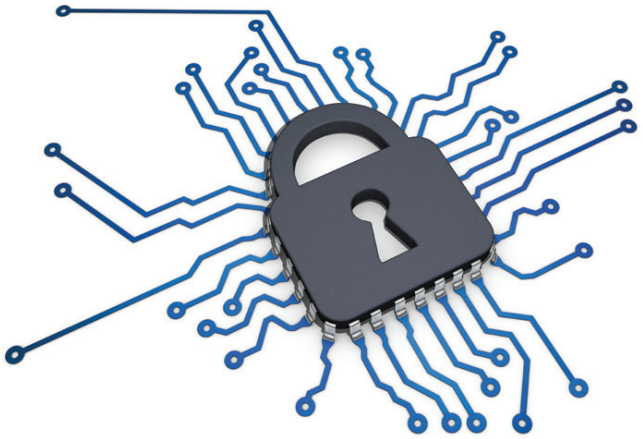
cantabriaconecta
datos y comunicaciones



Políticas de seguridad de los datos de muestra

Este documento ofrece tres ejemplos de políticas de seguridad de datos que cubren áreas de interés clave. No debe tomarse como una lista exhaustiva, sino que cada organización debe identificar las áreas adicionales que requieren de políticas de acuerdo con sus usuarios, datos, entorno regulatorio y otros factores relevantes.

Las tres políticas cubren:

1. Política de protección de datos: Requisitos para los empleados
2. Política de protección de datos: Prevención de fugas de datos – Datos en movimiento
3. Política de protección de datos: Cifrado completo de discos en estaciones de trabajo

Para ayudar en el uso de estas políticas se han añadido comentarios *en rojo*.

Política de protección de datos: Requisitos para los empleados

Cómo utilizar esta política

Esta política de ejemplo describe el comportamiento que se espera de los empleados a la hora de manejar datos y ofrece una clasificación de los tipos de datos con los que deben tener especial cuidado. Incluya esta política con la política de uso aceptable de la empresa, los programas de formación sobre seguridad y la política de protección de datos para proporcionar a los usuarios pautas sobre los comportamientos exigidos.

1.0 Objetivo

<Empresa X> debe proteger los datos confidenciales, restringidos o delicados para evitar que posibles fugas dañen el prestigio o afecten de forma negativa a los clientes. Tanto la protección de estos datos como la flexibilidad para acceder a ellos y la conservación de la productividad son requisitos críticos para la empresa.

Este control tecnológico no está diseñado para evitar robos maliciosos o detectar todos los datos. Su principal objetivo es fomentar la concienciación de los usuarios para evitar fugas accidentales. En esta política se describen los requisitos para la prevención de fugas de datos, las razones para su uso y su finalidad.

2.0 Alcance

1. Todos los empleados, contratistas o usuarios con acceso a los datos o a los sistemas de <empresa X>.
2. Definición de los datos protegidos *(identifique los tipos de datos y proporcione ejemplos a los usuarios para que puedan detectarlos cuando los utilicen)*
   - Información de identificación personal
   - Daños económicos
   - Datos restringidos o delicados
   - Datos confidenciales
   - Direcciones IP

3.0 Política: requisitos para los empleados

1. Realice los cursos de concienciación sobre seguridad de <empresa X> y comprométase a adherirse a la política de uso aceptable.
2. Si se encuentra con algún individuo desconocido, sin escolta o no autorizado en <empresa X>, comuníquelo inmediatamente a <introducir la información correspondiente>.
3. Las personas que visiten <empresa X> deben estar acompañadas por algún empleado autorizado en todo momento. Si está encargado de acompañar a las visitas, diríjalas solamente a las zonas adecuadas.
4. No está permitido hacer referencia a temas o datos delicados y confidenciales en público o a través de sistemas o canales de comunicación no controlados por <empresa X>. Por ejemplo, está prohibido utilizar sistemas externos de correo electrónico no alojados por <empresa X> para la distribución de datos.
5. Mantenga su escritorio organizado. Para conservar la seguridad de la información, no deje ningún dato englobado en esta política sin atender en su estación de trabajo.

