1. Datos de contacto

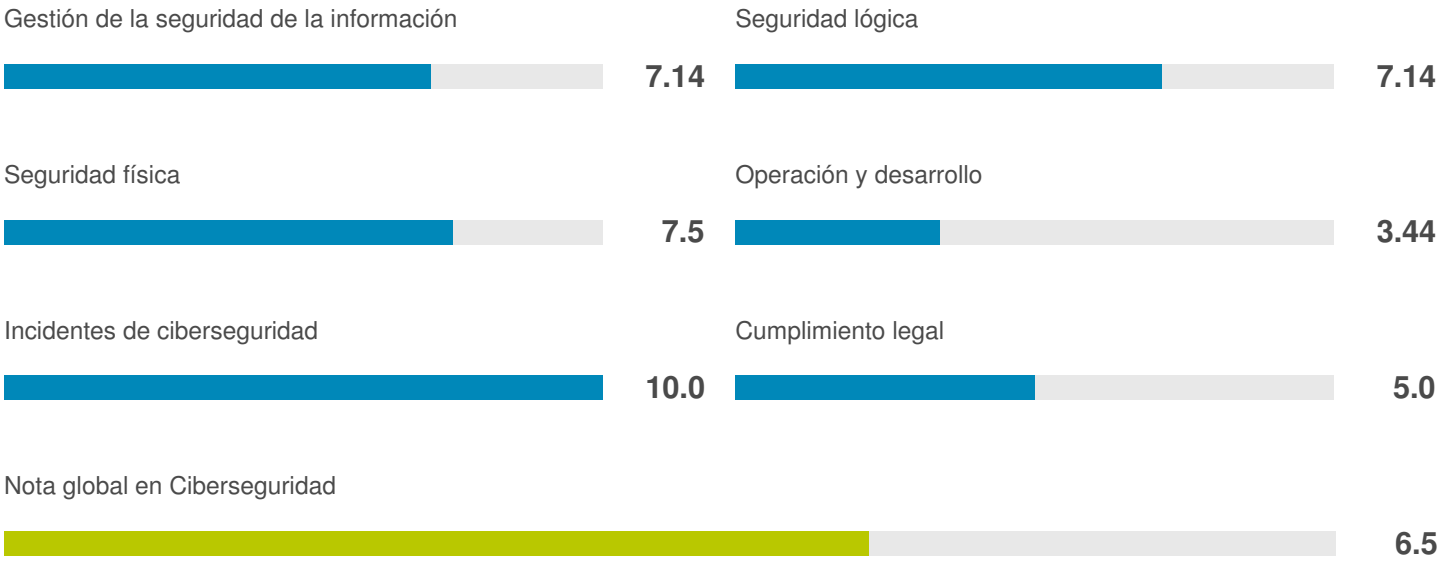
Empresa	Empresa S.A
Nombre	Nombre1 Apellido1 Apellido2
Cargo	Cargo1
Correo electrónico	correo@dominio.com

2. Información general

Este cuestionario se ha desarrollado a través de una colaboración entre Bankia y S2 Grupo, tomando como base la norma internacional de seguridad de la información ISO 27001, el principal estándar a nivel mundial para evaluar el estado de la seguridad de la información de una organización, con independencia de su naturaleza, sector y tamaño. Los resultados incluidos en este informe permiten obtener una idea aproximada del estado de la seguridad de la información de una organización, y constituyen un buen punto de partida para identificar carencias y puntos de mejora en esta materia. Para más información sobre cómo incrementar la seguridad de la información de su organización, puede ponerse en contacto con S2 Grupo en clientes@s2grupo.es o dejando sus datos en lasiguiente página.

A partir de la información proporcionada durante la cumplimentación del cuestionario, se muestran los aspectos positivos y de mejora identificados en cada uno de los seis bloques temáticos considerados. En el caso de los aspectos positivos, se incluyen recomendaciones para continuar mejorando la seguridad de la información. Los puntos de mejora hacen referencia a elementos que son clave para garantizar una protección adecuada de la información, los activos y los procesos de una organización. En este caso se recoge información adicional sobre su importancia, junto con algunas pautas para su implementación. Por último, en cada uno de los bloques temáticos se incluye un apartado de Herramientas, recursos y plataformas, que proporciona páginas web, documentos y recursos que permiten profundizar más en cada uno de ellos.

