe sugerir una serie de recomendaciones de buenas prácticas para implantar una sistemática de gestión de incidentes de ciberseguridad en una organización.

lista de chequeo 7		**Gestión de Incidentes de Ciberseguridad**		
nº	BUENA PRÁCTICA	PROPÓSITO	CARACTERÍSTICAS	VINCULACIÓN CON EL ENS
7.1.	Institucionalización de una Política de Ciberseguridad.	Aunque en una organización teóricamente podría establecerse un sistema de gestión y respuesta a incidentes de ciberseguridad, es improbable que sea eficiente y	Una política institucional de ciberseguridad corporativa debería definir y provisionar, al menos:	**Artículo 12.** Política de seguridad y requisitos mínimos de seguridad. **[org.1]** Política de seguridad. La política de seguridad, que se aprobará de conformidad con lo dispuesto en el artículo 12 de este real

lista de chequeo 7		Gestión de Incidentes de Ciberseguridad		
		efectivo si no está incardinado en una política de ciberseguridad o en un sistema de gestión de la seguridad de la información (SGSI). Las políticas de ciberseguridad no sólo aseguran la gobernanza de la ciberseguridad en una organización, sino que además definen y dotan los recursos necesarios para afrontar y gestionar las ciberamenazas, y sistematizan los procesos para proteger los sistemas informáticos. Además, una política institucionalizada de ciberseguridad crea una cultura de la ciberseguridad en la organización, necesaria para la concienciación en ciberseguridad en sus integrantes, que muchas veces son la primera línea de defensa ante multitud e ciberamenazas que llegan a través de correos electrónicos, sitios web, SMS o mensajes en redes sociales o en servicios de mensajería instantánea.	1. La organización institucional de la ciberseguridad. Roles y perfiles para la gestión de incidentes. 2. La/el Responsable de Seguridad de la Información. 3. La/el Responsable de Sistemas de Información. 4. La composición, funciones, recursos y procedimientos de un Equipo de Respuesta a Ciberincidentes. 5. Los mecanismos de gerencia y gestión de la ciberseguridad, que deben contemplar la preparación de la institución para afrontar incidentes de ciberseguridad mediante los equipos de respuesta; la dotación de medios para la detección, análisis e identificación de los incidentes; la articulación de capacidades de contención, mitigación y recuperación; y finalmente las actividades de post-incidente y de reporte.	decreto, se plasmará en un documento en el que, de forma clara, se precise, al menos, lo siguiente: **[org.1.1]** Los objetivos o misión de la organización. **[org.1.2]** El marco legal y regulatorio en el que se desarrollarán las actividades. **[org.1.3]** Los roles o funciones de seguridad, definiendo para cada uno los deberes y responsabilidades del cargo, así como el procedimiento para su designación y renovación. **[org.1.4]** La estructura del comité o los comités para la gestión y coordinación de la seguridad, detallando su ámbito de responsabilidad, las personas integrantes y la relación con otros elementos de la organización. **[org.1.5]** Las directrices para la estructuración de la documentación de seguridad del sistema, su gestión y acceso.

