Estudio sobre recomendaciones generales para la destrucción segura de datos personales en ambiente físico y electrónico

IFAI

Diciembre, 2014

EY
Construyendo un mejor entorno de negocios

Diciembre, 2014

María Adriana Báez Ricardéz
Directora General de Autorregulación
Instituto Federal de Acceso a la Información y Protección de Datos

Estimada María Adriana,

Agradecemos la confianza que nos han otorgado al permitirnos apoyarles en la ejecución del proyecto titulado “Estudio sobre recomendaciones generales para la destrucción segura de datos personales en ambiente físico y electrónico” para el Instituto Federal de Acceso a la Información y Protección de Datos (en lo sucesivo IFAI).

Como resultado de la ejecución de nuestro trabajo, hemos preparado este documento con el detalle del estudio realizado.

Agradecemos el apoyo que nos han brindado para la ejecución del proyecto y quedamos a sus órdenes para resolver cualquier duda o aclaración que al respecto pueda presentarse.

Cordialmente,

Christian Andreani
Information Technology Risk & Transformation
Socio
Advisory Services

Tabla de Contenido

Resumen ejecutivo

Introducción

Durante el periodo comprendido del 8 de octubre al 22 de diciembre de 2014 se ejecutó el proyecto titulado “Estudio sobre recomendaciones generales para la destrucción segura de datos personales en ambiente físico y electrónico”, atendiendo a la preocupación del IFAI de generar recomendaciones basadas en estándares y buenas prácticas internacionales, tomando como marco de referencia lo dispuesto por la Ley, su Reglamento y las Recomendaciones en materia de seguridad de datos personales. Esto con el fin de que los responsables y encargados del tratamiento de los datos personales logren implementar procedimientos que permitan una destrucción, borrado, eliminación o supresión segura de los datos personales, tanto en soporte físico como electrónico.

Para cumplir con lo anterior, se planteó el siguiente objetivo:

- Elaborar un estudio, a efecto de que el IFAI pueda desarrollar una guía para proporcionar a los responsables y encargados un documento de fácil comprensión, para orientarlos sobre los criterios generales de:

    i. Pérdida y recuperación de la información

    ii. Borrado seguro y destrucción de los datos personales en soportes físicos y electrónicos.

Antecedentes

- El 6 de julio de 2010 entra en vigor la Ley Federal de Protección de Datos Personales en Posesión de los Particulares y el IFAI se transforma en el Instituto Federal de Acceso a la Información y Protección de Datos. A partir de ese momento, la Ley se constituye como un marco general que contempla reglas, requisitos, condiciones y obligaciones mínimas para garantizar un adecuado tratamiento de los datos personales por parte de los responsables.

- Uno de los principios que regula el derecho a la protección de datos personales en la Ley es el de “calidad”. Este principio señala que cuando los datos personales hayan dejado de ser necesarios para el cumplimiento de las finalidades previstas por el aviso de privacidad y las disposiciones legales aplicables, deberán ser cancelados (artículo 11 de la Ley).

- El artículo 37 del Reglamento de la Ley establece que una vez cumplida las finalidades del tratamiento, y cuando no exista disposición legal o reglamentaria que establezca lo contrario, el responsable deberá proceder a la cancelación de los datos personales en su posesión previo bloqueo de los mismos, para su posterior supresión.

- Asimismo, el artículo 38 del Reglamento de la Ley prevé la obligación de los responsables de establecer y documentar los procedimientos para conservación, bloqueo y supresión de los datos personales. Cabe señalar que la supresión de datos se define en el artículo 2, fracción XII del Reglamento de la Ley, como la actividad consistente en eliminar, borrar o destruir el o los datos personales, una vez concluido el periodo de bloqueo, bajo las medidas de seguridad previamente establecidas por el responsable.

Alcance

El estudio abarca los siguientes temas:

1. **Introducción a la importancia de la destrucción y el borrado seguro de información**

    1.1. Importancia y beneficios de la destrucción y el borrado seguro de los datos personales en el marco de la Ley y el Reglamento.

    1.2. Causas de la pérdida de información en soportes físicos y electrónicos.

    1.3. Métodos y técnicas de recuperación de información en soportes físicos y electrónicos.

    1.4. Consecuencias legales, económicas y de imagen debido a una vulneración a la seguridad de los datos personales por una mala práctica de destrucción y/o borrado de información.

2. **Almacenamiento de los datos personales; Procedimiento que permita identificar el medio y la forma en que se almacenan datos personales, tomando en cuenta:**

    2.1. Flujo de los datos personales; procedimiento para identificar cómo se obtienen y hacia dónde van los datos personales dentro de la organización durante el ciclo de vida y tratamiento de los mismos.

    2.2. Diferentes soportes de almacenamiento físico y electrónico donde se resguardan datos personales, y sus características para la selección de la técnica de destrucción y/o borrado idónea.

    2.3. Criterios para definir la política, procedimientos y tiempos de almacenamiento de información que existen en la organización y que son relevantes para la destrucción y/o borrado seguro de los datos personales.

3. **Técnicas de destrucción y borrado seguro**

    3.1. Técnicas principales de destrucción y borrado seguro de información física y electrónica.

    3.2. Proporcionar información para orientar en la selección del método de destrucción y/o borrado idóneo para cada soporte de almacenamiento de datos personales.

    3.3. Generar una comparativa de ventajas y desventajas de cada una de las técnicas de destrucción y/o borrado, así como una relación del método adecuado en función del soporte de almacenamiento.

Es importante mencionar que para la ejecución del estudio se consideraron los siguientes aspectos:

Contexto Nacional	Contexto Internacional
Marco jurídico Mexicano en materia de Protección de datos personales • Ley Federal de Protección de Datos Personales en Posesión de los Particulares. • Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares. • Recomendaciones en materia de seguridad de datos personales (Publicadas en el DOF el 30 de Octubre de 2013). • Estudio para implementar un Sistema de Gestión de Seguridad de Datos Personales emitida por el IFAI. • El Manual en materia de seguridad de datos personales para MIPYMES y organizaciones pequeñas. 	Análisis de estándares relacionados con la destrucción y borrado seguro de información, considerando los siguientes: • BS 10012:2009 Data protection – Specification for a personal information management system. • COBIT 5 Framework. • Estudio sobre almacenamiento y borrado seguro de información del Observatorio Inteco. • ISO/IEC 27001:2013, Information Technology - Security techniques – Information security management systems – Requirements. • ISO/IEC 27002:2013, Information Technology - Security techniques – Code of practice for security management. • ISO/IEC 29100:2011, Information Technology - Security techniques -- Privacy framework. • ISO 15489-1:2001, Information and documentation - Records management • NIST SP 800-88 Guidelines for Media Sanitization. 

Ilustración 1. Estándares considerados para el estudio.

Glosario de términos

Administración de contenido empresarial (Enterprise Content Management o ECM). Es un marco de trabajo que consiste en la implementación de estrategias, métodos y herramientas que se utilizan durante el ciclo de vida de los documentos y contenido, con el objetivo de formalizar su organización y almacenamiento. Un ECM apoya a las organizaciones en la consolidación de información de distintos recursos en un repositorio de administración central que inclusive se puede utilizar para proteger el contenido contra el acceso no autorizado. Este proceso cubre la gestión de cualquier tipo de información ya sea que se encuentre en forma física o electrónica, (ej. Un documento en papel, un correo electrónico, un expediente digital).

Esquema de clasificación de información. Consiste en elegir en base a qué atributos vamos a agrupar la información y cómo vamos a organizar estos atributos con el objetivo de consolidar todo el contenido de una forma consistente y coherente de acuerdo a las necesidades de la empresa. El objetivo de este tipo de esquemas consiste en indicar la necesidad, la prioridad y el nivel de protección requerido para el tratamiento de cada tipo de dato de acuerdo a su criticidad.

Gobierno de gestión de la privacidad de la información. Es una estructura que busca determinar los riesgos asociados con la privacidad de la información, así como la forma de reducir y/o mitigar impactos relacionados con el tema mediante el establecimiento de un programa amplio y conciso que incluya el desarrollo y la implementación de normativas y el seguimiento necesario para validar el cumplimiento de estas.

Ley Federal de Protección de Datos Personales en Posesión de los Particulares[1]. Ley cuyo objetivo es buscar la protección de los datos personales en posesión de los particulares, con la finalidad de regular su tratamiento legítimo, controlado e informado, a efecto de garantizar la privacidad y el derecho a la autodeterminación informativa de las personas.

Robo de identidad. El robo de identidad consiste en que un tercero no autorizado utilice información personal de alguien más para realizar actividades fraudulentas.

Sistema de gestión de seguridad de datos personales. Es un Sistema por medio del cual se busca establecer, implementar, operar, monitorear, mantener y mejorar el tratamiento y seguridad de los datos personales según el riesgo asociado con los activos. El SGSI busca garantizar que las empresas conocen los riesgos relacionados con el tratamiento de datos personales, para que estos puedan ser gestionados.

Sanitización. Es el proceso mediante el cual se remueve información sensible o confidencial de un medio

Tiempos de retención. Periodo mínimo que deberá resguardarse cierta información. Este deberá definirse en base a las necesidades de la organización y a regulaciones aplicables.

[1] Ley Federal de Protección de Datos Personales en Posesión de los Particulares.

Estudio sobre recomendaciones generales para la destrucción segura de datos personales en ambiente físico y electrónico

Antecedentes de la protección de la información

La información se ha convertido en uno de los activos más importantes para las organizaciones ya que representa una ventaja competitiva. Conforme aumenta la capacidad de las empresas para explotar la información que utilizan, la toma de decisiones se vuelve más sólida, eficiente y efectiva. Esto se ve reflejado en el cumplimiento de objetivos lo cual a su vez, facilita la alineación de la operación con la estrategia organizacional, fomentando así el crecimiento del valor del negocio. Existe una gran variedad de información que las empresas utilizan diariamente para el desempeño de sus funciones, algunos ejemplos se muestran en la Ilustración 2:

Ilustración 2. Tipo de información que utiliza una empresa

Cada día es más común que los negocios soliciten y usen datos personales para proporcionar sus servicios. Asimismo, los avances tecnológicos se han convertido en un factor relevante que fomenta el uso de información para distintos fines por medio de herramientas que facilitan el tratamiento y la explotación de los datos.

La información personal es aquella relacionada con una persona que la haga identificable, estos datos mal utilizados podrían afectar al dueño de los datos, así como al responsable que realiza el tratamiento. Es por esto que la seguridad de la información se debe enfocar en proteger lo más importante: la información personal y sensible de la organización.

Actualmente, la seguridad de la información se ha convertido en un tema necesario para las organizaciones, sin embargo, de acuerdo a la XIV edición de la Encuesta Global de Seguridad de la Información realizada por EY, solamente el 30% de los encuestados calificaron el tema de la

privacidad como su principal prioridad en términos de inversión. Esto posicionó el tema en el décimo lugar de la jerarquía de temas de seguridad de la información. La privacidad necesita estar en un rango más alto. El Anexo A muestra el detalle del resultado de la encuesta con los temas prioritarios.

Modelos o estándares sobre destrucción y/o borrado seguro relevantes en los últimos años

Existen distintas regulaciones y estándares donde se establecen las normas y mejores prácticas que los responsables de la información deben o pueden acatar para garantizar la privacidad de la información de las personas físicas. Dichos documentos incluyen especificaciones relacionadas con el tema de la destrucción y el borrado de información que pueden servir como referencia para que las organizaciones implementen medidas de seguridad de acuerdo a sus necesidades.

En el 2010 se crea en México, la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP), la cual establece en su artículo 11 que los datos personales deben ser cancelados cuando ya no se requieran. Por su parte en el 2011 se publica el reglamento de la LFPDPPP, el cual define en su artículo 37 que una vez cumplida las finalidades del tratamiento, y cuando no exista disposición legal o reglamentaria que establezca lo contrario, el responsable deberá proceder a la cancelación de los datos personales en su posesión previo bloqueo de los mismos, para su posterior supresión. Asimismo, el artículo 38 de este mismo Reglamento prevé la obligación de los responsables de establecer y documentar los procedimientos para conservación, bloqueo y supresión de los datos personales.

En el 2013 se publican recomendaciones en materia de seguridad de datos personales en el Diario Oficial de la Federación, este documento consiste en mejores prácticas para la implementación de un Sistema de Gestión de Seguridad de Datos Personales (SGSDP), por medio del cual se puede facilitar la protección de la seguridad de los datos personales. Asimismo, el IFAI publica una Guía de implementación de un Sistema de Gestión de Seguridad de Datos Personales donde se explica de forma más detallada todo lo que debe considerarse dentro de este sistema.

En el 2014 se publica el Manual en materia de seguridad de datos personales para MIPYMES y organizaciones pequeñas, documento que proporciona recomendaciones para implementar medidas de seguridad adecuadas, así como un SGSDP enfocado en empresas más pequeñas.

Ilustración 3. Estándares nacionales.

Por su parte, en el ámbito internacional se publica el COBIT Framework en 1996. Este documento sirve como un modelo de referencia sobre mejores prácticas para guiar la gestión de las tecnologías de la información.

En el 2001 se publica el ISO 15489-1:2001 el cual regula la gestión de documentos y sistemas de archivos para proporcionar disponibilidad, autenticidad, fiabilidad e integridad a través de la implementación de una metodología definida por la norma. Para diseñar e implementar un sistema de gestión de documentos de archivo se deben considerar las siguientes etapas:

- Generalidades: identificar las funciones necesarias para gestionar documentos existentes.
- Documentación de operaciones: documentar de forma precisa las operaciones desarrolladas por cada tipo de documento.
- Soporte físico de almacenamiento y protección: considerar los soportes de almacenamiento, elementos para su protección física y procedimientos para su manipulación tomando en cuenta los plazos de conservación de los documentos de archivo
- Gestión distribuida: contemplar distintas ubicaciones de los documentos.
- Conversión y migración: el sistema debe garantizar la autenticidad, fiabilidad y el uso de los documentos, aunque se produzcan cambios.
- Acceso, recuperación y uso: el sistema debe facilitar el acceso y la recuperación de documentos de forma eficaz y oportuna para garantizar la continuidad de las actividades.
- Conservación y disposición: el sistema debe facilitar y aplicar decisiones relativas a la conservación y/o disposición de documentos en cualquier etapa del ciclo de vida.

En el 2013 se actualizan y publican los estándares ISO/IEC 27001:2013 y el ISO/IEC 27002:2013. El ISO 27001 proporciona los requerimientos para establecer, implementar, mantener y mejorar un sistema de gestión de seguridad de la información. Por su parte el ISO 27002 es una referencia para la selección de controles al momento de implementar el sistema de gestión. La norma proporciona 114 opciones de control agrupados en las siguientes cláusulas

Cláusulas de control de seguridad			
5. Políticas de SI	6. Organización de SI	7. Seguridad de los recursos humanos	8. Administración de los activos
9. Control de accesos	10. Criptografía	11. Seguridad física y ambiental	12. Seguridad en las operaciones
13. Seguridad en las comunicaciones	14. Adquisición, desarrollo y mantenimiento de sistemas		15. Relación con proveedores
16. Gestión de incidentes de SI	17. Aspectos de SI en la gestión de la continuidad del negocio		18.Cumplimiento

Ilustración 4. Cláusulas de control de ISO 27001 e ISO 27002.

En el 2009 se publica el BS 10012:2009, utilizado como una referencia para la implementación de un sistema para la gestión de información personal que apoye a las empresas a estar en cumplimiento con regulaciones sobre el tema.

En el 2011 Se publica el Estudio sobre almacenamiento y borrado seguro de información del Observatorio Inteco, documento que contiene información sobre la pérdida, recuperación y borrado de información, así como de legislaciones aplicables. En este mismo año se publica el ISO/IEC 29100, documento que busca apoyar a las organizaciones a definir los mecanismos de protección necesarios para proteger la información de identificación personal (PII) por medio de la definición e implementación de una estructura formada por los siguientes componentes:

Ilustración 5. Componentes de un esquema de privacidad.

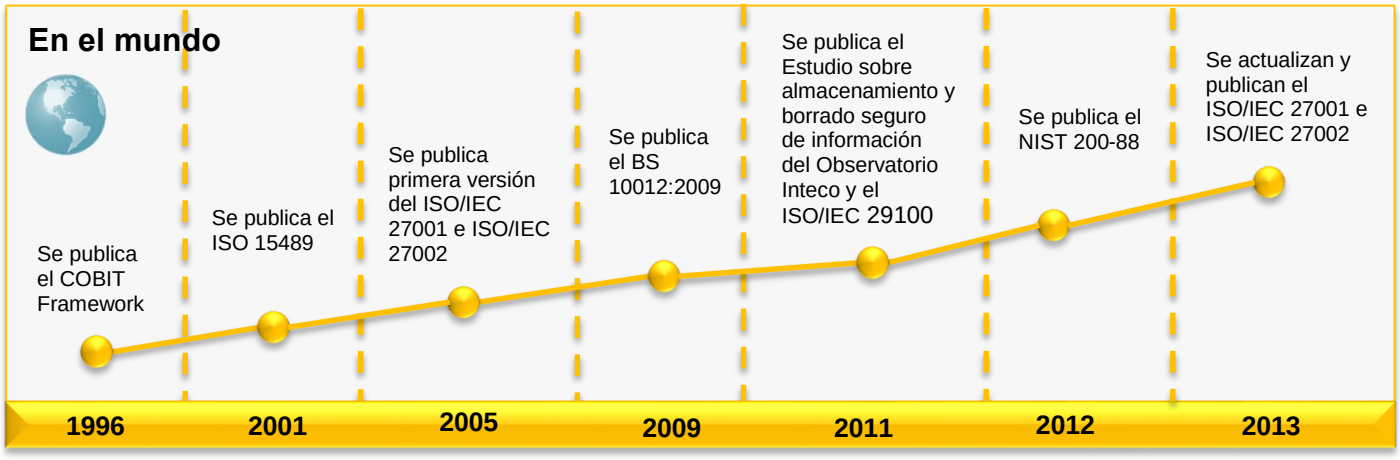


Ilustración 6. Estándares internacionales.

