

# Obtener el cumplimiento de los marcos normativos

---

# Cumplimiento de los marcos normativos

---

A menudo se requiere que las organizaciones cumplan con algún tipo de regulación de seguridad

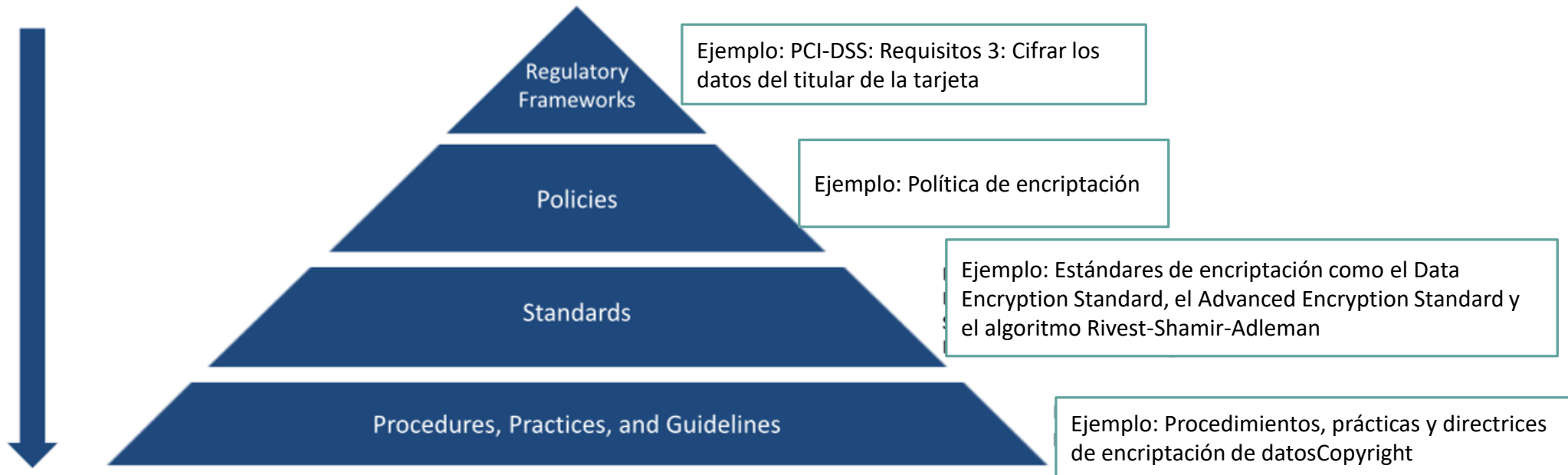
Cumplir con los marcos regulatorios es un esfuerzo de colaboración entre los gobiernos y los organismos privados para fomentar las mejoras voluntarias/obligatorias de la ciberseguridad

Los marcos regulatorios de seguridad informática contienen un conjunto de directrices y mejores prácticas

Los marcos regulatorios de seguridad informática informan a las empresas de que deben seguir estas directrices y mejores prácticas para cumplir con los requisitos reglamentarios, mejorar la seguridad y lograr ciertos objetivos empresariales

# Cumplimiento de los marcos normativos

Papel del cumplimiento de los marcos normativos en la seguridad administrativa de una organización



# ¿Por qué las organizaciones necesitan el cumplimiento de la normativa?

---

## **Mejora la seguridad**

- Los reglamentos y normas de seguridad informática mejoran la seguridad general de una organización al cumplir con los requisitos reglamentarios

## **Minimiza las pérdidas**

- La seguridad mejorada, a su vez, evita las violaciones de seguridad, que pueden costar pérdidas a la empresa

## **Mantiene la confianza**

- El cliente confía en la organización creyendo que su información está segura

# Determinar el marco normativo que hay que cumplir

Una organización debe evaluarse a sí misma para determinar qué marco normativo se le aplica mejor

Por ejemplo, la siguiente tabla muestra diferentes normativas y qué organización estaría sujeta al ámbito del marco normativo

| Marco normativo   | Organizaciones en el ámbito de aplicación  |
|---|--|
| Ley de Portabilidad y Responsabilidad del Seguro Médico (HIPAA)                             | Cualquier empresa u oficina que maneje datos sanitarios, incluidos, entre otros, los consultorios médicos, las compañías de seguros, los asociados comerciales y los empleadores                     |
| Ley Sarbanes Oxley Ley Federal de Gestión de la Seguridad de la Información de 2002 (FISMA) | Los consejos de administración de las empresas públicas estadounidenses, la dirección y las empresas de contabilidad pública   |
| Ley Gramm Leach Bliley (GLBA)   | Todas las agencias federales deben desarrollar un método de protección de los sistemas de información  |
| Norma de Seguridad de Datos del Sector de las Tarjetas de Pago (PCI-DSS)                    | Empresas que ofrecen productos o servicios financieros a particulares, como préstamos, asesoramiento financiero o de inversión, o seguros<br>Empresas que manejan información de tarjetas de crédito |

# Decidir cómo cumplir con el marco normativo

---

Cuando una organización entra en el ámbito de un determinado marco normativo, necesita interpretar correctamente los requisitos normativos del marco regulador que debe cumplir

Basándose en esos requisitos normativos, una organización necesita establecer políticas, procedimientos y controles de seguridad para gestionar y mantener el cumplimiento

Discutir los distintos marcos normativos,  
leyes y actos

---

# Payment Card Industry Data Security Standard (PCI-DSS)

---

La PCI-DSS es una norma de seguridad de la información patentada para las organizaciones que manejan información de los titulares de las principales tarjetas de débito, crédito, prepago, monedero electrónico, cajeros automáticos y puntos de venta

Se aplica a todas las entidades que participan en el procesamiento de las tarjetas de pago, incluidos los comerciantes, los procesadores, los adquirentes, los emisores y los proveedores de servicios, así como a todas las demás entidades que almacenan, procesan o transmiten datos de los titulares de las tarjetas

Panorama de alto nivel de los requisitos de la PCI-DSS elaborado y mantenido por el Consejo de Normas de Seguridad de la PCI



# Payment Card Industry Data Security Standard (PCI–DSS)

---

Normativa de seguridad de datos de la PCI:

- Visión general de alto nivel Construir y mantener una red segura
- Implementar fuertes medidas de control de acceso
- Proteger los datos de los titulares de las tarjetas
- Supervisar y probar regularmente las redes
- Mantener un programa de gestión de la vulnerabilidad
- Mantener una política de seguridad de la información

El incumplimiento de los requisitos de la PCI-DSS puede dar lugar a multas o a la cancelación de los privilegios de procesamiento de tarjetas de pago.

# Reglamento General de Protección de Datos (RGPD)

---

El reglamento GDPR entró en vigor el 25 de mayo de 2018 y es una de las leyes de privacidad y seguridad más estrictas a nivel mundial

El GDPR impondrá duras multas a quienes infrinjan sus normas de privacidad y seguridad, con sanciones que alcanzan decenas de millones de euros

## Principios de protección de datos del GDPR

Licitud, equidad y transparencia: El tratamiento debe ser lícito, justo y transparente para el interesado Limitación de la finalidad: Debe tratar los datos para los fines legítimos especificados explícitamente al sujeto de los datos cuando los recogió

Minimización de los datos: Debe recopilar y procesar sólo los datos necesarios para los fines especificados

Exactitud: Debe mantener los datos personales exactos y actualizados

Limitación del almacenamiento: Sólo puedes almacenar los datos de identificación personal durante el tiempo necesario para los fines especificados

Integridad y confidencialidad: El tratamiento debe realizarse de forma que se garantice la seguridad, integridad y confidencialidad adecuadas (por ejemplo, utilizando el cifrado)

Responsabilidad: El responsable del tratamiento es el encargado de demostrar el cumplimiento del GDPR con todos estos principios

# Reglamento General de Protección de Datos (RGPD)

---

El reglamento GDPR entró en vigor el 25 de mayo de 2018 y es una de las leyes de privacidad y seguridad más estrictas a nivel mundial

El GDPR impondrá duras multas a quienes infrinjan sus normas de privacidad y seguridad, con sanciones que alcanzan decenas de millones de euros

# Normativa de ciberseguridad en Europa

---

La **normativa europea de ciberseguridad** se rige por las siguientes leyes:

- **Directiva 2016/1148**, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad en las redes y sistemas de información de la Unión (Directiva NIS).
- [Reglamento Europeo de Protección de Datos](#) 2016/679 (RGPD). Establece la implantación de nuevas medidas de seguridad para las empresas europeas, los autónomos y la Administración pública.
- **Ley de Seguridad Cibernética** (Cybersecurity Act), aprobada el 27 de junio de 2019 por la UE. Esta ley moderniza y refuerza la Agencia de la UE para la ciberseguridad (ENISA) y establece un marco de certificación de la ciberseguridad en toda la UE para productos, servicios y procesos digitales.