lista de chequeo 7		Gestión de Incidentes de Ciberseguridad		
7.2.	Mecanismo de detección, análisis e identificación de ciberincidentes.	Los mecanismos, herramientas y recursos de detección de ciberincidentes están dirigidos a detectar indicadores de ciberataque y de las brechas de seguridad que un ciberataque pudiera producir en los sistemas informáticos, además de proporcionar una correcta identificación del incidente que propicie su adecuado análisis por parte del Equipo de Respuesta a Ciberincidentes.	Entre las funciones que un sistema institucionalizado de gestión de ciberincidentes debe estar en condiciones de asumir en esta fase están: 1) Capacidad para detectar precursores de un ciberincidente, es decir, elementos dentro del sistema informático que sugieren anticipadamente que se podría producir un ciberincidente en un período de tiempo en el futuro próximo. 2) Capacidad para detectar indicadores de un ciberincidente, es decir, elementos dentro del sistema informático que sugieren que un ciberincidente se está produciendo en el presente o se ha venido produciendo desde un pasado inmediato. 3) Esquema de procedimientos internos destinados a activar las primeras actuaciones corporativas y del personal ante una posible ciberamenaza. 4) Activación de protocolos de comunicación y notificación del ciberincidente, tanto en lo que se refiere a: • Comunicaciones internas en la organización. • Comunicaciones externas para alertas preliminares. • Comunicaciones exigidas por cumplimiento normativo.	**[op.exp.6]** Protección frente a código dañino. **Refuerzo R4**-Capacidad de respuesta en caso de incidente. **[op.exp.6.r4.1]** Se emplearán herramientas de seguridad orientadas a detectar, investigar y resolver actividades sospechosas en puestos de usuario y servidores (EDR - Endpoint Detection and Response). **[op.mon.1]** Detección de intrusión. **[op.mon.1.1]** Se dispondrá de herramientas de detección o prevención de intrusiones. **[op.mon.3]** Vigilancia. **Refuerzo R3**-Ciberamenazas avanzadas. **[op.mon.3.r3.1]** Se dispondrá de sistemas para detección de amenazas avanzadas y comportamientos anómalos. **[op.mon.3.r3.2]** Se dispondrá de sistemas para la detección de amenazas persistentes avanzadas (Advanced Persistent Threat, APT) mediante la detección de anomalías significativas en el tráfico de la red. **Refuerzo R1**-Correlación de eventos. [**op.mon.3.r1.1]** Se dispondrá de un sistema automático de recolección de eventos de seguridad que permita la correlación de los mismos. **[mp.per.3]** Concienciación. Se realizarán las acciones necesarias para concienciar regularmente al personal acerca de su papel y responsabilidad para que la seguridad del

lista de chequeo 7		Gestión de Incidentes de Ciberseguridad		
			5) Capacidades de clasificación del incidente, con determinación de su nivel de peligrosidad, y de análisis de la naturaleza, alcance, comportamiento y herramientas de la ciberamenaza.	sistema alcance los niveles exigidos. En particular, se recordará periódicamente: **[mp.per.3.2]** La identificación de incidentes, actividades o comportamientos sospechosos que deban ser reportados para su tratamiento por personal especializado. **[mp.per.3.3]** El procedimiento para informar sobre incidentes de seguridad, sean reales o falsas alarmas.
7.3.	Mecanismo de contención y mitigación de ciberincidentes.	Una vez un ciberincidente ha sido detectado e inicialmente evaluado, el sistema de gestión de ciberincidentes debe provisionar las capacidades para contener el avance de la ciberamenaza y mitigar sus efectos, evitando al máximo posible su propagación e insertando en el sistema contramedidas para detener su operativa.	Entre las funciones que un sistema institucionalizado de gestión de ciberincidentes debe desplegar para contener y mitigar la acción de una ciberamenaza están: 1) La evaluación de solicitudes de apoyo externo para contener el ciberincidente. 2) El aislamiento y/o desconexión de equipos y redes inicialmente afectados por el ciberincidente. 3) El filtrado de tráfico para sistemas críticos y la aplicación de técnicas de control de DNS. 4) El bloqueo de indicadores de la ciberamenaza. 5) La reubicación de equipos comprometidos en nuevas subredes aisladas de área local. 6) La documentación de todo el proceso para posteriores análisis.	**[op.mon.1]** Detección de intrusión. **[op.mon.1.r2.1]** Existirán procedimientos de respuesta a las alertas generadas por el sistema de detección o prevención de intrusiones. **[op.exp.7]** Gestión de incidentes. **[op.exp.7.1]** Se dispondrá de un proceso integral para hacer frente a los incidentes que puedan tener un impacto en la seguridad del sistema, que incluya el informe de eventos de seguridad y debilidades, detallando los criterios de clasificación y el escalado de la notificación. **Refuerzo R2** –Detección y Respuesta. El proceso integral para hacer frente a los incidentes que puedan tener un impacto en la seguridad del sistema deberá incluir: **[op.exp.7.r2.1]** Implantación de medidas urgentes, incluyendo la detención de servicios, el aislamiento del sistema afectado, la recogida de evidencias y protección de los registros, según convenga al caso. **[op.exp.7.r2.4]** Medidas para: a) Prevenir que se repita el incidente.

