

## Diplomado Teórico-Práctico en Protección de Datos Personales, Virtual Sincrónico

Incluye formación sobre ley 1918 del 2018 y aspectos de protección de datos asociados la Resolución 00013 de 2021 de la DIAN (Nómina Electrónica)

### Agenda

#### Criterios Institucionales

Con base en las exigencias de *accountability* que la Superintendencia de Industria y Comercio ha ido estableciendo a través de la *Guía del Principio de Responsabilidad Demostrada*, al igual que en sus diversos pronunciamientos efectuados a través de resoluciones sancionatorias y órdenes impartidas a Responsables y Encargados del tratamiento de datos personales con ocasión de sus incumplimientos a las obligaciones de la Ley 1581 de 2012 y demás normas reglamentarias de la protección de datos en Colombia, se ha identificado la necesidad de cualificar el personal que al interior de las organizaciones tratan datos personales, con el propósito de crear una cultura de seguridad y manejo responsable de aquellos en los procesos donde son tratados.

#### Componente Pedagógico

El proceso de globalización que impactó a América Latina durante la última década del siglo XX motivó a los gobiernos del área a realizar ajustes estructurales en sus constituciones, modificar sus legislaciones y lanzarse en la búsqueda de nuevos horizontes económicos. En desarrollo de tales circunstancias Colombia, al igual que la mayoría de países del continente, realizó ajustes a su marco constitucional en el año 1991, en el cual, entre otros muchos asuntos, incorporó un catálogo adicional de derechos fundamentales como el buen nombre, la intimidad y el derecho de Hábeas Data, señalando en el artículo 15 que todas las personas "...tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogidosobre ellas en los bancos de datos y en archivos de entidades públicas y privadas...", advirtiendo que en "...la recolección, tratamiento y circulación de datos" se deben respetar "...la libertad y demás garantías consagradas en la Constitución".

Con posterioridad, siguiendo las orientaciones de la OCDE y en acatamiento a pronunciamientos de la Corte Constitucional, en desarrollo del mandato superior, el Congreso de Colombia expidió la Ley 1266 de 2008 por medio de la cual se reglamentó el Hábeas Data para las personas naturales y jurídicas en relación con los datos referidos a asuntos económicos y financieros, y posteriormente, la Ley 1581 de 2012 y sus Decretos 1377 de 2013 y 886 de 2014 que concretaron el marco regulatorio de la protección de los datos personales, estos últimos decretos ahora refundidos en el Decreto 1074 de 2015.

El referido marco normativo otorgó a las personas la facultad de la autodeterminación informática y exigibilidad de protección de datos personales, e impuso a las organizaciones públicas y privadas que tratan datos personales, obligaciones que demandan la incorporación de ajustes en sus operaciones internas y externas, a fin de lograr su conformidad a la ley y evitar

los riesgos jurídicos por inadecuado tratamiento de datos, los que se pueden traducir en demandas de responsabilidad civil, imputaciones penales, sanciones administrativas por parte de la Superintendencia de Industria y Comercio y, en algunos casos, incluso juicios de responsabilidad fiscal y disciplinaria.

No obstante, los desarrollos jurisprudenciales, legislativos, reglamentarios y doctrinales en Colombia, a la fecha, en la inmensa mayoría de las organizaciones, que tratan datos personales, sus funcionarios carecen de una cultura de seguridad que prevenga el uso inadecuado de los mismos aumentando los riesgos jurídicos que ello implica tanto para Las organizaciones como para sus propios empleados a título personal. A lo anterior se suma que todos los días más, crecen los riesgos cibernéticos que pueden devenir en incidentes asociados a datos personales que generan violación de la confidencialidad, afectación de la integridad o de la disponibilidad de estos.

## Objetivo

Brindar capacitación al personal de los participantes, en Protección de Datos Personales, de forma que logre desarrollar las competencias para diseñar, gestionar y monitorear un sistema de protección de datos personales conforme a las normas colombianas, soportado en la plataforma tecnológica 1581-SPD, basados en los estándares de la ISO/IEC 27001:2013 y 27701:2019, para gestionar de forma integral los riesgos legales asociados con el tratamiento de datos personales en los procesos de la organización.

## Propósitos de formación

N°	Módulo	Propósitos del Módulo
1	La Información en las organizaciones como activo y responsabilidad colectiva	Comprender la importancia de la información al interior de La Organización.
2	El Ecosistema de Hábeas Data	Comprender los elementos que interactúan en un sistema de datos personales en una organización.
3	Principios de Hábeas Data	Apropiar los principios que rigen el tratamiento de los datos personales.
4	Marco Jurídico de Referencia	Aproximarse de manera general a las normas que reglamentan el Hábeas Data en Colombia. Incluye efectos colaterales de la Ley 1918 de 2018 y Resolución 0013 de 2021 de la DIAN.
5	Riesgos de Hábeas Data Más Frecuentes en las Organizaciones	Conocer los procesos que generan mayor riesgo de Hábeas Data en las organizaciones.

6	Autoridades de Hábeas Data y Responsabilidades	Tener presente las autoridades que vigilan el cumplimiento de las obligaciones de Hábeas Data y las consecuencias que se derivan del inadecuado tratamiento de los datos.
7	Desarrollo de habilidades para en el uso de la herramienta (SaaS) 1581 – SPD y orientación en el diseño, gestión/implementación y monitoreo del sistema de protección datos personales en la organización .	Desarrollar las habilidades para operar el software 1581 – SPD (SaaS) que permite el diseño, gestión/implementación y monitoreo del sistema de protección de datos personales en la organización .

