UNIVERSIDAD DISTRITAL
FRANCISCO JOSÉ DE CALDAS

Controles de protección de la privacidad en aquellos sistemas relacionados con el riesgo tratamiento de datos personales

OFICINA ASESORA DE TECNOLOGÍAS E INFORMACIÓN

4 de noviembre de 2024

Contenido

1. INTRODUCCION

En el entorno académico actual, la Universidad Distrital Francisco José De Caldas gestiona una gran cantidad de datos personales, que incluyen información privada y sensible de estudiantes, docentes y personal administrativo. La protección de estos datos es crucial no solo para cumplir con las regulaciones legales y normativas, sino también para mantener la confianza de la comunidad universitaria y garantizar la integridad institucional.

La Universidad Distrital Francisco José De Caldas enfrenta desafíos específicos en la protección de datos debido a su naturaleza abierta y colaborativa. Las instituciones académicas deben encontrar un equilibrio entre la accesibilidad de la información, necesaria para fomentar la investigación y el aprendizaje, y la protección de la privacidad y seguridad de los datos personales. Además, deben adaptarse continuamente a las amenazas emergentes y a los cambios tecnológicos, asegurando que las medidas de seguridad evolucionen junto con las nuevas vulnerabilidades y riesgos asociados.

Este equilibrio es fundamental para preservar la confianza de estudiantes, empleados y colaboradores, y para promover un entorno académico seguro que apoye tanto la innovación como la protección de la información personal.

2. OBJETIVO GENERAL

Determinar controles de protección de la privacidad en aquellos sistemas relacionados con el riesgo de tratamiento de datos personales con el fin de optimizar la gestión de la información, garantizar la confidencialidad, disponibilidad e integridad para así evitar divulgaciones de datos personales que puedan ocasionar problemas significativos para la Universidad Distrital Francisco José de Caldas.

3. OBJETIVOS ESPECIFICOS

- Conocer los controles que actualmente están implementados para la protección de datos personales, mediante reuniones con diferentes áreas tecnológicas de la Universidad Distrital, con el fin de identificar el estado actual de los controles para protección de datos personales.
- Conocer los requisitos exigidos por las buenas prácticas sobre controles de protección de datos personales, con el fin de identificar que controles se deben implementar para la protección de datos personales.
- Priorizar los controles de protección de datos personales que se identificaron, para definir su implementación.

4. ALINEACION CON PLAN INIDICATIVO 2022-2025

En el manual de políticas de tratamiento de datos personales, la Universidad Distrital a definido:

- La Universidad Distrital dando cumplimiento a la previsto en la Ley 1581 de 2012 “Por la cual se dictan disposiciones generales sobre la protección de datos personales”, adopta el presente manual interno de políticas y procedimientos para garantizar su cabal cumplimiento, en especial, para la atención de consultas y reclamos por parte de los titulares de los datos personales.
- Además, esta institución académica pretende el desarrollo del derecho constitucional del habeas data del cual son titulares todas las personas sobre quienes la Universidad haya recopilado, administre o conserve información de carácter personal garantizando la protección de sus derechos a la privacidad, intimidad y buen nombre e imagen

Estas dos premisas están alineadas para soportar el “Plan indicativo 2022-2025" detalladas a continuación:

Metas de preparación de las TIC para la protección de los datos personales

De acuerdo con el “Plan Indicativo 2022-2025", se plantean las siguientes metas de preparación de las TIC para la protección de los datos personales, alineado con:

- “Eje transformador 1. Fortalecimiento curricular y aseguramiento de la calidad” y el lineamiento “Implementación de estrategias que permitan contar con información institucional confiable y pertinente que redunden en reportes de información con criterios de calidad.”
- “Eje transformador 2. Modernización institucional” y los lineamientos “Conformación e implementación de una Unidad con carácter directivo que coordine y lidere los procesos relacionados con TIC en la U. Distrital” y “Fortalecimiento del Sistema Integrado de Gestión de la Universidad, SIGUD y su marco de referencia el Modelo Integrado de Planeación y Gestión, MIPG, de tal manera que se consolide como una herramienta integrada para la gestión institucional.”
- “Eje transformador 4. Talento Humano y Bienestar” y el lineamiento “Integrar la gestión de información que garantice la adecuada caracterización con transparencia de la información y las acciones realizadas para los diversos apoyos brindados a la comunidad universitaria.”
- “Eje transformador 5. Transformación digital” y el lineamiento “Implementación de una estrategia de transformación digital en la Universidad Distrital que este fundamentada en las tecnologías disruptivas para brindar servicios de alto valor además de emprendimientos digitales.”

