POSITIVA COMPAÑÍA DE SEGUROS | suma 5.0 | educa | comunica

EL FUTURO ES HUMANO

PLAN NACIONAL

Multimodal 2025

Fórmulas para la vida

Valores + Emociones + Competencias

Respeto + Alegría + Aprendizaje

16

POSITIVA COMPAÑÍA DE SEGUROS | suma 5.0 | educa | comunica

EL FUTURO ES HUMANO

Comunidad Nacional de Conocimiento en

Prevención de Peligros en la Administración Pública

Fórmulas para la vida

Valores + Emociones + Competencias

Paciencia + Esperanza + Pensamiento crítico

SESIÓN 10:
TRATAMIENTO DE DATOS PERSONALES (LEY 1581 DEL 2012) CON ARTICULACIÓN AL SST

CARLOS ANDRÉS VALENCIA HERNÁNDEZ

COMUNIDAD NACIONAL DE CONOCIMIENTO EN PREVENCIÓN DE PELIGROS EN LA ADMINISTRACIÓN PUBLICA

carlosvalencia21@hotmail.com

3145359820

MAGISTER EN GESTIÓN DE LA CALIDAD Y EN LAS ORGANIZACIONES, ESPECIALISTA EN GESTIÓN TERRITORIAL, SEGURIDAD PÚBLICA Y EN RIESGOS LABORALES, CON EXPERIENCIA DE MÁS DE 28 AÑOS EN ENTIDADES PÚBLICAS; ENTRE SUS CARGO FUE JEFE DEL SGSST EN LA POLICÍA NACIONAL DE COLOMBIA, ASESOR INTERNACIONAL DEL GOBIERNO DE GUATEMALA, INSTRUCTOR Y PROFESOR DE LA CRUZ ROJA COLOMBIANA, CONCEJO COLOMBIANO DE SEGURIDAD, CONFERENCISTA INTERNACIONAL, DOCENTE UNIVERSITARIO, ACTUALMENTE DIRECTOR DE OPERACIONES (COO) DE PROHUMANA SOLUCIONES.

Ruta de **conocimiento**

SESIÓN 1:
RESILIENCIA LABORAL Y PERSONAL - COMO SUPERAR LAS SITUACIONES CRÍTICAS EN EL TRABAJO Y EN LA VIDA PERSONAL

SESIÓN 2:
COMUNICACIÓN ASERTIVA EN EL TRABAJO - METODOLOGÍA PARA LOGRAR MINIMIZAR LOS CONFLICTOS

SESIÓN 3:
CÓDIGO DE INTEGRIDAD PARA LA FUNCIÓN PÚBLICA - UNA MIRADA DESDE LA PREVENCIÓN

SESIÓN 4:
PRIMER RESPONDIENTE Y RESPONDEDOR EN PRIMEROS AUXILIOS, ORIENTADO A LAS EMPRESAS DE LA ADMINISTRACIÓN PÚBLICA

SESIÓN 5:
GESTIÓN DEL RIESGO EN LA ADMINISTRACIÓN PÚBLICA - GUÍA

Ruta de **conocimiento**

06

SESIÓN 6:
PRÁCTICAS DE TRABAJOS SALUDABLES EN LA ADMINISTRACIÓN PÚBLICA

07

SESIÓN 7:
ARTICULACIÓN EN EMERGENCIAS PÚBLICAS - SISTEMA COMANDO DE INCIDENTES

08

SESIÓN 8:
SERVICIO DE ATENCIÓN AL CIUDADANO - (PREVENCIÓN DE SUS RIESGOS ASOCIADOS)

09

SESIÓN 9:
PROGRAMA DE TRANSPARENCIA Y ÉTICA EMPRESARIAL (PTE) HERRAMIENTA PARA LA MITIGACIÓN DE LOS RIESGOS LABORALES

10

SESIÓN 10:
TRATAMIENTO DE DATOS PERSONALES (LEY 1581 DEL 2012) CON ARTICULACIÓN AL SST


POSITIVA
COMPAÑÍA DE SEGUROS
suma 5.0
educa
comunica
EVALUÉMONOS
Fórmulas para la vida
Valores + Emociones + Competencias
Respeto + Gratitud + Ética y sostenibilidad

“Las organizaciones gastan millones de dólares en firewalls y dispositivos de seguridad, pero tiran el dinero porque ninguna de estas medidas cubre el eslabón más débil de la cadena de seguridad: la gente que usa y administra los ordenadores”

Kevin Mitnick: Fue uno de los hackers más famosos de la historia, y más tarde se convirtió en un consultor de seguridad.

