Delete Technology

Powered by blancco

GUIA NORMATIVA DEL CUMPLIMIENTO DEL BORRADO SEGURO Y CERTIFICADO

Delete Technology S.A de C.V - Blancco

ESQUEMA NACIONAL DE SEGURIDAD (ENS)

La Ley 11/2007 de "Acceso Electrónico de los Ciudadanos" reconoce el derecho de los ciudadanos a relacionarse con las Administraciones Públicas por medios electrónicos. La ley regula los aspectos básicos de la utilización de las tecnologías de la información en la actividad administrativa, en las rela-ciones entre las Administraciones Públicas, así como en las relaciones de los ciudadanos con las mismas. En su artículo 42 crea el **Esquema Nacional de Seguridad.** El Esquema Nacional de Seguridad **(ENS)**, regulado por el Real Decreto 3/2010 determina la política de seguridad que se ha de aplicar en la utilización de los medios electrónicos

El **ENS** está constituido por los principios básicos y requisitos mínimos para una protección adecuada de la información.

Será aplicado por las Administraciones Públicas para asegurar el acceso, integridad, disponibilidad, autenticidad, confidencialidad, trazabilidad y conservación de los datos, informaciones y servicios utilizados en medios electrónicos que gestiones en el ejercicio de sus competencias.

El ENS de obligado cumplimiento para todas las Administraciones Públicas

El ámbito de aplicación del Esquema Nacional de Seguridad es el establecido en el artículo 2 de la Ley 11/2007, de manera que es de aplicación:

- A la Administración General del Estado, Administraciones de las Comunidades. Autónomas y las Entidades que integran la Administración Local, así como las entidades de derecho público vinculadas o dependientes de las mismas.
- Fundaciones del sector público.
- Universidades Públicas.
- Grupos políticos de las Cortes Generales y de Corporaciones Locales.
- Colegios profesionales en las tareas que realizan para la administra-ción.
- Cámaras de comercio.
- Hospitales públicos.
- Federaciones deportivas.
- Empresas públicas (aguas, comunicaciones, transporte, radio y TV, au-topistas, etc.)
- A los ciudadanos en sus relaciones con las Administraciones Públicas.
- A las relaciones entre las distintas Administraciones Públicas.

El **ENS** es una norma de obligado cumplimiento para todos los Sistemas de Información de las AA.PP., independientemente de su ubicación. Por tanto, debemos exigir el cumplimiento del **ENS** no sólo a los Sistemas de Información que estén operados por personal de las AA.PP. y/o en dependencias de las AA.PP., sino también a aquellos otros que, estando operados por terceros e, incluso, en dependencias de terceros- desarrollan funciones, misiones, cometidos o servicios para las AA.PP

El **ENS** presenta un esquema basado en el análisis de los riesgos, el concepto de seguridad integral, la organización de la misma como instrumento para la gestión y por el desarrollo de procesos de revaluación, prevención, reacción y recuperación mediante la implantación de medidas de seguridad según la naturaleza y servicios de la organización.

El **ENS** es una norma jurídica de aplicación obligatoria a todas las Administraciones Públicas. El **ENS** que trata la 'protección' de la información y los servicios, contempla y exige la gestión continuada de la seguridad, para lo cual cabe aplicar un sistema de gestión. La normalización nacional e internacional, de cumplimiento voluntario, ofrece herramientas como la norma **UNE ISO/IEC 27001:2007** que es una norma de 'gestión' que contiene los requisitos para la construcción de un sistema de gestión de seguridad de la información, contra la que puede, en su caso, de forma voluntaria, certificarse una entidad (pública o privada) mediante un proceso de auditoría realizado por un auditor certificado externo.

