

Datos y sistemas de información

**Breve descripción:**

Los cambios que afrontan las organizaciones, producto de la globalización y de los avances tecnológicos, donde el almacenamiento y la clasificación de los datos es cada vez más importante, permite considerar la manipulación de dichos volúmenes de datos, lo cual trae consigo un alto grado de responsabilidad en seguridad, conservación y no duplicación, monitoreando siempre los riesgos que pueden presentarse.

Tabla de contenido

[Introducción 1](#_Toc161060707)

[1 Datos 4](#_Toc161060708)

[1.1 Clasificación 5](#_Toc161060709)

[1.2 Variable 5](#_Toc161060710)

[1.3 Analítica 8](#_Toc161060711)

[1.4 Normatividad 10](#_Toc161060712)

[1.5 Herramientas de análisis 11](#_Toc161060713)

[1.6 Big data 14](#_Toc161060714)

[1.7 Confidencialidad 17](#_Toc161060715)

[2 Sistemas de información 20](#_Toc161060716)

[2.1 “Software” malicioso 21](#_Toc161060717)

[2.2 Herramientas de seguridad 23](#_Toc161060718)

[2.3 Políticas de usuario 26](#_Toc161060719)

[2.4 Conservación de la información 27](#_Toc161060720)

[2.5 Gestión del sistema basado en riesgos 29](#_Toc161060721)

[Síntesis 34](#_Toc161060722)

[Material Complementario 35](#_Toc161060723)

[Glosario 37](#_Toc161060724)

[Referencias Bibliográficas 39](#_Toc161060725)

[Créditos 40](#_Toc161060726)

Introducción

La tecnología está presente en casi todos los rincones del mundo desde hace mucho tiempo, y en la actualidad presenta grandes niveles de sofisticación y costos de adquisición cada vez más bajos. La electricidad, el computador e incluso las telecomunicaciones avanzan a pasos agigantados y la ciencia de datos no es la excepción, debido al auge del tratamiento de millones de volúmenes de datos que implica una gran revolución en la sociedad. En el siguiente video se puede apreciar la importancia de la ciencia de datos en la toma de decisiones estratégicas empresariales.

El manejo de grandes volúmenes de información trae consigo también un alto grado de responsabilidad primero, porque la información no es propiedad de la empresa que gestiona los datos, sino de la persona directamente implicada, y segundo, porque la información mal utilizada puede ser robada, borrada o alterada, lo que afectaría su disponibilidad, veracidad y fidelidad, que pondrían en alto riesgo a los propietarios de esa información.

Por ejemplo, si la información etiquetada como confidencial por una empresa llegara a manos de su competidor, quedarían expuestos todos los registros de los clientes, las estrategias comerciales, los estados financieros y los datos de acceso a portales bancarios, lo que causaría pérdidas de negocios, clientes, demandas por exponer información confidencial, incluso, hasta el cierre de la compañía.

1. Introducción



Nota: tomado de https://stock.adobe.com

**Enlace de reproducción del video**

|  |
| --- |
| **Síntesis del video: Introducción** |
| Diariamente se convive con avances constantes en distintas áreas del conocimiento, y la información se convirtió en el insumo fundamental para el desarrollo.  La era de la web 2.0 fue una época decisiva para aquellas empresas y visionarios que lograron obtener beneficios de los datos que los usuarios dejaban registrados en todas las plataformas que navegaban.  Fenómeno que incrementó la oferta de diversas aplicaciones que solucionan necesidades o gustos de las personas a precio cero.  Mientras más se incrementaron los usuarios, más se incrementaron los datos que tenían ese valor oculto. Datos que por sí solos no dicen nada, pero que, al analizarlos, unirlos, crear variables y demás, se constituyen en información.  Es ahí donde toma importancia la ciencia de datos, debido a que el manejo adecuado de estos en tiempo real ayuda a predecir y posteriormente, a accionar eficazmente mediante soluciones frente a los problemas que surgen en diferentes áreas organizacionales como dirección, mercadeo, servicio al cliente, operación, logística, entre otros. En otras palabras, permite a los dirigentes tomar decisiones y plantear estrategias internas y externas que ayuden a un crecimiento organizacional eficiente.  Como conclusión el procesamiento de los datos que deriva en información, contribuye a mejorar la comunicación e interacción empresa-empleado-cliente. |

# Datos

Se denomina dato a cualquier objeto que pueda entregar información o significado para el lector. El dato puede ser manipulable en forma manuscrita o por medio de un computador, puede ser un carácter capturado desde un teclado, extraído de algún espacio de memoria en disco, almacenado en la memoria central, entre otras opciones. Los datos están conformados por algo más que números, pueden contener cualquier tipo de carácter bien sea alfabético, numérico, alfanumérico, símbolo especial, etc.

Ahora bien, para que estos puedan representar información y por ende, significado, deben pasar por una serie de procesos de emparejamiento o integración con los demás datos para entregar un mensaje, tal como se aprecia en el siguiente recurso.

Los datos deben ser clasificados y organizados para lograr una categorización en busca de determinar la importancia o estrategia a implementar en las empresas. El sistema de clasificación aportará eficazmente en definir las prioridades y la variedad de acciones que se deben realizar sobre el universo de datos recopilados, a su vez mejora la calidad de la información eliminando aquellos datos poco significativos.

La necesidad imperiosa de las empresas por crear una “cultura de datos” ha ido creciendo de manera acelerada a través del tiempo, dado que estas han comprendido el valor real que tienen en esa información. Muchas técnicas se han empezado a utilizar y están basadas en la seguridad de la información, el acceso transparente, la privacidad, la ética y la criticidad. Los pasos más comunes a seguir para clasificar los datos se pueden definir de esta manera:

## Clasificación

Los datos se pueden clasificar de acuerdo con su tipo y estructura, dependiendo en qué categoría estén se pueden manipular mediante operaciones aritméticas o lógicas que darán como resultado la información que se quiere entregar.

De acuerdo con el tipo de datos y su estructura se puede realizar una serie de operaciones básicas o aritméticas (si se quiere obtener un resultado de un conjunto de variables) y operaciones de comparación (si el resultado deseado es una respuesta lógica -verdadero o falso-). En cualquier caso, se pueden combinar los dos tipos de operaciones, siempre que la estructura del dato así lo permita, es decir, no se puede sumar un dato tipo entero con un dato tipo lógico o elevar a una potencia un dato real con un dato “string”. A continuación se describe en qué consiste cada una de estas operaciones.