CONTENIDO

OBJETIVOS

01 Garantizar que las políticas, procedimientos y controles implementados cumplan con la normativa vigente y protejan adecuadamente los datos personales de los titulares.

02 Detectar debilidades, riesgos o incumplimientos en el manejo de datos personales para implementar planes de acción correctiva y preventiva.

03 Documentar todas las evaluaciones, auditorías y ajustes realizados, asegurando que la organización pueda demostrar ante la autoridad de control que gestiona los datos de manera responsable y proactiva.

NORMATIVIDAD DOCUMENTAL

La normatividad para la gestión documental en Colombia se encuentra regulada por varias leyes, decretos y acuerdos. A continuación, algunas de las principales normas que rigen esta materia

LEY GENERAL DE ARCHIVO

Ley 594 de 2000

"**Ley General de Archivos",** establece los principios y reglas generales para la organización, conservación y acceso a los documentos y archivos públicos y privados

Decreto 1080 de 2015

Reglamenta la Ley 594 de 2000 y establece las normas para la organización, conservación y acceso a los documentos y archivos públicos y privados

Decreto 491 de 2020

Permite a las entidades públicas operar virtualmente, proteger contratos laborales y suspender trámites durante la emergencia sanitaria.

NTC - ISO 15489 - 2017 del

Es una norma que establece principios y metodologías para que las organizaciones gestionen documentos auténticos, confiables y accesibles. Abarca todo el ciclo de vida documental —desde su creación hasta su disposición final—, garantizando la trazabilidad de las operaciones y el cumplimiento legal. Su propósito es que los documentos reflejen el contexto normativo y funcionen como evidencia institucional.

DERECHO DE ACCESO A LA INFORMACIÓN

Art 74 de la CPC

Garantiza el derecho de acceso a los documentos públicos, salvo las excepciones que establezca la ley. También declara que el secreto profesional es inviolable.

Ley 1712 de 2014

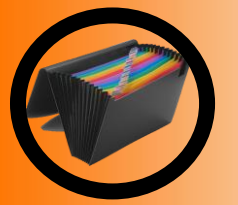
Regula el **derecho de acceso a la información** pública y establece los procedimientos para su ejercicio

Ley 2052 de 2020

Ley antitramites -promueve la simplificación de trámites administrativos en entidades públicas, impulsando la transformación digital, la eficiencia institucional y el acceso ciudadano, mediante la eliminación de procesos innecesarios y el fortalecimiento del principio de buena fe.

Guía para la Clasificación de la Información del Archivo General de la Nación (2015)

Establece criterios para identificar el nivel de seguridad que debe aplicarse a los documentos según su sensibilidad, valor institucional y riesgo asociado.



DOCUMENTOS RESERVADOS

Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuada de acceso a la ciudadanía por daño a intereses públicos y bajo cumplimiento de la totalidad de los requisitos consagrados en el artículo 19 de esta ley; Ley 1712/2014

- **Información de Seguridad**
- **Salud Publica**
- **Prevención, investigación y persecución de los delitos y las faltas disciplinarias**

Estabilidad Macroeconómica del país

Esta información no debe estar expuesta públicamente ni en redes sociales, debe ser información con nivel de compartimentación

DOCUMENTOS CLASIFICADOS

Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, pertenece al ámbito propio, particular y privado o semiprivado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados consagrados en el artículo 18 de esta ley; Ley 1712/2014

Contratos de proveedores

Documentos de propiedad intelectual

De investigación y desarrollo

Esta información puede estar asequible públicamente y se puede compartir y socializar con todo el personal de la institución.