Todos estos estándares y regulaciones, proporcionan una guía de mejores prácticas y recomendaciones, para el desarrollo de acciones que permitan a las empresas la implementación de un ambiente de control adecuado para la protección de su información.

1. Introducción a la importancia de la destrucción y el borrado seguro de la información

1.1. Importancia y beneficios de la destrucción y el borrado seguro de los datos personales en el marco de la Ley y el Reglamento

La facilidad de réplica que permite hoy en día la tecnología digital, la alta dependencia de las empresas en las TIs el aumento de ataques cibernéticos, entre otras cosas, han aumento la necesidad por parte de los responsables de la información, de destruir y/o eliminar la información, cuando esta ya no es requerida, no hacerlo puede dar lugar a violaciones sobre la protección de los datos personales y políticas de privacidad, problemas de cumplimiento y costos adicionales...

Durante el primer semestre del 2014 se reportaron 1,331 incidentes de seguridad lo cual expuso 502 millones de registros.

Es importante desde un enfoque de seguridad, que cuando la información cumpla con su finalidad sea destruida o borrada adecuadamente para así evitar que se encuentre expuesta a riesgos tanto internos como externos. Por otro lado, la acelerada y constante generación de información hace que las empresas tengan la necesidad de destruirla o borrarla cuando ya no la requieren debido al costo, riesgo y complejidad que implica el almacenamiento, protección y gestión de esta.

Importancia de la destrucción y el borrado seguro de la información personal

La ausencia de procesos adecuados para la destrucción o borrado de información pudiera ocasionar alguna de las siguientes situaciones de riesgo:

- Violación al artículo constitucional 16, donde se establece como derecho de las personas, la protección de sus datos personales.
- Afectación a la esfera social y financiera a personas físicas por la divulgación de información personal.
- Equipos que ya no son requeridos y contienen información sensible del negocio o datos personales/sensibles sean donados, regalados o vendidos a terceros, por lo que se divulgue información. El 92.4% de la información que ha sido eliminada de dispositivos de almacenamiento como discos duros, cintas, o memorias es recuperable.
- Personas no autorizadas sean capaces de recuperar información personal o sensible poniendo en riesgo la integridad de los titulares de la información, así como la reputación del responsable de los datos.
- Se presente un incumplimiento de contratos por la publicación de información. Esto a su vez pudiera causar consecuencias legales, de reputación y económicas.

- Robo de identidad de usuarios, clientes, proveedores, socios y/o empleados utilizando información que no fue eliminada de forma segura. México ocupa el octavo lugar en robos de identidad, delito que genera más de $100 millones en fraudes así como complicaciones legales que pueden tomar de 3 a 4 años para solucionarse

- Daño a marca y reputación por divulgación de información personal. La divulgación de información está entre las primeras tres causas que afectan la reputación de las organizaciones.

- Que se realicen fraudes utilizando información personal que fue divulgada sin autorización del titular.

- Litigios relacionados con daños a personas físicas ocasionados por la divulgación de información.

- Pérdidas financieras. En muchos casos las empresas enfrentan una disminución en los ingresos, así como la caída del valor de sus acciones

- Pérdida de valor de mercado por la falta de confianza en el responsable de los datos.

- Convertirse en el “ejemplo” de lo que puede salir mal.

- Ser víctima de espionaje industrial lo cual afecta a 35% de las empresas en México, con efectos directos a las utilidades y competitividad de los negocios.

- No estar en cumplimiento con regulaciones relacionadas con la protección de datos personales como la Ley Federal de Protección de Datos Personales en Posesión de los Particulares y su respectivo reglamento, lo que pudiera ocasionar sanciones económicas para el responsable de la información.

- Se incurra en gastos adicionales para los responsables de la información, ya que implica que deban contar con medidas de seguridad implementadas para proteger información que ya no es necesaria.

- La pérdida de clientes, proveedores u oportunidades de negocio derivado de la falta de confianza. Muchas personas afectadas por incidentes de seguridad, se quedan con la percepción de que su identidad está en riesgo.

- En general, cualquier afectación a los principios de seguridad de la información: integridad, confidencialidad y disponibilidad.

Según la onceava edición de la Encuesta Global de Seguridad de la Información realizada por EY, el 85% de los encuestados a escala global consideran que los daños a la reputación y la marca como resultado de incidentes de seguridad de la información, son los más significativos. El 77% coincidió en la preocupación por perder la confianza de los stakeholders, al 72% le preocupó la pérdida de ingresos y al 71% la pérdida de clientes.

Ilustración 7. Consecuencias de incidentes de seguridad de información.

Asimismo, un estudio de la fundación DataLossDB[2] muestra el tipo de información que se vio comprometida por incidentes de seguridad que ocurrieron durante la primera mitad del 2014. En este se puede observar que la mayoría de los registros afectados son datos personales.

Ilustración 8. Tipo de información afectada por incidentes de seguridad.

[2] https://www.riskbasedsecurity.com/reports/2014-MidYearDataBreachQuickView.pdf

Según una encuesta realizada por Microsoft, el 45% de las personas sienten que tienen poco o ningún control sobre la información personal que las organizaciones recaban sobre ellos[3].

Para evitar que se materialicen situaciones de riesgo por no borrar información electrónica de forma adecuada, se deben aplicar medidas de sanitización.

La sanitización es un elemento clave para buscar la confidencialidad de la información, en este proceso se busca proteger la información por medio de su eliminación o inclusive la destrucción de los dispositivos que ya no se requieren, donde se trataban datos personales. Existen distintas formas para aplicar el proceso de sanitización lo cual dependerá de la sensibilidad de la información que se encuentra almacenada en el dispositivo. Asimismo se recomienda implementar monitoreos periódicos para verificar que se está realizando una adecuada sanitización y destrucción de los medios de almacenamiento, así como aplicar pruebas sobre los procedimientos involucrados en la destrucción y borrado de información, con el objetivo de identificar áreas de oportunidad y posibles soluciones, buscando así una mejora continua en los procesos.

Beneficios de la destrucción y el borrado seguro de la información personal

La destrucción y el borrado seguro de la información puede considerarse un tema complejo, sin embargo contar con este tipo de medidas puede aportar beneficios significativos para las organizaciones como lo son:

- Destruir información que no se requiere, reduce el riesgo de que se presenten situaciones que expongan la integridad, confidencialidad y disponibilidad de la información.
- Reducción de espacios destinados al almacenamiento de información.
- Reducción de costos de almacenaje.

Con el objetivo de evitar las consecuencias por no borrar información y aprovechar los beneficios que esto implica, es importante establecer políticas y procedimientos adecuados para la destrucción y el borrado de la información cuando esta ya no se requiera.

[3] Data Privacy Day Privacy Survey 2013. Microsoft Corp.

1.2. Causas de la pérdida de información en soportes físicos y electrónicos

La pérdida de información se origina cuando se altera alguno de sus atributos, ya sea la integridad, disponibilidad y/o confidencialidad. Se conoce como pérdida definitiva de información cuando no se consigue el acceso a la misma o esta ha desaparecido.

El 97% de los casos en los que se pierde información, son ocasionados por alguna de las siguientes razones [4]:

- Fallas en el software.
- Fallas en el hardware.
- Errores humanos, por ejemplo que eliminen, formateen o sobre escriban archivos.
- Virus y código malicioso que infecte los medios de almacenamiento o dispositivos donde se trata la información.
- Desastres naturales que afecten las instalaciones donde se almacenan los equipos en los que se encuentra la información.

Otras situaciones que pudieran ocasionar la pérdida de información son:

- Configuración inadecuada de infraestructura que permite a personas no autorizadas materializar un ataque a algún componente donde se almacene información.
- Falta de un plan de respuesta a ataques cibernéticos lo cual implique que la organización no sepa cómo reaccionar.
- Falta de monitoreo del acceso y uso de los sistemas donde se tratan datos personales.
- Fallas en la lista de archivos de los dispositivos donde se almacena información.
- Fallos mecánicos en medios de almacenamiento que los vuelvan inservibles.
- Falta de controles criptográficos que protejan la información.
- Falta de un adecuado control de accesos físicos y electrónicos.

[4] http://www.krollontrack.co.uk/resource-library/newsletter-centre/ontrack-data-recovery-newsletter/understanding-data-loss/

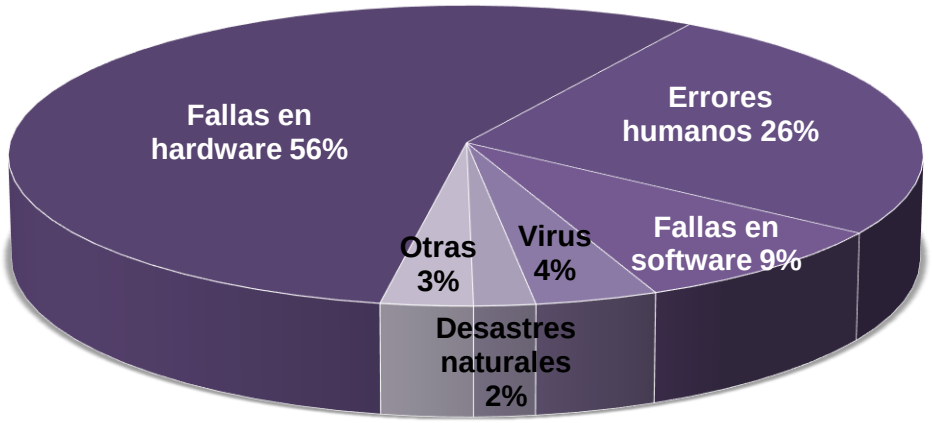


Ilustración 9. Causas de la pérdida de información.

Estas situaciones pudieran mitigarse por medio de la implementación de procedimientos en los que se defina como responder ante situaciones que pudieran ocasionar la pérdida de información, así como buenas prácticas para el uso de los dispositivos donde se almacena.

Actualmente existen distintas opciones de servicios tecnológicos que permiten transferir o compartir con terceros el riesgo asociado con la pérdida de información. De esta forma, las organizaciones pueden outsorcear procesos o actividades a proveedores especializados, mitigando así la materialización de algunos riesgos.

Uno de estos servicios es el cómputo en la nube o cloud computing. Este modelo permite que toda la información de una organización se almacene de forma permanente en servidores en internet que atienden peticiones en todo momento. De esta forma se puede tener acceso a la información por medio de una conexión a internet desde cualquier dispositivo sin importar la ubicación. La nube proporciona mayor capacidad de adaptación y recuperación completa de pérdida de datos, ya que periódicamente se realizan copias de seguridad.

Otra opción consiste en la contratación de servicios de almacenamiento a proveedores especializados en centros de cómputo con el objetivo de resguardar los servidores de la organización en una instalación que cuenta con medidas de seguridad adecuadas para proteger la seguridad de los equipos.

Cualquier medida seleccionada, deberá ser evaluada a través de un análisis de riesgo minucioso con el objetivo de garantizar que la opción implementada sea adecuada con respecto a las necesidades de la organización.

1.3. Métodos y técnicas de recuperación de información en soportes físicos y electrónicos

Con el objetivo de garantizar la disponibilidad de la información es necesario que esta se encuentre accesible y pueda ser utilizada por las personas autorizadas cuando la requieran. Es por esto que las empresas deben contemplar dentro de sus medidas de protección, procesos y actividades que permitan su recuperación.

Recuperación de información en soportes electrónicos

La recuperación de información electrónica es el proceso que se realiza para restablecer el acceso a la información que todavía se encuentra almacenada en algún dispositivo o medio electrónico, aun cuando esta ya no se encuentra disponible. Existen dos métodos de recuperación de este tipo de información:

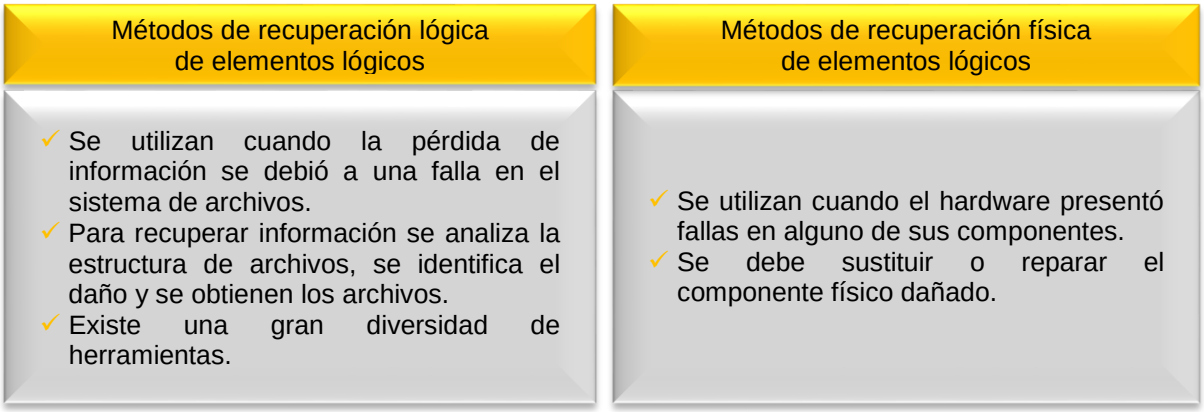


Ilustración 10. Métodos de recuperación de información en soportes electrónicos.

Otra medida que nos permitirá recuperar información electrónica de forma rápida y sencilla en el caso de que se presente una falla en un sistema que ocasione daños o pérdida de los datos, consiste en la generación de respaldos periódicos. Esto ayudaría a evitar poner en peligro la continuidad del negocio. Las organizaciones deben desarrollar e implementar una política de copias de seguridad, así como un plan de contingencia que incluya la planificación de estos respaldos.

Asimismo, existe una disciplina denominada informática forense, cómputo forense o análisis forense cuyo objetivo consiste en recuperar información previamente eliminada o aquella contenida en dispositivos que presentaron fallas, así como reconstruir de forma confiable, el uso y sobre todo, las actividades que se llevaron a cabo en dispositivos electrónicos de almacenamiento masivo como computadoras de escritorio, portátiles, servidores de datos y correo, smartphones, discos duros externos y memorias portátiles.

Esta disciplina busca examinar y recuperar datos que se intentaron eliminar de algún equipo. La recuperación de información depende del uso que se le dio al equipo, así como el proceso que se haya seguido para eliminarla. Por medio del cómputo forense podemos realizar actividades como las siguientes:

- Recuperar datos borrados de la papelera de reciclaje, o discos formateados.
- Recuperar correos enviados y recibidos (incluso eliminados).
- Obtener información de actividades de los navegadores web (Internet Explorer, Firefox).
- Identificar documentos impresos y archivos abiertos recientemente.
- Visualizar el histórico de dispositivos USB conectados.
- Acceder a conversaciones de mensajeros instantáneos.
- Acceder a respaldos de información de celulares.
- Acceder a archivos con contraseña y/o información restringida.
- Visualizar usuarios que accedían y utilizaban el equipo.
- Acceder a archivos temporales de internet (estados de cuenta bancarios).
- Rastrear mails internos.
- Recuperar fotografías y videos almacenados en toda la computadora.
- Identificar contraseñas almacenadas en el registro de Windows.
- Obtener acceso a archivos encriptados.

Recuperación de información en soportes físicos

Por otra parte, la recuperación de información física, se puede hacer por medio del siguiente método:

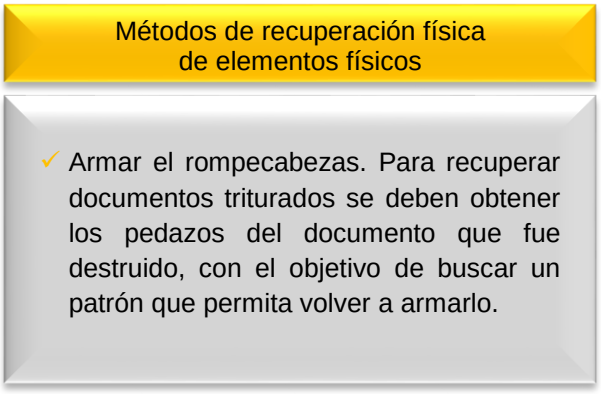


Ilustración 11. Métodos de recuperación de información en soportes físicos.

Recuperar información que se encuentra en soportes físicos, resulta un poco más complicado, el éxito de esto depende del estado en el que se encuentre el documento. Algunas situaciones en las que se pueden recuperar documentos físicos son las siguientes:

Situación	Estado del documento	Método de recuperación
Documentos quemados	Los documentos conservan condiciones favorables para su estudio	Uso de químicos o aparatos fotoscópicos
Documentos triturados	Se recuperaron los pedazos triturados y estos no son tan pequeños	Re armar el documento
Documentos tirados a la basura	Arrugados, sucios	Buscar el documento
Documentos enviados a reciclaje	En buen estado	Buscar el documento

Tabla 1. Métodos de recuperación de información.

Por lo anterior, es importante implementar controles adecuados en las ubicaciones donde se resguardan documentos físicos, así como procedimientos para digitalizar la información sensible que requiere la organización con el objetivo de evitar su pérdida.

1.4. Consecuencias legales, económicas y de imagen debido a una vulneración a la seguridad de los datos personales por una mala práctica de destrucción y/o borrado de información

Una de las preocupaciones actuales de las organizaciones consiste en como desechar correctamente equipos que ya no se requieren. Se calcula que existen más de 150 millones de computadoras obsoletas que se encuentran en desuso, así como 80,0000 teléfonos inteligentes (smartphones) usados disponibles diariamente en sitios de venta en línea. Estos equipos representan una amenaza tanto para el medio ambiente, como para las organizaciones ya que pudieran llegar a contener información sensible o datos personales que pudieran ser utilizados de forma inadecuada.