3. Resultados



Bloque temático: Gestión de la seguridad de la información

Aspectos positivos

- Contar con un presupuesto anual específico para proyectos de Seguridad de la Información es un gran paso, que para una mayor eficiencia y eficacia, debe ir precedido de un análisis que permita identificar y reforzar los puntos flacos, manteniendo un grado de protección homogéneo en todos los ámbitos de la organización.
- La definición de un conjunto adecuado y completo de políticas para la seguridad de la información es uno de los pilares básicos para garantizar la protección de los activos y la información. Es imprescindible que sean divulgadas entre el personal y se revisen de manera periódica para incorporar las modificaciones en los procesos y herramientas de la organización, así como en el ámbito legal.
- El compromiso de confidencialidad debe extenderse no solo al personal de la organización, sino también a las empresas proveedoras y a los empleados de estas, en definitiva a cualquier otra persona que pueda tener acceso a información interna (de manera regular o esporádica) en el desempeño de sus funciones.
- Para que un programa de concienciación en materia de Seguridad de la Información sea realmente efectivo, debe ser revisado de manera periódica, introduciendo las nuevas amenazas existentes, además de actualizarse con las herramientas que la organización tiene implantadas para hacerles frente, y estar formado por diferentes iniciativas. Si existen colaboradores trabajando en las instalaciones de la empresa, debería exigirse a los proveedores que el personal esté correctamente formado. La efectividad del programa debe ser evaluada mediante indicadores, que permitan hallar los ámbitos en los que existe un menor conocimiento.
- La clasificación de la información permite al personal saber cómo debe tratar y proteger la información según su nivel de criticidad o sensibilidad. Esta clasificación debe ir acompañada de procedimientos específicos de cada nivel (difusión interna y externa, copia, borrado, desclasificación, etc.), ser difundida a los usuarios pertinentes y su implementación ser auditada de manera periódica.

Aspectos de mejora

- La seguridad de la información es intrínseca a cualquier proceso que gestione información, por lo que definir y asignar las principales responsabilidades es el primer paso para garantizar su protección. Algunas de las principales son la asignación de los accesos en el plano técnico y su autorización funcional, la revisión de clausulados contractuales, gestión de incidencias de seguridad o la revisión de controles, pero estas deben ser acordes con el tamaño de la organización.
- Un riesgo se define como la ocurrencia de una amenaza sobre un activo. De este modo, a través de la realización de un análisis de riesgos, la organización identifica los activos que se encuentran más expuestos, qué amenazas son más susceptibles de ocurrencia y cuáles tienen un mayor impacto. Esto permite identificar la mejor estrategia de gestión (entre las cuatro siguientes: aceptar, mitigar, eliminar, transferir), de cara a optimizar los recursos y controlar el daño.

Herramientas, recursos y plataformas

- ISO 27001
  ISO 27001
- ENISA Threat and Risk Management (EN)
  ENISA Threat and Risk Management (EN)
- SANS Information Security Policy Templates (EN)
  SANS Information Security Policy Templates (EN)
- S2 Grupo - Seguridad para tod@s en la Sociedad de la Información
  S2 Grupo - Seguridad para tod@s en la Sociedad de la Información