DOCUMENTOS - PERSONALES CLASIFICADOS

Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, pertenece al ámbito propio, particular y privado o semiprivado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados consagrados en el artículo 18 de esta ley; Ley 1712/2014

Expedientes del personal

Información de salud

Documentos de seguridad social

Esta información no debe estar expuesta públicamente, debe ser información exclusiva de la empresa y los empleados. Es regula por la ley de tratamiento de datos personales en Colombia

DOCUMENTOS REGULADOS

Son documentos que contienen información personal de empleados, como:

De cumplimiento normativo

Informes de seguridad

De protección de datos

Esta información no debe estar expuesta públicamente, debe ser información exclusiva de la empresa y los **empleados.** Regulada por la ley de tratamiento de datos personales en Colombia 1581/12

DOCUMENTOS PÚBLICOS

Son todos documentos que teniendo en cuenta su información se pueden compartir libremente con el público y/o empleados de la organización como:

Informes anuales

Folletos publicitarios

Comunicados de prensa

Esta información puede estar asequible públicamente y se puede compartir y socializar con todo el personal de la institución.

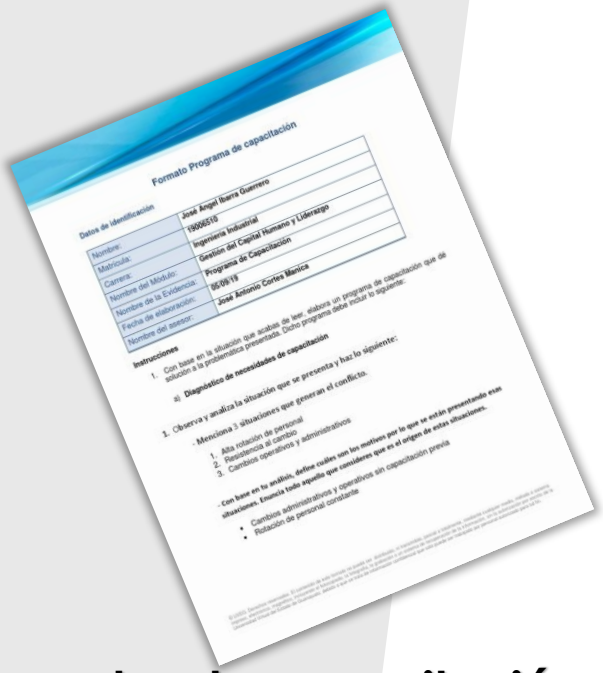
GUÍA PARA LA CLASIFICACIÓN DE LA INFORMACIÓN DE ACUERDO CON SUS NIVELES DE SEGURIDAD AGN Archivo General de la Nación de Colombia. https://www.archivogeneral.gov.co/sites/default/files/Estructura_Web/3_Transparencia/3.3%20Procesos%20y%20Procedimientos/GIT-G-01_GUIA_PARA_LA_CALIFICACI%C3%93N_DE_LA_INFORMACI%C3%93N_AGN.pdf

DOCUMENTOS INTERNOS

Son documentos que se comparten dentro de la empresa, pero no se hacen públicos o por decisión de la entidad o empresa se vuelven públicos, como:

Informes de gestión

Planes estratégicos



Documentos de capacitación

Esta información puede estar asequible exclusivamente con el personal de la institución.

DERECHO DE PETICIÓN

ART 23 Derecho de Petición

Consagra el derecho de petición, permitiendo a toda persona presentar solicitudes respetuosas a las autoridades por motivos de interés general o particular, y recibir una respuesta oportuna. Este derecho incluye pedir información, formular quejas, reclamos o solicitudes, sin necesidad de abogados

Ley 1755 de 2015

La Ley 1755 de 2015 regula el derecho fundamental de petición en Colombia, estableciendo sus modalidades, plazos, procedimientos y garantías para que toda persona pueda solicitar información, formular solicitudes o reclamos ante autoridades públicas y privadas que ejerzan funciones públicas.

ESTATUTO ANTICORRUPCIÓN

Ley 1474 de 2011

La Ley 1474 de 2011, conocida como el Estatuto Anticorrupción, establece medidas para prevenir, investigar y sancionar actos de corrupción en Colombia, fortaleciendo los mecanismos de control fiscal, disciplinario y penal, promoviendo la transparencia en la contratación pública y la gestión administrativa, y creando herramientas para mejorar la rendición de cuentas en entidades del Estado.