### Intensidad, Descripción y Contenido de los Módulos

El programa está integrado por SIETE (7) módulos cuya intensidad horaria, descripción y contenido es el siguiente:

Módulos	Número de horas Teóricas	Número de Horas Prácticas
1 La Información en las organizaciones como activo y responsabilidad colectiva	8	
2 El Ecosistema de Hábeas Data	8	
3 Principios de Hábeas Data	2	
4 Marco Jurídico de Referencia	2	
5 Riesgos de Hábeas Data Más Frecuentes en las Organizaciones	2	
6 Autoridades de Hábeas Data y Responsabilidades	2	
7 Capacitación en el uso de la herramienta (SaaS) 1581 – SPD y orientación en el diseño, gestión/implementación y monitoreo del sistema de protección de datos personales.		16
<b>TOTAL</b>		40 horas

## Descripción, Competencias, Contenidos y Referencias Bibliográfica de cada Módulo

<b>Módulo 1. La Información En Las Organizaciones Como Activo Y Gestión de la Seguridadde la Información</b>
<p><b>Descripción del módulo.</b></p> <p>El contenido de este módulo está orientado a abordar las siguientes temáticas:</p> <ol style="list-style-type: none"><li>1. Concepto de información al interior de las organizaciones.</li><li>2. Aplicabilidad de los Principios OCDE para la gestión segura de la información.</li><li>3. Acceso a la Información como derecho fundamental</li><li>4. Derecho de Petición como instrumento de acceso a la información. (Ley 1755 de 2016)</li><li>5. Sistemas de Gestión de Seguridad de la Información (NTC/ISO/IEC 270001:2013)</li></ol>
<p><b>Competencias generales del módulo:</b></p> <p>Al finalizar el curso el participante estará en la capacidad de:</p> <ol style="list-style-type: none"><li>1. Identificar claramente el concepto de información.</li><li>2. Describir los principios claves para la gestión segura de la información al interior deLa Organización.</li><li>3. Conocer acerca del uso y atención del derecho de petición como instrumento de acceso a la información.</li><li>4. Identificar las áreas en que debe tenerse en cuenta la seguridad de la información de manera preponderante para protegerla.</li><li>5. Comprender el proceso de implementación de un sistema de gestión de seguridadde la información soportado en el estándar ISO/IEC 27001:2013.</li></ol>
<p><b>Contenidos de aprendizaje</b></p> <p>El índice del contenido del presente capítulo será el siguiente:</p> <ol style="list-style-type: none"><li>1. Las organizaciones y la información, concepto, importancia y responsabilidades.</li><li>2. La OCDE y su relación con Colombia.</li><li>3. Principios de seguridad de la información recomendados por la OCDE.</li><li>4. El acceso a la información como derecho fundamental amparado por la Constitución Política.</li><li>5. Aspectos generales del Derecho de Petición de información regulados por la Ley 1715 de 2015.<ol style="list-style-type: none"><li>a. Petición en interés general</li><li>b. Petición en interés particular</li><li>c. Petición De Consulta e Información</li><li>d. Entre Autoridades</li></ol></li><li>6. Aspectos generales de la norma NTC/ISO/IEC 27001:2013<ol style="list-style-type: none"><li>a. Definición de un sistema de gestión de seguridad de datos personales</li><li>b. Áreas de Intervención soporte para un sistema de gestión de seguridad de hábeas data.</li></ol></li></ol>

## Referencias Bibliográficas:

- COTE PEÑA, Luis Fernando. “HÁBEAS DATA EN COLOMBIA UN TRASPLANTE NORMATIVO PARA LA PROTECCIÓN DE LA DIGNIDAD Y SU CORRELACIÓN CON LA NTC/ISO/IEC 27001:2013”, “Premio Protección de Datos Personales de Investigación 2015. Iberoamérica”. “IMPRESA NACIONAL DE LA AGENCIA ESTATAL BOLETÍN OFICIAL DEL ESTADO” - España
- NORMATIVA PARA PETICIONES, QUEJAS, RECLAMOS, SOLICITUDES Y DENUNCIAS(PQRSD) <https://www.sisben.gov.co/Documents/Informaci%C3%B3n/Leyes/Ley%20175%20de%202015%20Derechos%20de%20petici%C3%B3n.pdf>
- ICONTEC Norma Técnica NTC/ISO/IEC 27001 - 2013-12-11
- ICONTEC Norma Técnica NTC/ISO/IEC 27701 - 2019-08
- Tecnologías de la Información. Técnicas de Seguridad. Sistemas de Gestión de la Seguridad de la Información. Requisitos. Bogotá D.C.: Icontec.
- Kosutic, D. (2012). Ciberseguridad en 9 pasos - El manual sobre seguridad de la información para el gerente. (http://advisera.com/27001academy/es/books/ciberseguridad-en-9-pasos-el-manual- sobre-seguridad-de-la-informacion-para-el-gerente/, Ed., & G. Trentini, Trad.) Electrónico: EPPS Services Ltd, Zagreb.

## Módulo 2: El Ecosistema de Hábeas Data

### Descripción del módulo.

El contenido de este módulo está orientado a abordar las siguientes temáticas:

1. El ecosistema de Hábeas Data - HD y su relación con la seguridad de la Información.
2. Sujetos del ecosistema de HD
3. Objetos del ecosistema de HD
4. Gobierno de un ecosistema de HD
5. Los procesos del ecosistema de HB

### Competencias generales del módulo:

Al finalizar el curso el participante estará en la capacidad de:

1. Comprender en qué consiste el ecosistema de HB y su relación con la información de las organizaciones.
2. Entender los conceptos e identificar al interior de la organización:
  - a. Los sujetos del ecosistema de HB, esto es: Titulares, Responsables, Terceros Responsables y Encargados y Las Autoridades de HD.
  - b. Los objetos del ecosistema de HB: Datos, Medios de Recolección y Bases de Datos Consolidadas, Bases de Datos Genéricas.
  - c. Cómo se estructura y funciona un gobierno de HB.
3. Identificar al interior de las organizaciones, a través de sus procesos, las diferentes interacciones que se desarrollan entre sujetos y/o objetos del ecosistema de HB.