## Variable

Es el nombre que se le da a una serie de caracteres con el fin de categorizar o interpretar de una forma más sencilla alguna información que se quiera estudiar, también pueden almacenar distintos tipos de datos: enteros, reales, matriciales, caracteres, etc. Las variables cuentan con instrucciones de asignación que sirven para almacenar ese valor del dato, por ejemplo, VARIABLE = EXPRESIÓN, donde el signo = significa “ALMACENAR EN”.

**Figura 1**. ejemplo de almacenamiento

En la figura 1 muestra como hace una variable para almacenar un dato.
Nota: Figura alternativa


Nota. Tomada de <https://www.freepik.es>

Las variables se pueden clasificar según el nivel de medida y según su influencia. Según su nivel de medida se pueden subdividir en cualitativas y cuantitativas, y según su influencia, pueden ser independientes o dependientes.

Variable según su nivel de medida

1. **Variables cualitativas:** son las variables que expresan características y/o cualidades. Cada cualidad que se presente se denomina atributo o categoría. Las variables cualitativas pueden ser dicotómicas, es decir, solo toman dos valores, como falso o verdadero, sí o no, alto o bajo, hombre o mujer, etc., o también puede ser politómicas cuando pueden tomar tres o más valores, y se subcategorizan en ordinal y nominal.
2. **Variable cualitativa ordinal:** toman distintos valores ordenados de acuerdo con una escala predefinida, donde no es necesario que los intervalos de medición sean uniformes, por ejemplo, regular, bueno, excelente
3. **Variable cualitativa nominal:** los valores de las variables indican una categoría o atributo y no necesariamente debe ser ordenable, como por ejemplo, nacionalidad, color de piel, religión.
4. **Variables cuantitativas:** son las variables que se pueden expresar a través de cantidades numéricas, se categorizan como variables matemáticas. Las variables cuantitativas se pueden subcategorizar en discreta y continua.
5. **Variable discreta:** es la variable que presenta valores enteros, no presenta interrupciones en su escala de valor, por ejemplo, el número de hijos (1, 2, 3, 4, 5), cantidad de dedos de la mano (1, 2, 3, 4, 5).
6. **Variable continua:** es la variable que puede tomar un número infinito de valores entre dos valores aleatorios de una característica, por ejemplo, la altura de 3 amigos (1,74 m, 1,85 m, 1,92 m).

Variable según su nivel de influencia

1. **Variable independiente:** su valor no depende de otra variable. Es la característica que supone es la causa del fenómeno estudiado. Es la variable que determina el valor de la variable dependiente. En el plano cartesiano se ubica en el eje de las X o eje de abscisas, y se le asignan valores arbitrarios.
2. **Variable dependiente:** su valor depende de los valores que tome la variable independiente. Es la característica que supone el efecto del fenómeno de estudio. En el plano cartesiano se ubica en el eje de las Y o eje de ordenadas, y se le asignan valores arbitrarios y toma valores como resultado de los valores arbitrarios de la variable independiente.

## Analítica

En la actualidad existen procesos en las empresas que requieren ser optimizados y estos a su vez deben reflejar el análisis de la producción; de este modo, se puede realizar la comparación entre actividades realizadas por personas vs. las realizadas por las máquinas, teniendo como resultados conclusiones en cuanto a tiempo, desempeño y calidad de entrega del producto final. También permite conocer en qué épocas del año es más rentable producir cierto bien o servicio, para así estimar el tiempo de inicio de su producción.

De esta forma si se quiere vender productos para el día de la madre es conveniente revisar cuál es el más vendido. Se puede identificar si los electrodomésticos ya no son tan importantes en estas fechas, si las madres prefieren rosas o visitar un restaurante, o si por el contrario prefieren celebrar en casa con una comida especial, además sería conveniente tener los datos de cuántas madres han fallecido en el año anterior y cuántas personas pasan ese día visitando a su ser querido en el cementerio, así se puede obtener la certeza sobre qué producto ofrecer y el lugar óptimo para vender.

Todos los datos representan tendencias que ayudan e inciden en las condiciones del mercado. Cuando se sabe que hay un producto escaso o existen necesidades insatisfechas surge una posibilidad en el mercado para las empresas.

En la analítica de datos se pueden encontrar diversos procesos que buscan dar respuesta en tiempo y alcance a las situaciones que se presentan en el día a día. Existen diferentes tipos de análisis que se pueden realizar, entre los que se destacan:

**Figura 2.** tipos de análisis

Figura . Muestra los tipos de análisis de datos.
Nota: Figura Alternativa

Nota. Tomada de <https://www.freepik.es>

Tipos de Análisis

* **Análisis exploratorio:** somete los datos a un proceso de investigación con tratamiento estadístico de resumen y representaciones gráficas, para conocer los datos y comprender qué se puede explorar con estos
* **Análisis descriptivo:** explora los datos a través de una aproximación de análisis desde su descripción y diferentes perspectivas, sin una hipótesis previa para saber qué sucedió.
* **Análisis predictivo:** permite a través de análisis de datos predecir valores o respuestas a eventos que se estén estudiando.
* **Análisis prescriptivo:** Ofrece evaluación a decisiones en escenarios que generan un resultado positivo a futuro.

## Normatividad

En Colombia las normas asociadas a la explotación de datos surgen por diferentes necesidades y objetivos, que requieren un alcance que no está directamente relacionado con la aplicabilidad del “big data”; sin embargo, es importante conocer que existen normas, decretos y leyes que respaldan y protegen la explotación de los datos.

En el CONPES 3920 - Marco de la Política Nacional de Explotación de Datos el desarrollo de marcos normativos y políticas públicas se adaptan a todos los avances tecnológicos y responden de manera pertinente a los requerimientos de la sociedad; es por ello, que se ha convertido en una necesidad imperiosa el aprovechamiento óptimo y eficiente de los datos, que generan beneficios para todas las entidades cumpliendo con los requisitos de transparencia, divulgación de información y toma de decisiones.

El marco jurídico aplicable en Colombia para el aprovechamiento y recolección de datos está regido por la siguiente normativa.

La cantidad de datos que las entidades públicas recolectan y/o generan requieren la implementación de una adecuada gestión de la información para asegurar la protección, almacenamiento y acceso de los mismos.

