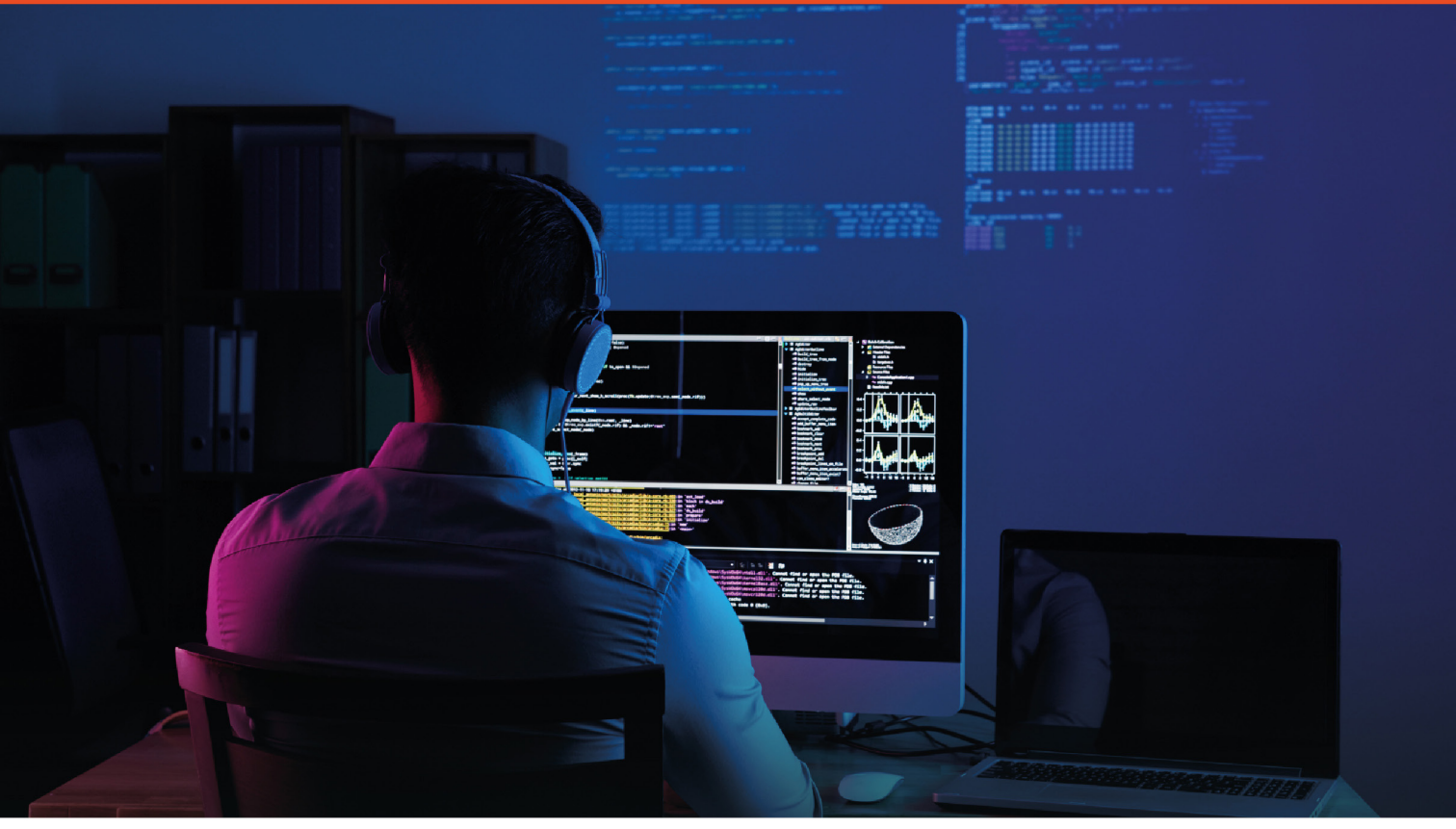
#9

ABC

Esquemas de ciberseguridad: Aspectos legales para proteger datos en las empresas



LLOREDA · CAMACHO &CO

Invest in Bogotá

1. ¿Cómo se encuentra regulada la ciberseguridad en Colombia?