lista de chequeo 7		Gestión de Incidentes de Ciberseguridad		
				b) Incluir en los procedimientos de usuario la identificación y forma de tratar el incidente. c) Actualizar, extender, mejorar u optimizar los procedimientos de resolución de incidentes.
7.4.	Mecanismo de evaluación y recuperación de sistemas afectados.	Tras la contención y la mitigación de la ciberamenaza y la introducción de contramedidas para evitar su avance, el sistema de respuesta a ciberincidentes despliega recursos para desactivar la actividad dañina en los sistemas informáticos.	Entre las funciones que un sistema institucionalizado de gestión de ciberincidentes debe poner en práctica para recuperar la continuidad de los sistemas informáticos tras la acción de una ciberamenaza estarían: 1) La erradicación de la actividad informática nociva y sospechosa. 2) El análisis de los procedimientos de retorno a operaciones normales, mediante el despliegue del correspondiente entorno de pruebas. 3) La aplicación de las copias de recuperación y respaldo. 4) La monitorización de nueva actividad sospechosa. 5) La restauración de los sistemas, la reinstalación que procediera del software, y la aplicación de mantenimiento correctivo si hubiere lugar.	**[op.exp.7]** Gestión de incidentes. **[op.exp.7.r2.2]** Asignación de recursos para investigar las causas, analizar las consecuencias y resolver el incidente.
7.5.	Reporte y comunicación post-incidente.	Una vez recuperados a una condición mínima de normalidad	El reporte post-incidente podría incluir, entre otras, las siguientes actividades:	**[op.exp.7]** Gestión de incidentes.

lista de chequeo 7		Gestión de Incidentes de Ciberseguridad		
		los sistemas afectados por la acción de una ciberamenaza, el sistemas de respuesta ante ciberincidentes debería elaborar un reporte del ciberincidente, incluyendo en ese reporte las provisiones que requiera el correspondiente cumplimiento normativo.	1) Una descripción detallada de todo el proceso, desde que los primeros precursores son detectados, y de las respuestas que se fueron dando en cada fase de respuesta. 2) Incluir los elementos a que hubiere lugar desde la perspectiva del cumplimiento normativo. 3) Un repertorio de lecciones aprendidas, conteniendo los puntos fuertes y débiles, y las propuestas de mejora, que la gestión del ciberincidente ha servido para poner de manifiesto en la organización.	**[op.exp.7.r2.3]** Informar del incidente a los responsables de la información y servicios afectados y de las actuaciones llevadas a cabo para su resolución. **[op.exp.9]** Registro de la gestión de incidentes. Se registrarán todas las actuaciones relacionadas con la gestión de incidentes, de forma que: **[op.exp.9.1]** Se registrarán los reportes iniciales, intermedios y finales de los incidentes, las actuaciones de emergencia y las modificaciones del sistema derivadas del incidente. **[op.exp.9.2]** Se registrará aquella evidencia que pueda dirimirse en un ámbito jurisdiccional, especialmente cuando el incidente pueda comportar acciones disciplinarias sobre el personal interno, sobre proveedores externos o en la persecución de delitos. En la determinación de la composición y detalle de estas evidencias, se recurrirá a asesoramiento legal especializado. **[op.exp.9.3]** Como consecuencia del análisis de los incidentes, se revisará la determinación de los eventos auditables.

3.7. CAPACITACIÓN EN CIBERSEGURIDAD DE USUARIO

Aunque en un porcentaje que varía dependiendo de las formas que adoptan los ciberataques, en un máximo número de ellos las acciones maliciosas de las ciberamenazas están diseñadas en una secuencia en donde, generalmente en sus estadios iniciales, es necesario el concurso involuntario e inadvertido de un usuario humano, cuyo dispositivo se intenta comprometer, para que realice algún tipo de comportamiento que active o de continuidad a la secuencia de ciberataque, por ejemplo a un infección por malware cuya primera fase se realiza mediante un correo electrónico con un fichero adjunto o un hipervínculo que se envía a una víctima potencial.

Con el propósito de lograr ese concurso involuntario del usuario de un sistema informático, el atacante suele recurrir a tácticas de engaño, de manipulación, que lleven al usuario a creer que es necesario, por ejemplo, hacer clic en un hipervínculo para descargarse una actualización de software, de la cual no sabe que es un virus. Al conjunto de engaños y manipulaciones que una ciberamenaza pone en marcha para lograr que un usuario lleve a cabo alguna conducta necesaria, pero involuntaria desde la perspectiva del usuario, para producir una acción maliciosa, se le denomina genéricamente **ingeniería social**. La manera más eficiente de combatir la ingeniería social desde una perspectiva de ciberseguridad es hacer al usuario más consciente y sensible respecto de cada una de las conductas de su comportamiento ante una interfaz informática.