5. RIESGOS EN PROTECCION DE DATOS PERSONALES

La protección de los datos personales en la Universidad Distrital enfrenta múltiples riesgos de seguridad de la información que pueden comprometer la confidencialidad, integridad y disponibilidad de la información.

Estos riesgos se pueden generar por acciones como:

- Abuso de privilegios por parte de personas con acceso legítimo a los sistemas para acceder a datos personales sin autorización.
- Terceras personas acceden a los datos vulnerado su confidencialidad
- Se modifican los datos perdiendo su integridad
- Uso ilegítimo de los datos que vulneran los derechos de los interesados

- Imposibilidad de acceso a los datos porque no están disponibles

La identificación y gestión de los riesgos es crucial para la protección efectiva de los datos personales en la Universidad Distrital. Implementar controles de seguridad de la información adecuados y mantener una cultura de concienciación y capacitación continua es esencial para mitigar estos riesgos y asegurar la privacidad y seguridad de la información.

6. PLANIFICACION

Para establecer los mecanismos de control de seguridad de la información necesarios para proteger los datos personales se deben adelantar las siguientes actividades, basado en el análisis de los controles existentes en la Universidad Distrital que no están cumpliendo al 100%.

Revisar y aceptar la priorización propuesta sobre los controles de protección de datos personales, teniendo en cuenta:

Controles Administrativos

- Definir las políticas o procedimientos sobre los controles de gestión de acceso a bases de datos, copias de respaldo, acceso remoto, intercambio de información, validación de datos personales y terceras partes.
- Definir reuniones para analizar la implementación de los controles con las siguientes áreas:
    - Proyecto Actas, Archivo y Microfilmación = Ciclo de vida datos personales
    - Oficina de Talento humano = Mejorar la seguridad de la información basado en análisis de incidentes.
    - Oficina de Control Interno = Plan de auditoria
    - Secretaria General = Procedimiento reporte ante la SIC. (nombres de las dependencias)
- Incluir un apartado con respecto al tema de datos personales en los documentos de continuidad del servicio, escritorio limpio, acceso a datos personales, riesgos en datos personales, monitoreo de logs, control de cambios y gestión documental para así tener control sobre estos y mitigar fugas de información.

Controles Técnicos

- Definir los controles sobre dispositivos móviles, DLP. IPS, IDS, correlación de eventos, teletrabajo, APIs, ofuscamiento, estaciones de trabajo.

Implementar los controles sobre cifrado, monitoreo de logs, accesos, servidores, firewall, correo, antivirus.

7. CONTROLES ESPECIFICOS RECOMENDADOS A IMPLEMENTAR

Para establecer los mecanismos de control de seguridad de la información necesarios para proteger los datos personales se tuvieron en cuenta los controles recomendados por las buenas prácticas como la Norma ISO 27001, las medidas de seguridad de la información establecidos en el Manual de Usuario del Registro Nacional de Bases de Datos – RNBD, los controles identificados

en el documento Brecha de seguridad de acuerdo al instrumento evaluación MSPI del MinTIC, el Checklist de revisión controles seguridad de datos – protección de datos personales definido por la alta consejería distrital de TIC y la información suministrada por la Oficina Asesora De Tecnologías e Información (OATI) sobre controles de seguridad implementados a nivel de sistemas de información y bases de datos.

Para esto se validó los controles existentes con las áreas de tecnologías, conocedoras de los controles implementados para protección de datos personales y como encargadas del manejo y resguardo de los datos personales: Unidad De Red De Datos (UDNET), Oficina Asesora de Planeación, Red De Investigaciones De Tecnología Avanzada (RITA), Oficina Asesora de Tecnologías e Información.