Bloque temático: Seguridad lógica

Aspectos positivos

- Muchas veces, al hablar de seguridad, solo se consideran las medidas técnicas, como cortafuegos, antivirus o sistemas de copias de respaldo. Sin embargo, las medidas más efectivas son las medidas de gestión planteadas a medio y largo plazo desde un punto de vista estratégico y táctico. Esto pasa indispensablemente por contar con personal especializado, con conocimientos y capacidad de adaptarse en cada momento a su entorno y de proponer nuevas soluciones, controles, defensas y contramedidas.
- Los procesos de gestión de altas, bajas y modificación de permisos de acceso deben ir acompañados de procesos que garanticen que los accesos se mantienen actualizados. Para ello se deben revisar de forma periódica dichos permisos, su vigencia y la correcta aplicación de las bajas y modificaciones.
- El cifrado es una medida de seguridad que proporciona una protección muy grande frente al robo de información, y especialmente cuando esta es gestionada en dispositivos: portátiles, USB, discos duros portátiles, etc., o enviada por e-mail. Sin embargo, la empresa debe ser consciente de la problemática que puede introducir un uso indiscriminado del cifrado, haciendo que algunas personas se conviertan en imprescindibles y que en el peor de los casos, la información no pueda ser descifrada. Por ello, es necesario que se implante una política de cifrado y gestión de claves que garantice que en ningún caso, la información corporativa es puesta en riesgo.
- El puesto del usuario, al ser uno de los principales canales de comunicación de la organización con el exterior, ya sea vía Internet o e-mail, se encuentra especialmente expuesto a amenazas como el malware o ataques de ingeniería social. Por tanto, es imprescindible no solo contar con las medidas básicas como un antivirus, parches de seguridad actualizados y usuarios con privilegios restringidos, sino que se debe trabajar para incorporar otras medidas como la ejecución de adjuntos desde dispositivos extraíbles, sistemas de cifrado, o limitar las acciones que la persona puede realizar.
- En la actualidad, la aparición de nuevas vulnerabilidades críticas es una constante, que en ocasiones están siendo activamente explotadas por los ciberdelincuentes incluso antes de que el fabricante emita una actualización. Por ello, además de disponer de un proceso ágil y formal de instalación de actualizaciones, es vital que la organización sea capaz de evaluar el impacto de su aplicación en entornos críticos, identificar medidas de mitigación alternativas y disponer de fuentes de información fiables que permitan actuar incluso antes del aviso formal del fabricante.

Aspectos de mejora

- Uno de los mayores problemas en seguridad informática radica en el empleo de contraseñas débiles para el acceso a la información corporativa y los recursos del sistema. Una contraseña débil puede comprometerse fácilmente y poner en peligro la seguridad de los sistemas. Para evitarlo, los sistemas de autenticación que se utilicen deben configurarse para que se empleen claves robustas, que caduquen y que no puedan repetirse al menos hasta X claves después.
- La seguridad perimetral está formada por aquellos elementos de la red de la organización que proporcionan seguridad frente a otras redes externas a la organización, ya sean proveedores, otras empresas o Internet. Su propósito es evitar que desde redes "no confiables" se pueda producir un ataque con éxito a los sistemas de la organización, para lo que se despliegan generalmente cortafuegos (firewalls) que limitan y filtran el tráfico hacia el interior de la organización. En la actualidad, no disponer de ningún dispositivo de seguridad perimetral, o disponer de uno mal gestionado, es prácticamente garantía de sufrir un ataque exitoso.

Herramientas, recursos y plataformas

- OSI - La importancia de las actualizaciones de seguridad

  OSI - La importancia de las actualizaciones de seguridad
- Security Art Work - Las contraseñas han muerto, larga vida a las contraseñas

  Security Art Work - Las contraseñas han muerto, larga vida a las contraseñas
- INCIBE - Avisos de seguridad

  INCIBE - Avisos de seguridad

Bloque temático: Seguridad física

Aspectos positivos

- La ubicación de los equipos en salas de acceso restringido los protege contra posibles daños ambientales, golpes y ataques malintencionados. Sin embargo, este es solo el primer paso para su protección, que puede mejorarse con diferentes sensores (humedad, temperatura, control de presencia, humo en el falso techo, etc.), suelo técnico, sistemas de extinción de incendios, y muchos otros mecanismos de uso común.
- Contar con protecciones contra accidentes ambientales o cortes del suministro es vital para poder mantener el negocio a salvo en caso de que estos se produzcan. Si se dispone de los principales elementos, el número de mejoras técnicas que se pueden aplicar es tan extenso como se desee, siempre manteniendo una proporcionalidad respecto a los activos que se protegen: extinción automática de incendios, suelo técnico, construcción ignífuga del CPD, redundancia de proveedores de red y electricidad, sistemas de alimentación ininterrumpida apoyados por grupos electrógenos, etc. Como es habitual, la implantación de cualquier medida debe ir acompañada de pruebas regulares que garanticen su correcto funcionamiento.
- La existencia de destructoras de papel y otros soportes como USB o DVD es un elemento imprescindible para garantizar la seguridad de la documentación, medida que debe ir acompañada de medidas de concienciación y comunicación a los empleados. Un paso adicional en el caso de grandes volúmenes de documentación es la contratación de empresas especializadas que proporcionan un certificado como garantía de destrucción.
- El borrado seguro o la destrucción de los dispositivos de almacenamiento de información permite asegurar que ningún tercero accederá a la información que resida en estos. Deben tenerse en cuenta también los dispositivos cuya naturaleza es tanto profesional como personal (un USB, un smartphone, una tableta), y que pueden ser reutilizados para uso personal por parte de terceros (familiares, amigos, etc.) sin el conocimiento de la organización ni la adopción de las medidas necesarias. Es recomendable, por otro caso, que los procesos de destrucción de dispositivos o borrado seguro, en el caso de que sean externalizados, lleven asociado un certificado de garantía.