## Herramientas de análisis

El análisis de datos es un proceso que permite obtener conocimiento de la información subyacente de los datos, con el propósito de extraer conclusiones que contribuyan a tomar decisiones informadas. Sin la analítica de datos, empresas y organizaciones se encuentran limitadas a la hora de examinar sus resultados y determinar la dirección a seguir para tener mayores probabilidades de éxito.

Existen herramientas que no implican realizar tareas de programación, dirigidas a usuarios sin conocimientos técnicos avanzados, y herramientas que presentan una mayor versatilidad, pero necesitan el manejo de lenguajes de programación, por lo que están dirigidas a usuarios con estos conocimientos

A continuación, se describen las herramientas de análisis de datos para no programadores.

1. **Weka**: Es una plataforma de “software” libre desarrollado por la Universidad de Waikato (Nueva Zelanda), que sirve para desarrollar minería de datos y aprendizaje automático mediante herramientas integradas de preparación, clasificación, regresión, agrupación, minería de reglas de asociación y visualización de datos. Weka está escrito en Java y se puede descargar en el siguiente enlace: https://www.cs.waikato.ac.nz/ml/weka/.
2. **Knime**: es una plataforma para minería de datos que permite desarrollar modelos en un entorno gráfico. El “software” permite crear mediante mezcla, transformación, modelación y visualización de los datos de manera gráfica, también permite la producción para implementar, administrar, consumir e interactuar con todo el volumen de datos recopilados.

KNIME tiene una versión de prueba que puede descargarse en: <https://www.knime.com/downloads>.

1. **Orange**: es un programa de código abierto que permite realizar minería de datos y análisis predictivo desarrollado por la Universidad de Ljubljana (Eslovenia). Permite crear flujos de trabajo de análisis de datos visualmente con una caja de herramientas grande y diversa. ORANGE puede descargarse en https://orangedatamining.com/ .

Ahora se expondrán las herramientas de análisis de datos para programadores.

1. **R (The R Project for statistical computing):** es un entorno de “software” libre para computación estadística y gráficos. Es unos de los lenguajes más populares, debido a que cuenta con una amplia gama de librerías que incrementan sus funcionalidades. La comunidad de R-Studio mantiene actualizaciones constantes y respaldo continuo. R puede ser descargado gratuitamente en https://www.r-project.org/.
2. **Python:** es un lenguaje de alto nivel de programación interpretado, permite un trabajo rápido e integración de sistemas de manera eficaz. Python tiene una gran variedad de bibliotecas que permiten el desarrollo de análisis de datos, “machine learning” e inteligencia artificial de una manera sencilla, logrando explotar al máximo la información recopilada. Python es un “software” de código abierto y puede descargarse en la página oficial https://www.python.org/.
3. **GNU Octave:** es un programa y lenguaje de programación que permite realizar cálculos numéricos. GNU Octave es considerado el equivalente de “software” libre de MATLAB. Presenta una sintaxis orientada a las matemáticas con herramientas de visualización y trazado 2D/3D, y se ejecuta GNU/Linux, macOS, BSD y Microsoft Windows. Por ser “software” libre se puede descargar una versión en su página oficial https://www.gnu.org/software/octave/index.
4. **Microsoft Power BI:** es una herramienta desarrollada por Microsoft que permite el análisis de datos, proporcionando visualización gráfica en el campo del “business intelligence”. Una de las grandes ventajas de Power BI es su integración con libros de Excel, lo cual permite ampliar el marco de trabajo desde lo más básico hacia lo más avanzado, además de tener un tablero de trabajo colaborativo para el seguimiento de objetivos personales y grupales. Por ser desarrollado por Microsoft no es de versión libre, pero se puede descargar una versión de prueba en https://powerbi.microsoft.com/es-es/.
5. **SAS:** es un “software” de solución para el análisis de datos. Permite explorar, analizar y visualizar datos independientemente de su fuente. SAS es muy usado en aplicaciones de redes sociales, “Web”, “marketing” digital que permite realizar o perfilar tipos de clientes para lograr predecir sus gustos y comportamiento de consumo. Se puede obtener una versión de prueba en https://www.sas.com/es\_co/home.html#.
6. **Excel:** es un “software” de hoja de cálculo desarrollado por Microsoft. Excel aprende patrones y organiza datos para el ahorro de tiempo. Permite el trabajo colaborativo en línea, presenta los datos de una forma convincente, con formato, minigráficos y tablas para una mejor interpretación y visualización. Quizá, la función más importante es su integración con Power BI. Por ser desarrollado por Microsoft no es versión libre, pero se puede descargar una versión de prueba para el hogar o la empresa en https://www.microsoft.com/es-es/microsoft-365/excel .

## Big data

El desarrollo de las Tecnologías de la Información y la Comunicación (TIC) y el aumento de la cobertura de Internet ha facilitado que en los últimos años se generen datos de manera exponencial y en diversas fuentes de información. El volumen, la velocidad y la variedad de los datos generados en este contexto inicialmente fue un reto tecnológico; pero con la aparición de nuevas técnicas y formas de almacenamiento, procesamiento, análisis y visualización se crearon las condiciones para aprovechar su potencial. Por medio de la datificación las elecciones de consumo, las preferencias individuales, colectivas y los aspectos de la vida diaria se han transformado en datos.

El reto actual para los distintos gobiernos y organizaciones privadas consiste en reducir las barreras de tipo técnico, jurídico y organizacional que disminuyen el aprovechamiento de los datos para generar valor social y económico. En ese contexto los datos se han convertido en uno de los activos más importantes para el sector público en la medida en que aportan beneficios para tomar decisiones informadas. La adecuada gestión de los datos a lo largo de todo su ciclo de vida, desde su recopilación o generación, clasificación, almacenamiento, uso, compartición y reutilización, conlleva a extraer el valor de estos para crear un análisis descriptivo, predictivo o prescriptivo que permita diseñar nuevas estrategias, analizar con un enfoque más amplio problemáticas de carácter público y tomar decisiones.

En el contexto actual uno de los habilitadores para la transformación digital es la explotación de los datos para aumentar el valor público de las entidades, de cara a la prestación de bienes y servicios para los ciudadanos.