Esquema Nacional de Seguridad

GOBIERNO DE ESPAÑA
MINISTERIO DE HACIENDA Y ADMINISTRACIONES PÚBLICAS

- ✓ **Es un instrumento legal - Real Decreto 3/2010**
  Desarrolla lo previsto sobre en la Ley 11/700
- ✓ **Establec la política de seguridad**
  En los servicios de administración-e.Está constituida por los principios básicos y requisitos mínimos que permitan la protección adecuada de la información.
- ✓ **Es de aplicación a todas las AA.PP.**
  Están excluidos de los sistemas que manejan la información clasificada.
- ✓ **Mecanismo de adecuación escalonado**
  Fecha límite 29.01.2014
- ✓ **Esfuerzo colectivo**
  AGE,CC.AA,CC.LLC,.-FEMP,CRUE+Opinión Industria TIC.

ens Esquema Nacional de Seguridad

LOS DATOS (artículo 21) Esquema Nacional de Seguridad

La Sociedad Española de Documentación e Información Científica (SEDIC), define metadato como “toda aquella información descriptiva sobre el contexto, calidad, condición o características de un recurso u objeto de información que tiene la finalidad de facilitar su recuperación, autentificación, evaluación, preservación y/o interoperabilidad”. 17. En el caso de fotografías digitales, por ejemplo, la propia cámara a la vez que captura las imágenes puede ir guardando en forma de metadatos, información de cómo fue tomada la fotografía: fecha, hora, diafragma, velocidad, uso de flash, modo de captura o localización. 18. En el caso de archivos de audio o vídeo, los metadatos pueden almacenar información como el título de la obra, álbum, año, autor, carátula o género. 19. En el caso de documentos ofimáticos, los metadatos pueden almacenar información de quién lo creó, quién lo modificó, quien realizó el último acceso al documento y las fechas correspondientes, tiempo que ha tardado en editarse el documento, dispositivo o software utilizado para la creación del documento, o compañía y departamento al que pertenece.

Cada organización, dentro de las políticas implantadas para el desempeño de sus actividades, dispondrá de una Política de Gestión Documental en la que se establecerán los criterios y normas en relación con la gestión de los documentos electrónicos.

Dentro de esta política se especificará el esquema de metadatos asociados a los documentos electrónicos para asegurar la gestión, recuperación y conservación de los mismos durante todo su ciclo de vida 25. Por otro lado, es importante indicar que tanto los dispositivos (ordenadores o cámaras, por ejemplo), como muchos de los programas de generación y tratamiento de documentos, insertan sus propios metadatos sin que en muchos casos el usuario sea consciente de ello. 26. Los metadatos normalmente se encuentran ocultos y no son visibles usando la configuración estándar de la aplicación con la que estemos trabajando sobre el archivo. Para visualizarlos es necesario establecer una configuración específica o incluso utilizar un software específico para revelar esos datos ocultos

ANEXO II Esquema Nacional de Seguridad

Medidas de seguridad

5. Medidas de protección [mp]

5.5.5 Borrado y destrucción [mp.si.5].

La medida de borrado y destrucción de soportes de información se aplica-rá a todo tipo de equipos susceptibles de almacenar información, incluyendo medios electrónicos y no electrónicos.

Nivel BAJO

a) Los soportes que vayan a ser reutilizados para otra información o libe-rados a otra organización serán objeto de un borrado seguro de su contenido.

Nivel MEDIO Y ALTO

b) Se destruirán de forma segura los soportes, en los siguientes casos:

1. Cuando la naturaleza del soporte no permita un borrado seguro.

2. Cuando así lo requiera el procedimiento asociado al tipo de información contenida.

c) Se emplearán productos certificados conforme a lo establecido en ([op. pl.5]).