Aspectos de mejora

- El bloqueo automático de la sesión es una buena práctica que evita que la información que gestiona un usuario sea accesible por personas no autorizadas cuando este se ausenta de su puesto de trabajo. En entornos controlados como oficinas sin acceso de personal externo es improbable (pero no imposible) que un empleado manipule la sesión de un compañero, pero en el caso de determinados perfiles, la información que se muestra en pantalla puede ser lo bastante sensible para despertar la curiosidad de otros. Este problema se agrava, como es evidente, cuando se trata de empresas con un gran número de colaboradores o acceso público.
- Aunque un Plan de Recuperación ante Desastres (también conocido como DRP) varía mucho de unas organizaciones a otras, disponer de uno garantiza que en el caso de producirse un evento catastrófico, como un incendio, una inundación o un robo, la organización sobrevivirá. Para ello, se deben tener en cuenta las necesidades existentes y aplicar medidas de seguridad informática proporcionales que permitan poner en funcionamiento los sistemas críticos en tiempos razonables. En el caso más simple, un DRP puede basarse en copias de seguridad de la información externalizadas y un documento que defina qué hacer y a quién avisar en caso de desastre.

Herramientas, recursos y plataformas

- INCIBE - Pon un CPD seguro en tu empresa
  INCIBE - Pon un CPD seguro en tu empresa
- Hipertextual - Borrado seguro de archivos en Windows
  Hipertextual - Borrado seguro de archivos en Windows
- Security Art Work - La otra seguridad de los soportes
  Security Art Work - La otra seguridad de los soportes
- Wikipedia - El Plan de Recuperación ante Desastres
  Wikipedia - El Plan de Recuperación ante Desastres
- Universidad Politécnica de Madrid - Guía de Desarrollo de un Plan de Continuidad de Negocio
  Universidad Politécnica de Madrid - Guía de Desarrollo de un Plan de Continuidad de Negocio

Bloque temático: Operación y desarrollo

Aspectos positivos

- Si bien la segregación de las redes es una medida de seguridad necesaria, no es suficiente para garantizar que es eficaz en la protección de los sistemas. Para ello, debe asegurarse que la visibilidad entre ellas se limita al mínimo imprescindible, y en la medida de lo posible, que los intentos de acceso reiterados no autorizados son monitorizados, para identificar potenciales intrusos o sistemas malintencionados.
- La monitorización de los sistemas y las redes es una medida que puede ampliarse tanto como se desee, siempre en consonancia con los recursos de que se disponga. No obstante, esta debe ser eficaz y eficiente, de manera que se reduzcan tanto los falsos positivos (incidencias que no lo son) como los falsos negativos (incidencias que no son detectadas), para que la gestión se centre en aquellas incidencias realmente destacables.
- Un proceso formal de gestión de cambios y actualización de entornos es un elemento indispensable en cualquier organización tecnológicamente madura. Una aplicación correcta garantiza que los cortes de servicio se reducen al mínimo, y que cualquier imprevisto tendrá un impacto reducido será adecuadamente gestionado.