De acuerdo con los controles identificados, en la Tabla 1 se relacionan las políticas, procedimientos controles administrativos y controles técnicos necesarios para proteger los datos personales, indicando su nivel de implementación, su prioridad de implementación recomendado y los responsables.

Tabla 1. Controles protección datos personales

CONTROLES	% CUMPLIMIENTO	ENUMERACIÓN	PRIODIDAD	RESPONSABLES
ADMINISTRATIVOS				
Gestión Riesgos Datos Personales	25,00%	A.1	2	Oficina Asesora de Tecnologías e Información Oficina Asesora de Planeación
Gestión de usuarios privilegiados en BD - DP	50,00%	A.2	2	Oficina Asesora de Tecnologías e Información Oficina Asesora de Planeación
Monitoreo consultas	0,00%	A.3	1	Oficina Asesora de Tecnologías e Información Unidad de red de datos UDNET Red de Investigaciones de

				Tecnología Avanzada
Definición de un Plan de continuidad y DRP	50,00%	A.4	2	Oficina Asesora de Tecnologías e Información Oficina Asesora de Planeación
Definición de la Gestión de seguridad de la información en proveedores	50,00%	A.5	2	Oficina Asesora de Tecnologías e Información Oficina Asesora de Planeación
Nombramiento de Oficial de protección de datos	0,00%	A.6	1	Oficina Asesora de Tecnologías e Información Oficina Asesora de Planeación
Capacitación en seguridad de la información	50,00%	A.7	2	Oficina Asesora de Tecnologías e Información Oficina Asesora de Planeación

Definición de un área de ingeniería forense	0,00%	A.8	1	Oficina Asesora de Tecnologías e Información Oficina Asesora de Planeación
Políticas				
Política de datos Personales	100,00%	AP.1		
Política de Acceso remoto a Datos Personales	0,00%	AP.2	1	Oficina Asesora de Tecnologías e Información
Política de Copias respaldo de Datos Personales	0,00%	AP.3	1	Oficina Asesora de Tecnologías e Información
Política de Control acceso Datos Personales	0,00%	AP.4	1	Oficina Asesora de Tecnologías e Información
Política de Ciclo de vida Datos Personales	0,00%	AP.5	1	Oficina Asesora de Tecnologías e Información
Política de Reporte BD - DP ante la SIC	0,00%	AP.6	1	Oficina Asesora de Tecnologías e Información
Política para mejorar la seguridad de la información personal a partir de los incidentes o vulnerabilidades detectados	0,00%	AP.7	1	Oficina Asesora de Tecnologías e Información

Política de Auditoria (BD)	0,00%	AP.8	1	Oficina Asesora de Tecnologías e Información
Política de Escritorio Limpio	50,00%	AP.9	2	Oficina Asesora de Tecnologías e Información
Formalización de la Política desarrollo seguro	0,00%	AP.10	1	Oficina Asesora de Tecnologías e Información
Procedimientos				
Procedimiento para la Gestión de usuarios con acceso a Datos Personales	0,00%	APT.1	1	Oficina Asesora de Tecnologías e Información
Procedimiento de requisitos de seguridad de los sistemas de Datos Personales	0,00%	APT.2	1	Oficina Asesora de Tecnologías e Información
Procedimiento de Auditoria Tecnológica	0,00%	APT.3	1	Oficina Asesora de Tecnologías e Información
Procedimiento intercambio de Datos Personales	0,00%	APT.4	1	Oficina Asesora de Tecnologías e Información
Procedimiento de Validación de datos	0,00%	APT.5	1	Oficina Asesora de Tecnologías e Información
Procedimiento de disposición final información	0,00%	APT.6	1	Oficina Asesora de Tecnologías e Información