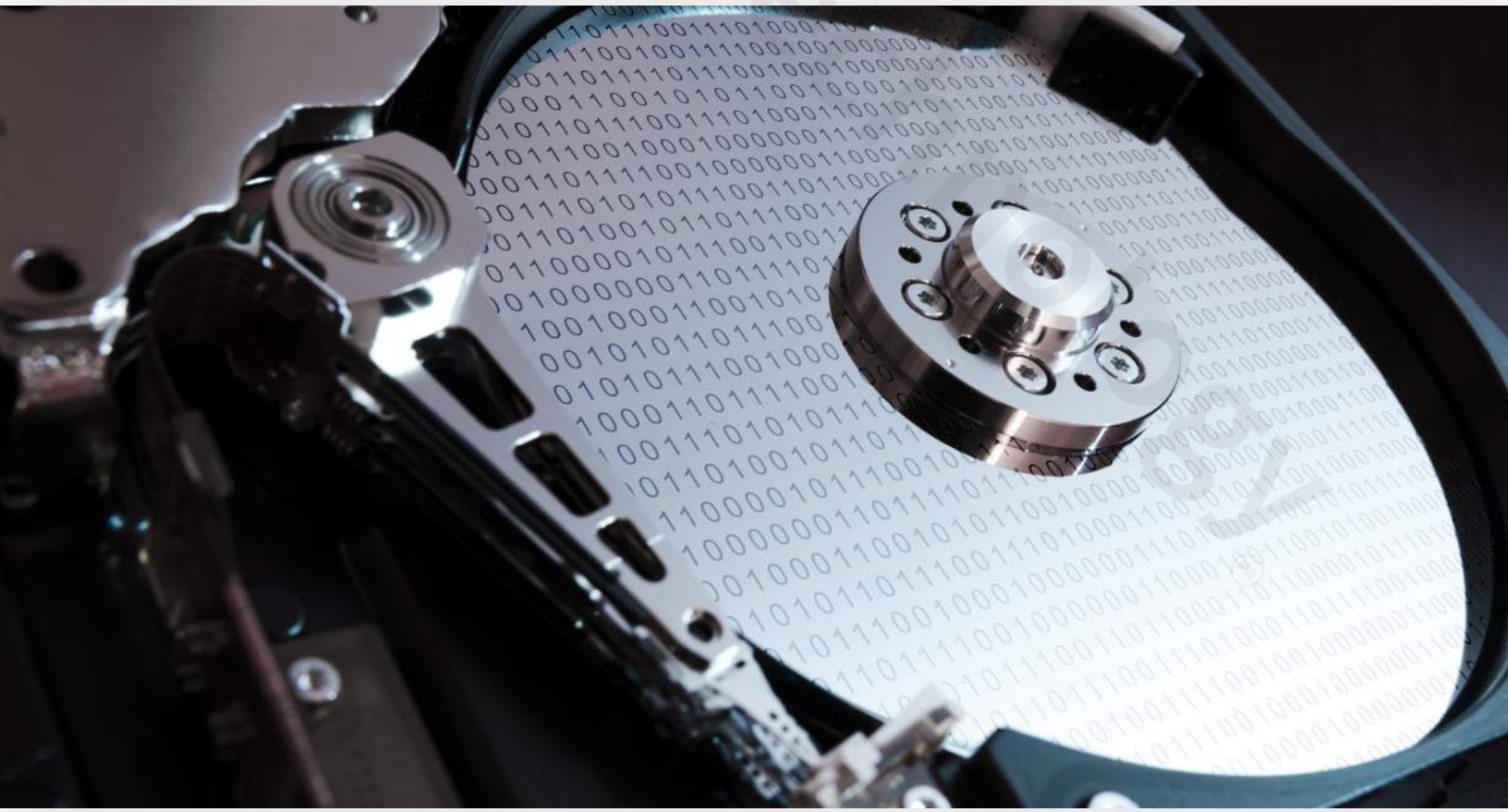
GUÍA DE SEGURIDAD (CCN-STIC-818)

BORRADO SEGURO

En el intercambio de información mediante dispositivos extraíbles de almace-namiento (lápices USB, discos duros externos, etc.), o al desechar ordenado-res, puede quedar información sensible accesible a personas no autorizadas, siendo por ello necesario contar con herramientas de borrado seguro que ga-ranticen que no es posible recuperar información que hemos eliminado pre-viamente.

Existen varias herramientas de este tipo, pero nos centraremos en aquellas que no destruyen el soporte físico, sino la información y que además lo hace mediante el uso de software, sin necesidad de contar con aparto alguno. Este tipo de herramientas normalmente borran la información sobrescribiéndola en numerosas ocasiones con caracteres sin valor (por ejemplo 0).

Las herramientas que se usen deberán cumplir con la política de borrado se-guro, la cual puede exigir un número determinado de sobre escrituras.



¿LAS EMPRESAS PRIVADAS TIENEN QUE CUMPLIR EL ENS?