En el sector público la explotación de datos suele referirse al uso de fuentes de datos no tradicionales y a las innovaciones en materia de datos, para que las soluciones gubernamentales tengan más capacidad de respuesta y sean más eficaces. Las entidades públicas tienen la oportunidad de aprovechar soluciones basadas en el “big data” para mejorar su productividad y reducir costos administrativos. Hoy el manejo de grandes bases de datos es una cuestión apremiante, especialmente en un momento en que muchos están preocupados por el papel de la información en las decisiones políticas. En el contexto actual, las entidades gubernamentales tienen que actuar como productoras, consumidoras y facilitadoras del “big data” (“World Bank Group”, 2017, citado en DNP, 2020).

El “big data” es un fenómeno que se caracteriza por la generación de grandes volúmenes de datos, en diversas fuentes de información y a una rápida velocidad en su generación. El siguiente video desarrolla un poco más en qué consiste.

1. **“Big data”**



Nota: tomado de https://stock.adobe.com

**Enlace de reproducción del video**

|  |
| --- |
| **Síntesis del video: “**Big data” |
| El “big data” es un sistema sociotécnico para la explotación masiva de datos que requiere, sobre todo sobre todo en las entidades públicas, la disponibilidad de recursos tecnológicos para enfrentar los retos de procesamiento, el diseño y la ejecución de estos, que permitan la replicabilidad y la sistematización de la explotación de datos y el recurso humano para ejecutarlos.  La explotación de datos, entonces, es el proceso mediante el cual se analizan datos de diversas fuentes de información y en distintos formatos para descubrir patrones y relaciones entre ellos, lo que permite extraer el valor de los datos para brindar una solución a una problemática específica.  Una adecuada explotación de datos requiere considerar su ciclo de vida, en el cual se presenta el paso a paso para su tratamiento, y el cual facilita la definición de técnicas para gestionar el volumen con el que se generan y capturan los datos, teniendo en cuenta, además, los aspectos legales relacionados con la creación o captura de datos, almacenamiento, transferencia, uso, explotación y conservación.  El “big data” y su explotación de datos permite generar información valiosa para todo tipo de entidades que busquen tomar decisiones acertadas  de acuerdo con sus necesidades. |

## Confidencialidad

Una gobernanza de datos implementada de manera efectiva facilita el cumplimiento de la normatividad vigente en Colombia, en la medida en que se identifican roles y responsables para acceder a los datos se clasifican, organizan y documentan; luego, se definen de manera clara mecanismos de acceso para su uso y compartición y finalmente, se gestionan los riesgos relacionados con la confidencialidad y protección de la información.

Todas las personas que intervengan en el tratamiento de datos personales que no tengan la naturaleza de públicos están obligadas a garantizar la reserva de la información, inclusive después de finalizada su relación con alguna de las labores que comprende el tratamiento, pudiendo solo realizar suministro o comunicación de datos personales cuando ello corresponda al desarrollo de las actividades autorizadas.

Ahora bien, dentro de ese vínculo la privacidad desde el diseño busca garantizar un correcto tratamiento de los datos en los procesos de inteligencia artificial, incluso antes de la materialización de los riesgos. Lo anterior conduce a que se use la privacidad como un factor relevante del diseño, la arquitectura de “software” o el algoritmo para fomentar el uso adecuado del tratamiento de los datos, porque la confidencialidad dentro del ciclo de vida del producto busca convertirse además en un modo de operación predeterminado para las organizaciones, en el que antes de recolectada la información se puedan adoptar medidas preventivas de diversa naturaleza que eviten fallas de seguridad, vulneración en los derechos de privacidad y confidencialidad, y el uso indebido del tratamiento de datos personales.

Las medidas adoptadas para asegurar el tratamiento de los datos en la inteligencia artificial deben cumplir con los siguientes objetivos.

1. Objetivos de tratamiento de datos

Nota: Se sugiere que esta gráfica sea una figura, tiene información relevante.



Nota: tomado de https://www.freepik.es/vector-gratis/ilustracion-concepto-extraccion-datos\_12079896.htm#query=data&position=26&from\_view=search

Objetivos de tratamiento de datos

* Evitar los accesos no autorizados a la información.
* Evitar la manipulación de la información.
* Evitar la destrucción de la información.
* Evitar los usos indebidos de la información.
* Evitar el suministro de información a personas no autorizadas

Cuando las medidas siguen estos objetivos se puede establecer un tratamiento debido a los datos personales desde cualquier perspectiva o naturaleza de los datos, a pesar que dentro del desarrollo de las tecnologías, “software” y algoritmo del sistema de información de la inteligencia artificial se presenten unos riesgos que influyen sobre la planificación en el tratamiento de los datos o sistemas de información.

Por ejemplo, dentro de la operación del algoritmo se pueden producir sesgos humanos o fallas técnicas en la implementación. A través de estas medidas se podrán controlar y evaluar los riesgos desde la normativa para que no afecten el tratamiento de los datos y no se vulneren los derechos de los titulares de los datos y se puedan proteger los mismos (Red Iberoamericana de Protección de Datos, 2019, citado en DNP, 2020).

En la actualidad, al realizar alguna investigación se obtienen grandes cantidades de datos debido a la medición de variables, que sin el uso de la tecnología es casi imposible su manipulación, estudio y análisis. Es por ello que un análisis eficiente de los datos aporta de manera significativa a estrategias que permiten crear soluciones a las diferentes problemáticas de las empresas, de los países y del mundo. Pero lo más importante es que la depuración eficiente y el análisis predictivo de una situación en concreto que se pueda medir contribuye a evitar sus consecuencias, aplicando acciones preventivas de acuerdo con las conclusiones que puedan derivarse del análisis de los datos.

# Sistemas de información

Las medidas de seguridad de la información son indispensables en cualquier empresa. Como uno de los activos más valiosos es la información, es importante tener claridad que día a día se ven diferentes ataques y vulnerabilidades que amenazan la confidencialidad de los datos en las empresas.

La seguridad en la información ha cobrado importancia en los últimos años; en el tema de calidad se han estandarizado los procesos y en la seguridad informática y de la información se han implementado algunos controles y planes, tal como se explica a continuación.