Política de procedimientos de Incidentes	50,00%	APT.7	2	Oficina Asesora de Tecnologías e Información
AWS				
BACKUP	100,00%			
WAF	100,00%			
Control DDoS	100,00%			
Desarrollo	100,00%			
Almacenamiento seguro de contraseñas	100,00%			
Monitoreo infraestructura	100,00%			
Revisión de Logs	100,00%			
Antimalware	100,00%			
Gestión de usuarios	100,00%			
Revisión de Alertas	100,00%			
Soporte	100,00%			
BD				
Cifrado	33,30%	B.1	2	Oficina Asesora de Tecnologías e Información Unidad de red de datos UDNET Rita
Cifrado de campos	33,30%	B.2	2	Oficina Asesora de Tecnologías e Información Unidad de red de datos UDNET Red de Investigaciones de

				Tecnología Avanzada.
Habilitación de Logs	100,00%	B.3		
Protección imágenes seguridad BD	100,00%	B.4		
Backup	100,00%	B.5		
Monitoreo de logs	50,00%	B.6	2	Oficina Asesora de Tecnologías e Información Unidad de red de datos UDNET Red de Investigaciones de Tecnología Avanzada.
Control de cambios	50,00%	B.7	2	Oficina Asesora de Tecnologías e Información
Control de acceso	50,00%	B.8	2	Oficina Asesora de Tecnologías e Información Unidad de red de datos UDNET Red de Investigaciones de Tecnología Avanzada
Parches software de gestión	33,30%	B.9	2	Oficina Asesora de Tecnologías e Información

				Unidad de red de datos UDNET Red de Investigaciones de Tecnología Avanzada
CONTROLES TECNICOS				
Seguridad Física	50,00%	C.1	2	Oficina Asesora de Tecnologías e Información
Control estaciones de trabajo	50,00%	C.2	2	Oficina Asesora de Tecnologías e Información
Control Dispositivos móviles	0,00%	C.3	1	Oficina Asesora de Tecnologías e Información
Protección de Red	100,00%	C.4		
Seguridad en Servidores	50,00%	C.5	2	Oficina Asesora de Tecnologías e Información Unidad de red de datos UDNET
Controles Sitios Web	100,00%	C.6		
Registro de Actividades	100,00%	C.7		
Monitoreo de Actividades	50,00%	C.8	2	Oficina Asesora de Tecnologías e Información
Monitoreo Firewall	50,00%	C.9	2	Oficina Asesora de Tecnologías e Información Unidad de red de datos UDNET

Cifrado	33,30%	C.10	2	Oficina Asesora de Tecnologías e Información Unidad de red de datos UDNET Red de Investigaciones de Tecnología Avanzada
DLP	0,00%	C.11	1	Oficina Asesora de Tecnologías e Información
IDS/IPS	0,00%	C.12	1	Oficina Asesora de Tecnologías e Información
Backup	100,00%	C.13		
Protección de Correo	50,00%	C.14	2	Oficina Asesora de Tecnologías e Información Unidad de red de datos UDNET
Antivirus	80,00%	C.15	3	Oficina Asesora de Tecnologías e Información Unidad de red de datos UDNET
Monitoreo eventos correlación de eventos	0,00%	C.16	1	Oficina Asesora de Tecnologías e Información
Política de Seguridad información	80,00%	C.17	3	Oficina Asesora de Tecnologías e Información
Roles y Responsabilidades	80,00%	C.18	3	Oficina Asesora de Tecnologías e Información

Gestión documental	25,00%	C.19	2	Oficina Asesora de Tecnologías e Información Oficina Asesora de Planeación Proyecto Actas, Archivo y Microfilmación
Trabajo remoto	0,00%	C.20	1	Oficina Asesora de Tecnologías e Información
Cifrado de información	33,30%	C.21	2	Oficina Asesora de Tecnologías e Información Unidad de red de datos UDNET Red de Investigaciones de Tecnología Avanzada
Aseguramiento de API	0,00%	C.22	1	Oficina Asesora de Tecnologías e Información
Controles de mantenimiento	50,00%	C.23	2	Oficina Asesora de Tecnologías e Información
Controles de ofuscamiento en ambientes de prueba	0,00%	C.24	1	Oficina Asesora de Tecnologías e Información
Restricción de los puertos que permitan la conexión y/o acceso a dispositivos de almacenamiento extraíbles (CD, USB, SD Card, etc.).	80,00%	C.25	3	Oficina Asesora de Tecnologías e Información Unidad de red de datos UDNET