Debido a los avances tecnológicos actuales que facilitan la generación, la réplica y la publicación de información, las consecuencias por una vulneración a la seguridad de los datos pueden llegar a tener un alcance global.

Una mala práctica de destrucción y/o borrado de información personal representa una amenaza significativa de robo de identidad lo cual pudiera poner en riesgo la privacidad, seguridad financiera u otros intereses del titular. El robo de identidad consiste en que un tercero no autorizado utilice información personal de alguien más para realizar actividades fraudulentas. El aumento de este tipo de delitos ha ocasionado consecuencias legales, económicas y de imagen a responsables que no implementaron medidas de seguridad suficientes para proteger la información en su poder.

El promedio de registros expuestos por incidentes relacionadas con una inadecuada eliminación de información es de 1,283.

Solo en los primeros 6 meses del 2014, se reportaron 589 incidentes de seguridad lo cual expuso más de 76 millones de registros. En este mismo periodo, se presentaron 16 incidentes relacionados con una mala destrucción o borrado de información, lo cual ocasionó que se viera afectada la confidencialidad de 20,534 registros.

Asimismo, la empresa Antivirus Firm Avast[5] recuperó 40,000 registros personales de 20 teléfonos inteligentes usados que compró en línea, los cuales supuestamente habían sido formateados antes de ser vendidos. Entre la información recuperada se identificaron fotos, correos electrónicos, mensajes de texto, búsquedas de Google, nombres y correos de contactos, e incluso en algunos casos se identificó al dueño del dispositivo.

Otras afectaciones importantes, han sido los robos masivos de información por parte de hackers a empresas multinacionales. Algunos de los casos más relevantes son los siguientes[6]:

- En el 2007 se obtuvo acceso al sistema de TJX donde se almacenaba información de tarjetas de crédito, débito, cheques y transacciones, afectando a 94 millones de clientes. Algunas de las consecuencias enfrentadas por la compañía fueron las siguientes:

[5] http://praguepost.com/technology/40082-czech-company-finds-naked-selfies-on-used-smartphones
[6] http://www.idtheftcenter.org/

- La compañía se comprometió a financiar hasta $40,900,000 para pagos de recuperación.
- Enfrentamiento de demandas presentadas por 7 bancos.
- Enfrentamiento de demandas presentadas por clientes
- La compañía reportó costos de aproximadamente $256 millones de dólares utilizados para enfrentar el incidente.
- Afectaciones a los clientes ya que muchas tarjetas bancarias fueron utilizadas para realizar fraudes.
- Disminución de las ventas

- En el 2011 Sony sufrió un ataque en el que se robaron información de cuentas de usuario de 77 millones de personas. Algunas de las consecuencias que sufrió la compañía fueron las siguientes:
  - La compañía se vio involucrada en varias demandas y sanciones.
  - Pago de aproximadamente $15 millones de dólares en producto a los clientes afectados.
  - La compañía reportó costos de aproximadamente $171 millones de dólares asociados con el incidente.
  - Enfrentamiento a 65 demandas
  - Reembolsos hasta por $2,500 a clientes que pudieran demostrar fraudes realizados como resultado del incidente de seguridad.
  - Costos por ofrecer a sus clientes afectados un año de protección contra robo de identidad, inmediatamente después de la violación.
  - La compañía se volvió un ejemplo sobre que pudiera salir mal.

- En el 2011, Betfair una compañía de un sitio de apuestas por internet, fue víctima de un ataque, lo cual expuso información de tarjetas de crédito y débito de aproximadamente 2,300,000 clientes. Algunas de las consecuencias que sufrió la compañía fueron las siguientes:
  - La compañía dañó su imagen ya que tardó 18 meses en reportar el incidente, esto ocasionó que se hiciera muy mala publicidad por esconder el robo de información.
  - La compañía despidió a la mayoría de los empleados trabajando en el área de seguridad.
  - La pérdida de la confianza de sus clientes, ya que anteriormente, la compañía había publicado un artículo sobre su compromiso con los clientes en el cual incluía temas relacionados con la seguridad de su plataforma tecnológica y de los datos personales almacenados en esta.
  - La compañía tuvo que invertir en robustecer la seguridad de su plataforma tecnológica.

- En el 2013 un ataque a una de las cadenas de retail más grandes de Estados Unidos, Target, causó el robo de información de tarjetas de crédito y débito de aproximadamente 56 millones de clientes. Algunas de las consecuencias que sufrió la compañía fueron las siguientes:
  - Las utilidades de la compañía cayeron un 46% en comparación al mismo periodo de un año anterior.
  - La compañía decidió invertir $100 millones de dólares para implementar tecnología más segura.

- Se estima que entre 1 y 3 millones de las tarjetas robadas fueron vendidas en el mercado negro y utilizadas para realizar fraudes, lo cual afectó a los titulares de las tarjetas.
- Costos por ofrecer a sus clientes un año de monitoreo y protección contra robo de identidad.
- Disminución en la inscripción de clientes para obtener la tarjeta de crédito que ofrece la tienda.
- El precio de las acciones de la compañía cayó un 14% los dos meses posteriores al ataque.
- La compañía reportó costos de más de $146 millones de dólares asociados con el incidente.
- El incidente no se manejó adecuadamente, lo cual generó mucha mala prensa para la compañía.

- En el 2014 Home Depot se vio involucrada en un robo de registros de tarjetas de crédito y débito de más de 40 millones de clientes. Algunas de las consecuencias que sufrió la compañía fueron las siguientes:
  - El precio de las acciones de la compañía cayó un 2%.
  - Algunos de los clientes afectados, fueron víctima de fraudes realizados con la información robada de sus tarjetas de crédito.
  - Costos incurridos por el reemplazo de las tarjetas de los titulares afectadas
  - Se estima que los costos para la investigación, el servicio de monitoreo de crédito y el centro de atención telefónica ascenderán los $62 millones de dólares.

- En el 2014 Viator, compañía de turismo, sufrió un robo de información de tarjetas de crédito afectando a 880,000 clientes. Algunas tarjetas fueron utilizadas para realizar fraudes dañando así la seguridad financiera de los titulares. A continuación se mencionan algunas consecuencias enfrentadas por la compañía:
  - El precio de las acciones de la compañía cayó un 4%.
  - Algunos de los clientes afectados, fueron víctima de fraudes realizados con la información robada de sus tarjetas de crédito.
  - Costos por ofrecer a sus clientes un año de membresía en servicios para proteger su ID.
  - Costos asociados con la contratación de servicios forenses para realizar la investigación.

A continuación se muestra un resumen de algunos de los ataques más relevantes por volumen de titulares afectados, incluyendo los mencionados anteriormente.

Compañía	Información comprometida	Titulares afectados	Consecuencia
TJX	Números de seguro social, licencias de manejo, tarjetas de crédito y débito, cheques y transacciones de clientes	94 millones de clientes	Daño de imagen Demandas Costos asociados con el incidente Afectación económica a clientes Disminución de las ventas
Sony	Información de cuentas de clientes	77 millones de clientes	Daño de imagen Demandas Costos asociados con el incidente Disminución de las ventas
Betfair	Tarjetas de crédito y débito de clientes	2.3 millones de clientes	Daño de imagen Despidos de personal Pérdida de confianza por promesas no cumplidas Costos asociados con el incidente
Target	Tarjetas de crédito y débito de clientes	56 millones de clientes	Daño de imagen Caída del valor de las utilidades Costos asociados con el incidente Afectación económica a clientes Caída del valor de las acciones Mala publicidad
Home Depot	PIN de tarjetas de débito	40 millones de clientes	Daño de imagen Caída del valor de las acciones Afectación económica a clientes Costos asociados con el incidente
Viator	Correo electrónico, datos de tarjeta de crédito, credenciales de acceso al sitio de la compañía.	880,000 clientes	Daño de imagen Caída del valor de las acciones Afectación económica a clientes Costos asociados con el incidente
JPMorgan Chase - U.S.	Nombres, direcciones, teléfonos	1 millón de clientes	Daño de imagen Costos asociados con el incidente Mala publicidad por no informar sobre el incidente en el momento en el que ocurrió
Community Health Systems / Tennova	Nombres, direcciones, fechas de nacimiento, teléfonos, números de seguro social	4.5 millones de pacientes	Daño de imagen Costos asociados con el incidente Caída del calor de las acciones Demandas Violación al “Health Insurance Portability and Accountability Act (HIPAA)”
Department of Public Health and Human Services	Nombres, direcciones, fechas de nacimiento, números de seguro social, información clínica	1,062,509 de pacientes	Daño de imagen Costos asociados con el incidente Demandas Violación al “HIPAA”
Michaels Stores	Información de tarjetas de crédito	2,600,000 de clientes	Daño de imagen Costos asociados con el incidente Demandas

Tabla 2. Ataques que han expuesto información personal.

Del 2005 a Octubre del 2014 se han identificado 4,854 incidentes de seguridad, lo cual ha afectado un total de 669,680,671 registros[7]. En el Anexo B se muestra el resumen de los incidentes ocurridos por categoría.

Con el objetivo de evitar que este tipo de situaciones se sigan presentando, la Ley Federal de Protección de Datos Personales en Posesión de los Particulares establece en su capítulo X, las conductas por las que se aplicarán sanciones, así como los montos de estas que pudieran llegar a ser desde $6,000 hasta $80'000,000 MN.

De igual forma, un mal uso de datos personales pudiera ocasionar a las empresas demandas civiles por afectaciones a titulares, consecuencias legales por incumplimiento de acuerdos o contratos con terceros, pérdida de clientes, proveedores e incluso empleados, disminución de ventas, afectación de la imagen de la organización, entre otras.

[7] http://www.idtheftcenter.org/images/breach/ITRCBreachStatsReportSummary_2005-2014.pdf

2. Almacenamiento de los datos personales; procedimiento que permita identificar el medio y la forma en que se almacenan datos personales

2.1. Flujo de los datos personales; procedimiento para identificar cómo se obtienen y hacia dónde van los datos personales dentro de la organización durante el ciclo de vida y tratamiento de los mismos.

Es necesario implementar medidas de seguridad para proteger los datos personales durante todo su ciclo de vida, desde que se obtienen hasta que se destruyen. Para poder realizar esto se requiere identificar todas las áreas y actividades de la organización en las que se están tratando datos personales, así como las finalidades del tratamiento, quién es el responsable de los datos, entre otras cosas.

En la Ilustración 12. Tratamiento de datos personales.se muestra de forma gráfica que el tratamiento de datos personales consiste en todas aquellas actividades relacionadas con la obtención, el uso, la divulgación, el almacenamiento, bloqueo y la cancelación o supresión de datos personales. El uso abarca cualquier acción de acceso, manejo, aprovechamiento o disposición de datos personales.

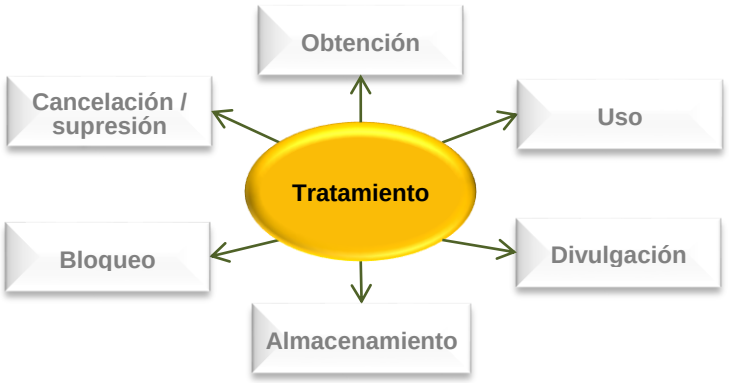


Ilustración 12. Tratamiento de datos personales.

Para identificar donde se está realizando algún tratamiento de datos personales de clientes, empleados o proveedores se deben realizar entrevistas a todos los responsables de las áreas donde se identifique algún uso de datos personales, tomando en cuenta al menos lo siguiente:

Tratamiento de datos personales					
Obtención	**Uso**	**Divulgación**	**Almacenamiento**	**Bloqueo**	**Cancelación / supresión**
• ¿Qué datos personales se recopilan? • ¿Qué tipo de datos personales se recopilan? • ¿Por qué medios se obtienen? • ¿Para qué finalidad se requieren? • ¿Quién es el responsable? • ¿Quién es el encargado? • ¿Quién maneja datos personales? • ¿Se muestra un aviso de privacidad? • ¿Se obtiene consentimiento del titular? • ¿Cómo se protege?	• ¿Quién tiene acceso a los datos personales? • ¿Para qué requieren acceso? • ¿Cómo se protege?	• ¿Se transfieren datos personales a internos o externos? • ¿Para qué se requiere transferir datos personales? • ¿Cómo se realizan las transferencias de datos personales? • ¿Se almacenan datos personales en tecnologías de cómputo en la nube? • ¿Se publican datos personales en sitios web? • ¿Se comparten datos personales en redes sociales? • ¿Se comparten datos personales por medio de carpetas compartidas? • ¿Cómo se protege?	• ¿En qué medios se almacena la información personal? • ¿Cómo se protege?	• ¿Cómo se realiza el bloquea de la información? • ¿Por cuánto tiempo se resguarda la información? • ¿Cómo se protege?	• ¿Cómo se identifica la información personal que requiere ser destruida o borrada? • ¿Cómo se destruye o borra la información personal? • ¿Cómo se valida la destrucción o borrado de los datos personales? • ¿Quién es el responsable de la destrucción o borrado? • ¿Cómo se protege?

Ilustración 13. Entendimiento de cómo se realiza el tratamiento.

A continuación, se muestra en mayor detalle los puntos señalados en la **¡Error! No se encuentra el origen de la referencia.**, con el objetivo de tener más claridad sobre la información que se debe obtener durante las entrevistas para poder tener una visión de la situación actual de la organización:

1. Obtención de datos personales

Con respecto a la obtención de datos personales, se requiere comprender todas las actividades involucradas en los procesos en los que se obtiene información personal. Esto implica indagar de forma exhaustiva lo siguiente:

- ¿Qué datos personales se recopilan? Se requiere entender qué datos personales se están obteniendo de cada figura (clientes, empleados o proveedores). Para esto se deben solicitar los formatos tanto físicos como electrónicos, utilizados los cuales deberán ser analizados con el objetivo de validar que la información se está obteniendo de forma lícita y que solo se están solicitando datos que se requieran.

- ¿Qué tipo de datos personales se recopilan? Se debe analizar a que categoría corresponden los datos personales obtenidos con el fin de identificar si se utilizan datos personales sensibles o patrimoniales. En caso de ser así, esta información debe de ser protegida con medidas de seguridad más robustas.

- ¿Por qué medios se obtienen? Se deben identificar los medios por los que se están obteniendo datos personales ya sean físicos o lógicos. Algunos ejemplos son: por página web, correo electrónico, teléfono, de forma física en un mostrador, entre otros. Una vez que se identifican todos los medios se requiere comprender el flujo que sique la

información posteriormente, es decir si se almacena en alguna aplicación o archivero, si se transfiere a algún interno o externo, si se copia, etc.

- ¿Para qué finalidad se requiere? El siguiente paso consiste en indagar sobre las finalidades para las que se obtienen los datos personales. Para esto se debe investigar con el responsable del proceso sobre la utilidad de la información y el objetivo de esta. En caso de identificar datos personales que se están recabando más sin embargo no se requieren, se deben implementar medidas para dejar de obtener esa información.

- ¿Quién es el responsable? Se debe identificar quién es la persona física o moral de carácter privado que decide sobre el tratamiento de los datos personales recabados. Asimismo, se recomienda identificar los roles que correspondan al responsable y al resto de los involucrados en el ciclo de vida de estos.

- ¿Quién es el encargado? Se debe identificar a la persona física o jurídica que sola o conjuntamente con otras, trata datos personales por cuenta del responsable. Esto implica entender qué proveedores se encuentran relacionados con el tratamiento de los datos, las finalidades de su relación con la organización, así como contar con procedimientos para validar que el encargado esté en cumplimiento tanto con regulaciones aplicables como con el aviso de privacidad del responsable de los datos.

- ¿Quién maneja datos personales? También se debe tomar en cuenta que es importante identificar al resto de los usuarios que están manejando datos personales, así como las actividades que realizan con estos.

- ¿Se muestra un aviso de privacidad? Es importante validar si el responsable de los datos muestra un aviso de privacidad antes de obtener datos personales directamente del titular. En caso de obtenerlos de forma indirecta, se debe validar que el aviso se muestre en el primer contacto con el cliente, o antes de realizar el tratamiento de los datos.

- ¿Se obtiene consentimiento del titular? Se debe verificar si se está obteniendo algún consentimiento por parte del titular. En caso de solicitar datos personales sensibles o patrimoniales es de suma importancia validar que se esté solicitando un consentimiento expreso previo a la obtención de la información.

- ¿Cómo se protege la información durante su obtención? Se debe investigar si existen controles implementados en las actividades en las que se realiza alguna obtención de información personal.

2. Uso

Para entender todas las actividades relacionadas con el uso de datos personales, se debe indagar en lo siguiente:

- ¿Quién tiene acceso a los datos personales? Durante las entrevistas se debe realizar un entendimiento y evaluación de los medios (ej. aplicaciones y archivos) que almacenan, procesan o transmiten datos personales con el objetivo de identificar las personas que tienen acceso a estos medios.

- ¿Para qué requieren acceso? Al identificar a las personas que tienen acceso a los datos personales, se debe analizar si estos efectivamente lo requieren para el desempeño de sus funciones. En caso de no ser así, se deben eliminar estos accesos.

- ¿Cómo se protege? Se deben identificarlos controles existentes para la protección de los datos personales almacenados.

3. Divulgación

Para entender todas las actividades que se realizan actualmente relacionadas con la divulgación de datos personales, se debe indagar lo siguiente:

- ¿Se transfieren datos personales a internos o externos? Es importante identificar si se transfieren datos personales ya sea a otras áreas internas, a organizaciones que forman parte del grupo o a alguna figura externa.