Con el advenimiento de la Norma ISO 27000 aparecen los conceptos de Gestión en Sistemas de Seguridad Informática y de la Información (SGSI), aprovechando las nuevas tecnologías y los sistemas de información, y junto a ellos se alinean otros estándares que hasta el momento habían sido aplicados al análisis de riesgos informáticos y que, posteriormente, han sido usados para la gestión de riesgos de seguridad de la información

El concepto clave de un SGSI es el diseño, implantación y mantenimiento de un conjunto de procesos para gestionar eficientemente la accesibilidad de la información, buscando asegurar los activos de información, el valor más importante en una organización, minimizando a la vez los riesgos de seguridad de la información: integridad, confidencialidad y disponibilidad.

En la actualidad, la mayor parte de la información reside en servidores, redes de información y almacenamientos como la nube, los discos extraíbles y “backups”, enmarcados dentro de lo que se conoce como sistemas de información. Dichos sistemas de información están sujetos a vulnerabilidades, ataques informáticos, riesgos e inseguridades, tanto dentro de la propia organización como desde fuera.

## “Software” malicioso

Más conocido como malware, es un “software” diseñado por un tercero con la única finalidad de obtener acceso no autorizado a un equipo para robar información o simplemente dañarlo. En la actualidad existen diferentes tipos de malware: spyware, registradores de pulsaciones, virus, gusanos, etc. En el siguiente video se explica en qué consiste este tipo de “software” y cómo se puede evitar en un inicio.

1. **“Software” Malicioso**



Nota: Tomada de https://stock.adobe.com/co/images/id/276609005?as\_audience=idp&as\_campaign=Freepik&get\_facets=1&order=relevance&safe\_search=1&as\_content=api&k=hackers,%20cyber%20attack&filterscontent\_typezip\_vector=1&tduid=b3bae388e2ce7c63a2cd50b418087c40&as\_channel=affiliate&as\_campclass=redirect&as\_source=arvato

Enlace de reproducción del video

|  |
| --- |
| **Síntesis del video:** “Software” Malicioso |
| Malware es un término genérico utilizado para describir una variedad de software hostil o intrusivo, que prolifera rápidamente, dada la constante creación de nuevos tipos de ataques cibernéticos.  Inicialmente, el malware se creó a manera de entretenimiento, pero luego evolucionó al vandalismo y destrucción de equipos.  Hoy en día, la mayoría de malwares son creados para ganar dinero mediante extorsión (“ransomware”), publicidad forzada (publicidad no deseada), difusión de spam o pornografía por correo electrónico (equipos zombis) o robo de información confidencial (“spyware”).  Junto al crecimiento de estos “software” aumentan sus víctimas muchas veces por desconocimiento.  Diversos factores pueden hacer que un equipo sea más vulnerable a ataques de malware, como no contar con la licencia de un antivirus confiable, desactualización de la base de datos del antivirus y sistemas operativos, defectos en el diseño del sistema operativo, equipos conectados a una red que estén ejecutando el mismo sistema operativo, entre otros.  Por tanto, la mejor forma de protegerse contra el malware es sin lugar a dudas ser cautelosos, no confiar en correos de remitentes no conocidos, no ejecutar archivos adjuntos de correo electrónicos no deseados, mantener actualizado el antivirus, no navegar por páginas poco confiables, descargar los programas que serán instalados en el computador de sitios confiables y mantener actualizadas las bases de datos y las mejoras del sistema operativo.  El riesgo más considerable para una organización, ante una exposición a malware, es la pérdida de control de la información. |

## Herramientas de seguridad

La seguridad informática y la seguridad de la información están encargadas de proteger los datos contra robo de información, acceso no autorizado, obstaculización al sistema informático, manipulación y/o eliminación de datos. Cuando se habla de procesos empresariales impulsados en la transformación digital con tecnología de punta se entiende que están expuestos a diferentes vulnerabilidades, amenazas y ataques informáticos dirigidos a la seguridad y la privacidad de la información. Mediante la Norma ISO 27001, la implementación del SGSI sigue el modelo Planificar – Hacer – Verificar – Actuar para la mejora continua de los procesos.

Sin embargo, la seguridad para las empresas es un tema cada vez más crítico y de preocupación constante, debido a que los ciberataques pueden ser tan catastróficos como un robo, explosión o un incendio. Para prevenir estos ataques informáticos se hace necesario el uso de una poderosa infraestructura de TI que ayude a detectar y frenar amenazas.

**Herramientas de seguridad**

1. **“Software” antivirus:** todos los computadores que estén conectados a una red interna o a Internet deben contar con un antivirus gratuito o pago, pero que sea confiable. Estos programas permiten contar con medidas de protección efectivas cuando el equipo se encuentre expuesto a “software” malicioso o a cualquier otro tipo de malware. Estos programas ofrecen la oportunidad de eliminarlo por completo o poner en estado de cuarentena.

Kaspersky, Avast, Nod32, McAfee, son algunas de las posibilidades que se pueden encontrar en el mercado actual; lo más importante es que cualquier solución de antivirus en la que el usuario quiera confiar debe tener la certeza que se adapte a las necesidades de seguridad y cuentan con actualizaciones constantes, debido a que los malware están en continua evolución.

1. **Firewall perimetral de red:** como su nombre lo indica, hace la función de una pared de bloqueo. Es un sistema cuya función es prevenir y protegerlo privado de ataques de otras redes.

Su funcionamiento es sencillo: escanea los paquetes de red, permitiéndoles o bloqueándolos según las reglas definidas por un administrador.

1. **Servidor “proxy”:** un “proxy” es un es un servidor, puede ser un programa o dispositivo físico, que actúa de intermediario entre conexiones del navegador e Internet, filtrando todos los paquetes entre ambos.

Asimismo, establece un sistema de autentificación, que limita el acceso a la red externa, por lo cual, se pueden generar los registros sobre sitios, visitas y demás datos de navegación.

1. Cifrado de punto final o “end point disk encryption”: Es un proceso de codificación de datos para que no pueda ser leído o utilizado por nadie que no tenga la clave de descifrado correcta.

En esencia, protege los sistemas operativos de la instalación de archivos de arranque corruptos, bloqueando los archivos almacenados en computadores, servidores, entre otros puntos finales

1. **Escáner de vulnerabilidades:** Es una de las herramientas de seguridad en sistemas informáticos fundamentales en las empresas de cualquier tamaño. Consiste en un “software” que se encarga de detectar, analizar y gestionar los puntos débiles del sistema.