### Contenidos de aprendizaje

El índice del contenido del presente capítulo será el siguiente:

1. El ecosistema de hábeas Data y su imbricación con la seguridad de la información.
2. Sujetos del ecosistema de HD
  - a. Los Titulares de los Datos
    - i. Concepto
    - ii. Titulares de especial protección
    - iii. Derechos de los titulares
  - b. El Responsable
    - i. Concepto
    - ii. Deberes
  - c. Los Encargados
    1. Concepto
    2. Deberes
  - d. El Gobierno del Ecosistema
    - i. Roles y competencias
3. Objetos del ecosistema de HD
  - a. Los Datos
    - i. Concepto
    - ii. Clasificación
    - iii. Excepciones de sometimiento a la ley
    - iv. Tratamiento
    - v. Finalidad
    - vi. Autorización
  - b. Los Medios de Recolección y Bases de Datos Consolidadas
  - c. Bases de Datos Genéricas
4. Los procesos vinculados con el ecosistema de HB
  - a. Estratégicos
  - b. Misionales
  - c. De apoyo
  - d. Transversales
  - e. El Proceso de Hábeas Data

#### Referencias Bibliográficas:

- COTE PEÑA, Luis Fernando. “HÁBEAS DATA EN COLOMBIA UN TRASPLANTE NORMATIVO PARA LA PROTECCIÓN DE LA DIGNIDAD Y SU CORRELACIÓN CON LA NTC/ISO/IEC 27001:2013”, “Premio Protección de Datos Personales de Investigación 2015. Iberoamérica”. “IMPRESA NACIONAL DE LA AGENCIA ESTATAL BOLETÍN OFICIAL DEL ESTADO”<https://drive.google.com/file/d/1v2nNVi78nnVi3TBadsV1W3dGeVspMUcO/view>
- Kosutic, D. (2012). Ciberseguridad en 9 pasos - El manual sobre seguridad de la información para el gerente. (<http://advisera.com/27001academy/es/books/ciberseguridad-en-9-pasos-el-manual-sobre-seguridad-de-la-informacion-para-el-gerente/>, Ed., & G. Trentini, Trad.) Electrónico: EPPS Services Ltd, Zagreb.
- Superintendencia de Industria y Comercio. (28 de Mayo de 2015). Superintendencia de Industria y Comercio. Recuperado el 19 de Junio de 2015, de [www.sic.gov.co](http://www.sic.gov.co): <http://www.sic.gov.co/drupal/noticias/guia-para-la-implementacion-del-principio-de-responsabilidad-demostrada>
- Sentencia C-748 de 2011, Magistrado. Ponente: Jorge Ignacio Pretelt Chaljub. Recuperado en <http://www.corteconstitucional.gov.co/relatoria/2011/c-748-11.htm>

## Módulo 3: Principios de Protección de Datos Personales

### Descripción del módulo.

El contenido de este módulo está orientado a abordar las siguientes temáticas:

1. Qué son principios jurídicos y que son reglas jurídicas y su diferencia.
2. Cuáles son los principios jurídicos que regulan el hábeas data.
3. Cuáles son los principios de HD más comúnmente violados y sancionados por la SIC.

### Competencias generales del módulo:

Al finalizar el curso el participante estará en la capacidad de:

1. Distinguir en entre un principio y una regla
2. Conocer los principios que regulan el HD.
3. Identificar las más comunes causas de violación de datos en las organizaciones para evitarlas previendo el riesgo personal y el institucional.

### Contenidos de aprendizaje

El índice del contenido del presente capítulo será el siguiente:

1. Concepto de principio jurídico y de regla jurídica y su carácter obligatorio.
2. Principios Constitucionales, Legales y Jurisprudenciales que regulan el HD.
3. Análisis de Decisiones de la Corte Constitucional sobre principios de HB.

### Referencias Bibliográficas:

- COTE PEÑA, Luis Fernando. "HÁBEAS DATA EN COLOMBIA UN TRASPLANTE NORMATIVO PARA LA PROTECCIÓN DE LA DIGNIDAD Y SU CORRELACIÓN CON LA NTC/ISO/IEC 27001:2013", "Premio Protección de Datos Personales de Investigación 2015. Iberoamérica". "IMPRESA NACIONAL DE LA AGENCIA ESTATAL BOLETÍN OFICIAL DEL ESTADO"
- COTE OTTENS, Luis Fernando y OLAYA VERA, Héctor Fernando. "PRINCIPIOS RECTORES DEL HÁBEAS DATA EN EL ORDENAMIENTO JURÍDICO COLOMBIANO A LA LUZ DE LA JURISPRUDENCIA DE LA CORTE CONSTITUCIONAL COLOMBIANA Y LAS RESOLUCIONES SANCIONATORIAS DE LA SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO, EN EL PERIODO 2012 – 2016"
- COTE OTTENS, Luis Fernando y OLAYA VERA, Héctor Fernando. ANEXO- ANÁLISIS DE JURISPRUDENCIAS DE LA CORTE CONSTITUCIONAL Y RESOLUCIONES SANCIONATORIAS DE LA SIC SOBRE HÁBEAS DATA EN LOS AÑOS 2012-2016

## Módulo 4: Marco Jurídico de Referencia

### Descripción del módulo.

El contenido de este módulo está orientado a abordar las siguientes temáticas:

1. Aspectos generales del Derecho de Protección de Datos regulado por la ley 1581 de 2012.
2. Aspectos generales del Derecho de Protección de Datos Financieros en relación con las Centrales de Riesgo regulado por la ley 1266 de 2008.
3. Aspectos generales de los Delitos Informáticos regulados por la ley 1273 de 2009.
4. Aspectos generales Ley 1918 de 2018 y sus implicaciones en protección de datos personales en las entidades obligadas.
5. Aspectos generales de la Resolución 0013 del 2021 de la DIAN sobre nómina electrónica y sus implicaciones en protección de datos personales en las entidades obligadas.