6. Según la política de contraseñas, deberá utilizar una contraseña segura en todos los sistemas de <empresa X>. Dichas credenciales deben ser exclusivas y no deben utilizarse en otros sistemas o servicios externos.
7. Al finalizar el contrato, los empleados deberán devolver todos los registros (en cualquier formato) que contengan información personal. *Este requisito debe ser parte del proceso de incorporación de los empleados en el que éstos deben firmar la documentación para confirmar que van a hacer esto* .
8. Si se produce el extravío de cualquier dispositivo que contenga datos englobados en esta política (por ejemplo, teléfonos móviles, portátiles, etc.), informe de inmediato a <introducir la información correspondiente>.
9. Si sospecha que algún sistema o proceso no cumple la política o pone en peligro la seguridad de la información, tiene el deber de informar a <introducir la información correspondiente> para que se tomen las medidas necesarias.
10. Si se le ha autorizado para trabajar de forma remota, tome medidas de precaución adicionales para asegurarse de que maneja los datos adecuadamente. Solicite ayuda a <introducir la información correspondiente> si no está seguro de sus responsabilidades.
11. Asegúrese de no exponer de forma excesiva los activos que contengan datos englobados en esta política, por ejemplo, a la vista en el asiento trasero del coche.
12. 12. Las transferencias de datos dentro de <empresa X> deben realizarse solamente a través de los mecanismos seguros proporcionados por la empresa (por ejemplo, correo electrónico, recursos compartidos, memorias USB cifradas, etc.). <Empresa X> le proporcionará los sistemas o dispositivos correspondientes para tal fin. No utilice otros mecanismos para el manejo de datos englobados en esta política. Si tiene alguna pregunta relacionada con el uso de cualquier mecanismo de transferencia o detecta alguno que no cumpla los requisitos empresariales, informe a <introducir la información correspondiente>.
13. 13. Toda información transferida a cualquier dispositivo móvil (por ejemplo, memorias USB u ordenadores portátiles) debe estar cifrada de acuerdo con las prácticas recomendadas del sector, y las leyes y normativas correspondientes. Si tiene alguna duda sobre los requisitos, solicite ayuda a <introducir la información correspondiente>.

Cantabria Conecta, C/General Davila, 127 - 39007 Santander, Cantabria | E. info@cantabriaconecta.es | T. 942 763 303
www.cantabriaconecta.es

Política de protección de datos: Prevención de fugas de datos – Datos en movimiento

Cómo utilizar esta política

Esta política de ejemplo tiene como finalidad servir de guía a aquellas empresas que deseen implementar o actualizar los controles de prevención de fugas de datos. Adáptela a los requisitos de usabilidad o según las normativas o los datos que necesite proteger. Esta política proporciona un marco para la clasificación de los datos que desee supervisar. Debe ampliarlas para que cubran a los activos sensibles en su negocio y en función a los tipos que usted utiliza.

Principios fundamentales

La prevención de fugas de datos está diseñada para concienciar a los usuarios sobre la naturaleza confidencial o las posibles restricciones de los datos que transfieren.

1.0 Objetivo

<Empresa X> debe proteger los datos confidenciales, restringidos o delicados para evitar que posibles fugas dañen el prestigio o afecten de forma negativa a los clientes. Tanto la protección de estos datos como la flexibilidad para acceder a ellos y la conservación de la productividad son requisitos críticos para la empresa.

Este control tecnológico no está diseñado para evitar robos maliciosos o detectar todos los datos. Su principal objetivo es fomentar la concienciación de los usuarios para evitar fugas accidentales. En esta política se describen los requisitos para la prevención de fugas de datos, las razones para su uso y su finalidad.