Si bien no existen normas específicas en materia de ciberseguridad, este tema se ha abordado desde la perspectiva de la protección de datos personales y privacidad:

Ley de Protección de Datos Personales (Ley 1581 de 2012)

Incluye el **principio de seguridad** por el cual la información procesada por responsables o encargados debe ser tratada con medidas humanas, técnicas y administrativas que permitan dotar de seguridad a los archivos, evitando de esa forma la adulteración, consulta o uso no autorizado o pérdida de la información. Además, deben garantizar condiciones adecuadas de seguridad y reportar incidentes a la Superintendencia de Industria y Comercio (SIC).

Decreto Único reglamentario del Sector Comercio, Industria y Turismo (Decreto 1074 de 2015)

Reglamenta la Ley 1581 de 2012 e indica que el responsable del tratamiento de datos personales debe demostrar haber implementado medidas apropiadas y efectivas para cumplir con la Ley, y para mitigar los riesgos potenciales que el tratamiento puede conllevar para titulares.

Capítulo II, Título V – Circular Única de la Superintendencia de Industria y Comercio

Las empresas obligadas al reporte en el Registro Nacional de Bases de Datos (RNBD) deberán reportar cualquier incidente de seguridad dentro de los 15 días hábiles siguientes al momento de su detección o conocimiento.

Ley de Delitos Informáticos (Ley 1273 de 2009)

Incorpora en el ordenamiento penal colombiano delitos relacionados con la protección de la información y de los datos.

Seguridad Digital (Decreto 338 de 2022)

Los particulares que cumplan funciones administrativas o públicas, así como privados que administren y gestionen infraestructuras críticas cibernéticas o presten servicios esenciales, deben implementar estrategias para asegurar una adecuada gobernanza de la seguridad digital e identificación de riesgos.

Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones (Decreto 1078 de 2015)

Regula de manera general el sector TIC en Colombia e incluye disposiciones en materia de seguridad digital:

(i) Deber de contar con una estrategia de seguridad y privacidad de la información, seguridad digital y continuidad de la prestación del servicio.

(ii) Obligación de implementar el Modelo de Gobernanza de Seguridad Digital con instancias como: la Coordinación, el Comité y los Grupos de trabajo Nacionales de Seguridad Digital, Las Mesas de Trabajo y los Puestos de Mando Unificado de Seguridad Digital.

(iii) A la fecha de publicación de este ABC, el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC) trabaja en un inventario de infraestructuras críticas públicas cibernéticas y de servicios públicos esenciales, vinculando sectores económicos como telecomunicaciones, que deben reportar incidentes en la Plataforma Nacional de Notificación y Seguimiento de Incidentes.

(iv) Concreta el "Modelo Nacional de Atención y Gestión de incidentes" como reacción a posibles ataques cibernéticos y establece los equipos de respuesta:

- El COLCERT - Equipo de Respuesta a Emergencias Cibernéticas de Colombia.
- El CSIRT - Gobierno (Equipo de Respuesta a Incidentes de Seguridad Digital de Gobierno).
- El CSIRT - Defensa (Equipo de Respuesta a Incidentes de Seguridad Digital del Sector Defensa).
- El CSIRT del Sector Inteligencia.
- Los CSIRT - Sectoriales (Equipos de Respuesta a Incidentes de Seguridad digital de los sectores definidos como críticos o prestadores de servicios esenciales).

2. Pronunciamientos relevantes de la Superintendencia de Industria y Comercio (SIC)

La SIC emite diversas guías sobre seguridad de la información, que, aunque no son vinculantes, proporcionan a los responsables y encargados lineamientos aplicables a esquemas de ciberseguridad en empresas.

a. Guía para la gestión de incidentes de seguridad en el tratamiento de datos personales[1]

Lineamientos para reportar incidentes de seguridad a la autoridad, así como recomendaciones para gestionar los incidentes de seguridad. El registro del incidente debe contener: i) una descripción general, las categorías de los titulares afectados, ii) las indagaciones e investigaciones realizadas internamente por la empresa, iii) las medidas correctivas aplicables, iv) la prueba del reporte a la SIC y v) una evaluación del nivel de riesgo derivado del incidente.

b. Guía para la implementación del principio de responsabilidad demostrada (accountability)[2]

Establece que las empresas deben crear un programa integral de gestión de datos personales que adopte y cree crear un componente de gestión de riesgos internos y externos en su estructura de seguridad organizacional y cibernética. Este programa implica crear un área o persona encargada de manejar los incidentes de seguridad en los sistemas de información donde se gestionan datos personales y archives físicos, así como mecanismos para notificar y reportar rápidamente a los titulares y a la SIC.