Las empresas del sector privado que prestan servicios a entidades públi-cas también deben cumplir los requerimientos del **ENS** según el tipo de servicio e información que tratan. Habitualmente son empresas tecnológicas y de servicios. Por ejemplo, empresas tecnológicas de desarrollo de software, servicios cloud, mantenimiento de sistemas, servicios de nóminas, contabili-dad, etc.
En caso de duda, el **Centro Criptológico Nacional** recomienda realizar un análisis concreto para cada tipo de servicio e información que se trata.

INTEGRACIÓN DEL ESQUEMA NACIONAL Y LA PROTECCIÓN DE DATOS

Desde el 2018 las entidades del sector público deben integrar la adaptación al ENS con el cumplimiento de las normativas de protección de datos: el **RGPD** y la nueva **LOPDGDD.**

La Ley de Protección de Datos y Garantía de los Derechos Digitales también regula las medidas de seguridad en el ámbito del sector público. La LOPDGDD establece que, en caso de tratamiento de datos personales por parte de las AAPP, estas deberán aplicar un grado de seguridad en base al ENS y el correspondiente

En conclusión:

- El **ENS** es una norma jurídica, el **Real Decreto 3/2010**, que se encuen-tra al servicio de la realización de derechos de los ciudadanos y es de aplicación obligatoria a todas las Administraciones Públicas.
- El **ENS** que trata la 'protección' de la información y los servicios, con-templa y exige la gestión continuada de la seguridad, para lo cual cabe aplicar un sistema de gestión.
- La normalización nacional e internacional, de cumplimiento voluntario, ofrece herramientas como la norma **UNE ISO/IEC 27001:2007** que es una norma de 'gestión' que contiene los requisitos para la construcción de un sistema de gestión de seguridad de la información, contra la que puede, en su caso, de forma voluntaria, certificarse una entidad (públi-ca o privada) mediante un proceso de auditoría realizado por un audi-tor certificado externo.

- Si bien cabe señalar que aquellas organizaciones que se encuentren certificadas contra **ISO 27001** tienen una buena parte del camino reco-rrido para lograr su conformidad con el ENS, toda vez que las medidas de protección que señala el ENS coinciden, en lo sustancial, con los controles que prevé la norma internacional.
- Por tanto, el **Esquema Nacional de Seguridad** y la norma **UNE ISO/IEC 27001:2007** difieren en su naturaleza, en su ámbito de aplicación, en su obligatoriedad y en los objetivos que persiguen.
- La norma **ISO 15713: 2010** Destrucción segura del material confiden-cial, código de buenas prácticas sirve de complemento a la LOPD para la destrucción de documentos que contienen datos personales en cualquier tipo de soporte. También es útil si queremos garantizar la destrucción de datos confidenciales, en el caso de que nos obligára-mos a ello por un contrato o acuerdo con otra empresa.

Cumplimiento Legal Prevención de fuga de información: Gestión del ciclo de vida de la información

¿Cuál es el plazo de conservación legal de la información de la empresa?

PLAZO DE CONSERVACIÓN LEGAL DE LA INFORMACIÓN (EMPRESA)							
	DATOS PERSONALES	DATOS CONTABLES	DATOS FISCALES	DATOS LABORALES	CONTROL DE ACCESO	VIDEO VIGILANCIA	COMUNICACIONES
PERIODO DE CONSERVACIÓN	DEPENDE. EJEMPLO 4 AÑOS DEUDAS TRIBUTARIAS	AL MENOS 6 AÑOS	AL MENOS 4 AÑOS	AL MENOS 5 AÑOS	MÁXIMO DE 1 MES	MÁXIMO DE 1 MES	AL MENOS 1 AÑO

En función del tipo de información de que se trate y su categorización, el plazo de conservación de la misma, debe al menos respetar los periodos de conservación legalmente establecidos, como son los siguientes.

✓ 1ºDatos Personales

Para el caso de documentos o ficheros que contengan datos personales, la AGPD establece que:
«Los datos de carácter personal serán cancelados cuando hayan dejado de ser necesarios o pertinentes para la finalidad para la cual hubieran sido recabados o registrados.
No serán conservados en forma que permita la identificación del interesado durante un período superior al necesario para los fines en base a los cuales hubieran sido recabados o registrados.»