2.0 Alcance

1. Todos los dispositivos de <empresa X> en los que se manejen datos de clientes, delicados o de la empresa, e información de identificación personal. Todos los dispositivos utilizados de forma habitual para acceder al correo electrónico e Internet, o realizar otras tareas relacionadas con el trabajo de los usuarios, y que no estén exentos de forma específica por razones tecnológicas o empresariales justificadas.
2. La política de protección de la información de <empresa X> definirá los requisitos para el manejo de información y el comportamiento de los usuarios. Esta política añade controles tecnológicos a la política de protección de la información.
3. Excepciones: en aquellos casos en los que ciertas necesidades empresariales exijan la exención de esta política (costes, complejidad o repercusiones en otros requisitos), debe realizarse una evaluación de los riesgos autorizada por la gestión de la seguridad. Consulte el proceso de **Evaluación de riesgos** *(referencia al proceso de evaluación de riesgos propio de la empresa).*

3.0 Política

1. La tecnología de prevención de fugas de datos (DLP) de <empresa X> detecta datos en movimiento.
2. La tecnología DLP identifica grandes volúmenes de datos englobados en la política (por tanto, con alto riesgo de contener información delicada y que pueden provocar graves consecuencias si se manejan de forma inadecuada). Se consideran grandes volúmenes de datos aquellos que superan los <introducir la cantidad correspondiente> registros *(ajuste la cantidad al tamaño de su empresa, por ejemplo, 1.000 registros).*

   Los datos dentro del alcance son: *(debe ajustar esto para reflejar los datos para los que está sometido a regulación, o que podrían ser más perjudiciales para su organización. Los ejemplos siguientes resultan adecuados para la mayoría de las empresas)*

   a. Datos de tarjetas de crédito, números de cuentas bancarias y demás información financiera
   b. Direcciones de correo electrónico, nombres, direcciones postales y otras combinaciones de datos de identificación personal
   c. Documentos marcados de forma explícita como información confidencial de <empresa X>.

3. La prevención de fugas de datos identifica contenido específico como, por ejemplo:
    a. Datos de ventas – principalmente previsiones, listas de renovaciones y listados de clientes
    b. Información de identificación personal exportada fuera de los sistemas controlados *(incluya en esta categoría los datos que más le preocupen y que desee asegurarse de que se detectan mediante la política de prevención de fugas de datos)*.
4. La prevención de fugas de datos se configurará para advertir a los usuarios cuando se sospeche que están transfiriendo datos delicados. Los usuarios podrán autorizar o denegar las transferencias. De esta forma, los usuarios tienen la oportunidad de tomar las decisiones adecuadas para proteger los datos sin afectar al funcionamiento de la empresa.
   La configuración de la solución de prevención de fugas de datos se modificará según el proceso de cambios informáticos de <empresa X> y bajo la autorización de los encargados de la gestión de la seguridad para identificar los ajustes necesarios en la política de protección de la información y las comunicaciones de los empleados.
5. La solución de prevención de fugas de datos registrará los incidentes de forma centralizada para facilitar su revisión. El departamento informático evaluará los eventos para identificar los datos que pueden ser delicados, las situaciones en las que se autorizó su transferencia y los posibles usos inadecuados. El departamento de recursos humanos recibirá notificaciones sobre dichos eventos para ocuparse de ellos según los procesos habituales y proteger a los empleados. *(Ajuste este apartado a su organización. En algunos casos, los encargados de realizar las evaluaciones son los propietarios de la empresa, en lugar del departamento informático)*.
6. Si cree que se ha producido una filtración de datos, siga el procedimiento de gestión de incidentes informáticos e informe a <introducir la información correspondiente> *(por ejemplo, el departamento de recursos humanos, legal o encargado de la seguridad)*.
7. El acceso a los eventos de prevención de fugas de datos estará restringido a una serie de individuos concretos para proteger la privacidad de los empleados. Dichos eventos no deben utilizarse como prueba de que un empleado haya provocado de forma accidental o intencionada una fuga de datos, pero pueden servir como base de las investigaciones para asegurarse de que los datos se han protegido adecuadamente.