Gracias a esta plataforma se puede mantener controlada la exposición de los recursos empresariales a las amenazas de ciberseguridad y sus posibles consecuencias. Además, permite alertar en tiempo real, lo que ayuda a la solución de problemas de forma oportuna y sin comprometer la continuidad del negocio.

## Políticas de usuario

Cuando una empresa está interesada en realizar un sistema exhaustivo de gestión de seguridad de la información debe iniciar documentando procesos y conociendo cómo opera la misma, también debe revisar el manual de funciones de cada empleado; esto es fundamental al empezar a aplicar el ciclo PHVA.

Asimismo, se hace necesario conocer los procesos digitales críticos en la organización, luego detalladamente, analizar toda la información para implementar controles que puedan proteger los procesos implementados ante amenazas cibernéticas, las cuales se podrán detectar si son de carácter interno o externo.

Las amenazas que están en Internet no son la causa de un ser humano con intenciones maliciosas, si no de los mismos empleados, que al no estar capacitados pueden descargar programas que vienen con troyanos o sin intención maliciosa que pueden mover un directorio o archivo.

De ahí la importancia de revisar también las políticas de usuario por el departamento TI de la organización, las cuales describen y establecen las reglas o requisitos que se deben tener en cuenta en los distintos procedimientos de uso en las cuentas del sistema de información de la empresa, entre ellas se encuentran las siguientes:

* **Proteger los equipos:** mantener actualizado el sistema operativo y el antivirus es fundamental porque corrigen agujeros de seguridad.
* **No descargar contenido pirata:** descargar música, libros, películas, videos, “software” de sitios recomendables, siempre tener cuidado con páginas poco conocidas.
* **Evitar dar datos personales:** mantener la cautela y desconfianza en redes sociales, no compartir datos con contactos o perfiles sospechosos, no aceptar sugerencias o amigos no conocidos.
* **Realizar una copia de seguridad:** es importante no depender de una sola fuente de información, es recomendable tener copia de respaldo de nuestro equipo, algún disco duro externo o en la nube.
* **Contraseñas fuertes:** números consecutivos, fechas de cumpleaños, nombre de nuestros hijos, equipo de fútbol favorito, son ejemplos de contraseñas poco seguras.

Se recomienda usar contraseñas cambiando letras mayúsculas y minúsculas, números y caracteres especiales, por ejemplo, AbgDho-9823\*#.

* **Utilizar protocolos de seguridad:** colocar una clave de acceso al computador o servidor, generar cuentas de usuario con contraseñas para equipos compartidos y bloquear el equipo cuando no se esté en frente de él, son buenos protocolos de seguridad.

## Conservación de la información

De acuerdo con los nuevos requerimientos de la administración pública derivadas de la Ley de Transparencia, Ley de Protección de Datos y Ley General de Archivos, nace la necesidad de crear una directriz que permita a las entidades garantizar la accesibilidad y perdurabilidad de la información digital. De este modo, se genera el uso de diversos formatos y medios de almacenamiento digital, también surgen nuevas formas de buscar y analizar la información.

La preservación digital de acuerdo con el Archivo General de la Nación (2018) aplica al documento electrónico de archivo de naturaleza digital con su medio correspondiente en cualquier etapa de su ciclo vital. Esta forma parte de los procesos de la gestión documental, específicamente del proceso de preservación a largo plazo e implica el establecimiento de acciones desde la planeación de la gestión documental hasta la disposición final de los documentos, tal como lo presenta el siguiente recurso.

**Procesos de Gestión Documental-valoración**

1. **Planeación:** está conformada por todas aquellas actividades administrativas que permiten la adecuada revisión y valoración de toda la información documental, teniendo en cuenta el contexto legal, técnico y funcional de la empresa.
2. **Producción:** se evalúan todos los documentos de la empresa, desde su creación, ingreso y categorización, sin olvidar su relevancia y funcionalidad en todos los procesos administrativos.
3. **Gestión y Trámite:** se analizan los documentos con base en su incidencia en los procesos internos y externos de la empresa. Es en este tercer paso se revisan a profundidad todos los trámites por los que debe pasar dicho archivo o documento.
4. **Organización:** se abarcan todas las operaciones técnicas de gestión documental. Se establecen los elementos de categorización, serie documental, valorización, tiempo de almacenamiento, departamento al que pertenece, tipo de archivo, entre otros.
5. **Transferencia**: aquí se implementan las políticas de transferencia a los documentos en su fase de archivo.
6. **Disposición de Documentos:** Aquí se consideran todos los procesos de selección y valoración del archivo o documento, todo en beneficio de su conservación. La adecuada disposición de documentos permite el seguimiento de todos los ciclos de vida de cada archivo, con el único fin de darle un tratamiento eficaz, lo que además sirve, posteriormente, para establecer los protocolos de seguridad para su eliminación y destrucción.

**Procesos de Gestión Documental- Preservación a largo Plazo**

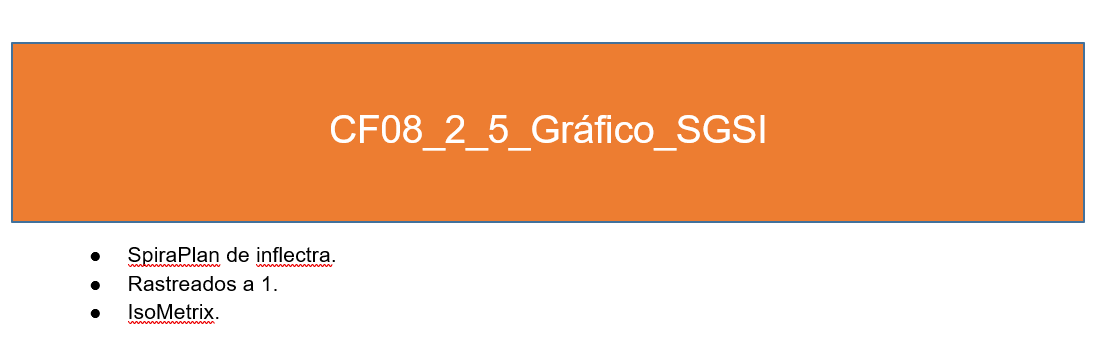
1. **Planeación:** se identifican todos los procedimientos y requerimientos que se deben llevar a cabo durante todo el procedimiento de gestión documental, de manera que se pueda garantizar su preservación a largo plazo.