Sin embargo, la cancelación de los datos no supone su eliminación automática, sino su bloqueo. Para su supresión o eliminación definitiva, deberá haber prescrito el plazo de conservación que haya podido ser legalmente establecido para su tratamiento. Cumplido este plazo deberá ser suprimido.

Por ejemplo, cuatro años de prescripción de las deudas tributarias, o 3 años en relación con las conductas constitutivas de infracción muy grave por la propia LOPD.

✓ 2º Datos contables

El plazo durante el cual los empresarios deben conservar sus libros obligatorios (diario, inventarios y cuentas anuales) como los no obligatorios (mayor, registros de impuesto sobre el valor añadido, auxiliares, etc.), así como la documentación y justificantes que sirven de soporte a las anotaciones registradas en los libros está fijado en seis años, tal y como dispone el Real Decreto del Código de Comercio.

✓ 3º Datos Fiscales

En relación con la prescripción del derecho de la Administración para determinar la deuda tributaria en base a los libros de contabilidad y demás documentación relacionada es de 4 años, plazo en el cual los empresarios deberán conservarán los libros.

✓ 4º Datos Laborales

Los datos laborales, inscripción de empresas y afiliación, altas y bajas en la Seguridad Social de los trabajadores deben conservarse durante un periodo mínimo de 5 años, a partir de la baja del trabajador, en base al Real Decreto 84/1996.

✓ 5º Control de acceso a edificios

Los datos incluidos en ficheros automatizados creados para controlar el acceso a edificios, deben ser destruidos transcurrido el plazo de un mes a partir de su obtención según Instrucción 1/1996 de la AEPD.

✓ 6º Videovigilancia

En la instrucción video vigilancia 1/2006 de la AEPD se establece como plazo máximo para la cancelación de las grabaciones de un mes desde su captación.

✓ 7º Comunicaciones

Los datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones, disponen que los operadores de redes de telecomunicaciones almacenen y conserven durante un año informaciones sobre las comunicaciones (los llamados metadatos) que establecemos con terceros, con el fin de, en su caso, utilizar esa información para la averiguación e investigación de delitos graves, en base a la ley 25/2007 de conservación de datos.

Control de la eliminación de documentos de la Administración General del Estado y sus Organismos Públicos.

Los requisitos legales previos a la eliminación de información La eliminación de documentos administrativos de la Administración General del Estado y de sus organismos públicos requiere el dictamen preceptivo de la Comisión Superior Calificadora de Documentos Administrativos (CSCDA) y se atiene al procedimiento establecido en el Real Decreto 1164/2002, de 8 de noviembre, por el que se regula la conservación del patrimonio documental con valor histórico, el control de la eliminación de otros documentos de la Administración General del Estado y sus organismos públicos y la conservación de documentos administrativos en soporte distinto al original.

Niveles de borrado/destrucción de la información

Se tendrá en cuenta la clasificación establecida por el Centro Criptológico Nacional , que distingue los niveles siguientes de borrado /destrucción de la información:

- * **Nivel 0**: Borrado usando comandos/utilidades estándar del sistema operativo. Estas técnicas generalmente marcan el espacio ocupado por los archivos a borrar como disponible, pero no eliminan realmente el contenido almacenado. Por este motivo, no impide la recuperación posterior de la información borrada ni proporciona ninguna garantía frente a la revelación no autorizada de la información. Este nivel se menciona aquí con carácter “académico” ya que no puede considerarse un método de borrado admisible.
- * **Nivel 1** ('clearing'): Borrado usando mecanismos de sobrescritura del espacio ocupado por los archivos a borrar. La recuperación de la información borrada sólo puede realizarse usando técnicas avanzadas. Recomendado cuando el nivel de confidencialidad de la información a borrar sea bajo, usando mecanismos de sobrescritura4 con un número reducido de pasadas sobre los mismos sectores (entre 2 y 5).
- * **Nivel 2** ('sanitizing'): Borrado seguro. Impide la recuperación de la información borrada incluso utilizando mecanismos avanzados. Algunas de las técnicas que se pueden utilizar para realizar este borrado son: la desmagnetización del soporte; el borrado seguro mediante 'firmware' incorporado al soporte físico; la sobrescritura de la información con protocolos que hagan imposible su reconstrucción (generalmente mediante una serie consecutiva de sobrescrituras); o el cifrado de la información con criptografía fuerte y ofuscación de la clave de cifrado empleada.