### Competencias generales del módulo:

Al finalizar el curso el participante estará en la capacidad de:

1. Describir las obligaciones generales establecidas por la ley 1581 de 2012 a tener en cuenta en La Organización
2. Describir las obligaciones generales establecidas por la ley 1266 de 2008 a tener en cuenta en La Organización , cuando resulte pertinente.
3. Comprender la ilegalidad de las conductas relacionadas con la información pueden constituir los delitos establecidas por la ley 1273 de 2009.
4. Comprender los deberes generados de la Ley 1918 de 2012 en relación con el sistema de protección de datos personales.
5. Comprender los deberes generados de la Resolución 0013 del 2021 de la DIAN en relación con el sistema de protección de datos personales.

### Contenidos de aprendizaje

El índice del contenido del presente capítulo será el siguiente:

1. Aspectos generales de la ley 1581 de 2012:
  - a. Descripción general
  - b. Ámbito de Aplicación
  - c. Obligaciones Principales
2. Aspectos generales de la ley 1266 de 2008:
  - a. Descripción general
  - b. Ámbito de Aplicación
  - c. Obligaciones Principales
3. Tipos Penales contenidos en la Ley 1273 de 2009
4. Aspectos generales de la Ley 1918 de 2018.
5. Aspectos de protección de datos requeridos para la implementación del sistema de nómina electrónica.

**Referencias Bibliográficas:**

COTE PEÑA, Luis Fernando. "HÁBEAS DATA EN COLOMBIA UN TRASPLANTE NORMATIVO PARA LA PROTECCIÓN DE LA DIGNIDAD Y SU CORRELACIÓN CON LA NTC/ISO/IEC 27001:2013", "Premio Protección de Datos Personales de Investigación 2015. Iberoamérica". "IMPRESA NACIONAL DE LA AGENCIA ESTATAL BOLETÍN OFICIAL DEL ESTADO"

- Ley 1581 de 2012
- Ley 1266 de 2008
- Ley 1273 de 2009
  
- Ley 1918 de 2018

**Módulo 5: Riesgos de Hábeas Data Más Frecuentes en las Organizaciones****Descripción del módulo.**

El contenido de este módulo está orientado a abordar las siguientes temáticas en perspectiva de las sanciones impuestas por la SIC y/o fallos de la Corte Constitucional:

6. Riesgos en los procesos de comunicación
7. Riesgo en los procesos de reportes a centrales de riesgos
8. Riesgos en los procesos de atención de PQR's
9. Riesgo en los procesos de registros de imágenes
10. Riesgo en la gestión de incidentes
11. Riesgos en la gestión del RNBD

**Competencias generales del módulo:**

Al finalizar el curso el participante estará en la capacidad de:

1. Podrá identificar los principales riesgos a que puede estar expuesto en las operaciones diarias de una organización
2. Estará en capacidad de actuar de manera que disminuya el riesgo personal e institucional por el tratamiento de datos personales.

## Contenidos de aprendizaje

El índice del contenido del presente capítulo será el siguiente:

1. Correos electrónicos como datos personales:
  - a. Correo electrónico público
  - b. Correo electrónico Privado
  - c. Correos masivos
  - d. Peticiones de supresión de correos
  - e. Análisis de Caso
2. Centrales de Riesgos y reportes de HD:
  - a. Aspectos generales de la ley 1266 de 2008
    - i. Actores
    - ii. Reglas y subreglas
  - b. Análisis de caso
3. Riesgos en los procesos de atención de PQR's
  - a. Identificación de PQR de hábeas data
  - b. Reclamos:
    - i. Concepto
    - ii. Tipologías y Detalles
    - iii. Atención
  - c. Consultas:
    - i. Concepto
    - ii. Atención
  - d. Consultas y Reclamos vía Centrales de Riesgos
  - e. Análisis de caso
4. Riesgo en los procesos de videovigilancia, imágenes y voz
  - a. Gestión de Sistemas de videovigilancia
  - b. Gestión de autorizaciones en de eventos
  - c. Gestión de registros en conferencias
  - d. Grabaciones de empleados por terceros
  - e. Análisis de caso
5. Riesgo en la gestión de incidentes
  - a. Concepto
  - b. Acciones previas
  - c. Acciones durante
  - d. Acciones después
  - e. Reporte del incidente al RNBD
  - f. Análisis de caso

### Referencias Bibliográficas:

- COTE PEÑA, Luis Fernando. “HÁBEAS DATA EN COLOMBIA UN TRASPLANTE NORMATIVO PARA LA PROTECCIÓN DE LA DIGNIDAD Y SU CORRELACIÓN CON LA NTC/ISO/IEC 27001:2013”, “Premio Protección de Datos Personales de Investigación 2015. Iberoamérica”. “IMPRESA NACIONAL DE LA AGENCIA ESTATAL BOLETÍN OFICIAL DEL ESTADO”<https://drive.google.com/file/d/1v2nNVi78nnVi3TBadsV1W3dGeVspMUcO/view>
- COTE OTTENS, Luis Fernando y OLAYA VERA, Héctor Fernando. “PRINCIPIOS RECTORES DEL HÁBEAS DATA EN EL ORDENAMIENTO JURÍDICO COLOMBIANO A LA LUZ DE LA JURISPRUDENCIA DE LA CORTE CONSTITUCIONAL COLOMBIANA Y LAS RESOLUCIONES SANCIONATORIAS DE LA SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO, EN EL PERIODO 2012 – 2016”

## Módulo 6: Autoridades de Hábeas Data y Responsabilidades

### Descripción del módulo.

El contenido de este módulo está orientado a abordar las siguientes temáticas:

1. Responsabilidad institucional
2. Responsabilidad personal
3. Autoridades de Hábeas Data
4. Sanciones por el tratamiento indebido de los datos

### Competencias generales del módulo:

Al finalizar el curso el participante estará en la capacidad de:

1. Entender las implicaciones que para la organización tiene el tratamiento inadecuado de los datos personales.
2. Entender que el tratamiento de los datos puede generarle también responsabilidad personal al empleado a título personal.
3. Comprender el rol que cumple cada una de las autoridades vinculadas con hábeas data y las sanciones que pueden derivarse del incumplimiento legal.