4.0 Pautas técnicas

Las pautas técnicas sirven para identificar los requisitos de implementación técnica y suelen estar relacionados con las tecnologías.

1. La tecnología elegida es <introducir la información correspondiente>
2. El producto se configurará para detectar el movimiento de datos en navegadores, programas de mensajería instantánea, clientes de correo electrónico, dispositivos de almacenamiento y medios de escritura óptica.

5.0 Informes

1. Informes de incidentes semanales a <introducir la información correspondiente>
2. Los incidentes de alta prioridad descubiertos por el departamento informático deben comunicarse de forma inmediata a <introducir la información correspondiente>
3. Informes mensuales sobre el porcentaje de dispositivos que cumplen la política de prevención de fugas de datos

Política de protección de datos: Cifrado completo de discos en estaciones de trabajo

Cómo utilizar esta política

Esta política de ejemplo tiene como finalidad servir de guía a aquellas empresas que deseen implementar o actualizar la política de control del cifrado completo de discos. Adáptela a los requisitos de usabilidad o según las normativas o los datos que necesite proteger.

Principios fundamentales

Hoy en día, el cifrado completo de discos es una tecnología fundamental para la mejora de la privacidad y un requisito obligatorio de muchas normativas.

1.0 Objetivo

<Empresa X> debe proteger los datos confidenciales, restringidos o delicados para evitar que posibles fugas dañen el prestigio o afecten de forma negativa a los clientes. Además, existen diferentes normativas generales (tales como <introducir la información correspondiente>) que obligan a la protección de una gran variedad de datos. Esta política ayuda a cumplir dichas normativas mediante la restricción del acceso a los datos alojados en los dispositivos <introducir la información correspondiente>.

Según las definiciones incluidas en diferentes estándares de cumplimiento y prácticas recomendadas del sector, el cifrado completo de los discos es necesario para evitar la divulgación de los datos si se extravía un activo. En esta política se definen los requisitos del cifrado completo de discos como medida de control, además de los procesos relacionados.

2.0 Alcance

1. Todas las estaciones de <empresa X>: ordenadores de escritorio y portátiles *(según los tipos de datos almacenados y los métodos físicos de protección, en algunas empresas, esta política afecta a los ordenadores portátiles)*.
2. Todos los equipos virtuales de <empresa X>.
3. Excepciones: en aquellos casos en los que ciertas necesidades empresariales exijan la exención de esta política (costes, complejidad o repercusiones en otros requisitos), debe realizarse una evaluación de los riesgos autorizada por la gestión de la seguridad. Consulte el proceso de **Evaluación de riesgos** *(referencia al proceso de evaluación de riesgos propio de la empresa).*

3.0 Política

1. Todos los dispositivos englobados en la política deberán tener activado el cifrado completo del disco.
2. La política de uso aceptable de <empresa X> y los cursos de concienciación sobre la seguridad deben obligar a que los usuarios informen a <introducir la información correspondiente> si creen que no cumplen esta política.
3. La política de uso aceptable y los cursos de concienciación sobre la seguridad deben obligar a que los usuarios informen a <introducir la información correspondiente> si se produce el robo o extravío de cualquier dispositivo.
4. La administración y la evaluación del cumplimiento de la política de cifrado son responsabilidad de <introducir la información correspondiente>. Los equipos deben enviar informes a la infraestructura central de gestión para poder demostrar el cumplimiento mediante registros de auditorías cuando sea necesario.
5. Si no es posible realizar una gestión centralizada y se utilizan funciones independientes de cifrado (siempre y cuando la evaluación de riesgos lo autorice), el usuario del dispositivo debe proporcionar una copia de la clave de cifrado activa al departamento informático.
6. <Introducir la información correspondiente> está autorizado a acceder a los dispositivos cifrados para realizar tareas de investigación, mantenimiento o en el caso de que el empleado principal con derechos de acceso al sistema de archivos no esté presente. <Introducir la información correspondiente>, la política de uso aceptable y los cursos de concienciación sobre la seguridad deben advertir a los usuarios sobre este requisito. *(Modifique este requisito según la política de uso aceptable de la empresa o los acuerdos con los empleados)*.