# Normativa de ciberseguridad en España

---

## Normativas de seguridad nacional

- **Ley 36/2015, de 28 de septiembre, de Seguridad Nacional**, que regula los principios y organismos clave así como las funciones que deberán desempeñar para la defensa de la Seguridad Nacional.
- **Orden TIN/3016/2011**, de 28 de Octubre, por la que se crea el Comité de Seguridad de las Tecnologías de la Información y las Comunicaciones del Ministerio de Trabajo e Inmigración.

## Normativas de seguridad

- **Ley Orgánica 4/2015**, de 30 de marzo, de protección de la seguridad ciudadana.
- **Ley 5/2014**, de 4 de abril, de Seguridad Privada.

# Referidas a las telecomunicaciones

---

- **Ley 34/2002**, de 11 de julio, de servicios a la sociedad de la información y comercio electrónico.
- Real Decreto 381/2015, de 14 de mayo, por el que se establecen medidas contra el tráfico no permitido o irregular con fines fraudulentos en comunicaciones electrónicas.
- **Ley 50/2003**, de 19 de diciembre, de firma electrónica.
- **La Ley 9/2014, de 9 de mayo, General de Telecomunicaciones.**
- **Ley 25/2007**, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones.

Todas esas **leyes relacionadas con la seguridad de la información** están diseñadas con el objetivo de ofrecer un marco normativo que permita garantizar la seguridad de la información digital y establecer una legislación común a nivel europeo.

# Sobre la ciberdelincuencia

---

- Código Penal.
- Ley Orgánica 5/2000, de 12 de enero, reguladora de la responsabilidad penal de los menores.
- Real Decreto de aprobación de la Ley de Enjuiciamiento Criminal.

# Ley sobre la seguridad de las redes y sistemas de información

---

El **Real Decreto-ley 12/2018**, de 7 de septiembre, de seguridad de las redes y sistemas de información tiene por objeto:

- Regular la seguridad de las redes y sistemas de información utilizados para la provisión de los servicios esenciales y de los servicios digitales, y
- Establecer un sistema de notificación de incidentes.



# Ley sobre la seguridad de las redes y sistemas de información

---

Para ello, la **nueva normativa sobre ciberseguridad** en España se adapta al ordenamiento jurídico español la Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo conocida como «**Directiva europea sobre ciberseguridad**»(NIS).

Esta **Ley de seguridad de la información** identifica los sectores en los que es necesario garantizar la **protección de las redes y sistemas de información**, y establece procedimientos para identificar los servicios esenciales ofrecidos en dichos sectores, así como los principales operadores que prestan dichos servicios.

# ¿A quién afecta la normativa de ciberseguridad?

---

**La normativa de seguridad informática se aplica a los «operadores de servicios esenciales».**

El problema está en determinar quiénes son esos operadores de servicios esenciales.

Para ver qué entidades se encuentran dentro de esta clasificación, se tienen en cuenta varios criterios.

- Si son servicios fundamentales para la sociedad y la economía
- Si dependen o no de otro sistema de redes
- Efectos perjudiciales que tendría una incidencia sobre la prestación de esos servicios o la seguridad pública.

# ¿A quién afecta la normativa de ciberseguridad?

---

Por tanto, la **normativa de seguridad de una empresa** incluye a compañías de los siguientes sectores:

- Energía

- Gas: suministradores, red de distribución, transporte o almacenamiento, compañías de gas natural, etc.
- Electricidad: empresas eléctricas, red de distribución y transporte.
- Petróleo: operadores de oleoductos y de producción, refinado, almacenamiento y transporte.

- Transporte

- Aéreo: compañías aéreas
- Ferrocarril: empresas ferroviarias
- Marítimo y fluvial: empresas de transporte de pasajeros o mercancías

- Banca

- Sector sanitario

- Suministro y distribución de agua potable
- Infraestructura digital

- Servicios digitales: tiendas online o nubes de almacenamiento de datos

# Empresas excluidas

---

La **regulación sobre ciberseguridad** excluye a las siguientes empresas:

- Empresas de suministro de redes públicas de comunicaciones
- Empresas de servicios de comunicaciones electrónicas disponibles al público
- Prestadores de servicios de confianza
- Sectores regulados por leyes específicas que establezcan similares requisitos de seguridad

# Obligaciones que establece la normativa

---

Las principales **obligaciones** que establece la **ley de ciberseguridad** son:

1. Mejorar sus sistemas de seguridad contra intrusiones y
2. Comunicar a las autoridades competentes las violaciones de seguridad que sufran.

# Mejora de los sistemas de seguridad

---

La **ley de seguridad informática en España** establece los siguientes mecanismos para mejorar en materia de ciberseguridad:

- **Prevención:** adoptar las medidas necesarias para prevenir ataques informáticos.
- **Detección:** si se produce una intrusión, debes detectar el momento en el que se produce y tomar las medidas necesarias para minimizar los daños.
- **Restauración:** debes restaurar el sistema dañado con las copias de seguridad realizadas anteriormente.
- **Análisis forense:** con él puedes ver las acciones que el atacante ha realizado en tu sistema.

# Notificar los incidentes de seguridad

---

Las Administraciones públicas o empresas del sector público están obligadas a **notificar al Centro Criptológico Nacional (CCN)** aquellos incidentes que tengan un impacto significativo en la seguridad de la información que manejan y los servicios que prestan en relación con la categoría del sistema.

En el sector privado, esta obligación se regula en el Reglamento europeo de Protección de Datos. Se deben notificar las [brechas de seguridad](#) tanto a los afectados como a la AEPD en un plazo de 72 horas.

# Formación

---

Para una correcta seguridad de la información en la empresa y evitar ser víctimas de ciberataques es fundamental una formación adecuada de los empleados en esta materia.

De esa forma aprenderán a adoptar las medidas necesarias para mantener segura la información que maneja la empresa y sabrán qué acciones no deben realizar porque pondrán en peligro la seguridad informática.

Existen multitud de cursos y máster con los que es posible adquirir esas competencias en ciberseguridad.



# Autoridad competente

---

Las **leyes informáticas en España** citan los organismos competentes en la materia:

- Para los operadores de **servicios esenciales**: la Secretaría de Estado de Seguridad, del Ministerio del Interior, a través del Centro Nacional de Protección de Infraestructuras y Ciberseguridad (CNPIC).
- En el caso de que no sean operadores críticos: la autoridad sectorial correspondiente por razón de la materia, según se determine reglamentariamente.
- Para los proveedores de **servicios digitales**: la Secretaría de Estado para el Avance Digital, del Ministerio de Economía y Empresa.
- Para los operadores de servicios esenciales y proveedores de servicios digitales que no siendo operadores críticos se encuentren comprendidos en el ámbito de aplicación de la Ley de Régimen Jurídico del Sector Público: el Ministerio de Defensa, a través del Centro Criptológico Nacional.

# Sanciones por delitos contra la ciberseguridad

---

Las infracciones de la normativa de ciberseguridad se clasifican en leves, graves y muy graves.

Las sanciones que se prevén son:

- Por la comisión de **infracciones muy graves**, multa de 500.001 hasta 1.000.000 euros.
- En caso de infracciones **graves**, multa de 100.001 hasta 500.000 euros.
- Por la comisión de infracciones **leves**, amonestación o multa hasta 100.000 euros.

# Relación de la normativa de ciberseguridad con la Protección de Datos

---

La relación entre ciberseguridad y protección de datos es evidente. Y más en un mundo globalizado como el actual.

De hecho, para proteger los datos personales que manejamos debemos implantar unas adecuadas medidas de seguridad informática.

Con la entrada en vigor del Reglamento europeo de Protección de Datos (RGPD) queda patente la relación existente entre ambas.

En relación con los incidentes de seguridad, cada organización deberá comunicar la brecha de seguridad a la autoridad de protección de datos y en casos graves a los afectados tan pronto sean conocidas en un plazo máximo de 72 horas.