Circular Externa 100-000011 de 2021 de la Superintendencia de Sociedades

Define el contenido mínimo del programa, incluyendo políticas de integridad, códigos de ética, canales de denuncia, matrices de riesgo y mecanismos de monitoreo y mejora continua

Ley 2195 de 2022

Refuerza la lucha contra la corrupción en Colombia mediante medidas de prevención, sanción y recuperación de daños, fortaleciendo la responsabilidad de personas jurídicas y promoviendo la cultura de la legalidad. **El Programa de Transparencia y Ética Empresarial (PTEE)** está establecido en la Ley 2195 de 2022

HABEAS DATA

ART 15 Habeas Data

Consagra el derecho al hábeas data, permitiendo a toda persona conocer, actualizar y rectificar la información que sobre ella se haya recogido en bases de datos públicas o privadas, garantizando la intimidad, el buen nombre y la protección de datos personales, bajo el respeto a la libertad y demás garantías constitucionales

Ley 1581 de 2012

Regula la protección de datos personales y establece los principios y reglas para su tratamiento.

Decreto 1377 de 2013

reglamenta parcialmente la Ley 1581 de 2012 sobre protección de datos personales, estableciendo mecanismos para obtener la autorización de los titulares cuando los datos fueron recolectados antes de la ley, y definiendo obligaciones para responsables y encargados del tratamiento en cuanto a seguridad, confidencialidad y manejo de información.

La Circular 100 de 2021

Superintendencia de Industria y Comercio establece lineamientos para que las organizaciones públicas y privadas implementen el principio de responsabilidad demostrada en el tratamiento de datos personales, recomendando la creación de un Programa Integral de Gestión de Datos Personales (PIGDP) con políticas, procedimientos, controles y evidencias que garanticen el cumplimiento de la Ley 1581 de 2012.

¿QUÉ ESTABLECE LA LEY?

DERECHO FUNDAMENTAL AL HABEAS DATA

Protege el derecho de las personas a controlar sus datos personales.

DEFINICIONES

Establece qué se entiende por "tratamiento", "dato personal", "base de datos", "titular", "responsable" y "encargado del tratamiento".

PRINCIPIOS

Guía las operaciones de tratamiento de datos personales con principios como seguridad, confidencialidad y veracidad.

DERECHOS DE LOS TITULARES

Los ciudadanos pueden solicitar conocer, suprimir, actualizar o rectificar sus datos personales en cualquier momento.

AUTORIZACIÓN

Para el tratamiento de datos personales, las entidades deben obtener una autorización previa, expresa e informada del titular.

OBLIGACIONES Y RESTRICCIONES DE LA LEY 1581DE 2012

DEBER DE INFORMAR

Al solicitar la autorización, el responsable del tratamiento debe informar al titular sobre la finalidad del tratamiento, los derechos que le asisten, y el carácter facultativo de algunas preguntas.

DATOS DE NNA

Se prohíbe el tratamiento de estos datos, a menos que sean de naturaleza pública, y se establece que es responsabilidad del Estado y entidades educativas informar y capacitar a sus tutores sobre los riesgos del uso indebido de datos.

MEDIDAS DE SEGURIDAD

Los responsables del tratamiento deben implementar medidas técnicas, humanas y administrativas para proteger los datos

ENTE DE VIGILANCIA Y CONTROL

Superintendencia de Industria y Comercio (SIC): Esta entidad es la encargada de vigilar el cumplimiento de las normas sobre protección de datos personales y puede sancionar a las entidades que no cumplan con la ley

La “Guía para la Implementación del Principio de Responsabilidad Demostrada”

fue publicada por la Superintendencia de Industria y Comercio (SIC) en 2015, y orienta a las organizaciones sobre cómo cumplir activamente con la Ley 1581 de 2012 en materia de protección de datos personales.

INTRODUCCIÓN

El concepto de **responsabilidad demostrada** aplicada al **tratamiento de datos personales** tiene mas de 30 años.

Ya en 1980, las guías para la protección de la privacidad y los flujos transfronterizos de datos personales, introdujeron el concepto conocido en ingles como **accountability,** donde se enfatizaba el rol del Responsable del Tratamiento como el llamado a implementar medidas dentro de la organización que le permitieran cumplir con el resto de principios consagrados por dicho instrumento.