- ¿Para qué se requiere transferir datos personales? En caso de identificar que si se realizan transferencias de datos personales, se deben evaluar las finalidades para las que se requieren

- ¿Cómo se realizan las transferencias de datos personales? También es importante identificar y evaluar la seguridad de los medios por los que se está realizando la transferencia de información (ej. De forma física, correo electrónico, por dispositivos de almacenamiento externo, memorias, etc.). Se debe analizar si una vez que la información se transfiere es eliminada del dispositivo utilizado para la trasferencia, y si se cuenta con controles adecuados para proteger la información.

- ¿Se almacenan datos personales en tecnologías de cómputo en la nube? Se requiere indagar en el uso de tecnologías de cómputo en la nube, ya que en caso de utilizarlas se debe revisar la existencia de acuerdos o instrumentos legales con los proveedores del servicio en los que se garantice la protección de la información personal.

- ¿Se publican datos personales en sitios web? Se debe investigar si se publican datos personales en páginas web ya sea internas o externas, en caso de ser así se debe averiguar qué tipo de datos se están publicando y con qué finalidad.

- ¿Se comparten datos personales en redes sociales? Se debe investigar si se publican datos personales en redes sociales, en caso de ser así se debe averiguar qué tipo de datos se están publicando y con qué finalidad.

- ¿Se comparten datos personales por medio de carpetas compartidas? Es importante investigar si se utilizan carpetas compartidas y si los permisos de estas se encuentran correctamente asignados. Se debe validar que solo las personas permitidas tienen acceso a la información y que no se cuenta con información personal que no deba ser publicada en estas carpetas.

- ¿Cómo se protege? Se deben identificar los controles existentes para la protección de los datos personales durante su uso.

4. Almacenamiento

Sobre el almacenamiento de la información, se requiere obtener un entendimiento detallado de lo siguiente:

- ¿En qué medios se almacena la información personal? Se deben identificar todos los medios ya sean físicos o electrónicos (ej. aplicaciones, sistemas, archiveros) donde se almacenan datos personales. Se recomienda contar con un inventario de estos medios para tener visibilidad de donde se encuentra almacenada toda la información utilizada por la organización.

- ¿Cómo se protege? Se deben identificar los controles existentes para la protección de los datos personales almacenados.

5. Bloqueo

Sobre el bloqueo de la información, se requiere obtener un entendimiento detallado de lo siguiente:

- ¿Cómo se realiza el bloquea de la información? Se debe identificar si se están realizando actividades para realizar el bloqueo de información, con el objetivo de evaluar si estas son adecuados.

- ¿Por cuánto tiempo se resguarda la información? Otro aspecto importante es identificar el tiempo de retención de los datos personales en cada proceso en el que son utilizados con el objetivo de evaluar si este es adecuado. La definición del tiempo de retención, se debe realizar tomando en cuenta la finalidad para la que se utilizan los datos personales, así como las regulaciones aplicables.

- ¿Cómo se protege? Se deben identificar los controles existentes para la protección de los datos personales durante su bloqueo.

6. Cancelación / supresión

Sobre la cancelación / supresión de la información, se requiere obtener un entendimiento detallado de lo siguiente:

- ¿Cómo se identifica la información personal que requiere ser destruida o borrada? Se debe entender el proceso ejecutado para identificar la información que ya cumplió su tiempo de retención y por lo tanto debe ser destruida o borrada.

- ¿Cómo se destruye o borra la información personal? Se deben identificar los mecanismos existentes para la destrucción y/o el borrado de información, así como la forma de aplicarlos y llevar un control.

- ¿Cómo se valida la destrucción o borrado de los datos personales? Es importante evaluar la forma en que se valida que se está destruyendo y borrando la información, especialmente si el medio de almacenamiento se utilizará nuevamente.

- ¿Quién es el responsable de la destrucción o borrado? Se debe identificar la persona responsable en cada caso, da la destrucción y el borrado de la información.

- ¿Cómo se protege? Se deben identificarlos controles existentes para la protección de los datos personales durante su cancelación o supresión.

A continuación se plantea un **caso práctico** para explicar cómo se pueden identificar los datos personales tratados en una organización, desde que se obtienen hasta que se eliminan. Este enfoque puede ser aplicado por pequeñas, medianas y grandes empresas, así como por organizaciones o personas morales con actividad empresarial.

- Inicio de caso práctico -

El Ingeniero Díaz, dueño de una empresa pequeña de manufactura de pinturas llamada PintaConColor, al tener conocimiento sobre la implementación de la LFPDPPP, decide realizar un análisis sobre la información que están solicitando a sus clientes, empleados y proveedores; así como las actividades en las que se está realizando algún tratamiento de éstos. Para esto, el señor Díaz solicitó al nuevo practicante, Ernesto Leal, investigue sobre toda la información personal que se está utilizando, el manejo que se le está dando y las finalidades para las que se requiere. Ernesto, preocupado por su nueva asignación, decide comenzar desde lo más general para obtener una mayor visión de las actividades de la empresa.

Inicialmente, Ernesto solicita un organigrama de la empresa para poder tener la visión y entendimiento de su estructura, el diagrama se muestra en la **¡Error! No se encuentra el origen de la referencia.**Ilustración 14.

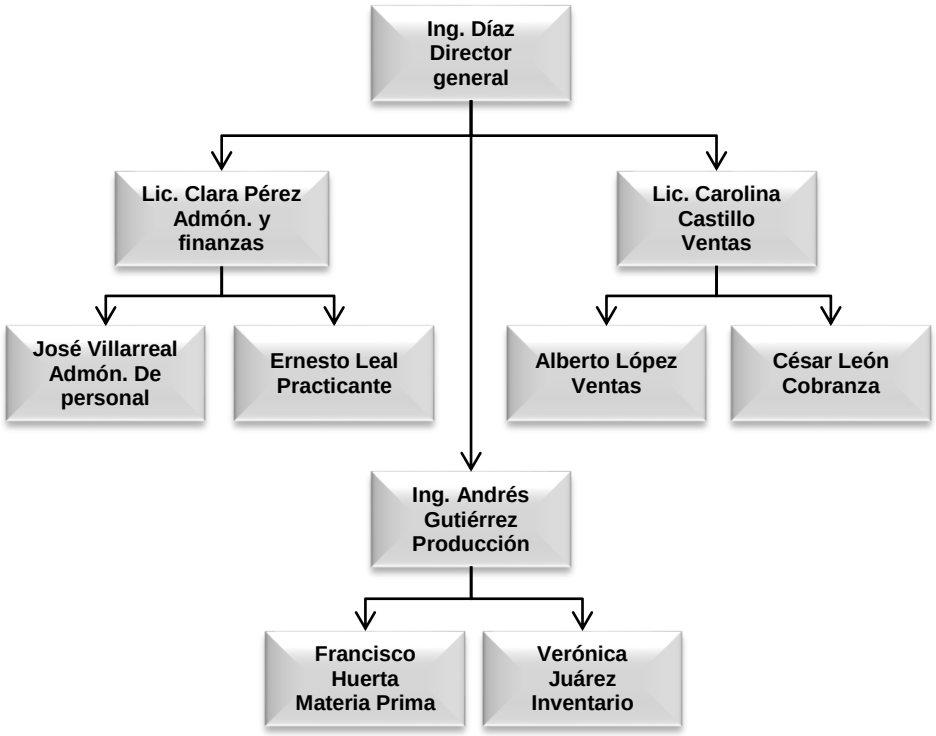


Ilustración 14. Organigrama de empresa

Con este diagrama Ernesto realizó un análisis de los departamentos que conforman PintaConColor, con el objetivo de identificar aquéllos en las que se pudieran estar tratando datos personales ya sea de clientes, empleados o proveedores (persona física). A partir de este análisis, Ernesto generó un listado con las áreas

Sr. Díaz – Director Gral. - NO MANEJA INFO. PERSONAL

Administración y finanzas
- Clara Pérez – Pago de nómina – INFORMACIÓN DE EMPLEADOS
- José Villarreal – Reclutamiento y manejo de personal - INFORMACIÓN DE EMPLEADOS
- Ernesto Leal – Actividades administrativas – NO MANEJA INFO. PERSONAL

Ventas
- Carolina Castillo – Reportes de ventas – NO MANEJA INFO. PERSONAL
- Alberto López – Ventas - INFORMACIÓN DE CLIENTES
- César León – Cobranza – INFORMACIÓN DE CLIENTES

Producción
- Andrés Gutiérrez – Reportes de producción – NO MANEJA INFO. PERSONAL
- Francisco Huerta – Materia prima - INFORMACIÓN DE PROVEEDORES
- Verónica Juárez – Inventario – NO MANEJA INFO. PERSONAL

identificadas incluyendo a sus respectivos responsables con el objetivo de agendar entrevistas con estas personas. El listado se muestra en la Ilustración 15.

Ilustración 15. Listado con áreas donde se identificó tratamiento de datos personales.

Para facilitar la cooperación de todos, el Ingeniero Díaz convocó una reunión para informar a todo el personal sobre lo que se estaba realizando. En ésta se solicitó a todos atender la entrevista con Ernesto, así como entregar cualquier requisito de información que pudiera surgir.

Posteriormente, Ernesto generó un plan de trabajo donde definió toda la información que debía obtener de cada una de las personas a las que entrevistaría para comprender en mayor detalle la operación de los procesos de PintaConColor y así identificar aquellas actividades específicas en

las que existía algún tratamiento de datos personales. Ernesto sabía que debía entrevistar a la persona que fuera necesario sin importar el puesto que tuviera ya que era importante identificar a todos los actores involucrados en el tratamiento de los datos personales para entender su rol y responsabilidad.

A continuación Ernesto comenzó con las entrevistas programadas. Inicialmente entrevistó al Sr. Díaz, Director general, con quien validó que no se encuentra realizando ningún tratamiento de datos personales, por lo que prosiguió con la entrevista a José Villarreal, Administración de personal, toda la información obtenida durante la entrevista fue documentada en la siguiente minuta.

Entrevistado: José Villarreal, Reclutamiento y manejo de personal **Ubicación:** Sala de juntas
Tema: Tratamiento de datos personales **Fecha:** 12/12/12

Minuta de reunión

Obtención:

1. **¿Qué datos personales se recopilan?**
   Nombre, RFC, CURP, religión, domicilio y celular, referencias laborales, sueldo anterior
2. **¿Qué tipo de datos personales se recopilan?**
   General, patrimonial, sensible
3. **¿Por qué medios se obtienen?**
   Solicitud de empleo, entrevista
4. **¿Para qué finalidad se requieren?**
   Evaluar si el candidato es apto para el puesto
   La religión no se utiliza para nada
5. **¿Quién es el responsable?**
   Lic. Clara Pérez, Admón. y finanzas
6. **¿Quién es el encargado?**
   Proveedor Reclutando
7. **¿Quién maneja datos personales?**
   José Villarreal, Ernesto Leal
8. **¿Se muestra un aviso de privacidad?**
   No
9. **¿Se obtiene consentimiento del titular?**
   No
10. **¿Cómo se protege?**
    No se sabe

Uso:

11. **¿Quién tiene acceso a los datos personales?**
    Clara Pérez, José Villarreal, Ernesto Leal
12. **¿Para qué requieren acceso?**
    Clara: realizar el pago de nómina
    José: administración de personal
    Ernesto: no requiere acceso
13. **¿Cómo se protege?**
    No se sabe

Divulgación:

14. **¿Se transfieren datos personales a internos o externos?**
    Se transfiere información a empresa Reclutando
    No se cuenta con cláusulas en el contrato para la protección de datos personales
    No se entregó al proveedor el aviso de privacidad de PintaConColor ya que no se cuenta con uno
15. **¿Para qué se requiere transferir datos personales?**
    Validar información de candidato
16. **¿Cómo se realizan las transferencias de datos personales?**
    Por correo electrónico, sin cifrar (se incluye información de empleo anterior)
17. **¿Se almacenan datos personales en tecnologías de cómputo en la nube?**
    No
18. **¿Se publican datos personales en sitios web?**
    No
19. **¿Se comparten datos personales en redes sociales?**
    No
20. **¿Se comparten datos personales por medio de carpetas compartidas?**
    Si, se comparte el archivo para realizar el pago de nómina con Clara Pérez
    Se revisaron los permisos de la carpeta, se identificó que no están bien configurados, el resto del personal tiene acceso
21. **¿Cómo se protege?**

Almacenamiento:

22. **¿En qué medios se almacena la información personal?**
    Carpeta compartida, Excel en computadora de José, Aplicación para pago de nómina, archivero
23. **¿Cómo se protege?**

Credenciales de acceso
Se identificó que no se cuenta con parámetros de contraseña robustos

Bloqueo:

24. ¿Cómo se realiza el bloquea de la información?
No se realiza bloqueo

25. ¿Por cuánto tiempo se resguarda la información?
N/A

26. ¿Cómo se protege?
N/A

Cancelación / supresión:

27. ¿Cómo se identifica la información personal que requiere ser destruida o borrada?
No se elimina información

28. ¿Cómo se destruye o borra la información personal?
No se elimina información

29. ¿Cómo se valida la destrucción o borrado de los datos personales?
No se elimina información

30. ¿Quién es el responsable de la destrucción o borrado?
No se elimina información

31. ¿Cómo se protege?
No hay controles

A partir de esta entrevista, Ernesto identificó que existen algunas áreas de oportunidad relacionadas con el tratamiento que se está realizando sobre datos personales, algunos de estos son los siguientes:

- No se está mostrando un aviso de privacidad al obtener datos personales del titular.
- No se está obteniendo el consentimiento expreso del titular.
- Se está solicitando un dato sensible que no se requiere para ninguna finalidad.
- No se sabe si se están protegiendo los datos al momento de obtenerlos
- Se identificó que el practicante cuenta con acceso al archivero donde se almacenan los expedientes, sin embargo no lo requiere para el desempeño de sus funciones.
- No se sabe si se están protegiendo los datos al momento de usarlos
- No se cuenta con cláusulas en el contrato que se tiene con el proveedor con el que se comparten datos para la protección de datos personales
- No se entregó al proveedor el aviso de privacidad de PintaConColor ya que no se cuenta con uno
- Se comparte información de empleados sin cifrar
- Se identificó que los permisos de las carpetas compartidas donde se almacena información de empleados no son adecuados.
- Se identificó que no se cuenta con parámetros de contraseña robustos
- No se realiza bloqueo
- No se ha definido el tiempo de resguardo para la información almacenada en el registro de Excel que contiene la información de los empleados.

Ernesto repitió este ejercicio con el resto de las personas que requería entrevistar. En cada reunión aprovechó para elevar el nivel de conciencia del personal involucrado con el tratamiento de datos personales, haciendo énfasis en las consecuencias a las que ellos, PintaConColor o ambos, deberían atenerse en caso de que se presente una acción de incumplimiento con la Ley. Ernesto logró que todo el personal comprendiera sus responsabilidades y deberes relacionados con la protección de los datos personales.

Al finalizar las sesiones utilizó toda la información obtenida para generar un inventario de datos personales el cual serviría a la organización para tener una visión sobre la trazabilidad de los datos, las finalidades para las que se utilizan, el flujo de la información dentro de los procesos de la empresa, así como la identificación y documentación de los datos sensibles y patrimoniales que se recaban.

Asimismo, Ernesto generó un inventario de los sistemas de tratamiento el cual contenía todos los soportes físicos y electrónicos donde se identificó se estaba realizando algún tratamiento de datos personales.

Después de dos meses de trabajo, Ernesto entregó los resultados y documentos generados al Sr. Díaz, quien quedó muy satisfecho. El Sr. Díaz le comentó al practicante que ahora tendrían conocimiento sobre la trazabilidad del uso y movimiento de los datos lo cual les permitiría responder a los requerimientos de los titulares para ejercer sus derechos ARCO, responder a la autoridad en caso de requerirse, supervisar la seguridad y el mantenimiento de los sistemas de archivos y conocer las finalidades específicas para las que se están utilizando los datos.

Finalmente, el Sr. Díaz y Ernesto convocaron a una reunión de cierre con todo el personal de PintaConColor, en la que se comunicaron los resultados obtenidos y se mostraron los inventarios generados. En la reunión se puso mucho énfasis en la importancia de mantener estos documentos actualizados con el objetivo de garantizar que reflejan la situación actual de la empresa en todo momento.

Con la entrega de los documentos generados, Ernesto incluyó una lista de las actividades posteriores que debe realizarse para poder estar en cumplimiento con la Ley:

- Generar un aviso de privacidad y definir la obtención y resguardo del consentimiento del titular cuando sea necesario.
- Generar normatividad interna donde se establezcan los lineamientos para el tratamiento de datos personales.
- Definir e implementar medidas de seguridad técnicas, físicas y administrativas.

- Fin del caso práctico -

En el anexo C se incluyen unas fichas que pudieran utilizarse para obtener la información requerida para analizar la situación actual de la compañía.

2.2. Diferentes soportes de almacenamiento físico y electrónico donde se resguardan datos personales y sus características para la selección de la técnica de destrucción y/o borrado idónea.

La información de una organización puede almacenarse de forma física y/o electrónica, en distintos tipos de soportes los cuales deben contar con medidas de seguridad que garanticen su confidencialidad, disponibilidad e integridad durante el periodo de tiempo que sea necesario. Asimismo, estas medidas deben proteger la información frente al acceso, pérdida o destrucción no autorizado, robos y catástrofes y deben buscar la recuperación de la información de forma, eficiente y oportuna, hasta donde sea posible.

Los soportes físicos son aquellos en los que se guarda la información que se encuentra en papel y los electrónicos son los utilizados para almacenar la información digital.

La mayoría de la información utilizada actualmente por las organizaciones se encuentra en soportes electrónicos. Con los avances tecnológicos, el uso de información física ha ido reduciendo.

A continuación se proporciona información más detallada de ambos tipos de soporte.