# Resumen

---

Orden TIN/3016/2011, de 28 de octubre, por la que se crea el Comité de Seguridad de las Tecnologías de la Información y las Comunicaciones del Ministerio de Trabajo e Inmigración

Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica

Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información

Real Decreto 43/2021, de 26 de enero, por el que se desarrolla el Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información

Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia

Ley Orgánica 2/2002, de 6 de mayo, reguladora del control judicial previo del Centro Nacional de Inteligencia

# Resumen Normativa Seguridad Nacional

---

Ley 9/1968, de 5 de abril, sobre secretos oficiales

Decreto 242/1969, de 20 de febrero, por el que se desarrollan las disposiciones de la Ley 9/1968, de 5 de abril sobre Secretos Oficiales

Ley Orgánica 4/1981, de 1 de junio, de los estados de alarma, excepción y sitio

Ley 1/2019, de 20 de febrero, de Secretos Empresariales

Orden PCI/487/2019, de 26 de abril, por la que se publica la Estrategia Nacional de Ciberseguridad 2019, aprobada por el Consejo de Seguridad Nacional

Real Decreto 1150/2021, de 28 de diciembre, por el que se aprueba la Estrategia de Seguridad Nacional 2021

# Resumen Normativa Seguridad

---

Orden INT/28/2013, de 18 de enero, por la que se desarrolla la estructura orgánica y funciones de los Servicios Centrales y Periféricos de la Dirección General de la Policía. [Inclusión parcial]

Ley Orgánica 4/2015, de 30 de marzo, de protección de la seguridad ciudadana

Ley 5/2014, de 4 de abril, de Seguridad Privada

Real Decreto 2364/1994, de 9 de diciembre, por el que se aprueba el Reglamento de Seguridad Privada

# Leyes que han de cumplir pymes y autónomos

---

La Ley Orgánica de Protección de Datos y Garantía de los Derechos Digitales, o LOPDGDD vela por la privacidad de los ciudadanos en lo relativo a seguridad de los datos personales que gestionan las empresas, ya sea en formato electrónico o papel. Aplica a empresas grandes, pymes y autónomos, ya que todos ellos utilizan como mínimo datos de contacto del personal propio, clientes y proveedores.

En 2016, la Unión Europea aprobó el Reglamento General de Protección de Datos Personales, el RGPD, que entró en vigor en los países miembros el 25 de mayo de 2018. Esta normativa, que se traspone en la legislación española en la citada LOPDGDD, tiene por objetivo reforzar los derechos de los ciudadanos, a la vez que favorece la creación de nuevos modelos de negocio que aprovechan los avances tecnológicos (como big data o IoT). Los cambios aprobados afectan a las empresas, en líneas generales, de la siguiente forma:

- Se obliga a ciertas empresas a disponer de un Delegado de Protección de Datos.
- Se elimina la necesidad de inscribir los ficheros en la Agencia Española de Protección de Datos (AEPD)
- Se incorpora el principio de «rendición de cuentas», por el cual las empresas tendrán que implantar mecanismos para garantizar el cumplimiento de sus responsabilidades de protección de datos.
- Aumenta las sanciones.

# Leyes que han de cumplir pymes y autónomos

---

La Ley de Servicios de la Sociedad de la Información y de Comercio Electrónico, o LSSI-CE y, cuando se apruebe, la propuesta de Reglamento ePrivacy que ofrecen garantías de seguridad en el comercio electrónico, las comunicaciones electrónicas y las transacciones online.

- La LSSI-CE afecta a aquellas empresas que realicen actividades lucrativas o económicas en Internet:
- comercio electrónico;
- contratación en línea;
- información y publicidad;
- servicios de intermediación (ISP o proveedores de acceso a Internet, alojamiento y almacenamiento, y enlaces a contenidos);
- prestadores de servicios de correo electrónico y similares;
- registros de dominio y agentes registradores de dominio.

Los requisitos de cumplimiento legal nos obligan a incluir información sobre la empresa y los servicios que ofrecemos en la página web, la aplicación móvil, los perfiles en redes sociales y en las comunicaciones electrónicas, para proteger los derechos de los consumidores.



# Leyes que han de cumplir pymes y autónomos

---

La Ley de Propiedad Intelectual, o LPI, crea un marco de protección legal para las obras intelectuales. Para ello, define el concepto de «obra intelectual», crea un registro de obras y regula en qué términos se pueden o no utilizar estas obras según el criterio del autor.

Son obras intelectuales las obras literarias, artísticas o científicas en cualquier medio o soporte, tangible o intangible, actualmente conocido o que se invente en el futuro:

- libros, folletos, impresos, escritos, discursos, conferencias y similares;
- proyectos, planos, maquetas y diseños de obras arquitectónicas y de ingeniería;
- gráficos, mapas y diseños relativos a la topografía, la geografía y, en general, a la ciencia;
- obras fotográficas;
- programas de ordenador.

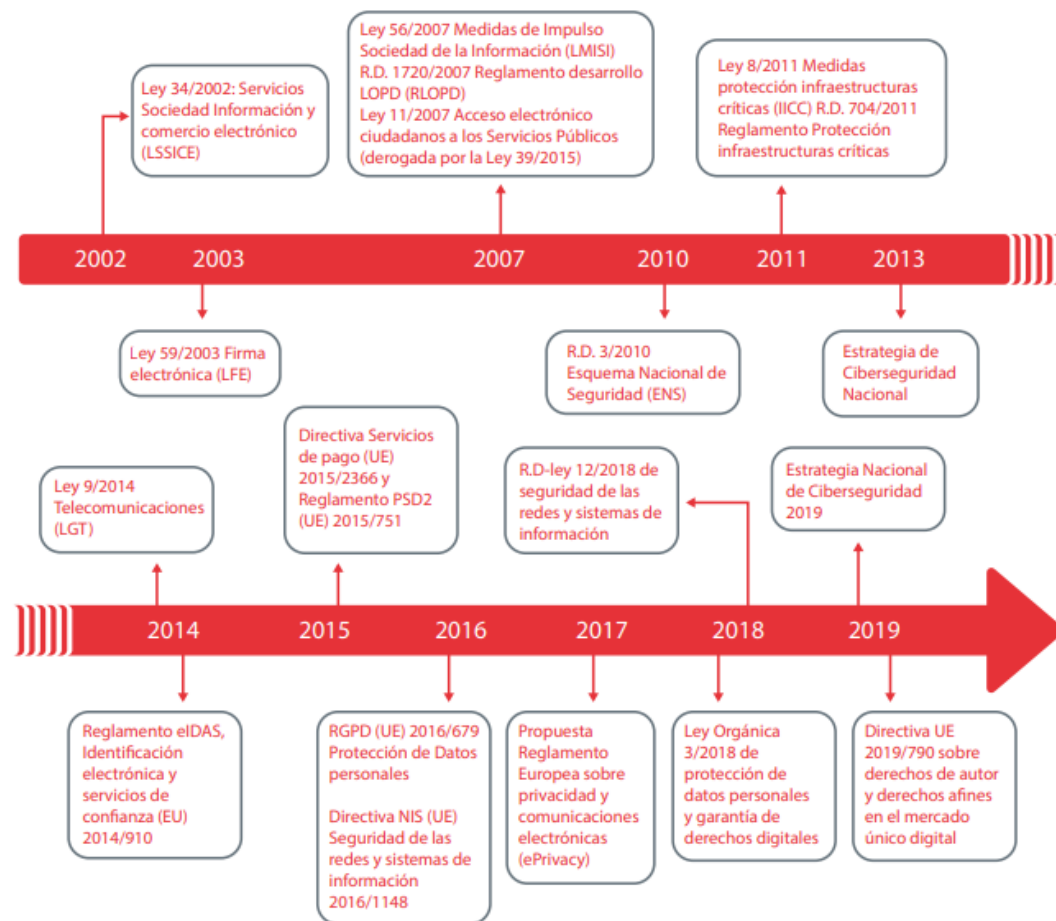
# Leyes que han de cumplir pymes y autónomos

---

Además de estas leyes, debemos tener en cuenta que en función de nuestro sector de negocio y clientes, debemos cumplir otros aspectos regulatorios adicionales que podrían afectarnos, por ejemplo:

- Ley 9/2014, General de Telecomunicaciones y otra normativa del Código de las Telecomunicaciones, en el caso de que nos dediquemos a la prestación de servicios de comunicaciones electrónicas.
- Ley 8/2011, por la que se establece medidas para la protección de infraestructuras críticas para mejorar la prevención, preparación y respuesta del Estado frente a atentados terroristas u otras amenazas que afecten a infraestructuras críticas.
- Ley 25/2013 de impulso de la Factura electrónica y creación del registro contable de facturas en el Sector Público, y su desarrollo. Esta ley obliga, desde el 15/01/2015 a las empresas que tienen relación comercial con la Administración Pública a emitir facturas electrónicas.
- Ley 59/2003, de Firma Electrónica y la Ley 11/2007, de Acceso Electrónico de los Ciudadanos a los Servicios Públicos (derogada en 2016, pero parcialmente en vigor hasta octubre de 2020) para cualquier relación con la Administración Pública.
- Ley 17/2001, de Marcas y la Ley 24/2015 de Patentes y otras leyes del Código de Propiedad Industrial, si nuestra actividad implica la gestión de patentes y marcas. Si tenemos un marco o logotipo corporativos tendremos en cuenta la Ley de Marcas.
- Ley 13/2011, de Regulación del Juego, si nuestra actividad tiene relación con el sector del juego online.