Reconociendo la importancia de un enfoque basado en el compromiso de la organización con incrementar sus estándares **de protección para garantizarle a los ciudadanos un tratamiento idóneo de su información personal.**

¿QUE ES LA SEGURIDAD DEMOSTRADA O ACCOUNTABILITY?

El principio de **responsabilidad demostrada** (también conocido por su término inglés *accountability*) es un concepto clave en la protección de datos personales, y lo explicita **la Superintendencia de Industria y Comercio (SIC)** en la *Guía para la implementación del principio de responsabilidad demostrada.*

La guía define que el término *accountability*, aunque tiene varias acepciones, en el contexto de datos personales se entiende como la forma en que una organización debe **cumplir efectivamente** las normas relativas al tratamiento de datos y, además, debe **demostrar** que ha implementado medidas que son útiles, pertinentes y eficientes

BENEFICIOS DE LA IMPLEMENTACIÓN DE LA RESPONSABILIDAD DEMOSTRADA

- **Reducción del riesgo sancionatorio:** Al implementar un programa de gestión de datos personales que cumpla con el principio de responsabilidad demostrada ("medidas apropiadas, efectivas y verificables"), la organización puede mostrar ante la SIC que ha hecho una gestión diligente, lo cual puede jugar a favor al momento de valorar una eventual sanción.
- **Mejora de la reputación y de la confianza del mercado:** Adoptar estándares elevados en protección de datos refleja un compromiso con la privacidad y puede convertirse en un valor diferencial frente a clientes, usuarios, proveedores y demás partes interesadas.
- **Optimización de la gestión de riesgos y mayor control interno:** La responsabilidad demostrada implica identificar, medir, controlar y monitorear los riesgos asociados al tratamiento de datos personales, lo que fortalece la capacidad de la organización para prevenir incidentes, fugas de datos o vulneraciones.

BENEFICIOS DE LA IMPLEMENTACIÓN DE LA RESPONSABILIDAD DEMOSTRADA

- **Mayor eficiencia operativa y claridad en los procesos**: Al implementar políticas, procedimientos, controles, monitoreo y evaluación, se establece una estructura clara (como el Programa Integral de Gestión de Datos Personales), lo que reduce la improvisación, fortalece la gobernanza y facilita la toma de decisiones.

- **Cultura organizacional orientada a la privacidad:** Al involucrar a la alta dirección, asignar responsabilidades, capacitar al personal y monitorear las acciones, la organización promueve una cultura de protección de datos que permea sus operaciones.

FUNDAMENTOS BÁSICOS DESARROLLO DE UN PROGRAMA INTEGRAL DE GESTIÓN DE DATOS PERSONALES

- Alta Dirección
- Oficial de Seguridad De Datos
- Presentación de Informes
- Controles del Programa
- Procedimientos Operacionales
- Inventario de Bases de Datos de Información Personal
- Políticas
- Sistema de Administración de Riesgos Asociados Al Tratamiento De datos Personales
- Requisitos de Formación y Educación
- Protocolo de Respuesta en el Manejo de Violaciones e Incidentes
- Gestión de los Encargados del Tratamiento en las Transmisiones Internacionales de Datos Personales
- Comunicación Externa

DESDE LA ALTA DIRECCIÓN

La Guía establece que el punto de partida para el desarrollo de un **Programa Integral de Gestión de Datos Personales (PIGDP)** es el compromiso explícito y verificable de la alta dirección.

La dirección debe asumir la protección de datos como una prioridad estratégica.

Debe garantizar recursos humanos, tecnológicos y financieros para su implementación.

La alta dirección debe designar un responsable o área de protección de datos, con independencia y autoridadi suficiente

OFICIAL PROTECCIÓN DE DATOS

El Oficial de Protección de Datos (OPD) es la persona o área designada por la organización para liderar, coordinar y supervisar el cumplimiento de la normatividad sobre protección de datos personales, asi como el desarrollo y mantenimiento del Programa Integral de Gestión de Datos Personales, asegurando su efectividad, seguimiento y mejora continua.

Toda organización debe contar con un responsable que lidere la implementación del principio de responsabilidad demostrada y la ejecución del Programa Integral de Gestión de Datos Personales.