### Contenidos de aprendizaje

El índice del contenido del presente capítulo será el siguiente:

1. Superintendencia de Industria y Comercio y la responsabilidad administrativa derivada del HD.
2. Procuraduría General de la Nación y la responsabilidad disciplinaria derivada del HD.
3. Fiscalía General de la República y la responsabilidad penal derivada del HD.
4. Contraloría General de la Nación y la responsabilidad fiscal derivada del HD.
5. El Mercado y la responsabilidad empresarial derivada del HD.

### Referencias Bibliográficas:

- COTE PEÑA, Luis Fernando. “HÁBEAS DATA EN COLOMBIA UN TRASPLANTE NORMATIVO PARA LA PROTECCIÓN DE LA DIGNIDAD Y SU CORRELACIÓN CON LA NTC/ISO/IEC 27001:2013”, “Premio Protección de Datos Personales de Investigación 2015. Iberoamérica”. “IMPRESA NACIONAL DE LA AGENCIA ESTATAL BOLETÍN OFICIAL DEL ESTADO” <https://drive.google.com/file/d/1v2nNVi78nnVi3TBadsV1W3dGeVspMUcO/view>

## Módulo 7: DISEÑO, GESTIÓN Y MONITOREO PRÁCTICO DE UN SISTEMA DE PROTECCIÓN DE DATOS SOPORTADO EN LA PLATAFORMA 1581 – SPD

### Descripción del módulo.

El contenido de este módulo está orientado a capacitar en el uso de la herramienta tecnológica en nube tipo SaaS 1581 – SPD y orientar la adopción del programa integral de protección de datos a partir de los cuatro módulos del software a saber:

5. Módulo de Diseño
6. Módulo de Gestión
7. Módulo de Monitoreo
8. Documentación

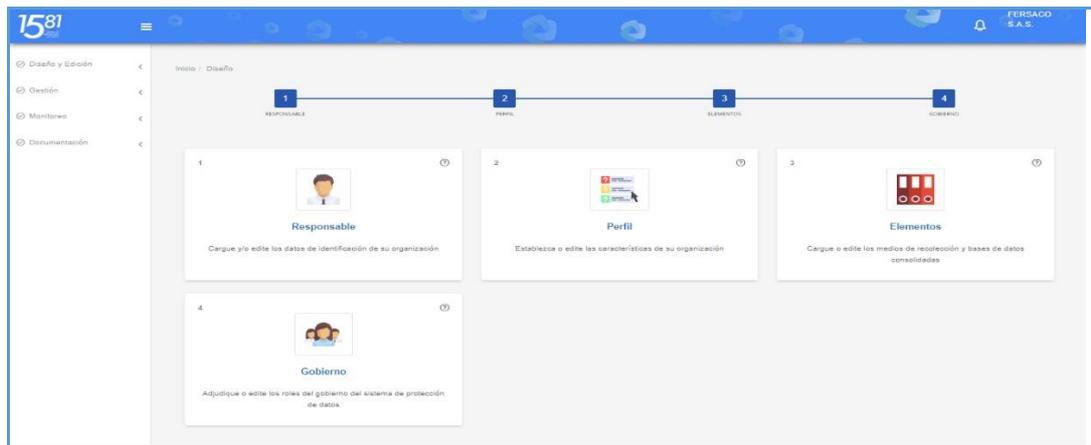
### Competencias generales del módulo:

Al finalizar el curso el participante estará en la capacidad de operar el software 1581 – SPD apoyado con los recursos multimedia que el sistema incorpora y habrá dejado las bases iniciales del sistema de protección de datos de su respectiva Organización .

### Contenidos de aprendizaje

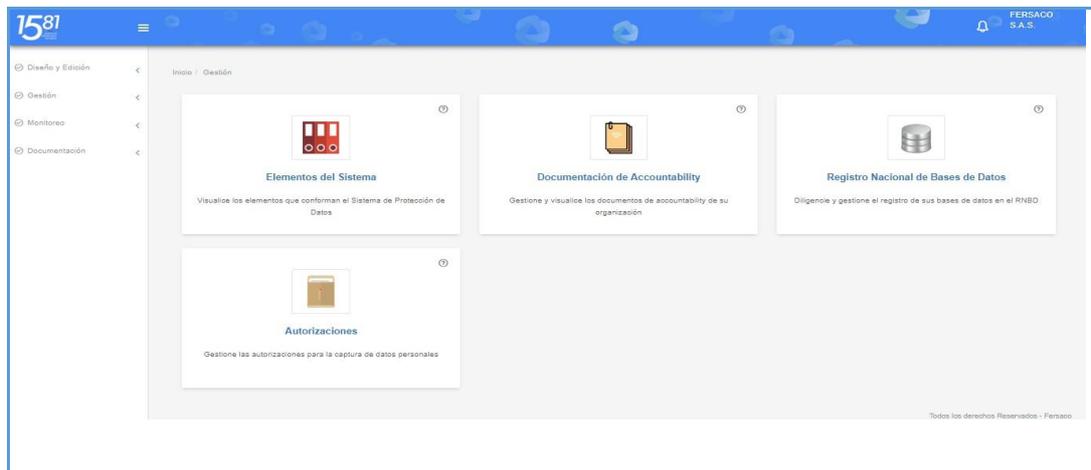
El índice del contenido del presente capítulo será el siguiente:

- a. **Módulo de Diseño del Sistema de Protección de Datos 1581.** Permite el diseño automático del sistema de protección de datos acorde a las características del cliente, a partir de la identificación y carga de los datos de referencia y su perfil, de los Medios de Recolección y/o las Bases de Datos Consolidadas que sean identificadas en los procesos de la organización y la definición de un gobierno del sistema.