# Leyes que han de cumplir pymes y autónomos



# LOPDGDD Y RGPD

---

La LOPDGDD y el RGPD son las normas que velan por la protección de los datos de carácter personal, es decir, por la privacidad de las personas ya sean clientes, empleados o proveedores.

Las empresas, sociedades, comunidades, asociaciones y autónomos que han de cumplir el RGPD son:

- los establecidos en la UE, independientemente de si el tratamiento se hace o no en la UE;
- los que ofrecen bienes o servicios a personas que se encuentren en la UE;
- los que monitorizan el comportamiento de personas que se encuentren en la UE.

# LOPDGDD Y RGPD

---

Además de los principios de privacidad y derechos de los individuos sobre sus datos personales, en esta normativa se tratan los siguientes aspectos:

| INFORMAR                          | OBTENER<br>CONSENTIMIENTO                             | GARANTIZAR<br>DERECHOS   | NOTIFICAR<br>VIOLACIONES                     |
|-----------------------------------|---|--------------------------|--|
| Tratamiento                       | Inequívoco  | Que puedan<br>ejercerlos | Que supongan<br>riesgo para la<br>privacidad |
| Decisiones<br>automatizadas       | No tácito   |                          |  |
| Perfiles                          | Expreso en caso de<br>datos de especial<br>protección | Según los<br>plazos RGPD | A la autoridad                               |
| Transferencias<br>internacionales |   |                          | A los usuarios                               |

# Normas ISO de seguridad de la información

---

La **serie ISO/IEC 27000** de normas son estándares de seguridad publicados por la [Organización Internacional para la Estandarización](#) (ISO) y la [Comisión Electrotécnica Internacional](#) (IEC).

La serie contiene las [mejores prácticas](#) recomendadas en [Seguridad de la información](#) para desarrollar, implementar y mantener Especificaciones para los Sistemas de Gestión de la Seguridad de la Información (SGSI). la mayoría de estas normas se encuentran en preparación e incluyen:

# Normas ISO de seguridad de la información

---

- **ISO/IEC 27000** - es un vocabulario estándar para el SGSI. Introducción y base para el resto. Tercera versión: enero de 2014. Quinta versión: febrero 2018. ISO/IEC 27000:2018
- **ISO/IEC 27001** - es la certificación que deben obtener las organizaciones. Norma que especifica los requisitos para la implantación del SGSI. Es la norma más importante de la familia. Adopta un enfoque de gestión de riesgos y promueve la mejora continua de los procesos. Fue publicada como estándar internacional en octubre de 2005. Revisada en septiembre de 2013.
- **ISO/IEC 27002** - *Information technology - Security techniques - Code of practice for information security management*. Previamente BS 7799 Parte 1 y la norma ISO/IEC 17799. Es código de buenas prácticas para la gestión de seguridad de la información. Fue publicada en julio de 2005 como ISO 17799:2005 y recibió su nombre oficial ISO/IEC 27002:2005 el 1 de julio de 2007. Última versión: 27002:2013, de septiembre de 2013.

# Normas ISO de seguridad de la información

---

- **ISO/IEC 27004** - son métricas para la gestión de seguridad de la información. Es la que proporciona recomendaciones de quién, cuándo y cómo realizar mediciones de seguridad de la información. Publicada el 7 de diciembre de 2009, no se encuentra traducida al español actualmente.
- **ISO/IEC 27005** - trata la gestión de riesgos en seguridad de la información. Es la que proporciona recomendaciones y lineamientos de métodos y técnicas de evaluación de riesgos de Seguridad en la Información, en soporte del proceso de gestión de riesgos de la norma ISO/IEC 27001. Es la más relacionada con la actual British Standard BS 7799 parte 3. Publicada en junio de 2008. Revisada en junio de 2011.
- **ISO/IEC 27006** - Requisitos para la acreditación de las organizaciones que proporcionan la certificación de los sistemas de gestión de la seguridad de la información. Esta norma especifica requisitos específicos para la certificación de SGSI y es usada en conjunto con la norma 17021-1, la norma genérica de acreditación. Publicada en 2007 y revisada en diciembre de 2011 y septiembre de 2015.



# Normas ISO de seguridad de la información

---

- **ISO/IEC 27007** - es una guía para auditar al SGSI. Publicada en noviembre de 2011.
- **ISO/IEC 27008** - es una guía para auditar los controles seleccionados para implantar un SGSI. No es certificable. Publicada en octubre de 2011.
- **ISO/IEC 27009** - detalla los requisitos para usar la norma ISO/IEC 27001 en cualquier otro ámbito. No es certificable. Publicada en junio de 2016.

# Normas ISO de seguridad de la información

---

**ISO/IEC 27010** - es una guía para gestionar la seguridad de la información cuando se comparte entre distintas organizaciones. Es aplicable a todas las formas de intercambio y difusión de información. Publicada en octubre de 2012 y revisada en noviembre de 2015.

- **ISO/IEC 27011** - es una guía de interpretación de la información y gestión de la seguridad de esta información en organizaciones del sector de telecomunicaciones. Publicada en diciembre de 2008 y fue revisada en diciembre de 2016.

- **ISO/IEC 27014** - es una guía de gobierno corporativo de la seguridad de la información. Publicada en abril de 2013.

- **ISO/IEC 27015** - es una guía de SGSI orientada a organizaciones del sector financiero y de seguros. Publicada en noviembre de 2012.

# Normas ISO de seguridad de la información

---

- [ISO/IEC 27016](#) - es una norma que se concentra en un análisis financiero y económico de equipos y procedimientos de la seguridad de la información. Publicada en febrero de 2014.
- [ISO/IEC 27017](#) - es una guía de seguridad para Cloud Computing. Publicada en diciembre de 2015.
- [ISO/IEC 27018](#) - es una guía para controlar la protección de datos para servicios de computación en *cloud computing*. Publicado en julio de 2014.
- [ISO/IEC 27019](#) - es una guía para el proceso de sistemas de control específicos relacionados con el sector de la [industria de la energía](#).

# Normas ISO de seguridad de la información

---

- **ISO/IEC 27031** - es una guía de apoyo para la adecuación de las tecnologías de la información y comunicación. No es certificable. Publicada en marzo de 2011.
- **ISO/IEC 27032** - es una guía de apoyo para identificar las líneas generales para fortalecer el estado de la Ciberseguridad en una empresa. Publicada en julio de 2012.
- **ISO/IEC 27033** - es una guía detallada de seguridad de la administración, operación y uso de las redes. Publicada en 2010.
- **ISO/IEC 27034**: es una referencia en el área de tecnología de la información, técnicas de seguridad y seguridad de la aplicación. Publicado en 2011.

# Normas ISO de seguridad de la información

---

**ISO/IEC 27035:2011** - Seguridad de la información – Técnicas de Seguridad – Gestión de Incidentes de Seguridad. Este estándar hace foco en las actividades de: detección, reporte y evaluación de incidentes de seguridad y sus vulnerabilidades. Publicada en agosto de 2011.<sup>1</sup>

- **ISO/IEC 27036**: 2013 Tecnología de la información - Técnicas de seguridad - Seguridad de la información para las relaciones con los proveedores.
- **ISO/IEC 27038** - es una guía de especificación para seguridad en la redacción digital.
- **ISO/IEC 27039** - es una guía para la selección, despliegue y operación de sistemas de detección y prevención de intrusión.

# Normas ISO de seguridad de la información

---

- **ISO/IEC 27040** - es una guía para la seguridad en medios de almacenamiento.
- **ISO/IEC 27041** - es una guía para garantizar la idoneidad y adecuación de los métodos de investigación.
- **ISO/IEC 27042** - es una guía con directrices para el análisis e interpretación de las evidencias digitales.
- **ISO/IEC 27043** - desarrolla principios de investigación para la recopilación de evidencias digitales.