1.3 PRESENTACIÓN DE INFORMES

La presentación de informes es uno de los pilares básicos del **Programa Integral de Gestión de Datos Personales**, ya qué permite a la organización rendir cuentas y demostrar ante la alta dirección, los titulares de los datos y la Superintendencia de Industria y Comercio (SIC) que cumple efectivamente con la normatividad de protección de datos personales.

CONTROLES DEL PROGRAMA

Son los **mecanismos, políticas, procedimientos y acciones** que una organización adopta para **garantizar que el tratamiento de datos personales se realice de manera segura, lícita, transparente y verificable**.

Estos controles constituyen el **núcleo operativo del Programa Integral de Gestión de Datos Personales (PIGDP).**

Son la evidencia práctica del **principio de responsabilidad demostrada (accountability).**

PROCEDIMIENTOS OPERACIONALES

Los **procedimientos operacionales** son el conjunto de **acciones, procesos y protocolos internos** que una organización implementa para **garantizar el cumplimiento efectivo y verificable** de las políticas de protección de datos personales.

Constituyen la **materialización práctica** del **Programa Integral de Gestión de Datos Personales (PIGDP)**, pues establecen **cómo se ejecutan** las actividades diarias relacionadas con el tratamiento de la información.

INVENTARIO DE BASES DE DATOS DE INFORMACIÓN PERSONAL

El **inventario de bases de datos** es uno de los **controles esenciales** del Programa Integral de Gestión de Datos Personales (PIGDP).
Consiste en la **identificación, registro y documentación detallada** de todas las bases de datos que contienen información personal dentro de una organización, sin importar el medio (físico o digital) ni el área responsable de su manejo.

Este inventario es la **base estructural** sobre la cual se construyen y gestionan los demás elementos del programa, ya que permite **conocer qué datos personales se tratan, con qué propósito, bajo qué condiciones y quién es responsable de ellos**.

POLÍTICAS

Las políticas de protección de datos personales son el marco normativo interno que **guía el tratamiento de la información personal dentro de una organización**.

Constituyen un instrumento de control y cumplimiento que traduce las obligaciones legales en reglas, principios y directrices aplicables a todos los procesos que involucren el manejo de datos personales.

"las políticas de tratamiento de la información personal deben reflejar el compromiso institucional con la protección de los datos y definir las reglas claras sobre la **recolección, uso, almacenamiento, circulación y supresión de los mismos**."

SISTEMA DE ADMINISTRACIÓN DE RIESGOS ASOCIADOS AL TRATAMIENTO DE DATOS PERSONALES

El **Sistema de Administración de Riesgos (SAR) asociados al tratamiento de datos personales** es un **mecanismo preventivo y de control** que permite identificar, evaluar, tratar y monitorear los riesgos que podrían afectar la **confidencialidad, integridad y disponibilidad de la información personal**.

Este sistema busca **proteger los derechos de los titulares** y garantizar el **cumplimiento normativo** en concordancia con la Ley 1581 de 2012, los decretos reglamentarios y las directrices de la SIC.

REQUISITOS DE FORMACIÓN Y EDUCACIÓN

La **formación y educación en protección de datos personales** es un componente crítico del Programa Integral de Gestión de Datos Personales (PIGDP).

Su propósito es asegurar que **todos los colaboradores, directivos y contratistas** comprendan:

- La **importancia de proteger los datos personales**.
- Sus **responsabilidades en el tratamiento de información**.
- Los **procedimientos y políticas internas** para garantizar el cumplimiento normativo

PROTOCOLO DE RESPUESTA EN EL MANEJO DE VIOLACIONES E INCIDENTES

El **protocolo de respuesta ante violaciones e incidentes de datos personales** es un **conjunto de procedimientos documentados** que permiten a la organización **actuar de manera rápida, coordinada y eficiente** ante cualquier situación que pueda comprometer la confidencialidad, integridad o disponibilidad de la información personal. Su finalidad es **minimizar impactos, cumplir con obligaciones legales y preservar la confianza de los titulares de los datos**.

GESTIÓN DE LOS ENCARGADOS DEL TRATAMIENTO EN LAS TRANSMISIONES INTERNACIONALES DE DATOS PERSONALES

Cuando una organización transfiere datos personales a **encargados del tratamiento ubicados en el exterior**, debe asegurarse de que **estos terceros cumplan con niveles adecuados de protección de datos personales**. El objetivo es garantizar que los datos **conserven sus derechos fundamentales** incluso cuando se encuentran fuera del país, y que la organización pueda **demostrar la diligencia y responsabilidad** en el manejo de la información.