Aspectos de mejora

- Si la seguridad de la información no es un ámbito aislado, sino que impregna cualquier proceso de la organización, esto es aún más cierto en el caso de la informática, vista desde un punto de vista general. La gestión de los sistemas y las redes tiene tal importancia en cualquier organización que requiere una gestión dedicada y especializada, realizada por personal debidamente formado, que permita responder con soluciones adecuadas a las necesidades de la organización.
- Documentar los principales procesos de la operación de los sistemas es una buena práctica que garantiza la homogeneidad en la aplicación de los procedimientos, reduce la dependencia del personal crítico y facilita que se mejoren y automaticen las tareas más habituales.
- Las copias de seguridad son una de las principales medidas de seguridad, si no la principal, para proteger la información ante pérdidas: infecciones de malware, intrusos, corrupción masiva o incidentes catastróficos. Para ello debe definirse una periodicidad adecuada, utilizar medios de almacenamiento que proporcionen garantías de funcionamiento, y almacenar una copia en un lugar seguro diferente a la de los servidores que alojan los datos.
- La separación de los entornos de desarrollo o test y los de producción tiene múltiples ventajas, entre las que se encuentran evitar las modificaciones no controladas sobre los servidores en producción (que son los que prestan el servicio a la organización), limitar el acceso a la información confidencial por parte del personal desarrollador, y minimizar las pérdidas de servicio. Cualquier desarrollo, actualización o modificación sobre el código de los programas o servidores debe probarse antes en un entorno controlado, tras lo cual, una vez verificada su corrección, puede trasladarse a los entornos de producción mediante un proceso formal de gestión de cambios.
- Se ha demostrado que considerar los requisitos de seguridad en la fase de especificación y desarrollo de una aplicación reduce los problemas de seguridad que pueden surgir con posterioridad, así como el coste de su resolución. Es más, evita que el desarrollo arrastre problemas de seguridad que con posterioridad son incluso irresolubles. Este proceso puede comenzar con un pequeño cuestionario que valore el tipo de perfiles que va a acceder a la información, si requiere estar cifrada, si le aplica algún tipo de requisito legal, con que aplicaciones o sistemas va a interactuar, tipos de registro que necesita, etc.

Herramientas, recursos y plataformas

- The Open Web Application Security Project (OWASP)
  The Open Web Application Security Project (OWASP)
- ITIL (Information Technology Infrastructure Library)
  ITIL (Information Technology Infrastructure Library)

Bloque temático: Incidentes de ciberseguridad

Aspectos positivos

- Un procedimiento de gestión de ciberincidentes es un elemento imprescindible para reaccionar con rapidez y eficacia frente a potenciales ciberataques, que cualquier empresa es susceptible de sufrir en el futuro. El procedimiento y todos los elementos que lo apoyan debe mantenerse constantemente actualizado sin necesidad de esperar a las pruebas periódicas, involucrando de manera activa tanto al personal técnico como al de gestión.
- Las pruebas periódicas del procedimiento de respuesta frente a ciberincidentes son imprescindibles para garantizar que todos los elementos involucrados en un ciberincidente se encuentran "a punto", y que la documentación y procesos relacionados han sido actualizados con los nuevos sistemas, amenazas, cambios de personal, con el fin de incrementar su eficacia y utilidad. Tras las pruebas debe realizarse un informe de resultados, con un plan de acción, que garantice que los puntos flacos y errores detectados se solventan y no se producen en un ciberincidente real.
- La implicación de los usuarios en el reporte de incidencias es imprescindible para mantener un grado de protección óptimo. Además de realizar recordatorios periódicos para los usuarios que ya han sido informados, este tipo de obligaciones debe incluirse en los pack de bienvenida de los nuevos empleados. Trasladar a los empleados estadísticas periódicas sobre el número de incidencias reportadas puede considerarse un medio útil para mejorar la concienciación y la implicación del personal.

Herramientas, recursos y plataformas

- CERTSI - Reporte de ciberincidencias
  CERTSI - Reporte de ciberincidencias
- ENISA - Guía ENISA para la Gestión de Incidentes
  ENISA - Guía ENISA para la Gestión de Incidentes
- Centro Criptológico Nacional - Guía del CCN para la Gestión de Incidentes
  Centro Criptológico Nacional - Guía del CCN para la Gestión de Incidentes

Bloque temático: Cumplimiento legal

Aspectos positivos

- Dado que la práctica totalidad de las empresas gestiona datos personales (al menos de sus empleados), la legislación en materia de datos de carácter personal es una de las más importantes en el ámbito de la seguridad de la información, responsable de garantizar el derecho a la privacidad de las personas. Las revisiones periódicas deben ir acompañadas de sesiones de formación para el conjunto del personal y de planes de acción para subsanar aquellas anomalías que se hayan detectado.