1. **<u>Soportes de almacenamiento de información física.</u>**
   Existen distintos soportes de almacenamiento de documentos físicos:


Archiveros


Gavetas / cajones


Bodegas


Estantes


Oficinas


Carpetas

Ilustración 16. Repositorios de documentos físicos.

   a) **Archiveros.** Es muy común encontrar información personal en archiveros que no se encuentren protegidos con llaves y que por lo tanto cualquier persona con acceso a las instalaciones pueda obtener general, o incluso sensible y/o patrimonial.

b) Gavetas. El personal de las organizaciones resguarda información personal en sus gavetas, sin embargo no siempre son lo suficientemente cuidadosos como para proteger este soporte por medio del uso de llaves.

c) Bodegas. Muchas organizaciones utilizan bodegas para almacenar su archivo muerto. Es muy común encontrar en este tipo de repositorios, gran cantidad de información personal y sensible del negocio que no se requiere y que solo está ocupando espacio.

d) Estantes. Las organizaciones suelen almacenar expedientes y carpetas con información personal en estantes de oficinas, en muchas ocasiones esta información está disponible a toda persona que tenga acceso a las instalaciones.

e) Oficinas. Es común identificar información personal en oficinas, ya sea sobre los escritorios, en corchos, o en áreas de impresión. En muchas ocasiones las oficinas cuentan con áreas de impresión donde se utilizan hojas reciclables. Se recomienda prestar atención en el tipo de documentos que se mandan a reciclar con el objetivo de validar que no se utilicen hojas que puedan contener datos personales y/o sensibles ya que estos pudieran ser divulgados o expuestos a finalidades distintas a las establecidas en el aviso de privacidad del responsable.

f) Carpetas. Es común que las organizaciones resguarden sus documentos en carpetas, sin embargo estas no siempre son almacenadas en lugares seguros.

La principal característica de esta información consiste en que se encuentra en papel. Las técnicas de destrucción que se pueden utilizar están enfocadas a la destrucción de los documentos no al soporte de almacenamiento.

2. <u>Soportes de almacenamiento electrónico</u>

Existen distintos tipos de soportes de almacenamiento de información electrónica:

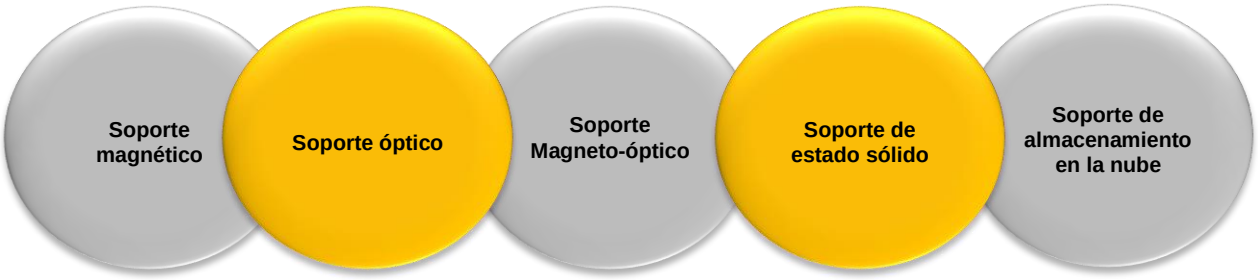


Ilustración 17. Repositorios de documentos digitales.

a) Soporte magnético. Estos dispositivos se basan en la aplicación de campos magnéticos causando una reacción de partículas lo que hace que cambien de posición la cual se mantiene una vez que se deja de aplicar el campo magnético. Las posiciones representan los datos almacenados. Algunos ejemplos de este tipo de medios son:

- Disco duro. Es el principal soporte de almacenamiento, se utiliza para guardar información, archivos de programas, software, multimedia, entre otro tipo de archivos en una computadora.

- Disco duro externo o portátil. Se utiliza para almacenar grandes cantidades de información (multimedia, archivos, software, texto, etc.) en un soporte que puede ser fácilmente transportable.

- Cintas magnéticas. Se utilizan principalmente para realizar respaldos de bases de datos, servidores o equipos de organizaciones.

La principal característica de estos soportes consiste en el uso de las propiedades magnéticas de los materiales para guardar información. Los métodos de destrucción de este tipo de dispositivos se enfocarán en esto, en la posibilidad de sobre-escribir información o en la destrucción total del dispositivo.

b) Soporte óptico (discos ópticos). Dispositivos capaces de guardar datos utilizando un rayo láser. La información queda grabada en la superficie de manera física por medio de ranuras microscópicas quemadas, es por esto que las ralladuras pueden ocasionar la pérdida de los datos.

- CD-ROM / DVD-R. Son utilizados para almacenar datos en formato digital, ya sean audio, imágenes, videos, documentos, texto, entre otros. Estos dispositivos sólo pueden utilizarse una vez para escribir información, posteriormente solo sirven para la lectura de los datos que contienen.

- CD-RW / DVD-RW. Funcionan igual que un CD-ROM / DVD-R con la diferencia que estos pueden sobre escribirse múltiples veces.

- HD-DVD. Consiste en un estándar para el DVD de alta definición

- Blu-Ray (BD-R). Se utiliza para almacenar videos de alta definición y datos de alta densidad. Esta tecnología permite escribir datos solo una vez, por lo que se utiliza mayormente para lectura.

- Blu-Ray re-grabable (BD-RE). Es un Blu-Ray que permite escribir datos varias veces.

- Disco UDO. Es una especie de cartucho que almacena hasta 60 GB. Se utiliza para trabajo pesado o entornos de uso prolongado y su posterior recuperación.

La principal característica de estos soportes, que se debe tomar en cuenta para seleccionar una técnica de destrucción adecuada, consiste en que el estado de la superficie del dispositivo es fundamental para poder tener acceso a la información que se encuentra en el mismo. Si esta se daña, la información que está contenida en ella ya no puede leerse, por lo que se pueden aplicar métodos de destrucción como trituración para poder eliminar la información y el soporte.

c) Soporte magneto-óptico. Consiste en un sistema combinado que graba información de forma magnética bajo la incidencia de un rayo láser y la reproduce por medios ópticos. Tiene la capacidad de un disco óptico, pero puede utilizarse para escribir datos múltiples veces con la facilidad con que se hace en un disco magnético. Son soportes resistentes que pueden almacenar datos durante 30 años sin distorsiones ni pérdidas, adicionalmente

este tipo de soportes verifican la información después de escribirla por lo que resultan confiables. Algunos ejemplos de este tipo de dispositivos son:

- Disco magneto-óptico. Medio óptico de almacenamiento de datos en el que la información se codifica, guarda y almacena haciendo unos surcos microscópicos con un láser sobre la superficie del disco.

- MiniDisc. Es un disco óptico pequeño (7 cm x 6,75 cm x 0,5 cm) y regrabable que permite almacenar audio.

- HI-MD. Es una evolución del MiniDisc, que permitió aumentar su capacidad 6 veces.

La característica principal de los soportes magneto-ópticos consiste en que los datos se almacenan en su superficie, por lo que los métodos de destrucción de este tipo de dispositivos se enfocarán en la destrucción total del dispositivo.

d) Soporte de estado sólido. Son dispositivos de almacenamiento que usan tecnología de memoria flash estática, resisten caídas y golpes ya que no tiene elementos mecánicos. Su uso es más común en empresas por su alto costo. Algunos dispositivos de este tipo son los siguientes:

- Pendrive / USB. Se utilizan para almacenar información, sin embargo puede incluir otros servicios como, lector de huella digital, radio FM, grabación de voz y reproducción de audio. Son muy útiles y prácticos por su tamaño y porque pueden almacenar gran cantidad de información.

- Tarjetas de memoria (Flash drive). Se usan para almacenar fotos y videos en cámaras digitales. También se utilizan para aumentar la capacidad de almacenamiento de teléfonos móviles y tabletas.

- Dispositivo de estado sólido. Usan una memoria no volátil como la flash. Son menos sensibles a los golpes, prácticamente no hacen ruido y tienen un menor tiempo de acceso y de latencia en comparación con los discos duros convencionales.

La principal característica de estos soportes que se debe tomar en cuenta para seleccionar una técnica de destrucción adecuada, consiste en que el dispositivo se puede utilizar varias veces para escribir información, por lo que se pueden utilizar tecnologías, métodos y/o herramientas para sobrescribir lo contenido en el soporte. Esta técnica no es la más segura, sin embargo se requiere contactar al proveedor del soporte para obtener más información sobre como eliminar información de forma segura.

e) Servicios de almacenamiento en la nube. Es un servicio en internet para almacenar contenido estático como imágenes, documentos, videos, etc., en espacios virtualizados. Este servicio normalmente es proporcionado por un proveedor de servicios.

La principal característica de estos soportes, que se debe tomar en cuenta para seleccionar una técnica de destrucción adecuada, consiste en que la información es almacenada por un tercero, por lo que la destrucción de la información será responsabilidad del proveedor del servicio.

A continuación se muestran las consideraciones que se deben tomar en cuenta para el tratamiento de cada tipo de dispositivo, así como algunos riesgos a los que están expuestos.

Tipo de soporte	Consideración en el tratamiento	Posible vulneración
Soportes de almacenamiento físicos		
Archiveros, gavetas / cajones, bodegas, estantes, oficinas.	• Proteger el acceso físico del lugar en el que se encuentra el soporte (cámaras de seguridad, guardias, acceso restringido con tarjeta de proximidad, entre otros). • Considerar la digitalización de la información. • Resguardar en ambiente físico protegido contra desastres naturales.	• Robo de soporte • Desastres naturales (incendio, inundación) • Acceso no autorizado • Pérdida de soporte
Soportes de almacenamiento electrónico		
Soportes magnéticos	• Mantener un registro de los soportes existentes • Asignar a un responsable • Cifrar el soporte • Resguardar el acceso físico al soporte • Validar estado del soporte de forma periódica	• Daño físico del soporte • Pérdida o robo de soporte
Soportes ópticos	• Mantener un registro de los soportes existentes • Asignar a un responsable • Cifrar el soporte • Resguardar el acceso físico al soporte • Validar estado del soporte de forma periódica	• Daño físico del soporte • Pérdida o robo de soporte
Soportes Magneto-ópticos	• Mantener un registro de los soportes existentes • Asignar a un responsable • Cifrar el soporte • Resguardar el acceso físico al soporte • Validar estado del soporte de forma periódica	• Daño físico del soporte • Pérdida o robo de soporte
Soportes de estado sólido	• Mantener un registro de los soportes existentes • Asignar a un responsable • Cifrar el soporte • Resguardar el acceso físico al soporte • Validar estado del soporte de forma periódica	• Daño físico del soporte • Daño lógico del soporte (virus, malware, etc.) • Pérdida o robo de soporte
Soportes de	• Contar con un contrato vigente	• Divulgación de la

almacenamiento en la nube	• Definir como se protegerá la información por medio de cláusulas de confidencialidad agregadas en el contrato	información por ataque. • Falta de claridad en cláusulas de confidencialidad definidas con el proveedor

Tabla 3. Consideraciones en el tratamiento de datos y sus respectivos riesgos.

Otro tema importante que se debe considerar, es cuando compartimos medios de almacenamiento con proveedores externos, con el objetivo de realizar algún mantenimiento o reparación a los mismos, sin considerar que pudiéramos estar poniendo en riesgo la confidencialidad de la información. Esto significa que no es suficiente borrar la información de un dispositivo, debemos tomar en cuenta medidas adicionales sobre los soportes donde se resguardaba información sensible o personal para garantizar su protección.

Por último también se debe considerar que algunas organizaciones han optado por implementar un modelo de negocio donde los empleados realizan home office, es decir trabajan desde casa. En estos casos también deben implementarse medidas de seguridad para garantizar que los documentos con información personal sean trasladados a la oficina para así garantizar que sean destruidos o eliminados de forma adecuada. Para hacer esto posible, se recomienda implementar programas de concientización para los empleados, enfocados en la importancia de proteger la información de la organización.

2.3. *Criterios para definir la política, procedimientos y tiempos de almacenamiento de información que existen en la organización y que son relevantes para la destrucción y/o borrado seguro de los datos personales.*

Hoy en día las organizaciones requieren de un proceso sistemático, documentado y conocido por todos para proteger la información personal que utilizan. Este proceso es el que constituye un Sistema de Gestión de Seguridad de Datos Personales (SGSDP)[8] el cual tiene como objetivo proveer dirección, soporte y un marco de referencia para mantener y garantizar que se está en cumplimiento con regulaciones y prácticas líder, así como garantizar la privacidad y el derecho a la autodeterminación informativa de los titulares, buscando que el tratamiento de los datos sea legítimo, controlado e informado.

El SGSDP debe formar parte del Gobierno para la Gestión de la Privacidad de la Información o esquemas similares que hayan sido definidos por la organización. Este sistema debe considerar los riesgos asociados a los activos utilizados para el tratamiento de los datos personales, así como los principios de la Ley, buenas prácticas y estándares relacionados con el tema.

Por medio de este sistema, se debe desarrollar toda la normatividad interna necesaria que consideren la generación, aplicación y mantenimiento de medidas de seguridad adecuadas. A continuación se muestra una recomendación de una estructura de un sistema de gobierno donde se incluye únicamente la normatividad contenida en el documento actual.

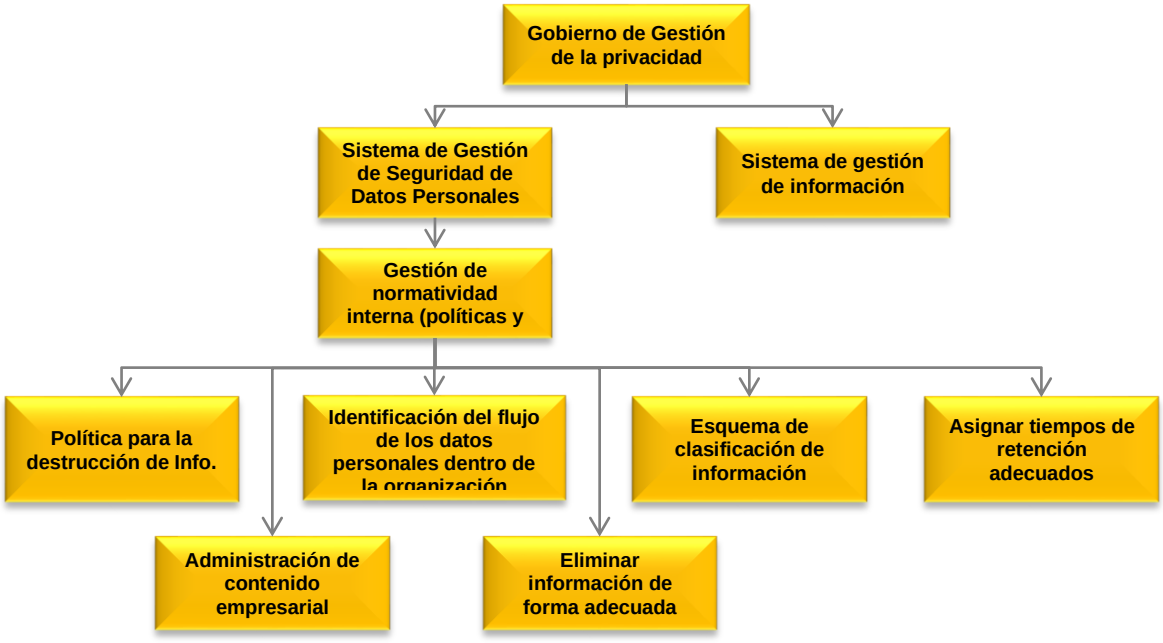


Ilustración 18. Sistema de gobierno para la gestión de la información enfocado en la destrucción de esta.

[8] BS 10012:2009 Data protection – Specification for a personal information management system.

Criterios para definir la política para la destrucción y/o borrado de información personal

A continuación se incluyen los criterios mínimos que se deben tomar en cuenta para definir la política de destrucción y borrado seguro de información física y lógica:

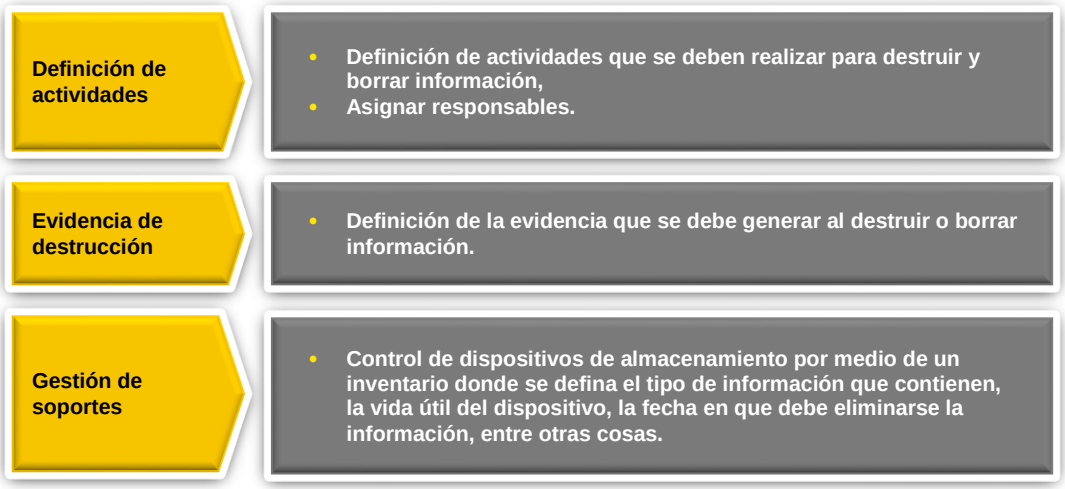


Ilustración 19. Consideraciones de política de destrucción y borrado de información.