COMUNICACIÓN EXTERNA

La **comunicación externa** en un Programa Integral de Gestión de Datos Personales (PIGDP) se refiere a los **mecanismos y estrategias para informar a terceros, clientes, proveedores y titulares de datos** sobre:

•La política de privacidad de la organización.
•Los derechos de los titulares.
•Procedimientos para ejercer derechos y reportar incidentes.
•Compromisos de seguridad y tratamiento responsable de los datos personales.

Esta comunicación debe ser **clara, accesible, veraz y transparente**, de manera que fortalezca la confianza de los titulares y evidencie la **responsabilidad demostrada** ante la autoridad de control.

MEJORA CONTINUA

El programa debe contar con un **Plan de Supervisión y Revisión** que establezca la periodicidad, metodología y responsabilidades para llevar a cabo las evaluaciones.

Deben realizarse auditorías internas o revisiones sistemáticas para verificar el cumplimiento de políticas, procedimientos, controles, capacitación, etc.

Los hallazgos de esas auditorías o revisiones deben permitir identificar **brechas, debilidades o áreas de mejora**, y generar planes de acción para corregirlas.

Las mejoras implementadas deben documentarse, evidenciarse y presentar informes de seguimiento, los cuales deben ser reportados a la alta dirección

Este ciclo de revisión y mejora continua es indispensable para cumplir con el principio de responsabilidad demostrada, dado que demuestra que la organización no solo ha adoptado medidas, sino que las mantiene y las mejora según evolución de riesgos, tecnología y normativa.

DELITOS INFORMÁTICOS

La ley 1273 de 2009 adiciona al Código Penal un título que hace referencia a la protección de la información y de los datos, los delitos tipificados en dicha ley son:

Art. 269A Acceso abusivo a un sistema informático: "El que, sin autorización o por fuera de lo acordado, acceda en todo o en parte a un sistema informático protegido o no con una medida de seguridad, o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo…"Es el delito que se comete cuando se accede sin autorización a todo o en parte a un sistema informático que está protegido o no con una medida de seguridad.

Art. 269B Obstaculización ilegítima de sistema informático o red de telecomunicación: "Este delito consiste en impedir u obstaculizar el funcionamiento o acceso normal a un sistema informático.

Art. 269C Interceptación de datos informáticos: "El que, sin orden judicial previa intercepte datos informáticos en su origen, destino o en el interior de un sistema informático, o las emisiones electromagnéticas provenientes de un sistema informático que los transporte…"Es cuando sin una orden judicial previa se interceptan los datos informáticos en su origen, destino o en el interior de un sistema informático.

DELITOS INFORMÁTICOS

Art. 269D Daño informático: "Es cuando se destruye, daña, borra, deteriore, alteran o suprimen datos informáticos sin estar facultados para hacerlo.

Art. 269E Uso de software malicioso: "Es cuando una persona produce, trafique, adquiere, distribuye, venda, envíe, introduzca o extraiga del territorio nacional software malicioso u otros programas de computación de efectos dañinos.

Art. 269F Violación de datos personales: "Es cuando con provecho propio o de un tercero se obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique o emplee códigos personales, datos personales, contenidos en ficheros, archivos, bases de datos o medios semejantes.

Art. 269G Suplantación de sitios web para capturar datos personales Quien con un fin ilícito diseñe, desarrolle, trafique, venda, ejecute, programe o envíe páginas electrónicas, enlaces o ventanas emergentes.

DELITOS INFORMÁTICOS

Art. 269I Hurto por medios informáticos y semejantes: *"El que, superando medidas de seguridad informáticas, realice la conducta señalada en el artículo 239 manipulando un sistema informático, una red de sistema electrónico, telemático u otro medio semejante, o suplantando a un usuario ante los sistemas de autenticación y de autorización establecidos, incurrirá en las penas señaladas en el artículo 240 de este Código".*

Art. 269J Transferencia no consentida de activos: *"El que, con ánimo de lucro y valiéndose de alguna manipulación informática o artificio semejante, consiga la transferencia no consentida de cualquier activo en perjuicio de un tercero…"*
Igualmente, "…quien fabrique, introduzca, posea o facilite programa de computador destinado a la comisión del delito descrito en el inciso anterior, o de una estafa".