## Gestión del sistema basado en riesgos

La valoración del riesgo asegura que el SGSI logre los efectos previstos, donde con las mismas herramientas se puede prevenir o reducir efectos indeseados, logrando la mejora progresiva, integrando e implementando acciones en los procesos del sistema de gestión de la seguridad de la información. El siguiente recurso presenta visualmente el SGSI y la gestión del riesgo.

* Establecer el contexto, evaluar el riesgo y planificar el tratamiento.
* Implementar el plan de tratamiento del riesgo.
* Monitorear y revisar continuamente los riesgos
* Mantener y mejorar el proceso de gestión del riesgo en la seguridad de la información.

Nota Revisar la lista no concuerda con el orden lógico del CF



* SpiraPlan de inflectra.
* Rastreados a 1.
* IsoMetrix.

En la identificación de riesgos se debe recordar que la inseguridad se enuncia en procesos de la composición de los resultados de un suceso y la probabilidad de ocurrencia asociada. A continuación, se presentan las posibles fuentes de riesgos y consecuencias que pueden traer a la seguridad de la información de la organización.

1. Riesgos y consecuencia de SGSI

Nota: Se sugiere que esta gráfica sea una figura, tiene información relevante.



Nota: tomada de https://www.freepik.es/vector-gratis/ilustracion-concepto-informe-datos\_6195525.htm#&position=3&from\_view=detail#query=a&position=3&from\_view=detail

**Fuentes de Riesgos**

* Legales.
* Comportamiento humano (interno y externo).
* Comerciales.
* Economía y mercado.
* Circunstancias políticas
* Tecnología.
* Eventos naturales.
* Organizacionales.

**Posibles Consecuencias**

* Pérdidas de confidencialidad.
* Integridad.
* Disponibilidad.
* No-repudio.
* Autenticidad.
* Confiabilidad de los activos.
* Incumplimiento de la legislación.
* Pérdidas financieras.
* Impacto de orden público.
* Impacto de orden internacional.

El impacto, por su parte, es la capacidad de saber el estado real de seguridad de un activo antes y después de materializar las amenazas. En un SGSI al concretarse una amenaza el activo cambia de estado, es decir, antes de producirse la amenaza se tiene un valor al activo y después que se efectúe la amenaza se tiene la diferencia entre el estado anterior y el posterior a la amenaza. Se clasifica según el tipo de impacto como:

Suelen medirse de acuerdo con el impacto económico que este pueda causar.

1. Clasificación de del impacto SGSI

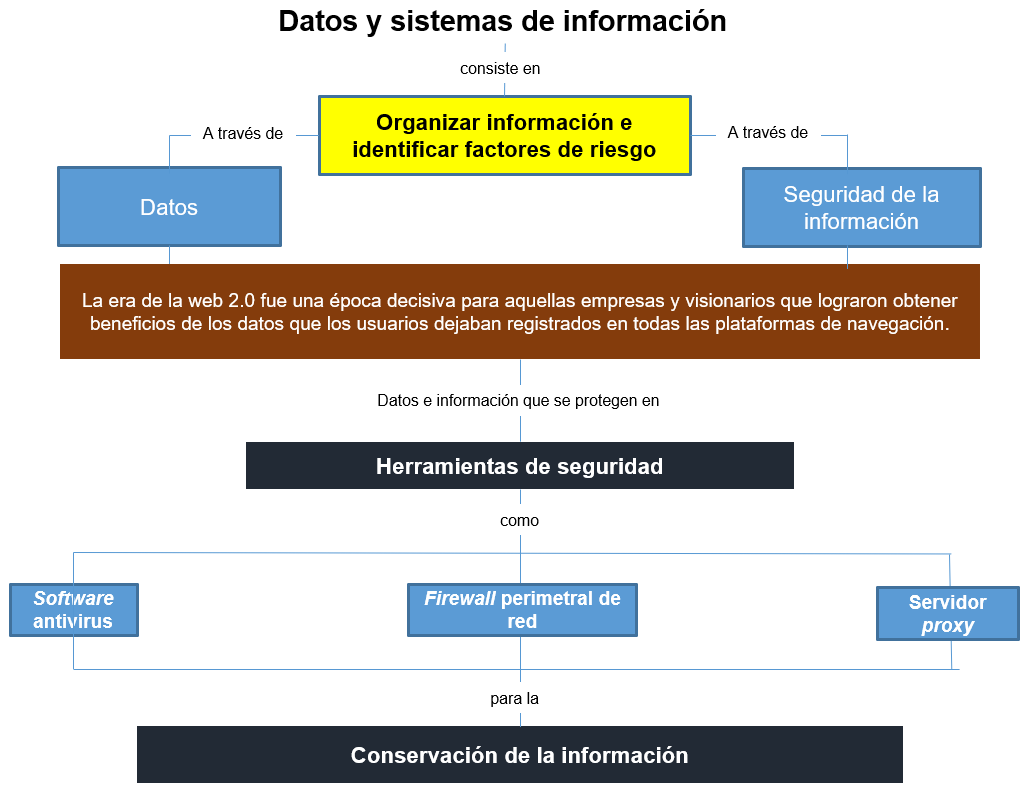
|  |  |
| --- | --- |
| Impacto Económico | Valor |
| Extremo | Menos de 1000 euros |
| Importante | Menos de 10000 euros |
| Moderado | Menos de 100000 euros |
| Menor | Menos de 1000000 euros |
| Incidental | Menos de 10000000 euros |

Nota: cada clasificación se puede crear o dar, dependiendo el tamaño de la organización y el valor podría darse en un rango de 0 a 5.

Ahora bien, adicional a todo lo anterior, en la era de la cuarta revolución industrial las organizaciones migraron al teletrabajo, “home office” y nacieron consigo conceptos como nómadas digitales, donde un trabajador desde cualquier parte del mundo puede cumplir con sus obligaciones y funciones contractuales, generando nuevos riesgos organizacionales, por lo que es fundamental el análisis constante del mercado y sus tendencias para blindarse de la fuga de información y de posibles ataques cibernéticos.