- **Definición de actividades.** Se deben definir los procedimientos y las actividades que se deben ejecutar para poder destruir y/o borrar información de forma adecuada, así como sus respectivos responsables. Es importante considerar al menos lo siguiente:

  1. Identificar la información personal tratada, esto se puede realizar por medio del procedimiento para identificar como se obtienen y hacia dónde van los datos dentro de una organización, planteado anteriormente.

  2. Identificar las regulaciones aplicables a la compañía tanto internas como externas.

  3. Analizar y definir qué regulación le aplica a cada tipo de dato con el objetivo de poder identificar limitaciones para la asignación de los tiempos de retención.

  4. Identificar todos los sistemas de tratamiento de datos personales, como aplicaciones, o bases de datos, así como a los proveedores que pudieran estar contratados por la organización como outsourcing a los cuales se les involucra en el tratamiento de los datos.

  5. Identificar los riesgos asociados al tratamiento de datos para poder definir controles adecuados para su destrucción.

  6. Definir las notificaciones que se implementarán para poder identificar que se debe destruir o borrar información, por ejemplo asignar alertas por medio de un sistema que comunique a su respectivo responsable que el tiempo de retención ya se venció.

  7. Definir todas las actividades que se deben efectuar para poder destruir o borrar la información, por ejemplo notificar al proveedor externo contratado para que asista a las instalaciones de la organización, solicitar la autorización para realizar la destrucción,

definir la persona responsable de realizar la destrucción, preparar la evidencia de la destrucción y el registro de esto.

8. Definir cómo se realizará el monitoreo de todas las actividades involucradas en la destrucción de la información, para validar que éstas se estén ejecutando de forma adecuada.

9. Establecer cómo se medirá la eficiencia de los procedimientos implementados, por ejemplo definir métricas como las siguientes: medios de soporte que no fueron eliminados de forma oportuna o dispositivos que no contaban con un tiempo de retención asignado.

10. Establecer un procedimiento de mejora continua por medio de la implementación de auditorías donde se identifiquen actividades que no se están realizando correctamente, o que presentan áreas de oportunidad, con el objetivo de planear mejoras a los procedimientos.

- **Evidencia de destrucción.** Definir qué evidencia se generará de la destrucción de la información, para poder garantizar que se cuenta con un registro de auditoría. Adicionalmente se recomienda mantener un registro de todos los procesos de borrado por activo de información para contar con un registro de auditoría donde se guarde todas las áreas que lo han utilizado.

- **Gestión de soportes.** Se recomienda definir e implementar un inventario de soportes de almacenamiento, para contar con un control de estos dispositivos donde se defina el tipo de información que contienen, la vida útil del dispositivo, la fecha en que debe eliminarse la información que contienen, entre otras cosas. Este documento ayudará a las organizaciones a tener visión sobre cuándo se debe eliminar la información.

Criterios para definir procedimientos para destruir y/o borrar información personal

Asimismo, se recomienda generar procedimientos que permitan la destrucción y/o borrado de información de forma oportuna. A continuación se mencionan los procedimientos mínimos necesarios.

1. **Procedimiento para identificar el flujo de los datos personales dentro de la organización.** Ver sección 2.1 del presente documento.

2. **Esquema de clasificación de información[9]**. Se debe desarrollar un esquema de clasificación de información para asegurar que la información sea utilizada con un nivel adecuado de protección según la importancia que esta tenga para la organización. Es importante clasificar la información de acuerdo a requerimientos legales, a su valor, criticidad y sensibilidad. También se debe considerar la implementación de etiquetas o marcas a la información, así como la definición de actividades necesarias para el manejo adecuado de los activos de la organización tomando en cuenta el esquema de clasificación adoptada por el negocio.

[9] ISO/IEC 27001:2013, Information Technology - Security techniques – Information security management systems – Requirements.

El procedimiento debe considerar al menos lo siguiente:

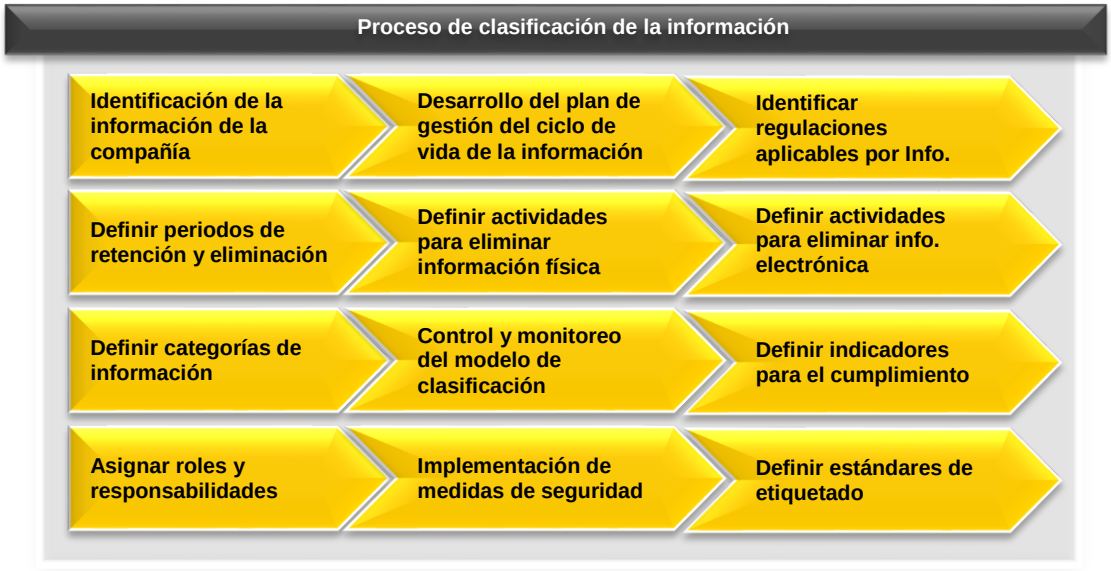


Ilustración 20. Consideraciones de un esquema de clasificación de información.

- **Identificación de la información de la compañía.** Para poder clasificar la información, se requiere saber qué información se está tratando en la organización.

- **Desarrollo del plan de gestión del ciclo de vida de la información.** Definir cómo se administrará el ciclo de vida de la información: desde que ésta se crea, se transmite, se procesa, se almacena hasta que se destruye.

- **Identificar regulaciones aplicables por tipo de dato.** Analizar las regulaciones que le aplican a los datos en cada proceso donde se tratan.

- **Definir los periodos de retención y eliminación de información.** Se debe definir en base a regulaciones aplicables y a las necesidades de la organización, el periodo que debe resguardarse cada tipo de información.

- **Definir actividades para eliminar información física.** Se debe definir como se realizará la eliminación de información física cuando esta ya no se requiera.

- **Definir actividades para eliminar información electrónica.** Se debe definir como se realizará la eliminación de información electrónica cuando esta ya no se requiera. Para mayor detalle, refiérase al capítulo III del presente documento.

- **Definir categorías de información.** Una vez que se cuenta con toda la información existente en la organización, se deben crear categorías que se utilizarán para clasificar la información y en base a eso, se deberán aplicar controles adecuados para su protección. Las categorías variarán de acuerdo a las necesidades de la empresa. A continuación se incluye un ejemplo[10]:

10 Integrating Privacy Using Generally Accepted Privacy Principles. AICPA/CICA

- **Información pública.** El nivel de seguridad más bajo destinado a la información de dominio público. Se requiere implementar controles de seguridad mínimos.

- **Información confidencial.** Nivel de seguridad medio destinado a personal autorizado; se requiere implementar una seguridad moderada.

- **Información secreta.** Nivel más alto de seguridad destinado a la información más sensible; el acceso a ésta información se encuentra restringido a un número mínimo de personas que operan bajo los controles de seguridad más altos.

- **Control y monitoreo del modelo de clasificación.** Se deben definir procedimientos para controlar y monitorear el modelo de clasificación desarrollado, con el objetivo de buscar áreas de oportunidad. Ejemplo: implementar auditorías periódicas de la clasificación asignada a la información.

- **Definir indicadores para el cumplimiento.** Se deben definir indicadores por medio de los cuáles se evaluará el cumplimiento de lo establecido en el esquema de clasificación.

- **Asignar roles y responsabilidades.** Se deben asignar roles y responsabilidades para todas las actividades relacionadas con la clasificación de información.

- **Implementación de medidas de seguridad. Implementar medidas** ya sean tecnológicas u organizacionales, dependiendo de la clasificación asignada a la información

- **Definir estándares de etiquetado.** Definir estándares para etiquetar la información en base a las categorías definidas, incluyendo tiempos de retención, criticidad, entre otros.

Un esquema de clasificación de información, se debe implementar con el objetivo de facilitar la definición y asignación de los tiempos de retención de cada tipo de información (ver siguiente punto) y poder darle seguimiento a su destrucción y/o borrado de forma oportuna.

3. **Asignar tiempos de retención adecuados.** Las decisiones sobre la asignación de periodos de retención se deben basar en lo siguiente:

   - El entorno legal o normativo, ya que pudieran exigir periodos mínimos de conservación.

   - Las necesidades de gestión y de rendición de cuentas.

   - El riesgo asociado a cada tipo de documento.

   En la toma de dichas decisiones se debe incluir a la unidad encargada de la actividad, así como al responsable designado para la gestión de documentos y cualquier otra área relacionada, con el objetivo de garantizar que se tomen en cuenta a las partes interesadas a la hora de determinar el periodo de conservación.

   Las organizaciones deben definir cronogramas donde se establezcan los periodos de retención mínimos definidos por las leyes que apliquen al tipo de información en cuestión.

Adicionalmente se debe documentar la justificación de la asignación de los tiempos de retención y por último, en caso de aplicar, se deben documentar las razones para resguardar información más tiempo del necesario. Para la elaboración de estos cronogramas es importante tomar en cuenta regulaciones aplicables, estándares internacionales, prácticas líder y las necesidades de la organización. Asimismo es importante implementar procedimientos para comunicar los cronogramas definidos a todo el personal de la compañía, con el objetivo de que estos se apliquen como corresponda.

4. **Administración de contenido empresarial (Enterprise Content Management o ECM).** Consiste en un proceso para la implementación de estrategias, métodos y herramientas que se utilizan durante el ciclo de vida de los documentos y contenido, con el objetivo de formalizar su organización y almacenamiento, estos procesos se pueden precisar utilizando las mejores prácticas definidas en el estándar ISO 15489-1:2001 - Gestión de documentos. Para implementar un ECM. Este debe considerar, al menos, lo siguiente:

Ilustración 21. Modelo de administración de contenido empresarial.

- **Digitalización de documentos.** La digitalización de contratos legales, archivos electrónicos, correos y contenidos multimedia entre otros. Como parte de esta actividad, es importante establecer las acciones de captura, procesamiento y acceso al contenido de todo tipo.

- **Administración de documentos de la organización.** Esta práctica está orientada a establecer los mecanismos de seguridad para el manejo de archivos, como contraseñas en documentos, cifrado de archivos, impresión segura de documentos, etc. Es importante la asignación de responsables.

- **Establecer flujos de documentos.** Se debe identificar en qué áreas son utilizados y resguardados. En este punto es importante definir la realización de respaldos de los equipos de empleados clave que contengan información importante.

- **Implementación de herramienta.** Se puede considerar la implementación de un software que apoye en el proceso de administración de contenido.

Este procedimiento ayudará a las empresas a tener una mayor visión y por lo tanto control sobre todos los documentos que utilice.

5. **Gestión de copias de seguridad.** Las organizaciones deben desarrollar e implementar una política de copias de seguridad, así como un plan de contingencia que incluya la planificación de estos respaldos. Se debe considerar al menos lo siguiente:

   - Identificación de los datos cuya pérdida afectaría al negocio por lo que es importante que se respalden.
   - Definición de la periodicidad de los respaldos.
   - Definición del medio que se utilizará para la generación de los respaldos, por ejemplo cintas magnéticas o discos duros; así como su vida útil.
   - Establecimiento de la ubicación donde se almacenarán las copias realizadas, esta puede ser externa o interna a la organización.
   - Control y protección de los dispositivos donde se realizaron las copias de seguridad por medio de la restricción del acceso físico al lugar donde se encuentran, por ejemplo resguardar las copias realizadas en una caja fuerte y/o restringir el acceso a la oficina en la que se guarden los respaldos.
   - Implementación de pruebas de restauración para garantizar que la información se puede recuperar.
   - Monitoreo del proceso de respaldos para validar que estos se están haciendo como fueron planeados.
   - Definición del periodo de validez de las copias de seguridad realizadas.
   - Definición de proceso de borrado seguro para medios cuya vida útil llegó a su fin.

6. **Eliminar información de forma adecuada[11].** Posteriormente, se deben definir e implementar procedimientos para aplicar mecanismos seguros de destrucción o borrado seguro de información una vez que se vencieron los tiempos de retención definidos en los cronogramas.

   El proceso por medio del cual se destruye o elimina información de manera tal que no sea posible recuperarla se conoce como sanitización, esto se hace impidiendo el acceso a los medios o soportes donde se encuentra la información.

   La retención de documentos con datos personales se debe organizar de tal forma que se satisfagan las necesidades de gestión tanto presentes como futuras, por lo que se deben considerar las siguientes situaciones antes de destruir o borrar información:

   - Se debe conservar información relacionada con decisiones y actividades presentes y pasadas para apoyar decisiones y actividades en el presente y en el futuro.

[11] Estudio sobre almacenamiento y borrado seguro de información del Observatorio Inteco.

- Se deben conservar elementos de prueba de las actividades presentes y pasadas para cumplir las obligaciones de rendición de cuentas.
- Se debe conservar el contexto del documento para permitir a usuarios futuros juzgar su autenticidad y fiabilidad.

- Cumplir los requisitos legales, garantizando que se documente, entiende e implementa la normativa aplicable a la gestión de los documentos producidos en el ejercicio de las actividades.

- Identificar intereses relacionados con la conservación de documentos durante un periodo de tiempo superior al requerido por la propia organización. Ejemplo: para cumplir requisitos de rendición de cuentas por auditorías, autoridades o investigadores.

- Identificar y evaluar los beneficios legales, financieros, políticos y/o sociales que se deriven de la conservación de los documentos.

No se debe destruir o borrar ningún documento si no se garantiza que este ya no se necesita, que no queda ninguna labor pendiente de ejecución y que no existe ningún litigio o investigación, en el momento actual o pendiente de realización que implique la utilización del documento como prueba. Para esto, se debe definir que siempre se debe contar con las autorizaciones pertinentes por escrito de los dueños o responsables de la información antes de eliminarla o destruirla, esto podrá realizarse utilizando formatos oficiales o por correo electrónico.

La destrucción de los documentos debe realizarse de tal manera que se preserve la confidencialidad de la información que contengan.

El éxito de las medidas implementadas, dependerá también del nivel de concientización de los empleados.

3. Técnicas de destrucción y borrado seguro

3.1. Técnicas principales de destrucción y borrado seguro de información física y electrónica.

Las técnicas de destrucción de información, buscan que no sea posible recuperar la información tanto física como electrónica y evita que personas no autorizadas puedan tener acceso a esos datos. Las características que deben este tipo de destrucción son:

- Es irreversible. Garantiza que no se pueda recuperar la información.
- Es segura y confidencial. Los documentos se tratan con la misma seguridad con que se han mantenido durante su existencia.
- Es favorable al medio ambiente.

Métodos de sanitización

La sanitización es un elemento clave para buscar la eliminación segura de información física y electrónica[12]. A continuación se muestran los métodos de sanitización más comunes para soportes de almacenamiento:

- **Limpieza (clearing).** También conocida como "sanitización lógica". Aplica técnicas lógicas en las ubicaciones donde se encuentran almacenados los datos del usuario para borrarlos y protegerlos contra algunos métodos de recuperación.
    - Técnicas lógicas. Se realiza sobrescribiendo el espacio de almacenamiento con otros datos, es decir escribiendo nueva información sobre los datos viejos. La sobre-escritura no puede utilizarse en medios dañados o no regrabables, tampoco es la forma adecuada para borrar información en todos los dispositivos. La operación de este método de limpieza varía ya que algunos medios de almacenamiento no soportan la sobre-escritura, solo ofrecen la posibilidad de devolver el dispositivo al estado de fábrica.
    - Técnicas físicas. Consisten en la aplicación de métodos de destrucción como la trituración en la que se generan fragmentos de un tamaño regular.
- **Purga (purge).** También conocida como "sanitización analógica". Son métodos que degradan la señal analógica que codifica los datos para que la reconstrucción de esta sea imposible, aun utilizando equipo avanzado. La sanitización por purga aplica técnicas lógicas o físicas.
    - Técnicas lógicas. Incluyen la sobre-escritura, borrado de bloques o borrado criptográfico a través del uso de comandos.
    - Técnicas físicas. Consisten en la aplicación de métodos de destrucción, como la incineración, trituración, desintegración, desmagnetización y pulverización.

12 NIST SP 800-88 Guidelines for Media Sanitization

Técnicas de destrucción para información física

Dentro de las técnicas de destrucción física, existen varios métodos y/o procesos para eliminarla, esto son:

- **Trituración.** Existen distintas máquinas de trituración las cuales se clasifican según el tamaño y la forma de los fragmentos que producen. Pueden ser tan sencillas como unas tijeras, o tan complejas como equipos industriales. El tamaño del triturado deberá depender de la sensibilidad de la información, si los documentos contienen datos personales sensibles o patrimoniales, deberán triturarse de tal forma que no sean recuperables.

  1. **Trituradora de línea recta o tiras**. Cortan el documento en tiras delgadas. No es muy segura, la información puede ser recuperada rearmando los fragmentos, por lo que se recomienda utilizar para eliminar información con riesgo bajo o clasificada con nivel estándar.

  2. **Trituradoras de corte cruzado**. Corta el documento de forma vertical y horizontal generando fragmentos cuadrados muy diminutos, lo cual hace prácticamente imposible que se puedan unir. Se recomienda utilizar para eliminar datos con riesgo alto. o clasificados con nivel sensible.