BIBLIOGRAFÍA

- Ley 1581 del 2012 que habla del tratamiento de datos personales
- Ley 1712 del 2014 Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones.
- GUÍA PARA LA CLASIFICACIÓN DE LA INFORMACIÓN DE ACUERDO CON SUS NIVELES DE SEGURIDAD AGN Archivo General de la Nación de Colombia. https://www.archivogeneral.gov.co/sites/default/files/Estructura_Web/3_Transparencia/3.3%20Procesos%20y%20Procedimientos/GIT-G-01_GUIA_PARA_LA_CALIFICACI%C3%93N_DE_LA_INFORMACI%C3%93N_AGN.pdf
- ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection — Information security management systems — Requirements. International Organization for Standardization.
- ISO/IEC 27701:2019. Security techniques — Extension to ISO/IEC 27001
- ISO/IEC 27002 for privacy information management — Requirements and guidelines.
- OCDE (2002). Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.Floridi, L. (2018).
- The Ethics of Information. Oxford University Press.Solove, D. J. (2006).
- A Taxonomy of Privacy. University of Pennsylvania Law Review.

PREGUNTAS


POSITIVA
COMPAÑÍA DE SEGUROS
suma 5.0
educa
comunica
EVALUÉMONOS
Fórmulas para la vida
Valores + Emociones + Competencias
Respeto + Gratitud + Ética y sostenibilidad

POSITIVA COMPAÑÍA DE SEGUROS | suma 5.0 | educa | comunica

Recuerda que POSITIVA tiene para ti:

Posipedia

https://posipedia.com.co/

- Cursos virtuales
- Artículos
- Audios
- Juegos digitales
- OVAS
- Guías
- Mailings
- Videos

POSITIVA COMPAÑÍA DE SEGUROS | suma 5.0 | educa | comunica

¿Quieres profundizar tus conocimientos y potenciar tus competencias en SST?

¡Capacítate y fortalece
la seguridad de tu empresa!

CURSOS

VIRTUALES SG-SST DE 50 Y 20 HORAS

Escanea e inscríbete

Para trabajadores de todas las empresas, áreas y sectores.

¡TE ESPERAMOS!

Positiva Prevención

Hacienda

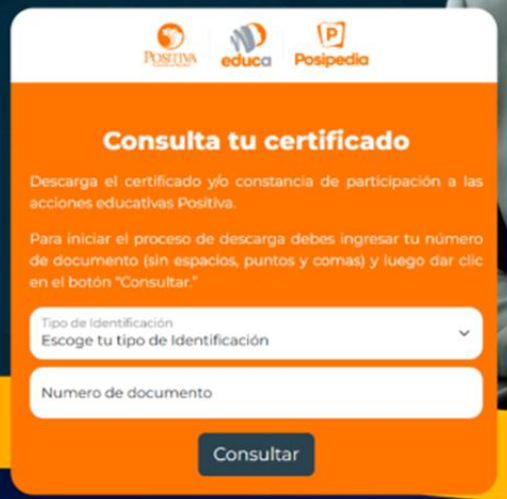
POSITIVA COMPAÑÍA DE SEGUROS | suma 5.0 | educa | comunica | Posipedia

Conoce cómo

descargar los certificados de las acciones educativas

01

02



03

Paso 1:
Escanea el código QR

Paso 2:
Selecciona el **tipo de documento** y escribe el **número**, una vez diligenciados da clic en consultar.

Paso 3:
Encontrarás tu historial académico y podrás generar la descarga de tu certificado en el icono

POSITIVA COMPAÑÍA DE SEGUROS | suma 5.0 | educa | comunica

¡CONÉCTATE A NUESTRO CANAL de WhatsApp!

POSITIVA PREVENCIÓN

Descubre campañas, novedades y tips en Seguridad y Salud en el Trabajo (SST) que te ayudarán a fortalecer tu bienestar y la cultura de prevención laboral.

¡Únete y sé parte de la comunidad de Positiva!