7. La tecnología de cifrado debe configurarse de acuerdo a las prácticas recomendadas del sector para que resulte efectiva contra los posibles ataques.
8. <Introducir la información correspondiente> registrará y auditará todos los eventos relacionados con la seguridad para detectar accesos inadecuados a los sistemas u otros usos malintencionados.
9. El servicio de asistencia de <introducir la información correspondiente> tiene permiso para emitir desafíos y respuestas fuera de banda con el fin de acceder a los sistemas en caso de fallos, pérdidas de credenciales u otros requisitos que impidan la continuidad del negocio. Los desafíos y respuestas se proporcionarán solamente en aquellos casos en los que la identidad del usuario pueda determinarse mediante los atributos documentados en la política de contraseñas.
10. *(Algunas empresas pueden contar con requisitos que obliguen a utilizar métodos graduales para la protección de los datos. Es posible que ciertos usuarios manejen datos especialmente delicados y necesiten medidas de seguridad más estrictas. Si no es el caso de su empresa, puede eliminar este punto)*.

    La política de restricción de datos determinará un grupo de datos delicados y usuarios especiales. Los usuarios de dicho grupo necesitarán la autorización de algún miembro de <introducir la información correspondiente> *(por ejemplo, el director informático)* para cambiar claves o emitir desafíos y respuestas. El servicio de asistencia no podrá acceder a dichos sistemas sin autorización. Estos sistemas tienen acceso a datos muy delicados y de uso restringido y deben permanecer separados. Cuando la política de restricción de datos y autenticación así lo determine, los sistemas y los usuarios deberán utilizar autenticaciones de doble factor según el estándar <introducir la información correspondiente> definido. La autenticación tendrá lugar en el entorno previo al arranque.
11. Los cambios en la configuración se realizarán mediante el proceso de control de cambios de <introducir la información correspondiente> para identificar riesgos y cambios de implementación importantes en la gestión de la seguridad.

4.0 Pautas técnicas

Las pautas técnicas sirven para identificar los requisitos de implementación técnica y suelen estar relacionados con las tecnologías.

1. <Introducir la información correspondiente> es el producto estándar.
2. Deben utilizarse estándares criptográficos sólidos y recomendados en el sector. AES-256 es una implementación aprobada.
3. La BIOS se configurará con una contraseña segura (según lo definido en la política de contraseñas) almacenada por el departamento informático. El disco duro cifrado contará con un orden de arranque fijo. Si un usuario solicita anularlo por razones de urgencia o mantenimiento, el servicio de asistencia puede autenticar al usuario y proporcionarle la contraseña de la BIOS. El objetivo es evitar que los usuarios no autorizados puedan arrancar y atacar el sistema.
4. Se configurará la sincronización de las credenciales de Windows para que el entorno de arranque coincida con las credenciales del usuario y solo sea necesario iniciar sesión una vez.
5. Se utilizará un entorno de arranque previo para la autenticación. Se utilizarán credenciales para la autenticación del usuario según la política de protección de contraseñas de <introducir la información correspondiente>. *(Si su empresa obliga a utilizar autenticaciones de doble factor, indíquelo)*.

5.0 Informes

1. Informe mensual del porcentaje de sistemas cifrados en comparación con los activos englobados en la política
2. Informe mensual del estado del cumplimiento de los sistemas cifrados y administrados
3. Informe mensual del número de activos extraviados y de la evaluación del manejo adecuado de dichos dispositivos