**Ilustración. Módulo de Diseño de 1581 Sistema de Protección de Datos**

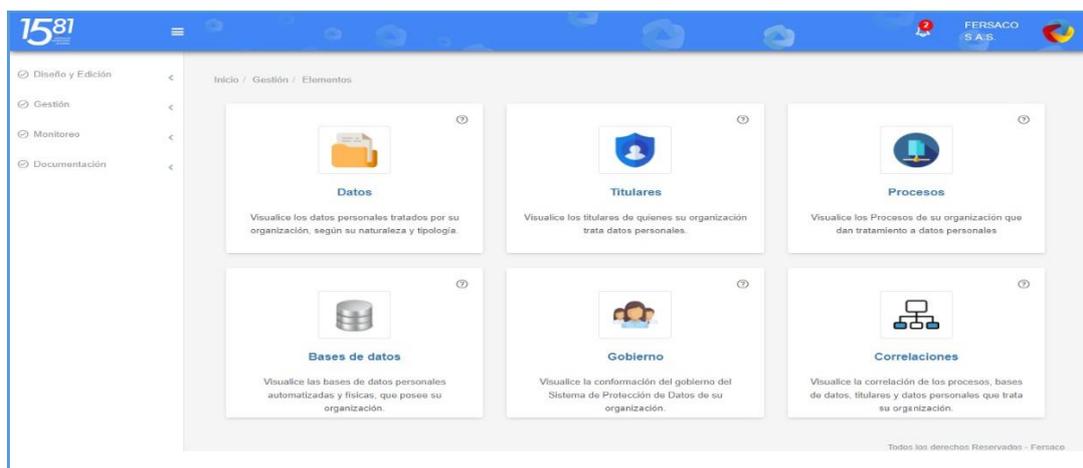
**b. Módulo de Gestión del Sistema de Protección de Datos 1581.** A partir de este módulo se logra acceder a cuatro (4) submódulos: *Elementos del Sistema*, *Documentación Accountability*, *Registro Nacional de Bases de Datos* y *Autorizaciones*, a través de los cuales se logran realizar las acciones que a continuación se describen:



**Ilustración. Módulo de Gestión del Sistema de 1581 Sistema de Protección de Datos**

- ✓ Generar inventario y correlacionar la información sobre bases de datos, procesos, titulares y datos personales categorizados.

- ✓ Permitir la gestión de los roles y actividades del Gobierno del Sistema de Protección de Datos conforme al Manual de políticas y procedimientos de seguridad que el sistema provee.
- ✓ Generar la Política de Tratamiento de Información y notificar el requerimiento de actualización.
- ✓ Generar el Aviso de Privacidad y notificar el requerimiento de su actualización.
- ✓ Proveer el Manual de Políticas y Procedimientos de Seguridad de Datos Personales, estructurado a partir de las obligaciones de los roles del Gobierno del Sistema de Protección de Datos.
- ✓ Proveer formatos y registros de Accountability para el desarrollo y cumplimiento de las Políticas y Procedimientos de Seguridad de Datos.
- ✓ Generar Contratos de transmisión de datos personales, necesarios para asegurar la circulación de datos con Terceros Encargados del tratamiento.
- ✓ Generar el contenido de las Autorizaciones para el tratamiento de datos y orienta su incorporación en los medios de recolección de datos que utiliza la organización.
- ✓ Actualizar el marco jurídico del sistema a las nuevas normativas y proveer normograma de protección de datos conforme al área de operación de la organización.



**Ilustración. Interfaz Elementos del Sistema de 1581 Sistema de Protección de Datos**

- ✓ Generar Guías para la inscripción de las bases de datos en el RNBD de la Superintendencia de Industria y Comercio y notificar el requerimiento de actualización y reporte en dicha plataforma, cuando a ello hubiere lugar.

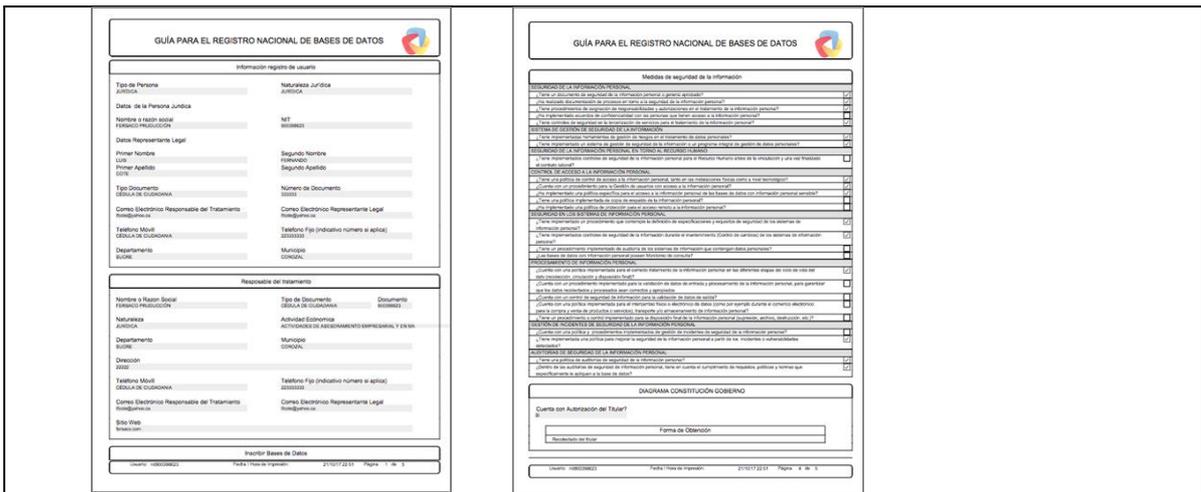


Ilustración. Guía de RNBD diligenciada para registro de base de datos.