# Normas ISO de seguridad de la información

---

- **ISO/IEC 27050** - desarrolla en tres partes sobre la información almacenada en dispositivos electrónicos.
- **ISO/IEC 27103:2018** - es una norma desarrollada para proporcionar orientación sobre cómo aprovechar las normas existentes en un marco de ciberseguridad.
- **ISO/IEC 27701**
- **ISO/IEC 27799:2008** - es una guía para implementar ISO/IEC 27002 en la industria de la salud.

# ISO 27001

La ISO/IEC 27001 se basa en el conocido "[Ciclo de Deming](#)" **Plan-Do-Check-Act** (**PDCA** o **PHVA**) que significa "Planificar-Hacer-Verificar-Actuar" siendo este un enfoque de mejora continua:

- **Plan** (*planificar*): es una fase de diseño del SGSI, realizando la evaluación de riesgos de seguridad de la información y la selección de controles adecuados .
- **Do** (*hacer*): es una fase que envuelve la implantación y operación de los controles.
- **Check** (*verificar*): es una fase que tiene como objetivo revisar y evaluar el desempeño (eficiencia y eficacia) del SGSI.
- **Act** (*actuar*): en esta fase se realizan cambios cuando sea necesario para llevar de vuelta el SGSI a máximo rendimiento.

SGSI es descrito por la ISO/IEC 27001 y [ISO/IEC 27002](#) y relaciona los estándares publicados por la [International Organization for Standardization](#) (ISO) y la [International Electrotechnical Commission](#) (IEC). JJO también define normas estandarizadas de distintos SGSI.





# ¿Qué son los controles de CIS?

---

Desarrollados por el Center for Internet Security®, los Controles de Seguridad Crítica de CIS son un conjunto prescriptivo y prioritario de mejores prácticas en seguridad cibernética y acciones defensivas que pueden ayudar a prevenir los ataques más peligrosos y de mayor alcance, y apoyar el cumplimiento en una era de múltiples marcos.

Los controles de CIS proporcionan una orientación específica y una vía clara para que las organizaciones alcancen las metas y los objetivos descritos por múltiples marcos jurídicos, reglamentarios y normativos.

# ¿Qué son los controles de CIS?

---

La implementación de los Controles de Seguridad Críticos de CIS en su organización puede ayudarle eficazmente a:

- Desarrolle una estructura fundamental para su programa de seguridad de la información y un marco para toda su estrategia de seguridad.
- Siga un enfoque probado de gestión de riesgos para la ciberseguridad basado en la eficacia del mundo real.
- Concéntrese en el conjunto de medidas técnicas más eficaces y específicas disponibles para mejorar la postura de defensa de su organización.
- Cumpla fácilmente con otros marcos y regulaciones, incluido el marco de ciberseguridad NIST, NIST 800-53, NIST 800-171, serie ISO 27000, PCI DSS, HIPAA, NERC CIP y FISMA.

# Aprender a diseñar y desarrollar políticas de seguridad

---

# Política de seguridad

---

Una política de seguridad es un conjunto bien documentado de planes, procesos, procedimientos, normas y directrices necesarias para establecer un estado ideal de seguridad de la información de una organización

Las políticas de seguridad se utilizan para informar a las personas sobre cómo trabajar de manera segura y protegida; definen y guían las acciones de los empleados sobre cómo tratar las operaciones, los datos o los recursos sensibles de la organización.

La política de seguridad es una parte integral de un programa de gestión de la seguridad de la información para cualquier organización

# Política de seguridad

## Necesidad de una política de seguridad

Proporcionar una aplicación coherente de los principios de seguridad en toda la organización

Garantizar el cumplimiento de las normas de seguridad de la información

Limitar la exposición de la organización a las amenazas externas a la información

Definir el compromiso de la alta dirección en el mantenimiento de un entorno seguro

Proporcionar protección legal

Responder rápidamente a los incidentes de seguridad

Reducir el impacto de un incidente de seguridad

Minimizar el riesgo de una violación de datos

Mejorar la seguridad general de los datos y la red

# Características de una buena política de seguridad

---

Conciso y claro

Utilizable

Económicamente viable

Comprensible

Realista

Coherente

Procedimentalmente tolerable

Cumplimiento legal

Basado en normas y reglamentos

# Contenido de una política de seguridad

---

## Requisitos de seguridad de alto nivel

- Esta característica de los requisitos de un sistema cuando se implementan las políticas de seguridad que incluyen la seguridad de la disciplina, la seguridad de las salvaguardias, la seguridad de los procedimientos y la seguridad de la garantía

## Descripción de la política basada en el requisito

- Se centra en las disciplinas de seguridad, las salvaguardias, los procedimientos, la continuidad de las operaciones y la documentación

## Concepto de operación de la seguridad

- Define los roles, las responsabilidades y las funciones de una política de seguridad

## Asignación de la aplicación de la seguridad a los elementos de la arquitectura

- Proporciona una asignación de la arquitectura del sistema informático a cada sistema del programa
- Copyright

# Contenido típico del documento de política

|                                |                                      |  |
|--------------------------------|--------------------------------------|--|
| <b>Control de documentos</b>   | <b>Resumen</b>                       | <b>Declaraciones de política</b>                 |
| <b>Ubicación del documento</b> | <b>Propósito</b>                     | <b>Sanciones e infracciones</b>                  |
| <b>Historial de revisiones</b> | <b>Alcance</b>                       | <b>Normas, políticas y procesos relacionados</b> |
| <b>Aprobaciones</b>            | <b>Definiciones</b>                  | <b>Información de contacto</b>                   |
| <b>Distribución</b>            | <b>Funciones y responsabilidades</b> | <b>Dónde encontrar más información</b>           |
| <b>Historia del documento</b>  | <b>Destinatarios</b>                 | <b>Glosario/ Acrónimos</b>                       |



# Declaraciones políticas

---

Una política es tan eficaz como las declaraciones políticas que contiene; las declaraciones políticas deben estar escritas en un estilo muy claro y formal

## Varios ejemplos de una declaración política son:

|           |   |           |  |
|-----------|---|-----------|--|
| <b>01</b> | Todos los ordenadores deben tener activada la protección antivirus para proporcionar una protección continua en tiempo real | <b>04</b> | 06Todos los programas informáticos deben ser adquiridos por el departamento de TI de acuerdo con la política de adquisiciones de la organización                           |
| <b>02</b> | Todos los servidores deben tener los servicios mínimos configurados para realizar sus funciones designadas                  | <b>05</b> | Se debe conservar una copia de todos los medios de copia de seguridad y restauración junto con los medios de copia de seguridad externos                                   |
| <b>03</b> | Todo el acceso a los datos se basa en una necesidad empresarial válida y está sujeto a un proceso de aprobación formal      | <b>06</b> | Mientras se utilice Internet, no se permite a ningún usuario abusar, difamar, acechar, acosar, amenazar a nadie ni violar las leyes cibernéticas locales e internacionales |

# Pasos para crear e implementar políticas de seguridad

|           |   |           |  |           |   |
|-----------|---|-----------|--|-----------|---|
| <b>01</b> | Realice una evaluación de riesgos para identificar los riesgos para los activos de una organización | <b>02</b> | Aprenda de las directrices estándar y de otras organizaciones      | <b>03</b> | Incluya a la alta dirección y a otros miembros del personal en el desarrollo de la política |
| <b>04</b> | Establecer sanciones claras y hacerlas cumplir  | <b>05</b> | Publique la versión final a todos los miembros de una organización | <b>06</b> | Asegúrese de que todos los miembros de su personal lean, firmen y comprendan la política    |
| <b>07</b> | Despliegue herramientas para hacer cumplir las políticas  | <b>08</b> | Capacite a los empleados y edúquelos sobre la política             | <b>09</b> | Revise y actualice periódicamente   |

# Consideraciones antes de diseñar una política de seguridad

---

¿Cuál es el objetivo de la política?

¿Es un valor añadido o una mera formalidad?

¿Está la política en consonancia con los programas de formación?

¿Cumple la política con los objetivos de la organización?

¿Es la política una guía de buenas prácticas o debe basarse en alguna norma?

¿Cuántas personas entran en el ámbito de la política y quiénes son?

¿Cuál es el mínimo de información que debe conocer cada empleado para realizar su trabajo?

¿Se requieren todos los detalles en la política?

¿Pueden vincularse las políticas?

¿Cuál es el mejor método?

¿Qué necesita entender el personal de las políticas?