Por eso, la capacitación de los usuarios de sistemas informáticos es imprescindible para la ciberseguridad de una organización, no meramente para proporcionar capacitación práctica a esos usuarios, sino porque son el eslabón más importante de la ciberseguridad, la primera línea de defensa de los sistemas informáticos, precisamente los usuarios que, en su mayor parte, no son ni técnicos en ciberseguridad ni en informática. Aunque no sea una comparación lineal sino metafórica, hoy en día tan importante es tener un usuario sensibilizado y capacitado en rutinas de autoprotección en seguridad, como disponer de software antivirus.

Las capacidades de las que debería disponer un usuario convencional de sistemas informáticos para minimizar las **posibilidades de que sea explotado como una vulnerabilidad del sistema** por parte de una ciberamenaza están englobadas, en general, en proveerse de una serie de rutinas de autoprotección en ciberseguridad a través de una serie de buenas prácticas de conocimiento.

lista de chequeo 8		Capacitación en Ciberseguridad de Usuario		
nº	BUENA PRÁCTICA	PROPÓSITO	CARACTERÍSTICAS	VINCULACIÓN CON EL ENS
8.1.	Concienciación en seguridad de la información y en ciberseguridad.	La base de la capacitación en ciberseguridad a nivel de usuario de sistemas informáticos pasa por la concienciación, por entender que representa el usuario y sus dispositivos en el conjunto del sistema informático de una organización, qué papel juega ese sistema informático en una organización, y qué consecuencias tendría una disrupción de ese sistema.	Los contenidos de capacitación que podrían impartirse en este módulo son: 1) Implicaciones de la tecnología en la continuidad de procesos en la vida de las personas en general, y en la vida de un partido político en particular. 2) Por qué un usuario de tecnologías es un elemento troncal en la ciberseguridad de una organización, proporcionándole una visión esquemática del mapa completo de las tecnologías de un partido político. 3) Por qué el eslabón crítico de la ciberseguridad no son los elementos tecnológicos, sino el factor humano.	**[mp.per.3]** Concienciación. Se realizarán las acciones necesarias para concienciar regularmente al personal acerca de su papel y responsabilidad para que la seguridad del sistema alcance los niveles exigidos. En particular, se recordará periódicamente: **[mp.per.3.1]** La normativa de seguridad relativa al buen uso de los equipos o sistemas y las técnicas de ingeniería social más habituales. **[mp.per.3.2**] La identificación de incidentes, actividades o comportamientos sospechosos que deban ser reportados para su tratamiento por personal especializado. **[mp.per.3.3]** El procedimiento para informar sobre incidentes de seguridad, sean reales o falsas alarmas.
8.2.	Visión general de las tácticas, técnicas y procedimientos de ciberamenazas.	Tras entender el papel de los sistemas informáticos en la continuidad de procesos de una organización, y la función que desempeñan esos sistemas los usuarios de dispositivos y servicios digitales, el siguiente paso es proporcionar al usuario conocimiento sobre las motivaciones de las ciberamenazas, y sus tácticas y procedimientos genéricos.	1) ¿Qué busca una ciberamenaza atacando las tecnologías de un partido político? 2) ¿En qué categorías podrían dividirse las ciberamenazas convencionales, y qué caracteriza a cada una de ellas? • Movidos por ideologías. • Movidos por lucro personal. 3) Más allá de las ciberamenazas convencionales: las Amenazas Persistentes Avanzadas (APT). • Visión panorámica del cibercrimen organizado global.	**[mp.per.3]** Concienciación. Se realizarán las acciones necesarias para concienciar regularmente al personal acerca de su papel y responsabilidad para que la seguridad del sistema alcance los niveles exigidos.