Síntesis

Identificar, organizar y sistematizar datos masivos, de acuerdo con métodos de analítica y herramientas tecnológicas le permite a una organización tomar decisiones estratégicas en su diario operativo. Es por ello que su sistema de información y la gestión del mismo deben garantizar no solo la confiabilidad del procesamiento, sino la alineación con la normativa y políticas establecidas para la seguridad y uso del tratamiento de la información. El siguiente gráfico presenta una síntesis de lo desarrollado en este componente.



|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | Nombre | Cargo | Dependencia  *(Para el SENA indicar Regional y Centro de Formación)* | Fecha |
| Autor (es) | Abel Fernando Becerra Carrillo | Experto temático | Regional Norte de Santander - Centro de la Industria, la Empresa y los Servicios | Abril de 2022 |
| Miroslava González Hernández | Diseñadora y evaluadora instruccional | Regional Norte de Santander - Centro de la Industria, la Empresa y los Servicios | Mayo de 2022 |
| Silvia Milena Sequeda Cárdenas | Asesora metodológica | Regional Distrito Capital - Centro de Diseño y Metrología | Mayo de 2022 |
| Rafael Neftalí Lizcano Reyes | Responsable Equipo de desarrollo curricular | Regional Santander – Centro Industrial del Diseño y la Manufactura | Mayo de 2022 |
|  | Julia Isabel Roberto | Correctora de estilo | Regional Distrito Capital - Centro de Diseño y Metrología | Mayo de 2022 |

Material Complementario

|  |  |  |  |
| --- | --- | --- | --- |
| **Tema** | **Referencia** | **Tipo de material** | **Enlace del recurso** |
| “Big data  ” | Dawn, H. & Otero-Piñeiro, D. (2018). *Big data: una breve introducción*. Antoni Bosch Editor. <https://sena-primo.hosted.exlibrisgroup.com/permalink/f/1j5choe/sena_elibroELB122682> | Libro | <https://sena-primo.hosted.exlibrisgroup.com/permalink/f/1j5choe/sena_elibroELB122682> |
| “Big data” | Spain BS. (2015). *Webinar "big data para dummies*" [video]. YouTube. <https://www.youtube.com/watch?v=fZhpLdZx5Qg&ab_channel=SpainBS> | Video | <https://www.youtube.com/watch?v=fZhpLdZx5Qg&ab_channel=SpainBS> |
| Sistemas de información | Instituto Colombiano de Normas Técnicas y Certificación. (2014). *Tecnología de la información: técnicas de seguridad. Gestión de incidentes de seguridad de la información.* ICONTEC. <https://sena-primo.hosted.exlibrisgroup.com/permalink/f/q6j6k0/sena_aleph000075887> | Libro | <https://sena-primo.hosted.exlibrisgroup.com/permalink/f/q6j6k0/sena_aleph000075887> |
| “Software”malicioso | Razak, M., Anuar, N., Salleh, R. & Firdaus, A. (2016). The rise of “malware”: bibliometric analysis of malware study. *Journal of network and computer applications* (75), p. 58-76. <https://sena-primo.hosted.exlibrisgroup.com/permalink/f/1i756fj/TN_cdi_gale_infotracacademiconefile_A518245030> | Artículo | <https://sena-primo.hosted.exlibrisgroup.com/permalink/f/1i756fj/TN_cdi_gale_infotracacademiconefile_A518245030> |

Glosario

**“Big data”:** fenómeno que se caracteriza por la generación de grandes volúmenes de datos en diversas fuentes de información y a una rápida velocidad en su generación. Es un sistema sociotécnico para la explotación masiva de datos, que requiere en las entidades públicas la disponibilidad de recursos tecnológicos para enfrentar los retos de procesamiento, el diseño y ejecución de procesos que permitan la replicabilidad y la sistematización de la explotación de datos y el recurso humano para ejecutarlos.

**Datos**: se denomina dato a cualquier objeto que pueda entregar información o significado para el lector. El dato puede ser manipulable en forma manuscrita o por medio de un computador. Puede ser un carácter capturado desde un teclado, extraído de algún espacio de memoria en disco o almacenado en la memoria central.

**Seguridad de la información:** es la encargada de proteger los datos contra robo de información, acceso no autorizado, obstaculización al sistema informático, manipulación y/o eliminación de datos. Cuando se habla de procesos empresariales impulsados en la transformación digital con tecnología de punta se entiende que están expuestos a diferentes vulnerabilidades, amenazas y ataques informáticos dirigidos a la seguridad y la privacidad de la información. Mediante la Norma ISO 27001 la implementación del SGSI sigue el modelo Planificar – Hacer – Verificar – Actuar para la mejora continua de los procesos.

**Variables**: es el nombre que se da a una serie de caracteres con el fin de categorizar o interpretar de una forma más sencilla alguna información que se quiera estudiar, también pueden almacenar distintos tipos de datos: enteros, reales, matriciales, caracteres, etc.

Referencias Bibliográficas

Archivo General de la Nación. (2018). Fundamentos de preservación digital a largo plazo. Archivo General de la Nación. <https://www.archivogeneral.gov.co/caja_de_herramientas/docs/6.%20preservacion/DOCUMENTOS%20TECNICOS/FUNDAMENTOS%20PRESERVACION%20DIGITAL%20LARGO%20PLAZO.pdf>

DNP. (2020). Guía normativa aplicable a la explotación de datos. DNP. <https://colaboracion.dnp.gov.co/CDT/Desarrollo%20Digital/Documentos/Modelo%20Explotacion%20de%20datos/2.3%20Gu%C3%ADa%20normativa%20explotaci%C3%B3n%20de%20datos_VF.pdf>

Glosarioit.com. (2022). Dato - Sección informática. Glosarioit. <https://www.glosarioit.com/Dato>

Créditos

|  |  |  |
| --- | --- | --- |
| Nombre | Cargo | Regional y Centro de Formación |
| Abel Fernando Becerra Carrillo | Experto temático | Regional Norte de Santander - Centro de la Industria, la Empresa y los Servicios |
| Miroslava González Hernández | Diseñadora y evaluadora instruccional | Regional Norte de Santander - Centro de la Industria, la Empresa y los Servicios |
| Silvia Milena Sequeda Cárdenas | Asesora metodológica | Regional Distrito Capital - Centro de Diseño y Metrología |
| Rafael Neftalí Lizcano Reyes | Responsable Equipo de desarrollo curricular | Regional Santander – Centro Industrial del Diseño y la Manufactura |
| Julia Isabel Roberto | Correctora de estilo | Regional Distrito Capital - Centro de Diseño y Metrología |