[1]Disponible en: https://www.sic.gov.co/sites/default/files/files/Publicaciones/Guia_gestion_incidentes_dic21_2020.pdf
[2]Disponible en: https://www.sic.gov.co/sites/default/files/files/2021/2021%20Gu%C3%ADas%20para%20implementaci%C3%B3n%20del%20principio%20de%20responsabilidad%20demostrada%202021.pdf

c. Guía para la implementación del principio de responsabilidad demostrada en las transferencias internacionales de datos personales[3]

Se recomienda adoptar mecanismos de privacidad desde el diseño y por defecto para garantizar la seguridad de los datos transferidos. Esto implica implementar medidas tecnológicas, organizacionales y humanas preventivas a lo largo del ciclo de vida de los datos, considerando factores como la naturaleza de la información, posibles consecuencias de una vulneración y recursos disponibles. Las medidas de seguridad deben ser revisadas continuamente para asegurar su efectividad y alinearse con el contexto y finalidades del tratamiento.

Además, se sugiere realizar evaluaciones de impacto de privacidad que contengan:

- Descripción detallada de las operaciones de tratamiento de datos.
- Evaluación de los riesgos específicos para los derechos y libertades de los titulares de datos.
- Identificación y clasificación de riesgos, adopción de medidas para mitigarlos.

[3]Disponible en: https://www.sic.gov.co/sites/default/files/files/2023/guia-implementacion-clausulas-contractuales-modelo-tidp-es.pdf

d. Guía sobre el Oficial de Protección de Datos Personales (OPD)[4]

El OPD debe funcionar como un enlace entre las políticas de protección de datos de las diversas áreas de la organización. En caso de producirse incidentes de seguridad, es importante que dentro del organigrama interno de la empresa exista un sistema de consulta y reporte inmediato al OPD, para que este pueda asumir medidas correctivas y mitigar los riesgos generados por el incidente.

e. Guía con recomendaciones para el tratamiento de datos personales mediante servicios de computación en la nube[5]

Recomienda realizar evaluaciones de impacto de privacidad antes y durante el uso del servicio en la nube, así como incorporar estándares de ética y seguridad desde el diseño y por defecto, adoptando medidas de seguridad proporcionales niveles de riesgos del tratamiento, la naturaleza o sensibilidad de los datos, la magnitud del daño que se puede causar a los titulares y al responsable, la cantidad de información y las categorías de datos que serán objeto del tratamiento.

[4]Disponible en: https://www.sic.gov.co/sites/default/files/files/2023/Guia%20de%20datos%202023%20(2).pdf
[5]Disponible en: https://www.sic.gov.co/sites/default/files/files/2021/Guia%20cloud%20computing%202021.pdf

3. Pronunciamientos relevantes del MinTIC

Guía para la implementación de Seguridad de la Información en una MYPYME[6]

Señala aspectos relacionados con ciberseguridad y la importancia de que las pequeñas y medianas empresas cuenten con una política preventiva que minimice las vulnerabilidades en materia de ciberseguridad.

Documento Maestro del Modelo de Seguridad y Privacidad de la Información – MSPI[7]

Dirigido a entidades públicas de orden nacional y territorial, así como a proveedores de servicios de la Política de Gobierno Digital y estrategia de seguridad digital. Se dispone un sistema de gestión de seguridad de la información – SGSI y seguridad digital, para generar confianza en el uso del entorno digital.

Guía para la Gestión y Clasificación de Incidentes de Seguridad de la Información[8]

Establece un marco para gestionar incidentes de seguridad de la información, definiendo roles, procedimientos y medidas para identificar, responder y minimizar impactos. Además, promueve la mejora continua mediante el análisis de lecciones aprendidas y el monitoreo de riesgos, con el objetivo de garantizar la protección de los activos de información en Colombia.

Para mayor información:
https://gobiernodigital.mintic.gov.co/portal/Manual-de-Gobierno-Digital/150511:Controles-de-seguridad-y-privacidad-de-la-informacion .

[6]Disponible en: https://gobiernodigital.mintic.gov.co/692/articles-150522_Guia_Seguridad_informacion_Mypimes.pdf
[7]Disponible en: https://gobiernodigital.mintic.gov.co/seguridadyprivacidad/704/articles-237872_maestro_mspi.pdf
[8]Disponible en: https://gobiernodigital.mintic.gov.co/692/articles-150509_G21_Gestion_Incidentes.pdf

Invest in Bogotá

https://es.investinbogota.org/ | Invest in Bogotá

Suscríbase a nuestros contenidos especializados.