# Diseño de una política de seguridad

---

**Las directrices deben abarcar los siguientes puntos de la estructura de la política:**

Descripción detallada de los aspectos de la política

Funcionalidades de los afectados por la política

Es necesario el nivel de compatibilidad de la política

Consecuencias del incumplimiento

Aplicabilidad de la política al entorno

Descripción del estado de la política

Derechos de autor

# Tipos de políticas de seguridad de la información

| Política de seguridad de la información de la empresa (EISP)   | Política de seguridad específica (ISSP)   | Política de seguridad específica del sistema (SSSP)  |
|--|---|--|
| <p>La EISP impulsa el alcance de una organización y proporciona dirección a sus políticas de seguridad</p> <p>Ejemplos de EISP:</p> <ul style="list-style-type: none"><li>• Política de aplicaciones</li><li>• Política de seguridad de redes y dispositivos de red</li><li>• Auditoría de políticas de seguridad</li><li>• Política de copias de seguridad y restauración</li><li>• Política de seguridad de sistemas</li><li>• Políticas para servidores</li></ul> | <p>La ISSP orienta al público sobre el uso de los sistemas basados en la tecnología con la ayuda de directrices</p> <p>Ejemplos de ISSP:</p> <ul style="list-style-type: none"><li>• Políticas de acceso remoto e inalámbrico</li><li>• Plan de respuesta a incidentes</li><li>• Políticas de contraseñas</li><li>• Políticas para dispositivos personales</li><li>• Políticas de cuentas de usuario</li><li>• Políticas de uso de Internet y de la web</li></ul> | <p>La SSSP dirige a los usuarios durante la configuración o el mantenimiento de un sistema</p> <p>Ejemplos de SSSP:</p> <ul style="list-style-type: none"><li>• Política de DMZ</li><li>• Política de cifrado</li><li>• Política de uso aceptable</li><li>• Políticas para la computación segura en la nube</li><li>• Políticas de detección y prevención de intrusiones</li><li>• Política de control de acceso</li></ul> |

# Políticas de acceso a Internet

---

## Política promiscua

- Sin restricciones en el acceso a Internet/remoto
- No se bloquea nada

## Política permisiva

- Servicios peligrosos conocidos/ataques bloqueados
- La política comienza sin restricciones
- Agujeros conocidos tapados; peligros conocidos detenidos
- Imposible mantenerse al día con los exploits actuales; Los administradores siempre se ponen al día

## Política paranoica

- Todo está prohibido
- No hay conexión a Internet, o el uso de Internet está muy limitado
- Los usuarios encuentran maneras de evitar las restricciones demasiado severas

## Política prudente

- Proporciona la máxima seguridad al tiempo que permite los peligros conocidos, pero necesarios
- Todos los servicios están bloqueados
- Los servicios seguros/necesarios están habilitados individualmente
- Los servicios/procedimientos no esenciales que no pueden hacerse seguros no están permitidos
- Todo queda registrado

# Política de uso aceptable

---

Una política de uso aceptable define el uso adecuado de la información, los dispositivos informáticos electrónicos, las cuentas de sistema, las cuentas de usuario y los recursos de red de una organización

## Consideraciones de diseño:

- ¿Deben los usuarios leer y copiar archivos que no son suyos, pero a los que pueden acceder?
- ¿Deben los usuarios modificar los archivos a los que tienen acceso de lectura y escritura, pero que no son de su propiedad?
- ¿Se debe permitir a los usuarios utilizar archivos .rhosts, incluso cuando las entradas son aceptables?
- ¿Se debe permitir a los usuarios compartir cuentas?
- ¿Deben los usuarios hacer copias de las configuraciones del sistema para su uso personal o proporcionarlas a otras personas?
- ¿Deben los usuarios hacer duplicados de software protegido por derechos de autor?

# Política de cuentas de usuario

---

La política de cuentas de usuario define el proceso de creación de cuentas de usuario e incluye los derechos y responsabilidades de los usuarios

## Consideraciones sobre el diseño

- ¿Quién tiene la autoridad para aprobar las solicitudes de cuentas?
- ¿Quiénes (empleados, cónyuges, hijos o visitantes de la empresa) están autorizados a utilizar los recursos informáticos?
- ¿Pueden los usuarios tener varias cuentas en un mismo sistema? ¿Pueden los usuarios compartir cuentas?
- ¿Cuáles son los derechos y responsabilidades del usuario?
- ¿Cuándo se debe desactivar y archivar una cuenta?



# Política de acceso remoto

---

La política de acceso remoto define quién puede tener acceso remoto, los medios de acceso y los controles de seguridad del acceso remoto

## Consideraciones de diseño

¿Quién tiene permitido el acceso remoto?

¿Qué métodos específicos (como el módem por cable/DSL o el acceso telefónico) admite la empresa?

¿Están permitidos los módems de marcación en la red interna?

¿Existen requisitos adicionales, como la obligatoriedad de un antivirus y un software de seguridad en el sistema remoto?

¿Pueden otros miembros de la familia de un empleado utilizar la red de la empresa?

¿Existe alguna restricción sobre los datos a los que se puede acceder de forma remota?

# Política de protección de la información

---

La política de protección de la información define las directrices para el tratamiento, el almacenamiento y la transmisión de información sensible

## Consideraciones sobre el diseño

¿Cuáles son los niveles de sensibilidad de la información?

¿Quién puede acceder a la información sensible?

¿Cómo se almacena y transmite la información sensible?

¿Qué nivel de información sensible puede imprimirse en impresoras públicas?

¿Cuál es el proceso para eliminar la información sensible de los medios de almacenamiento (tritución de papel, limpieza de discos duros o desmagnetización de discos)?

# Política de gestión de cortafuegos

---

La política de gestión de cortafuegos define el acceso, la gestión y la supervisión de los cortafuegos en la organización

## Consideraciones sobre el diseño

¿Quién tiene acceso a los sistemas de cortafuegos?

¿Quién puede recibir solicitudes para realizar cambios en la configuración del cortafuegos?

¿Quién puede ver las reglas de configuración del cortafuegos y las listas de acceso?

¿Con qué frecuencia debe revisarse la configuración del cortafuegos?

# Política de acceso especial

---

La política de acceso especial define los términos y condiciones de la concesión de acceso especial a los recursos del sistema

## Consideraciones sobre el diseño:

¿Quién puede recibir solicitudes de acceso especial?

¿Quién puede aprobar las solicitudes de acceso especial?

¿Cuáles son las normas de contraseña para las cuentas de acceso especial?

¿Con qué frecuencia se cambian las contraseñas?

¿Qué razones o situaciones pueden llevar a la revocación de los privilegios de acceso especial?

# Política de conexión a la red

---

La política de conexión a la red define las normas para establecer la conexión de ordenadores, servidores u otros dispositivos a la red

## Consideraciones de diseño:

¿Quién puede instalar nuevos recursos en la red?

¿Quién aprueba la instalación de nuevos dispositivos?

¿Quién debe ser notificado cuando se añaden nuevos dispositivos a la red?

¿Quién documenta los cambios en la red?

¿Existen requisitos de seguridad para los nuevos dispositivos que se añaden a la red?

# Política de socios comerciales

---

La política de los socios comerciales define los acuerdos, las directrices y las responsabilidades para que los socios comerciales lleven a cabo sus actividades de forma segura

## Consideraciones sobre el diseño

- ¿Es obligatorio que una empresa tenga una política de seguridad por escrito?
- ¿Debe cada empresa tener un cortafuegos u otro dispositivo de seguridad perimetral?
- ¿Cómo se comunicarán (VPN por Internet o línea alquilada)?
- ¿Cómo se solicitará el acceso a los recursos del socio?
- ¿Debe cada socio llevar cuentas, libros y registros precisos relacionados con la empresa?

# Política de seguridad del correo electrónico

---

Una política de seguridad del correo electrónico define el uso adecuado del correo electrónico corporativo

## Consideraciones de diseño:

Definir el uso prohibido

Definir el uso personal, si está permitido

Los empleados deben saber si sus correos electrónicos son revisados y/o archivados

Qué tipos de correos electrónicos deben conservarse y durante cuánto tiempo

Cuándo cifrar los correos electrónicos

Consecuencias de la violación de la política de seguridad del correo electrónico

# Política de contraseñas

---

La política de contraseñas proporciona directrices para el uso de contraseñas seguras para los recursos de una organización

## Consideraciones de diseño:

Longitud y formación de las contraseñas

Complejidad de la contraseña

Listas negras de contraseñas

Duración de la contraseña

Práctica común de contraseñas



# Política de seguridad física

---

La política de seguridad física define las directrices para garantizar que se aplican las medidas de seguridad física adecuadas

## Consideraciones sobre el diseño:

- ¿Se revisan periódicamente las deficiencias de protección del edificio?
- ¿Existe un proceso para identificar a las personas ajenas a la empresa, como visitantes, contratistas y vendedores, antes de darles acceso a las instalaciones?
- ¿Existen sistemas de iluminación adecuados?
- ¿Están debidamente bloqueados todos los puntos de entrada?
- ¿Se auditan periódicamente las tarjetas de identificación, las cerraduras, las llaves y los controles de autenticación?
- ¿Se controlan regularmente las grabaciones de videovigilancia?
- ¿Se mantiene regularmente un inventario adecuado de los activos de la organización?