- ✓ Facilitar el registro y orientar los reportes a la SIC, de los reclamos de titulares e incidentes de seguridad de datos personales.
- ✓ Notificar por medio de alertas, los requerimientos de modificación, actualización, registros y reportes que deban ejecutarse para el correcto funcionamiento del Sistema de Protección de Datos.

### NOTIFICACIONES DEL SISTEMA

Requerimientos de actualización, registros y reportes:

- Actualización de Gobierno del Sistema
- Actualización de Política de Tratamiento de la Información
- Actualización de Aviso de Privacidad
- Actualización de Manual de Políticas y Procedimientos
- Actualización de Contratos de Transmisión
- Actualización de Autorizaciones de Medios de Recolección
- Reporte de Reclamos de titulares a la SIC
- Reporte de Incidentes de Seguridad a la SIC
- Actualización y Registro de Guías del RNBD
- Actualización General RNBD

**Elementos cambiantes:**

- Finalidades
- Datos personales
- Canales de atención
- Medidas de seguridad
- Encargados del tratamiento

Miércoles, 29 de Agosto de 2018

**Notificación de cambio de parámetros de guías del registro nacional de bases de datos**

Se evidenciaron modificaciones en los parámetros de Finalidades, se requiere actualizar la guía para el Registro Nacional de Bases de Datos de las bases de datos señalados con un "No" en la columna "Guía RNBD".

[\[Revisar\]](#)

Base Datos	Guía RNBD
<input type="checkbox"/> CONSOLIDADA	<a href="#">CONSOLIDADA_28/08/2018</a>
<input type="checkbox"/> VIDEOVIGILANCIA	<a href="#">VIDEOVIGILANCIA_29/08/2018</a>
<input type="checkbox"/> BD_PRUEBA	<a href="#">BD_PRUEBA_29/08/2018</a>
<input type="checkbox"/> BD_PRUEBA 1	No

Ilustración. Notificaciones de 1581 Sistema de Protección de Datos.

c. **Módulo de Monitoreo y Control de Sistema.** Permite monitorear el Sistema de Protección de Datos, mediante Evaluación de cumplimiento de exigencias legales, Evaluación de riesgos de las bases de datos y Medición de indicadores de desempeño.

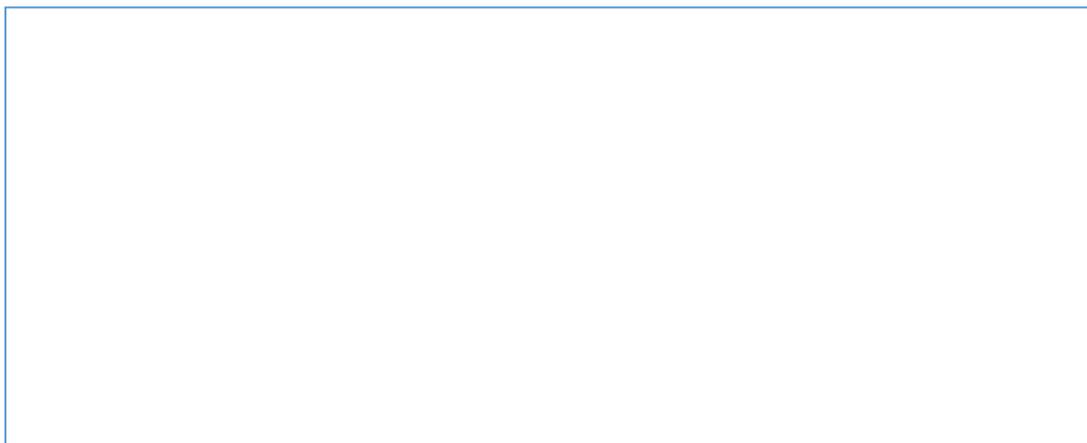


**Ilustración. Interfaz Monitoreo de 1581 Sistema de Protección de Datos.**

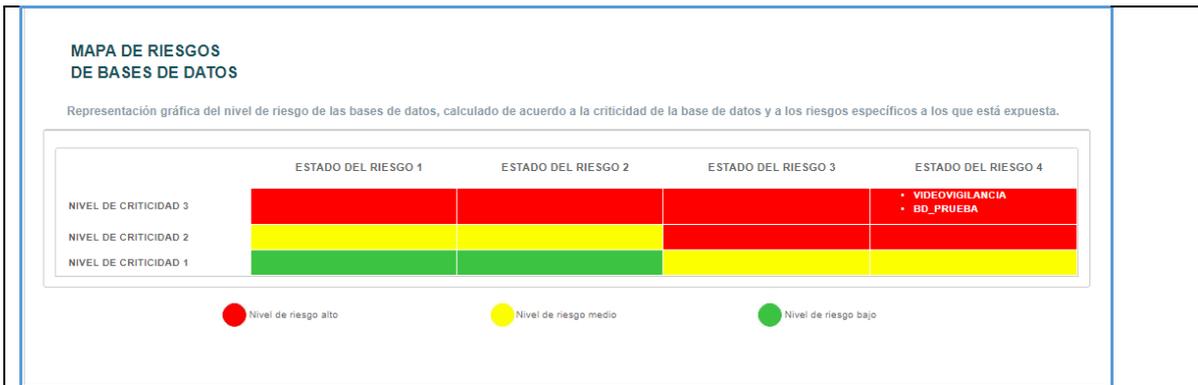
En este módulo se cuenta con cuadro de mando que visualiza integradamente los resultados gráficos de los diferentes instrumentos de monitoreo.