lista de chequeo 8		Capacitación en Ciberseguridad de Usuario		
			• Ciberamenazas estatales, apoyadas por Estados o sirviendo a intereses geopolíticos. • Acciones enmascaradas o de falsa bandera. 4) Ciberamenazas híbridas y tácticas de desinformación a través de Internet y de medios digitales.	
8.3.	Tácticas de ciberataque más comunes.	Después de entender, de manera genérica, las motivaciones de las distintas tipologías de ciberamenazas y qué tácticas y procedimientos despliegan en sus ciberataques, es conveniente que los usuarios conozcan más individualmente las tácticas de ciberataque más comunes que intentarán explotarlos como vulnerabilidad.	1) BEC o comprometimiento de la organización y/o de sus finanzas a través del correo electrónico. 2) Phishing, SMSmishing, Vishing, y Spam: ingeniería social para la diseminación de código dañino y contenidos no deseados. 3) Watering hole o ataques de abrevadero. Cuando el usuario es dirigido a conectarse a una web infectada con virus, o cuando se infecta con virus una web donde el usuario se conecta habitualmente. 4) Fraude de suplantación de identidad.	**[mp.per.3]** Concienciación. Se realizarán las acciones necesarias para concienciar regularmente al personal acerca de su papel y responsabilidad para que la seguridad del sistema alcance los niveles exigidos.

lista de chequeo 8		Capacitación en Ciberseguridad de Usuario		
			5) Propagación de contenidos sexuales, violentos o de odio. 6) Ingeniería social a través de servicios digitales. 7) Diversas tácticas de acoso y extorsión a través de medios digitales.	
8.4.	Tecnologías y herramientas de ciberseguridad.	Es conveniente que el usuario tenga un conocimiento superficial de las herramientas de ciberseguridad que tiene desplegadas su organización, y también más en profundidad de las herramientas antimalware que puede manejar un usuario.	1) Visión panorámica del mapa completo de la ciberseguridad de una organización y de sus herramientas. 2) Herramientas de ciberseguridad a nivel usuario.	**[mp.per.4]** Formación. **[mp.per.4.1]** Se formará regularmente al personal en aquellas materias relativas a seguridad de la información que requiera el desempeño de sus funciones, en particular en lo relativo a: a) Configuración de sistemas. b) Detección y reacción ante incidentes. c) Gestión de la información en cualquier soporte en el que se encuentre. Se cubrirán al menos las siguientes actividades: almacenamiento, transferencia, copias, distribución y destrucción. Además, se evaluará la eficacia de las acciones formativas llevadas a cabo.
8.5.	Rutinas de prevención en ciberseguridad. Chequeo diario de ciberseguridad.	Finalmente, tras haber adquirido un conocimiento genérico del sistema informático de la organización, de las amenazas a que está expuesto, y de las herramientas de las que dispone para prevenir y contener los ciberataques, se proporciona al usuario una serie de rutinas de prevención en	1) ¿Cuál es el estado de mi dispositivo la primera que lo consulto cada día? Señales de alerta o sospecha. 2) ¿Estoy suscrito a alertas de ciberseguridad y me entero de las últimas novedades en cuanto a los ciberataques a usuarios en población general o en mi sector?	**[mp.per.4]** Formación. **[mp.per.4.1]** Se formará regularmente al personal en aquellas materias relativas a seguridad de la información que requiera el desempeño de sus funciones, en particular en lo relativo a: d) Configuración de sistemas. e) Detección y reacción ante incidentes. f) Gestión de la información en cualquier soporte en el que se encuentre. Se cubrirán al

lista de chequeo 8		Capacitación en Ciberseguridad de Usuario		
		ciberseguridad para que las adopta como una buena práctica diaria.	3) ¿Qué tengo instalado en el teléfono? • Prevención ante la descarga e instalación desde Internet o desde redes compartidas de aplicaciones software. • ¿Alguna de las aplicaciones es poco confiable? • ¿Tengo instaladas aplicaciones de ocio junto a aplicaciones que gestionan o almacenan información sensible? 4) Aplicar las prevenciones adquiridas ante los mensajes con ficheros adjuntos recibidos por redes sociales o por correo electrónico. 5) Aplicar las enseñanzas aprendidas respecto al reconocimiento de señales de ingeniería social. 6) Pensar en los posibles riesgos antes de conectar un dispositivo externo en el ordenador, teléfono o tablet que estoy utilizando. 7) Pensar en los riesgos potenciales asociados respecto de los sitios web, redes sociales o redes de intercambio de ficheros a la que estoy conectando con los dispositivos que estoy utilizando, aplicando las enseñanzas aprendidas sobre señales de sospecha acerca de potencial actividad peligrosa.	menos las siguientes actividades: almacenamiento, transferencia, copias, distribución y destrucción. Además, se evaluará la eficacia de las acciones formativas llevadas a cabo.