  3. **Trituradoras de papel de partículas**. Trituran el documento en partículas de aproximadamente 5x5 mm. Se recomienda utilizar para eliminar datos con riesgo medio y alto, o aquellos clasificados con nivel especial.

  La norma DIN 32757-1[13], es un estándar que se ha adoptado a nivel mundial para la destrucción de documentos creado por el Instituto Alemán para la Estandarización, establece cinco grados de seguridad y determina el tamaño máximo de la tiras o partículas en función de la criticidad de la información. En la Tabla 4 se muestra una relación entre el nivel de seguridad que se debe utilizar para destruir documentos dependiendo de la clasificación asignada a cada dato. Es recomendable definir esta clasificación de acuerdo la Guía para implementar un Sistema de Gestión de Seguridad de Datos Personales[14]

Nivel	Tamaño máximo del fragmento	Tipo de documento	Categoría de datos a eliminar por nivel
1. General	Tiras de 12 mm de ancho	Documentos generales que deben hacerse ilegibles	Datos clasificados con nivel estándar
2. Interno	Tiras de 6 mm de ancho	Documentos internos que deben hacerse ilegibles	Datos clasificados con nivel estándar
3. Confidencial	Tiras de 2 mm de ancho Partículas de 4x80 mm	Documentos confidenciales	Datos clasificados con nivel sensible
4. Secreto	Partículas de 2x15 mm	Documentos de importancia vital para la organización que deben mantenerse en secreto	Datos clasificados con nivel especial
5. Alto Secreto	Partículas de 0,8x12 mm	Documentos clasificados para los que rigen exigencias de seguridad muy elevadas.	Datos clasificados con nivel especial

Tabla 4. Grados de seguridad para la destrucción de documentos.

13 http://www.ebaspain.es/info-lopd/normas-din-32757/
14 Guía para implementar un Sistema de Gestión de Seguridad de Datos Personales. Ifai. Enero 2014

- **Incineración**. La incineración de documentos consiste en su destrucción a través del uso del fuego. Actualmente la práctica de la incineración no es muy recomendable por cuestiones relacionadas con el cuidado del medio ambiente, sin embargo es una opción segura para la destrucción de información, siempre y cuando se valide que el documento se redujo a cenizas.

- **Uso de químicos.** En algunos casos también se destruyen documentos por medio de químicos, sin embargo esta opción tampoco es muy recomendable por temas ambientales.

A continuación se presentan dos modalidades para aplicar algunos de los métodos mencionados anteriormente.

1. **Por medio de un tercero en las instalaciones de la organización**. Actualmente existen empresas que se dedican a prestar el servicio de destrucción de documentos de forma segura, estos proveedores cuentan con la infraestructura necesaria, así como certificaciones de garantía de destrucción. La ventaja de realizar la destrucción en las instalaciones de la organización consiste en que el procedimiento se realiza frente a testigos del negocio, validando así que la información sea destruida de forma adecuada. En caso de elegir esta opción, es muy importante establecer el contrato donde se defina de forma detallada el servicio que se prestará el tercero, así como las responsabilidades de ambas partes.

2. **Por medio de un tercero en las instalaciones del proveedor del servicio**. La organización debe validar que el proveedor ofrezca y certifique el transporte seguro de los documentos hacia sus instalaciones. De igual forma se debe definir un procedimiento para la validación de la destrucción, ya sea que una persona de la organización sea testigo de la destrucción de los documentos, o que se defina algún tipo de evidencia de esto. Se debe contar con un contrato donde se defina de forma detallada el servicio que se prestará, así como las responsabilidades de ambas partes.

Técnicas de destrucción para soportes electrónicos

A continuación se presentan los métodos existentes para eliminar información electrónica:

- **Desmagnetización.** Con este método se exponen los dispositivos de almacenamiento a un campo magnético para eliminarlo o reducirlo por medio de un dispositivo denominado des-magnetizador, diseñado para el medio específico que se borrará. También hace posible que el hardware donde se encuentra la información se vuelva inoperable por lo que solo debe aplicarse si no se volverá a utilizar el medio / soporte. La potencia requerida para borrar el dispositivo depende de su tamaño y forma. Es un método más seguro que algunos procesos de destrucción física.

- **Sobre-escritura.** Consiste en sobre escribir todas las ubicaciones de almacenamiento utilizables, es decir, en escribir información nueva en la superficie de almacenamiento sobre los datos existentes por medio de software. El método más simple consiste en realizar una sola sobre-escritura, para implementar una mayor seguridad se pueden efectuar múltiples sobre-escrituras con variaciones en los caracteres grabados. En la Tabla 3 se muestran distintos métodos de borrado que existen con su respectiva descripción y

nivel de seguridad[15]. Asimismo, se muestra una relación entre el método de sobre escritura que se puede utilizar dependiendo de la clasificación asignada a cada dato.

Método de borrado	Métodos de sobre-escritura aplicado sobre el soporte	Nivel de Seguridad	Categoría de datos a eliminar por técnica
Grado 1. Super Fast Zero Write	1. Valor fijo (0×00) una vez cada 3 sectores	Bajo	Datos clasificados con nivel estándar
Grado 2. Fast Zero Write	1. Valor fijo (0×00) una vez todos los sectores	Bajo	Datos clasificados con nivel estándar
Grado 3. Zero Write	1. Valor fijo (0x00) en todo el área	Bajo	Datos clasificados con nivel estándar
Grado 4. Random Write	1. Valores aleatorios. La fiabilidad aumenta con la cantidad de pasadas	Medio	Datos clasificados con nivel sensible
Grado 5. Random & Zero Write	1. Valores aleatorios 2. Valor fijo (0x00) 3. Valores aleatorios 4. Escritura de valor cero	Medio	Datos clasificados con nivel sensible
Grado 6. US Navy, NAVSO P-5239-26 – MFM. Para discos codificados con MFM (Modified Frequency Modulation)	1. Valor fijo (0xffffffff) 2. Valor fijo (0xbfffffff) 3. Valores aleatorios 4. Se verifica la sobre-escritura	Medio	Datos clasificados con nivel sensible
Grado 7. US Navy, NAVSO P-5239-26 – RLL. Para discos duros y soportes ópticos (CD, DVD, BlueRay)	1. Valor fijo (0xffffffff) 2. Valor fijo (0x27ffffff) 3. Valores aleatorios 4. Se verifica la sobre -escritura	Medio	Datos clasificados con nivel sensible
Grado 8. Bit Toggle	1. Valor (0x00) 2. Valor (0xff) 3. Valor (0x00) 4. Valor (0xff) Total de sobre-escrituras: 4	Medio	Datos clasificados con nivel sensible
Grado 9. Random Random Zero	1. Dos veces con valores aleatorios 2. Valor fijo (0x00) 3. Dos veces con valores aleatorios 4. Con ceros	Medio	Datos clasificados con nivel sensible
Grado 10. US Department of Defense (DoD 5220.22-M)	1. Valor fijo determinado 2. Valor complementario (0xff) 3. Valores aleatorios 4. Se verifica la sobre-escritura	Medio	Datos clasificados con nivel sensible
Grado 11. US Air Force, AFSSI5020	1. Valor fijo (0x00) 2. Valor fijo (0xff) 3. Valor aleatorio constante 4. Se verifica sobre-escritura de un mínimo del 10% del disco	Medio	Datos clasificados con nivel sensible

15 http://www.lc-tech.com/pc/file-definitions/

Grado 12. North Atlantic Treaty Organization (OTAN) NATO standard	1. Seis veces con valores fijos alternativos entre cada pasada (0x00) y (0xff) 2. Valor aleatorio Total de sobre-escrituras: 7	Alto	Datos clasificados con nivel especial
Grado 13. Peter Gutmann Secure Deletion	1. Valores aleatorios 4 veces sobre cada sector 2. Valores pseudo aleatorios sobre cada sector por veintisiete pasadas 3. Valores aleatorios durante cuatro pasadas sobre cada sector Total de sobre-escrituras: 35	Alto	Datos clasificados con nivel especial
Grado 14. US Department of Defense (DoD 5220.22-M) + Gutmann Method	Combina los grados 13 y 10 Total de sobre-escrituras: 35	Muy Alto	Datos clasificados con nivel especial

Tabla 5. Algoritmos de borrado por sobre-escritura.

- **Destrucción.** Consiste en destruir completamente el dispositivo de almacenamiento por medio de técnicas como las siguientes:
  - Trituración. Refiérase a la página 50 del presente documento.
  - Desintegración. Separación completa o pérdida de la unión de los elementos que conforman algo, de modo que deje de existir.
  - Incineración. Quema de una cosa para reducirla a cenizas
  - Abrasión / fundición. Acción de arrancar, desgastar o pulir algo por rozamiento o fricción:
  - Pulverización. Procedimiento mediante el cual un cuerpo sólido se convierte en pequeñas partículas de polvo.
  - Fusión. Paso de un cuerpo del estado sólido al líquido por la acción del calor.

La técnica de destrucción deberá seleccionarse dependiendo de las características de la información y del soporte de almacenamiento que se use y de donde se encuentra.

3.2. Proporcionar información para orientar en la selección del método de destrucción y/o borrado idóneo para cada soporte de almacenamiento de datos personales.

La destrucción y borrado de información es un tema de vital importancia para proteger su confidencialidad, integridad y disponibilidad, es por esto que las empresas deben analizar los medios eficaces que deben implementar para evitar que la información que ya no requieren, pueda recuperarse una vez que es eliminada. En la siguiente sección se plantean métodos de eliminación que pueden utilizarse para cada tipo de soporte de almacenamiento.

Métodos de eliminación utilizados en soportes que almacenan información física

Como se mencionó anteriormente, el método para la destrucción de información física debe orientarse al documento donde se encuentran los datos personales / sensibles. Por ello es recomendable seleccionar cualquier método de destrucción ya sea trituración, incineración, uso de químicos o por medio de un tercero especializado.

Métodos de eliminación utilizados en soportes que almacenan información electrónica

A continuación se presentan los métodos existentes para eliminar información que se encuentra en soportes electrónicos.

3. **Soportes magnéticos**

   A continuación se mencionan algunas situaciones que pudieran presentarse, así como el método de eliminación que deberá seleccionarse:

   - Si la organización reutiliza equipos informáticos, por lo que borra y redistribuye las unidades de disco duro o cintas magnéticas en un ambiente con controles de seguridad equivalentes a los establecidos en donde se utilizó inicialmente, se puede aplicar el proceso de sanitización de limpieza (clearing).

   - Para los discos duros o cintas magnéticas que se trasladarán a un entorno menos seguro o inclusive saldrán de la organización para su reventa o eliminación, los métodos de sanitización que se recomienda aplicar son los de purga (purge).

   - Cuando el dispositivo se vuelve inoperable por algún fallo electrónico o físico, se deben aplicar métodos de destrucción, ya sea por medio de desmagnetización o destrucción física del disco.

   También es recomendable que los discos duros (internos y/o externos) sean destruidos por empresas especializadas en un lugar seguro y aislado para garantizar la eliminación del material magnético.

4. **Soportes ópticos**

   A continuación se muestran algunas situaciones que pudieran presentarse, así como el método de eliminación que es recomendable elegir:

   - Si el dispositivo permite la sobre-escritura, es posible aplicar métodos de sanitización. Por medio de estos métodos se elimina información utilizando funciones de borrado disponibles en el software de grabación que manejan una función de 'borrado rápido' para suprimir las

secciones de encabezado del disco. Sin embargo esto no elimina totalmente los archivos, y por ende es posible recuperar información.

- Los dispositivos ópticos que son de "una sola escritura", recomendamos eliminarlos usando los métodos de destrucción fisca.

    - Trituración. Es recomendable reducir los soportes ópticos a partículas cuyas dimensiones no asciendan los .5 mm de borde y los .25 mm^2 de superficie.

    - Incineración. Para llevar a cabo la incineración de dispositivos, es recomendable realizarlo con un proveedor especializado y asegurar que los residuos deban reducirse a ceniza blanca.

5. <u>Soportes magneto-ópticos</u>

A continuación se mencionan algunas situaciones que pudieran presentarse, así como el método de eliminación que se recomienda seleccionar:

- Si el soporte es reutilizado bajo un ambiente con controles de seguridad, es posible aplicar el proceso de sanitización de limpieza (clearing), por medio de técnicas de sobre-escritura.

- Para los soportes que se trasladan a un entorno menos seguro o inclusive saldrán de la organización, los métodos de sanitización que pueden aplicarse son los de “purga”. En este caso también aplican técnicas de sobre-escritura, sin embargo estas deben ser robustas. Adicionalmente es importante validar que se hayan eliminado los datos antes de volver a utilizar el soporte.

- Cuando el dispositivo se vuelve inoperable por algún fallo electrónico o físico, se recomienda aplicar métodos de destrucción física como la pulverización, trituración de corte transversal o la quema.

6. <u>Soportes de estado sólido</u>

A continuación se mencionan algunas situaciones que pudieran presentarse, así como el método de eliminación que deberá considerarse:

- Si el soporte es reutilizado en un ambiente con controles de seguridad, es posible aplicar el proceso de sanitización de limpieza (clearing). Para ello se requiere sobre-escribir el soporte mínimo una vez con un patrón simple y un valor fijo.

- Para los soportes que se trasladarán a un entorno menos seguro o inclusive saldrán de la organización, los métodos de sanitización que pueden aplicarse son los de “purga”. A continuación se muestran las opciones disponibles:

    - Comandos de sanitización incorporados en el dispositivo. Estos comandos no siempre se encuentran disponibles en los dispositivos.

    - Utilizando comandos de sanitización SCSI para alterar la información en la memoria caché y en la unidad lógica, sin embargo esté método no permite verificar si los datos fueron eliminados por completo.

- Para los soportes que tienen seguridad criptográfica implementada por medio de OPAL, (especificación de seguridad para dispositivos de almacenamiento definida por Trusted Computing Group), o por medio de eDrive, (especificación de seguridad definida por Microsoft), la información se borra por eliminación criptográfica. Este proceso elimina el lugar donde se almacena la llave con la que se protege la información, lo que ocasiona que también se destruya toda la información almacenada. Asimismo los mecanismos de seguridad se desactivan, por lo que los soportes pueden reutilizarse con alguna otra aplicación de seguridad.

- Cuando el dispositivo se vuelve inoperable, se recomienda aplicar métodos de destrucción física para asegurar que la recuperación de los datos es prácticamente imposible. A continuación se muestran los métodos de destrucción más efectivos para este tipo de soportes:

    - Desintegración. En este proceso se rompe el dispositivo en trozos lo suficientemente pequeños para asegurar que las placas de los circuitos impresos, así como los chips integrados se destruyan de forma adecuada.

    - Incineración. Los procesos de incineración derriten el plástico que protege el dispositivo y los circuitos internos que componen el soporte. Estas técnicas deben ser llevadas a cabo por especialistas.

    - Trituración. Se recomienda destruir las tarjetas de memoria con tijeras o con una trituradora de tiras que genere fragmentos de un ancho máximo de 2 mm. Las tarjetas se deben insertar en la trituradora de forma diagonal, en un ángulo de 45 grados para así garantizar la destrucción del microchip, el código de barras, la banda magnética y por lo tanto la información escrita en la tarjeta.

7. <u>Soporte de almacenamiento en la nube</u>

Las actividades para eliminar información almacenada en servicios de nube dependerán de cada proveedor que proporcione el servicio, sin embargo, se debe considerar la inclusión de cláusulas de confidencialidad en el contrato en el que se definan las condiciones del servicio, que incluyan al menos lo siguiente:

- Definición del responsable de los datos personales almacenados

- Definición de controles mínimos para la protección de la información

- Definición de niveles de servicio por parte del proveedor

- Definición de multas por incumplimiento.

3.3. Generar una comparativa de ventajas y desventajas de cada una de las técnicas de destrucción y/o borrado, así como una relación del método adecuado en función del soporte de almacenamiento.

Ventajas y desventajas de técnicas de destrucción de información física

En la Tabla 6 se muestra una relación de las ventajas y desventajas que conlleva la implementación o el uso de los métodos de destrucción de información física. Asimismo, se incluye la relación de la categoría de información que se recomienda eliminar con la respectiva técnica de destrucción.

Técnica de destrucción / borrado	Ventajas	Desventajas	Categoría de datos a eliminar por técnica
Trituración	• Hay trituradoras de oficina a un bajo costo. • La destrucción de documentos puede hacerse en las instalaciones de la organización. • No se requiere contratar a un proveedor externo. • Los documentos triturados pueden ser reciclados.	• No prevé la generación de informes del proceso de borrado necesarios para demostrar el cumplimiento normativo. • Si no se tritura la información de forma adecuada, esta puede ser recuperada.	Ver Tabla 4. Grados de seguridad para la destrucción de documentos.
Incineración	• Los datos son totalmente irrecuperables.	• Daña el medio ambiente. • No prevé la generación de informes del proceso de borrado necesarios para demostrar el cumplimiento normativo. • Puede resultar peligroso.	Datos clasificados con nivel estándar, sensible y especial.
Uso de químicos	• Los datos son totalmente irrecuperables.	• Daña el medio ambiente • No prevé la generación de informes del proceso de borrado necesarios para demostrar el cumplimiento normativo. • Puede resultar peligroso.	Datos clasificados con nivel sensible y especial.
Por medio de un tercero en las instalaciones de la organización	• Proporcionan certificados de destrucción de información. • La destrucción la realizan proveedores especializados en un ambiente controlado. • El responsable de la información puede ser testigo de la destrucción de la información. • No se requiere adquirir equipo para la destrucción de documentos. • En algunos casos el proveedor apoya a supervisar los plazos de conservación de los documentos, cuando estos vencen informan al cliente para iniciar, previa autorización, su destrucción.	• Implica costos adicionales para la contratación del servicio.	Datos clasificados con nivel sensible y especial.
Por medio de un tercero en las instalaciones del proveedor del servicio	• Proporcionan certificados de destrucción de información. • La destrucción la realizan proveedores especializados en un ambiente controlado. • No se requiere adquirir equipo para la	• Implica costos adicionales para la contratación del servicio.	Datos clasificados con nivel sensible y especial.

	destrucción de documentos. • En algunos casos el proveedor apoya a supervisar los plazos de conservación de los documentos, cuando estos vencen informan al cliente para iniciar, previa autorización, su destrucción.		