**Ilustración. Informe de Monitoreo del SPD 1581 Sistema de Protección de Datos.**



**Ilustración. Indicador de Empleados Sensibilizados / Informe de Monitoreo del SPD 1581**



**Ilustración. Mapa de Riesgos de Bases de Datos / Informe de Monitoreo1581 SPD**

**d. Módulo de Documentación.** Provee documentación normativa, bibliográfica, manual del Usuario y archivos multimedia para la formación de talento humano y el mantenimiento de la cultura organizacional en Protección de Datos

El desarrollo del abordaje de este módulo práctico, se llevará a cabo sobre la plataforma 1581 – SPD de propiedad de FERSACO S.A.S. y provista por ella para el proceso de aprendizaje sincosto alguno, conforme a la planeación que se presenta a continuación,

Sesión	Requerimiento	Descripción	Hora	Producto
<b>Sesión Práctica 1:</b> Requerimiento	<ul style="list-style-type: none"> <li>✓ Equipo de cómputo</li> <li>✓ Conexión a internet</li> <li>✓ Presentación</li> <li>✓ Matrices de Recolección de Datos.</li> <li>✓ EDT</li> </ul>	Presentación del aplicativo 1581 Sistema de Protección de Datos  Requerimiento de la información necesaria para realizar el Diseñodel Sistema de	4 horas	- Requerimiento al participante de: <ul style="list-style-type: none"> <li>✓ Información de Responsable.</li> <li>✓ Perfil.</li> <li>✓ Medios de Recolección de Datos.</li> <li>✓ Bases de Datos Consolidadas.</li> <li>✓ Gobierno del Sistema.</li> </ul>

		Protección de Datos a través de las matrices correspondientes.		
<b>Sesión Práctica 2:</b> Diseño	<ul style="list-style-type: none"> <li>✓ Equipo de cómputo</li> <li>✓ Conexión a internet</li> <li>✓ Información requerida en la sesión anterior</li> <li>✓ Acceso a 1581 SPD a cada participante</li> </ul>	<p>Orientación en el Diseño del Sistema de Protección de Datos.</p> <p>Orientación para la verificación de cargue del módulo de Diseño del aplicativo 1581SPD en el Módulo de Gestión/Elementos del Ecosistema</p>	4 horas	<ul style="list-style-type: none"> <li>- Sistema cargado con: <ul style="list-style-type: none"> <li>✓ Información de Responsable.</li> <li>✓ Perfil.</li> <li>✓ Medios de Recolección de Datos.</li> <li>✓ Bases de Datos Consolidadas.</li> <li>✓ Gobierno del Sistema.</li> </ul> </li> </ul>
<b>Sesión Práctica 3:</b> Gestión	<ul style="list-style-type: none"> <li>✓ Equipo de cómputo</li> <li>✓ Conexión a internet</li> <li>✓ Módulo de Diseño del aplicativo cargado (Responsable, Perfil, Elementos, Gobierno)</li> <li>✓ Herramienta de planeación de implementación</li> <li>✓ Acceso a 1581 SPD a cada participante</li> </ul>	Orientación en la Gestión del Sistema de Protección de Datos.	4 horas	<ul style="list-style-type: none"> <li>- Elementos siguientes: <ul style="list-style-type: none"> <li>✓ PTI provisional generada.</li> <li>✓ Aviso Provisional de Privacidad.</li> <li>✓ Manual de Procedimientos de Seguridad de la entidad.</li> <li>✓ Implementación de Autorizaciones.</li> </ul> </li> </ul>
<b>Sesión Práctica 4:</b> Registro y Monitoreo	<ul style="list-style-type: none"> <li>✓ Equipo de cómputo</li> <li>✓ Conexión a internet</li> <li>✓ Actividades del módulo de Gestión implementadas y cargadas en el aplicativo</li> </ul>	Orientación para el uso de la plataforma del Registro Nacional de Bases de Datos de la SIC	4 horas	<ul style="list-style-type: none"> <li>- Guías provisionales del RNBD generadas.</li> <li>- Participantes informados en : <ul style="list-style-type: none"> <li>✓ Registro de Bases de Datos.</li> <li>✓ Reporte de Incidentes.</li> <li>✓ Reporte de Reclamos de Habeas Data.</li> </ul> </li> </ul>

	<ul style="list-style-type: none"> <li>✓ RUT descargado de la web de laDIAN</li> <li>✓ Acceso al correo registrado en elRUT</li> </ul>	Orientación en el Monitoreo del Sistema de Protección de Datos y formación de competencias	<ul style="list-style-type: none"> <li>- Evaluación provisional del Estado de Cumplimiento de habeas data del OPD.</li> <li>- Medición provisonal de Indicadores de Desempeño del Sistema.</li> </ul>
		del Oficial de Protección de Datos	<ul style="list-style-type: none"> <li>- Evaluación provisional de riesgos del Sistema de Protección de Datos.</li> </ul>
<b>TOTAL</b>			<b>16 horas</b>
<p><b>Referencias Bibliográficas:</b></p> <p>Contenido Multimedia del Software 1581 - SPD</p>			

### Metodología para el desarrollo de los contenidos de cada módulo

Las actividades se desarrollarán, así:

1. Se dictarán 20 sesiones de dos horas cada una, los miércoles, jueves y viernes de 4pm a 6 pm., según programación final que se apruebe.
2. Encuentros virtuales en la plataforma teams.
3. Se dictarán conferencias magistrales y se ejecutarán talleres prácticos soportados en la herramienta 1581 – SPD, se atenderán tutorías grupales.

### Metodología para seguimiento y evaluación del aprendizaje

La metodología de evaluación del programa será formativa: Consiste en el proceso por medio del cual se irá evaluando al participante durante el recorrido del programa para determinar el nivel de comprensión conceptual que va adquiriendo y su capacidad de aplicación de estos a las varias acciones del programa que les brinda ocasión de poner en evidencia su apropiación cognitiva, tales como respuestas en sesiones de trabajo, resolución de casos, presentación de avances, etc. Con base en esta evaluación se podrá ir verificando si se requieren oportunidades de aprendizaje adicional para asegurar el éxito del proceso de formación.

De igual forma se harán procesos de evaluación cognitiva durante el desarrollo del programa, los cuales serán calificados como aprobadas o reprobadas por el respectivo responsable del módulo.