# Política de seguridad del sistema de información

---

La política de seguridad de los sistemas de información define las directrices para salvaguardar los sistemas de información de una organización del uso malicioso

## Consideraciones de diseño:

¿Están los sistemas de información protegidos con antimalware? ¿Se actualiza regularmente el antimalware?

¿Se actualiza y parchea regularmente el sistema operativo?

¿Están protegidos con políticas sólidas de contraseñas?

¿Están protegidos con políticas sólidas de seguridad física?

# Política de "Traiga sus propios dispositivos" (BYOD)

---

Una política BYOD proporciona un conjunto de directrices para maximizar los beneficios de la empresa y minimizar los riesgos mientras se utiliza el dispositivo personal de un empleado en la red de una organización

## Consideraciones de diseño:

- ¿Qué dispositivos personales están permitidos para su uso bajo BYOD?
- ¿A qué recursos se puede acceder a través de los dispositivos BYOD?
- ¿Qué características deben deshabilitarse en los dispositivos BYOD?
- ¿Cuáles son las consideraciones de almacenamiento de datos para los dispositivos BYOD?
- ¿Qué medidas de seguridad son necesarias para los datos y los dispositivos BYOD?

# Política de seguridad de software/aplicaciones

---

La política de seguridad de las aplicaciones exige medidas adecuadas que mejoren la seguridad de las aplicaciones propias y adquiridas

## Consideraciones de diseño:

Gestión de la configuración

Protección de los datos en el almacenamiento y el tránsito

Autenticación de la autorización

Gestión de errores y excepciones

Gestión de usuarios y sesiones

Validación de datos

Registro y auditoría

Encriptación

# Política de copias de seguridad de datos

---

La política de copias de seguridad ayuda a una organización a recuperar y salvaguardar la información en caso de un incidente de seguridad/fallo de la red

## Consideraciones de diseño:

Ubicación de las copias de seguridad de los datos

Nombre y contacto del personal autorizado que puede acceder a las copias de seguridad

Programación de las copias de seguridad

Tipo de método de copia de seguridad utilizado

Requisitos de hardware y software para realizar las copias de seguridad

# Política de datos confidenciales

---

La política de datos confidenciales define las directrices para identificar los datos confidenciales de una organización y los procedimientos para manejarlos

## Consideraciones de diseño:

Tratamiento de los datos confidenciales, incluido el almacenamiento, el acceso, la transmisión, la compartición, la eliminación, la manipulación y la divulgación de los datos confidenciales

Control de la seguridad de los datos confidenciales

Acceso de emergencia a los datos

# Política de clasificación de datos

---

Una política de clasificación de datos establece un marco para clasificar los datos de la organización en función de su nivel de sensibilidad, valor y criticidad dentro de la política de seguridad informática

Los datos de la organización se clasifican en uno de los tres niveles de sensibilidad o clasificaciones: restringido, privado y público

## Consideraciones sobre el diseño:

Clasificación adecuada de los datos por parte de los propietarios de los mismos

Protección de los datos en reposo

Protección de los datos en tránsito  
Etiquetado de los datos

# Política de uso de Internet

---

La política de uso de Internet rige la forma en que la conexión a Internet de la organización es utilizada por todos los dispositivos de la red

## Consideraciones de diseño:

Límite de uso de Internet tanto para el uso oficial como para el personal

Marco de tiempo para el uso personal

Adopción de métodos para la supervisión del uso de la web

Niveles de privacidad para los empleados

Contenido restringido



# Política de servidores

---

La política de servidores establece un estándar para la configuración base del servidor de una organización

Una política de servidores eficaz restringe el acceso no autorizado a los datos y la tecnología de una organización

## Consideraciones de diseño:

Consideración de la ubicación y la protección de los servidores

Configuración de los servidores

Supervisión de los servidores

# Política de redes inalámbricas

---

Una política de red inalámbrica establece las reglas y normas de acceso a los recursos de la red inalámbrica de una organización

## Consideración de diseño:

Definición de un punto de acceso para una WLAN

Colocación de un punto de acceso

Tecnologías utilizadas para la conectividad inalámbrica

Procedimiento de integración de un nuevo sistema en el entorno inalámbrico

Procedimiento de supervisión de la red

# Política de control de acceso de usuarios

---

La política de control de acceso de los usuarios da a una organización la capacidad de controlar, restringir, supervisar y proteger la disponibilidad, integridad y confidencialidad de los recursos corporativos

## Consideraciones de diseño:

¿Quién puede acceder (personas, procesos o máquinas)?

¿A qué recursos del sistema se puede acceder?

¿Qué archivos se pueden leer?

¿Qué programas se pueden ejecutar?

¿Cómo se comparten los datos con otras entidades?

# Política de seguridad de los interruptores

---

La política de seguridad de los conmutadores describe una configuración de seguridad mínima requerida para los conmutadores de la red

## Consideraciones sobre el diseño:

¿Se supervisan regularmente los datos de los conmutadores?

¿Se bloquean los servicios y aplicaciones innecesarios?

¿Están encriptadas todas las contraseñas y datos sensibles almacenados?

¿Se encuentra el conmutador en una zona restringida?

# Política de detección y prevención de intrusiones (IDS/IPS)

---

La política de IDS e IPS facilita la detección y prevención de intrusiones en la red de una organización

## Consideraciones sobre el diseño:

Implantación de un sistema IDS estándar

Supervisar continuamente los archivos de registro de un IDS

Actualizar periódicamente la definición del intruso en la lógica del IDS para todas las amenazas en evolución

# Política de encriptación

---

La política de cifrado define un uso y una gestión aceptables de los métodos, técnicas y herramientas de cifrado en toda la empresa

La política es aplicable a todos los recursos de red de la empresa

## **Consideraciones sobre el diseño:**

Debe definir los estándares de encriptación que se deben utilizar en una comunicación de datos por cable/inalámbrica de la empresa

# Política de enrutamiento

---

La política del router describe una configuración de seguridad mínima requerida para todos los routers de la red

## Consideraciones de diseño:

Autenticación de usuarios

Reglas de acceso

Colocación

Gestión de contraseñas

Servicios requeridos/no permitidos/bloqueados

# Lista de control de la aplicación de la política

---

Una vez creada la política de seguridad, la parte más difícil del proceso es desplegarla en toda la organización

1. Asegúrese de que la política de seguridad es aprobada por la alta dirección
2. Asegúrese de que la política de seguridad se adopta oficialmente como política de la empresa
3. Revise cada política y decida cómo puede aplicarse dentro de una organización
4. Asegúrese de que existen las herramientas y técnicas adecuadas para ajustarse a la política
5. Desarrolle un plan de cambio de política tanto para la red como para la propia política
6. Coordine con otros departamentos el desarrollo de procedimientos basados en las políticas
7. Ofrezca a los empleados una formación básica de concienciación sobre la seguridad de la información



# Realización de cursos de sensibilización en materia de seguridad

---

# Sensibilización y formación de los empleados

---

Los empleados son uno de los principales activos de la organización y pueden formar parte de la superficie de ataque de una organización

Una organización necesita proporcionar una formación formal de concienciación sobre la seguridad a sus empleados cuando se incorporan y, posteriormente, de forma periódica, para que los empleados sepan:

- Cómo defenderse a sí mismos y a la organización contra las amenazas
- Siguen las políticas y los procedimientos de seguridad para trabajar con TI
- Sepan a quién dirigirse si descubren una amenaza a la seguridad
- Puedan identificar la naturaleza de los datos basándose en la clasificación de los mismos
- Proteger los activos físicos e informativos de esa organización

Además, la organización debería proporcionar formación de concienciación sobre la seguridad a los empleados para cumplir con los requisitos normativos, si quieren cumplir con cierto marco normativo

Los diferentes métodos para formar a los empleados son:

- Formación en el aula
- Formación en línea
- Mesas redondas
- Página web de concienciación sobre la seguridad Proporcionar consejos
- Hacer cortometrajes
- Realizar seminarios

# Concienciación y formación de los empleados: Política de seguridad

---

La formación sobre la política de seguridad enseña a los empleados a desempeñar sus funciones y a cumplir la política de seguridad