Aspectos de mejora

- El primer paso para lograr un cumplimiento adecuado de la legislación aplicable a la organización es conocer en qué grado le aplica. No conocerla puede acarrear sanciones legales y económicas importantes. Por tanto, deben asignarse las responsabilidades adecuadas para identificar y aplicar la legislación y las medidas correspondientes que la organización debe adoptar.
- La existencia de un inventario de licencias es no solo garantía de cumplimiento legal, sino también de protección frente al malware que a menudo acompaña al software "pirateado". Además, debe tenerse en cuenta que en ocasiones, el software sin licencia no recibe las actualizaciones de seguridad del fabricante, incrementando el nivel de exposición a nuevas amenazas y que podrían afectar a la organización.

Herramientas, recursos y plataformas

- Ley de Servicios de la Sociedad de la Información y del Comercio Electrónico
  Ley de Servicios de la Sociedad de la Información y del Comercio Electrónico
- Reglamento General de Protección de Datos (BOE)
  Reglamento General de Protección de Datos (BOE)
- Agencia Española de Protección de Datos
  Agencia Española de Protección de Datos
- Protección de datos 2.0
  Protección de datos 2.0

4. Respuestas

Gestión de la seguridad de la información

Se dispone de un presupuesto anual para poner en marcha iniciativas directamente relacionadas con la Seguridad de la Información Sí

¿Están definidas y asignadas las responsabilidades en materia de Seguridad de la Información? No

¿Se han definido e implantado políticas relacionadas con la Seguridad de la Información? Sí

¿Se revisan de manera periódica los riesgos de la organización y se ponen en marcha acciones para gestionarlos? No

¿Los empleados y proveedores firman un compromiso de confidencialidad antes del acceso a la información? Sí

¿Existe un programa de concienciación para empleados en materia de Seguridad de la Información? Sí

¿Está la información clasificada según su nivel de confidencialidad? Sí

Seguridad lógica

¿Existe personal dedicado específicamente a velar por la seguridad de los sistemas y las redes? Sí

¿Existe un proceso formal de alta, baja y modificación de los permisos de acceso de los usuarios a los sistemas y la información? Sí

¿Los sistemas exigen que las contraseñas cumplan requisitos de complejidad? No

¿Los usuarios utilizan habitualmente aplicaciones de cifrado para gestionar la información? Sí

¿Los equipos de los usuarios tienen medidas de protección implantadas? Sí

¿Hay instalados elementos de seguridad perimetral? No

¿Se gestionan las vulnerabilidades técnicas de los servidores y equipos de los usuarios? Sí

Seguridad física

¿Están los equipos ubicados en una sala específica con acceso restringido? Sí

¿Los equipos de los usuarios se bloquean automáticamente tras un periodo de inactividad? No

¿Se ha desarrollado un plan de respuesta ante desastres informáticos? No

¿Están los sistemas críticos protegidos contra cortes de electricidad, cortes de red, inundaciones, fuego, etc.? Sí

¿Disponen los empleados de trituradoras de papel u otros mecanismos semejantes para eliminar soportes? Sí

Antes de reutilizar o desechar un equipo o dispositivo, ¿se borra la información de manera segura / se destruye sin posibilidad de recuperación? Sí

Operación y desarrollo

¿Existe personal dedicado específicamente al mantenimiento y operación de los sistemas y las redes? No

¿Están documentados los principales procedimientos de la operación de los sistemas y las redes? No

¿Las redes de la organización están segregadas? Sí

¿Se controla o monitoriza la seguridad de los sistemas y las redes de la organización? Sí

¿Se controla o monitoriza la seguridad de los sistemas y las redes de la organización? Sí

¿Se realizan y prueban las copias de seguridad con regularidad? No

¿Existe un proceso formal de gestión de cambios y actualización de entornos/programas? Sí

¿Los entornos en los que se desarrollan o prueban programas son diferentes a los de producción? No

¿Se tiene en cuenta las implicaciones de seguridad de las aplicaciones antes y durante su desarrollo? No

Incidentes de ciberseguridad

¿Existe un procedimiento de gestión de ciberincidentes? Sí

¿Se realizan pruebas periódicas para comprobar la respuesta frente a ciberincidentes? Sí

¿Los usuarios son informados con regularidad de que deben reportar cualquier incidencia o actividad sospechosa? Sí

Cumplimiento legal

¿Está identificada la legislación aplicable que tenga implicaciones sobre la Seguridad de la Información? No

¿Se revisa con regularidad la adecuación de la organización a la legislación de protección de datos personales? Sí

¿Dispone la empresa de un inventario de licencias de software propietario? Ns/Nc