Tabla 6. Ventajas y desventajas de técnicas de destrucción de información física.

Ventajas y desventajas de técnicas de destrucción de información electrónica

En la Tabla 7 se muestra una relación de las ventajas y desventajas que conlleva la implementación o el uso de los métodos de destrucción de información electrónica más comunes.

Técnica de destrucción / borrado	Ventajas	Desventajas	Categoría de datos a eliminar por técnica
Desmagnetización	• Hace que los datos sean totalmente irrecuperables. • Es un método rápido. • Permite la eliminación de información aunque el soporte se encuentre dañado.	• Implica costos para transportar dispositivos a donde se encuentre el desmagnetizador. • El dispositivo deja de ser utilizable. • Dificultad para verificar borrado de datos. • Dificultad para calcular la potencia requerida para borrar cada equipo. • No prevé la generación de informes del proceso de borrado necesarios para demostrar el cumplimiento normativo. • Requiere un desmagnetizador por cada tipo de soporte. • Se debe tener cuidado para evitar daños a equipos magnéticos cercanos. • Personas con ciertas condiciones médicas o que tienen marcapasos deben permanecer alejados.	Datos clasificados con nivel sensible y especial.
Sobre-escritura	• Facilidad para comprobar la eliminación de la información. • Se puede hacer en las instalaciones de la organización. • Permite la reutilización de dispositivos. • Bajo costo. • Prevé la generación de informes del proceso de borrado necesarios para demostrar el cumplimiento normativo.	• No se puede utilizar en dispositivos dañados. • No se puede utilizar en dispositivos que no sean regrabables. • No sirve en discos con funciones de gestión de almacenamiento avanzadas.	Ver Tabla 4. Grados de seguridad para la destrucción de documentos.
Destrucción (Trituración, desintegración, incineración, abrasión / fundición, pulverización, fusión)	• Proporciona la máxima seguridad de destrucción absoluta de los datos.	• Implica métodos industriales de destrucción. • Implica costos de transportación de los dispositivos. • El dispositivo deja de ser utilizable.	Datos clasificados con nivel estándar, sensible y especial.

Tabla 7. Ventajas y desventajas de técnicas de destrucción de información electrónica.

Métodos de destrucción adecuados, en función del soporte de almacenamiento

En la Tabla 8 se muestra una relación de los métodos de destrucción adecuados en función al tipo de soporte de almacenamiento que se utilice.

Tipo de soporte	Soporte	Método de destrucción
Soportes de información física	• Archiveros • Gavetas • Bodegas • Estantes • Oficinas	• Trituración • Incineración • Uso de químicos • Por medio de un tercero
Magnético	• Disco duro • Disco duro externo o portátil • Cintas magnéticas	• Sobre-escritura • Comandos de sanitización incorporados en el dispositivo • Desmagnetización • Destrucción física (trituración, desintegración, incineración) • Por medio de un tercero
Óptico	• CD-ROM / DVD-R • HD-DVD • Blu-Ray (BD-R) • Disco UDO	• Destrucción física (trituración, incineración) • Por medio de un tercero
Óptico (dispositivos re-grabables)	• CD-RW / DVD-RW • Blu-Ray re-gradable (BD-RE)	• Sobre-escritura • Destrucción física (trituración, desintegración, incineración) • Funciones de borrado rápido del software (es posible recuperar información). • Por medio de un tercero
Magneto-óptico	• Disco magneto-óptico • MiniDisc • HI-MD	• Sobre-escritura • Destrucción física (pulverización, trituración de corte transversal o la quema) • Por medio de un tercero
Estado sólido	• Pendrive / USB • Tarjetas de memoria (Flash drive) • Dispositivo de estado sólido	• Sobre-escritura • Comandos de sanitización incorporados en el dispositivo • Comandos de sanitización SCSI • Eliminación criptográfica • Destrucción física (desintegración, incineración, trituración) • Por medio de un tercero
En la nube	• Almacenamiento en Internet	• Variable, sin embargo hay que considerar que es información electrónica. • El proveedor del servicio será el responsable de realizar el borrado de la información.

Tabla 8. Métodos de destrucción por soporte de almacenamiento.

Es recomendable tomar en cuenta la sección anterior para poder seleccionar la mejor opción de acuerdo a la situación o el ambiente en el que se encuentra la información que se quiere eliminar.

A continuación se presenta un ejemplo práctico sobre como seleccionar un método de destrucción de información.

- Inicio de caso práctico -

La Lic. Guerra trabaja en un despacho contable donde recientemente se asignó al Ing. Reyes como responsable de los datos personales para que guie y apoye en la protección y privacidad de los datos y represente a la empresa en todos los asuntos relacionados con la Ley. El Ing. Reyes se encuentra analizando los documentos en papel que contienen datos personales para identificar aquellos que ya cumplieron con su finalidad y proceder con su destrucción. La primera área que visita es la de Recursos Humanos donde identifica los siguientes documentos que contienen datos cuya finalidad ya se cumplió:

Documentos físicos:

- Archiveros con contratos de empleados que no se generaron correctamente.
- Cajones en la oficina de RH con recibos de nómina de personal dado de baja hace más de 5 años.
- Expedientes de empleados dados de baja hace más de 5 años en el archivo muerto del despacho.
- Pólizas de seguro vencidas en estantes de los empleados de RH.
- CVs de candidatos que no fueron contratados en la oficina del gerente de RH
- IFEs y estados de cuenta de empleados como hojas reciclables dentro de las áreas de impresión.

Documentos electrónicos:

- Recibos de nómina que ya no se requieren en un USB.
- CD’s con información de estudios médicos de años pasados en la oficina de RH.
- Expedientes de empleados que ya no laboran en la compañía en un disco duro.
- Cinta magnética con un respaldo de la aplicación de RH donde se gestiona la nómina y estudios médicos de hace más de 10 años.

El Ing. Reyes identifica a la Lic. Guerra, directora de RH, como responsable de esta información, por lo que solicita y obtiene su autorización para eliminar esta información, sin embargo la Lic. Guerra se encuentra preocupada por el tipo de información contenida en los expedientes ya que se trata de datos personales patrimoniales y datos sensibles. El Ing. Guerra analiza las opciones que tiene para destruir la información física:

- Trituración
- Incineración
- Uso de químicos
- Por medio de un tercero

Inicialmente descarta la destrucción de documentos por uso de químicos e incineración ya que el despacho cuenta con una cultura que fomenta el cuidado al medio ambiente, por lo que decide eliminar la información personal general por medio de trituración. Para la destrucción de la información patrimonial y sensible decide analizar la posibilidad de contratar a un tercero. El Ing. Reyes revisa el presupuesto que le fue asignado y valida que si es posible contratar este servicio por lo que analiza varias opciones. Finalmente elige a un proveedor que ofrece la opción de destruir los documentos en las instalaciones del despacho ya que prefiere estar presente cuando se realice la destrucción.

Para la destrucción de la información electrónica, realiza el siguiente análisis:

Información	Tipo de información	Soporte	Tipo de soporte	Método de destrucción
Recibo de nómina	Nivel sensible	USB	Soporte de estado sólido	Sobre-escritura (grado 4)
Estudios médicos	Nivel sensible	CD	Soporte óptico	Por medio de un tercero: Sobre-escritura (grado 4) Destrucción física (trituración nivel confidencial)
Expedientes de empleados (información patrimonial, sensible y general)	Nivel especial	Disco duro (ya no se utilizará el soporte)	Soporte magnético	Por medio de un tercero: Desmagnetización Destrucción física (trituración nivel confidencial)
Nómina y estudios médicos	Nivel especial	Cinta magnética (ya no se utilizará el soporte)	Soporte magnético	Por medio de un tercero: Desmagnetización Destrucción física (trituración nivel confidencial)

Tabla 9. Caso práctico.

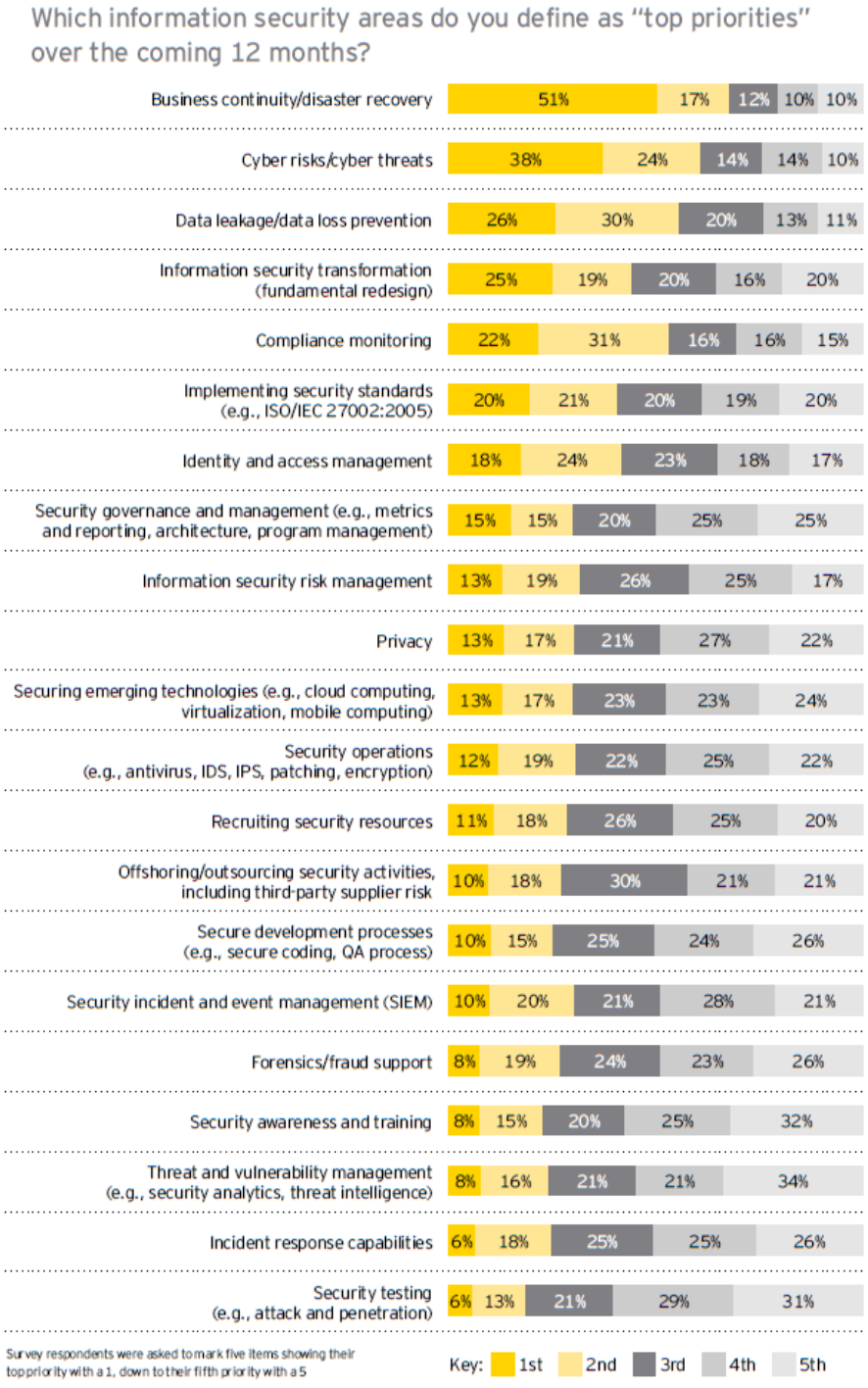
Adicionalmente, el Ing. Reyes establece como procedimiento formal la destrucción de información sensible y patrimonial ya sea física o electrónica por medio de un tercero especializado y los documentos o soportes con información general por medio de trituración. Dentro de la normatividad define que se debe de validar que los documentos o soportes triturados sean destruidos de tal forma que no puedan ser recuperados. Por último, decide incluir en la política de protección de datos personales las normas pertinentes para evitar que se utilicen documentos que contienen datos personales como hojas reciclables dentro de las áreas de impresión e incluye este tema dentro del programa de concientización.

El Ing. Reyes publica la normatividad generada para que todo el personal del despacho se familiarice con esta y solicita a los responsables de áreas donde se tratan datos personales que realicen el mismo ejercicio para identificar documentos que ya cumplieron con sus finalidades y procedan a eliminarlos.

- Fin del caso práctico -

Anexos

Anexo A. Importancia del tema de la privacidad



Anexo B. Resumen de incidentes por categoría.

Identity Theft Resource Center

2005 - 2014 Data Breach Category Summary

How is this report produced? What are the rules? See last page of report for details.

Totals for Category:	**Banking/Credit/Financial**	**# of Breaches: 363**	**# of Records:**	**84,818,946**
		% of Breaches: 7.6%	**%of Records:**	**13.2%**
Totals for Category:	**Business**	**# of Breaches: 1732**	**# of Records:**	**356,689,643**
		% of Breaches: 36.1	**%of Records:**	**55.6%**
Totals for Category:	**Educational**	**# of Breaches: 760**	**# of Records:**	**16,494,886**
		% of Breaches: 15.9	**%of Records:**	**2.6%**
Totals for Category:	**Government/Military**	**# of Breaches: 749**	**# of Records:**	**134,633,394**
		% of Breaches: 15.6	**%of Records:**	**21.0%**
Totals for Category:	**Medical/Healthcare**	**# of Breaches: 1190**	**# of Records:**	**48,400,821**
		% of Breaches: 24.8	**%of Records:**	**7.6%**
	Totals for All Categories:	**# of Breaches: 4794**	**# of Records:**	**641,037,690**
		% of Breaches: 100.0	**%of Records:**	**100.0%**

2005 to 2014 Breaches Identified by the ITRC as of: 9/18/2014

Total Breaches: 4,794
Records Exposed: 641,037,690

The ITRC Breach database is updated on a daily basis, and published to our website on each Tuesday. Unless noted otherwise, each report includes breachs that occurred in the year of the report name (such as "2014 Breach List", or became public in the report name year, but were not public in the previous year. Each item must be previously published by a credible source, such as Attorney General's website, TV, radio, press, etc. The item will not be included at all if ITRC is not certain that the source is real and credible. We include in each item a link or source of the article, and the information presented by that article. Many times, we have attributions from a multitude of media sources and media outlets. ITRC sticks to the facts as reported, and does not add or subtract from the previously published information. When the number of exposed records is not reported, we note that fact. When records are encrypted, we state that we do not (at this time) consider that to be a data exposure. However, we do not consider password protection as adequate, and we do consider those events to be a data exposure.

The ITRC Breach Report presents individual information about data exposure events and running totals for the year. The ITRC Breach Stats Report develops some statistics based upon the type of entity involved in the data exposure.

The ITRC would like to thank IDentityTheft911 for its financial support of the ITRC Breach Report, ITRC Breach Stats Report and all supplemental breach reports.

9/18/2014

Anexo C. Fichas para documentar el tratamiento de datos personales.

Responsable de datos personales: Sr. Díaz									
Persona entrevistada / responsable del proceso: José Villarreal, Administración de personal									
Tratamiento: 1. Obtención de datos personales en el proceso de reclutamiento									
Formato	Datos recopilados			Aviso de priv.		Medio de obtención	Flujo	Finalidad	Encargado
	Dato	¿Se requiere?	Tipo de datos	¿Se muestra?	Consentimiento				

Tratamiento: 2. Almacenamiento de datos personales en el proceso de reclutamiento						
Datos personales	Soporte					
	Físico	Tiempo Almacenamiento	Controles	Digital	Tiempo Almacenamiento	Controles

Tratamiento: 3. Uso de datos personales en el proceso de reclutamiento					
Datos personales	Tiene acceso	¿Requiere acceso?	Método de destrucción	Validación de destrucción	Responsable de destrucción / borrado

Tratamiento: 4. Divulgación de datos personales en el proceso de reclutamiento										
Datos personales	Transferencia						Divulgación			
	Interna	Motivo	Medio	Externa	Motivo	Medio y controles	Nube	Sitios web	Carpetas compartidas	
									¿Se usan?	Acceso

EY

Auditoría | Asesoría de Negocios | Fiscal-Legal | Fusiones y Adquisiciones

Acerca de EY
EY es líder global en servicios de auditoría, asesoría de negocios, fiscal-legal y fusiones y adquisiciones. A nivel mundial, nuestros 152,000 profesionales están unidos por los mismos valores y un compromiso sólido con la calidad. Marcamos la diferencia al ayudar a nuestra gente, clientes y comunidades a lograr su potencial.

Para mayor información por favor visite www.ey.com/mx

Nuestras oficinas	Clave	Teléfono	Nuestras oficinas	Clave	Teléfono
Aguascalientes	449	912-82-01	Mexicali	686	568-45-53
Cancún	998	884-98-75	México, D.F.	55	5283-13-00
Chihuahua	614	425-35-70	Monterrey	81	8152-18-00
Ciudad Juárez	656	648-16-10	Navojoa	642	422-70-77
Ciudad Obregón	644	413-32-30	Puebla	222	237-99-22
Culiacán	667	714-90-88	Querétaro	442	216-64-29
Guadalajara	33	3884-61-00	Reynosa	899	929-57-07
Hermosillo	662	260-83-60	San Luis Potosí	444	825-72-75
León	477	717-70-62	Tijuana	664	681-78-44
Los Mochis	668	818-40-33	Torreón	871	713-89-01
Mérida	999	926-14-50	Veracruz	229	922-57-55