Las organizaciones deben formar a los nuevos empleados antes de concederles acceso a la red o proporcionarles un acceso limitado hasta que completen su formación

## Ventajas:

- Implementación efectiva de una política de seguridad
- Las políticas se siguen y no sólo se aplican
- Crea conciencia sobre cuestiones de cumplimiento
- Ayuda a una organización a mejorar su seguridad de red

# Concienciación y formación de los empleados: Seguridad física

---

Se debe impartir una formación adecuada para educar a los empleados en materia de seguridad física

La formación aumenta los conocimientos y la concienciación sobre la seguridad física

La formación debe educar a los empleados sobre cómo:

- Minimizar las infracciones
- Identificar los elementos más propensos al robo de hardware
- Evaluar los riesgos que conlleva el manejo de datos sensibles
- Garantizar la seguridad física en el lugar de trabajo

# Concienciación y formación de los empleados: Ingeniería social

Formar a los empleados sobre las posibles técnicas de ingeniería social y cómo combatirlas

| Áreas de riesgo  | Técnicas de ataque                     | Formar a los empleados/el servicio de asistencia en:   |
|------------------|--|--|
| Teléfono         | Suplantación de identidad              | <ul style="list-style-type: none"><li>• No proporcionar ninguna información confidencial, si esto ha ocurrido</li></ul>  |
| Bolsas de basura | Buscar en el contenedor de basura      | <ul style="list-style-type: none"><li>• No tirar los documentos sensibles a la basura</li><li>• Destruir el documento antes de tirarlo a la basura</li><li>• Borrar los datos magnéticos antes de tirarlos a la basura</li></ul> |
| E-mail           | Phishing, archivos adjuntos maliciosos | <ul style="list-style-type: none"><li>• Diferenciar entre un correo electrónico legítimo y un correo de phishing dirigido</li><li>• No descargar un archivo adjunto malicioso</li></ul>  |

# Formación y concienciación de los empleados: Clasificación de datos

---

Niveles típicos de clasificación de la información:

- Top Secret (TS)
- Secreto
- Confidencial
- Restringido
- Oficial
- No clasificado
- Información compartimentada

Las etiquetas de seguridad se utilizan para marcar los requisitos de nivel de seguridad de los activos de información y controlar el acceso a los mismos

Las organizaciones utilizan las etiquetas de seguridad para gestionar la autorización de acceso a sus activos de información

Discutir otras medidas administrativas de seguridad

---

# Proceso de contratación y cese del personal

---

Considere y aplique medidas de seguridad del personal, empezando por la selección y contratación de personal o contratistas hasta el relevo de sus funciones

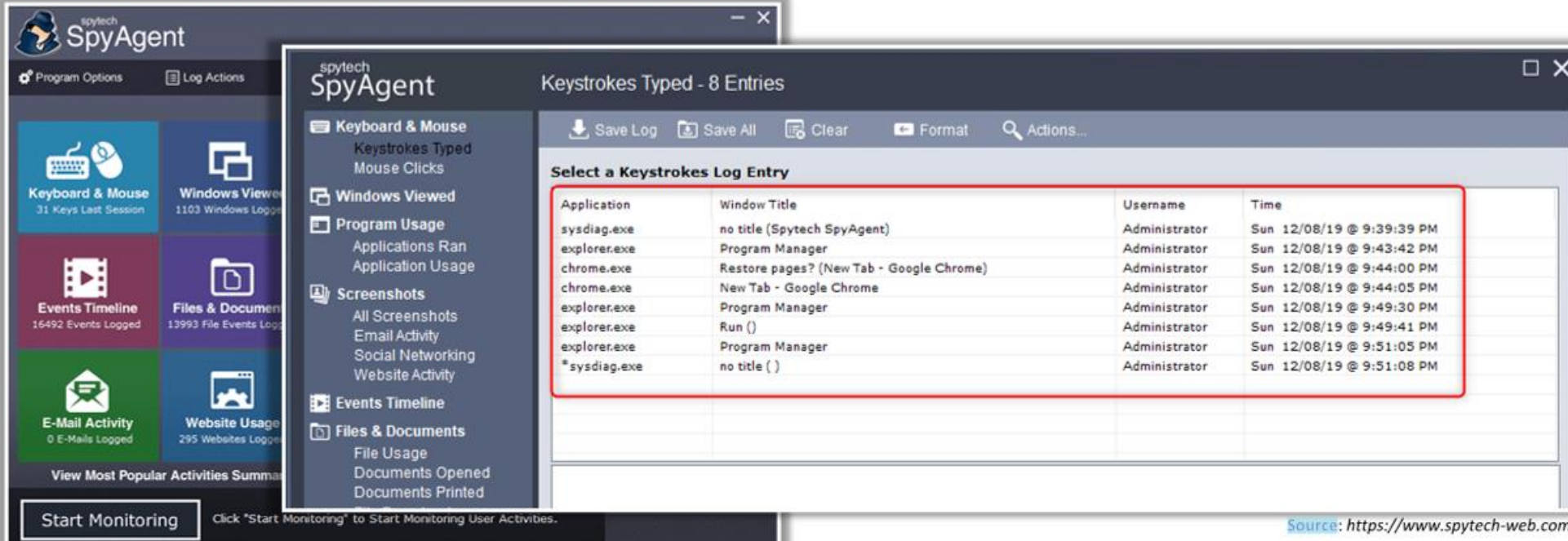
- Ofrecer sesiones de orientación en las que se expliquen los antecedentes de la empresa, junto con sus funciones y responsabilidades, y las políticas de seguridad
- Insertar cláusulas en el contrato para aplicar la seguridad del personal a los contratistas y auditar su cumplimiento
- Retirar los derechos de acceso y recoger todos los activos de la empresa de los empleados y contratistas cuando abandonen la organización
- Contratar a los empleados tras una exhaustiva verificación de la identidad y de los antecedentes
- Los contratistas deben ser contratados con la misma diligencia debida que los empleados internos



# Employee Monitoring

La organización debe llevar a cabo una supervisión indiscriminada de las actividades de los empleados para detectar cualquier acto relacionado con la violación de la política

Utilice una herramienta de supervisión de empleados como Spytech SpyAgent para supervisar el comportamiento de los empleados Fuente



The image shows the Spytech SpyAgent software interface. The main window has a sidebar with various monitoring categories: Keyboard & Mouse (31 Keys Last Session), Windows Viewed (1103 Windows Logged), Events Timeline (16492 Events Logged), Files & Documents (13993 File Events Logged), E-Mail Activity (0 E-Mails Logged), and Website Usage (295 Websites Logged). A 'Start Monitoring' button is at the bottom left. A secondary window titled 'Keystrokes Typed - 8 Entries' is open, displaying a table of logged keystrokes. The table has columns for Application, Window Title, Username, and Time. The data is as follows:

| Application  | Window Title                             | Username      | Time                      |
|--------------|--|---------------|---------------------------|
| sysdiag.exe  | no title (Spytech SpyAgent)              | Administrator | Sun 12/08/19 @ 9:39:39 PM |
| explorer.exe | Program Manager                          | Administrator | Sun 12/08/19 @ 9:43:42 PM |
| chrome.exe   | Restore pages? (New Tab - Google Chrome) | Administrator | Sun 12/08/19 @ 9:44:00 PM |
| chrome.exe   | New Tab - Google Chrome                  | Administrator | Sun 12/08/19 @ 9:44:05 PM |
| explorer.exe | Program Manager                          | Administrator | Sun 12/08/19 @ 9:49:30 PM |
| explorer.exe | Run ( )                                  | Administrator | Sun 12/08/19 @ 9:49:41 PM |
| explorer.exe | Program Manager                          | Administrator | Sun 12/08/19 @ 9:51:05 PM |
| *sysdiag.exe | no title ( )                             | Administrator | Sun 12/08/19 @ 9:51:08 PM |

Source: <https://www.spytech-web.com>

# Resumen del módulo

---

Las políticas de seguridad describen las restricciones mediante normas y reglamentos relativos a todos los aspectos de la seguridad de la red de una organización

La política de seguridad es una parte integral del Programa de Gestión de la Seguridad de la Información para las organizaciones

Las declaraciones de política deben estar escritas en un estilo muy claro y formal

La política de seguridad del sistema de información define las directrices para salvaguardar los sistemas de información de una organización del uso malicioso

Una política BYOD proporciona un conjunto de directrices para maximizar los beneficios del negocio y minimizar los riesgos durante el uso del dispositivo personal de un empleado en la red de una organización

La formación y la concienciación sobre la política de seguridad son necesarias para la aplicación efectiva de las políticas de seguridad