Es el nivel recomendable cuando el grado de confidencialidad de la información a borrar sea medio o alto. Se utilizan funciones de sobrescritura más avanzadas, equiparables en seguridad al método Gutmann completo.

PRINCIPAL NORMATIVA ESPAÑOLA RESPECTO DEL BORRADO SEGURO

***El artículo 17 de la Ley 39/2015**, del Procedimiento Administrativo Común de las Administraciones, establece que el Archivo de documentos, además de tratar el archivo electrónico de expedientes finalizados menciona que la eliminación de los documentos electrónicos.

***El artículo 13 de la Ley 39/2015**, Derechos de las personas en sus relaciones con las Administraciones Públicas, establece asimismo la obligación de la Administración de proteger los datos de carácter personal de los ciudadanos que figuren en sus archivos.

***El artículo 49 de la Ley 16/1985**, de Patrimonio Histórico Español, establece que forman parte del Patrimonio Documental los documentos "generados, conservados o reunidos en el ejercicio de su función por cualquier organismo o entidad de carácter público".

***El artículo 55 de la Ley 16/1985** determina por otro lado que los documentos que forman parte del Patrimonio Documental no podrán destruirse "en tanto subsista su valor probatorio de derechos y obligaciones de las personas o los entes públicos".

***El Real Decreto 1164/2002**, de 8 de noviembre, por el que se regula la conservación del patrimonio documental con valor histórico, el control de la eliminación de otros documentos de la Administración General del Estado y sus organismos públicos y la conservación de documentos administrativos en soporte distinto al original, define el procedimiento de eliminación de documentos.

***El Real Decreto 3/2010**, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica, incluye una medida de protección específica (borrado y destrucción mp.si.5) relativa a los soportes de información: "borrado seguro" para aquellos que se puedan reutilizar y "destrucción de forma segura" cuando las características de un soporte de información impidan su borrado seguro o cuando el tipo de información que contengan así lo requiera.

***El Real Decreto 4/2010**, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el marco de la Administración Electrónica, contempla la destrucción reglamentaria como la fase final del ciclo de vida de los documentos electrónicos que no han sido seleccionados para su conservación permanente, señalando que "si el resultado del procedimiento de evaluación documental así lo establece, borrado de la información, o en su caso, destrucción física de los soportes, de acuerdo con la legislación que resulte de aplicación, dejando registro de su eliminación."

***El Real Decreto 1708/2011**, de 18 de noviembre, por el que se establece el Sistema Español de Archivos y se regula el Sistema de Archivos de la Administración General del Estado y de sus Organismos Públicos y su régimen de acceso, en su artículo 20, señala la necesidad de que el "borrado de la información" o "la destrucción física de los soportes" sean consecuencia de un "procedimiento regulado".

***Guía de Aplicación de la NTI de Política de Gestión de Documentos Electrónicos**, considera que "el proceso de eliminación de documentos electrónicos constituye un proceso clave en la gestión de documentos y tiene como objetivo impedir su restauración y posterior reutilización. Para ello, es necesario aplicar un proceso que incluya tanto el borrado de la información (el propio documento y sus metadatos) como la destrucción física del soporte, en función de las características del formato y las del propio soporte".
Guía se aborda el proceso de gestión documental de destrucción o eliminación, recogido en la Política de Gestión de Documentos Electrónicos del MINHAP en su apartado "2.5.9 Destrucción o eliminación". Se tratan aspectos como la distinción entre distintos niveles de borrado de documentos electrónicos, los tipos de soportes de almacenamiento, la gestión interna o externa de los mismos, los métodos y técnicas de borrado y destrucción seguros, el nivel de protección de la información y se exponen las pautas para ejecutar un proceso de eliminación segura en función de su alcance y de los motivos que han llevado a ponerlo en marcha.

Delete Technology Group
Av. Ejército Nacional 826A Oficina 104 Col. Polanco CDXM 11540 México

Delete Technology
Powered by blancco