Implementación de las opciones de hibernación y/o suspensión automática.	0,00%	C.26	2	Oficina Asesora de Tecnologías e Información

Prioridad

- **1**: Controles con 0% de cumplimiento, que son críticos para la seguridad de los datos personales.
- **2**: Controles con cumplimiento entre 25% y 50%, que deben ser mejorados para cumplir con los estándares.
- **3**: Controles con cumplimiento entre 50% y 99%, que, aunque están en progreso, aún requieren atención.

7.1. DETALLE DE CONTROLES A IMPLEMENTAR

De acuerdo con la identificación de los controles que están implementados, los no implementados y los implementados parcialmente, los siguientes controles deben ser revisados y mejorados o implementados para lograr la protección de los datos personales de la Universidad Distrital.

7.1.1. CONTROLES ADMINISTRATIVOS

7.1.1.1. SEGURIDAD DE LA INFORMACION PERSONAL – SIC RNBD

7.1.1.1.1. SEGURIDAD DE LA INFORMACIÓN PERSONAL

- Definir documento de seguridad de la información personal o general aprobado

  Un documento de seguridad de la información personal es aquel que contiene los lineamientos y/o políticas administrativas, humanas y técnicas que se deben adoptar por todas las áreas de la organización y cada uno de sus integrantes en el cuidado de los datos personales, con el objeto de cumplir el principio de seguridad a que se refiere la ley 1581 de 2012 que en su artículo 4, literal g enuncia: “Principio de seguridad: La información sujeta a tratamiento por el responsable del Tratamiento o encargado del tratamiento a que se refiere la presente ley, se deberá manejar con las medidas técnicas, humanas y administrativas que sean necesarias para otorgar seguridad a los registros evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.” **(Tabla 1: AP.1.)**

- Documentación de procesos en torno a la seguridad de la información personal

  Se refiere a la existencia de documentos que describan los procesos relacionados con la seguridad de la información que involucra datos personales.

- Definir procedimientos de asignación de responsabilidades y autorizaciones en el tratamiento de la información personal.

  Se refiere a si tiene por escrito o documentado quién tiene la responsabilidad en el tratamiento de datos personales en los pasos de los procesos y/o procedimientos relacionados con dicho tratamiento. **(Tabla 1: APT.2)**

- Implementar acuerdos de confidencialidad con las personas que tienen acceso a la información personal

  Está relacionado con el principio de Confidencialidad contemplado por la Ley 1581 de 2012, que indica: "Principio de confidencialidad: 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 sólo realizar suministro o comunicación de datos personales cuando ello corresponda al desarrollo de las actividades autorizadas en la presente ley y en los términos de la misma."

- Implementar controles de seguridad en la tercerización de servicios para el tratamiento de la información personal

  Corresponde a aquellos controles implementados en los procesos o tratamiento de datos que se realizan a través de terceros ajenos a la organización, que corresponden a encargados del tratamiento de datos personales.

7.1.1.1.2. SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

- Implementar herramientas de gestión de riesgos en el tratamiento de datos personales

Herramientas de gestión de riesgo se denomina a la combinación de sistemas, controles, instrumentos, metodologías, etc., que permiten facilitar los procesos de prevención, mitigación y preparación de las capacidades de la organización para evitar, disminuir o transferir los efectos adversos o impactos negativos de las amenazas detectadas en un proceso de análisis del entorno durante cada una de las etapas del ciclo del dato y la naturaleza de estos. El responsable es libre de utilizar la herramienta o metodología que desee, de acuerdo con sus necesidades y capacidades organizacionales. Se debe tener una documentación de la metodología utilizada para la evaluación del riesgo. **(Tabla 1: A.1.)**

- Implementar un sistema de gestión de seguridad de la información o un programa integral de gestión de datos personales

Un sistema de gestión de seguridad de la información o SGSI es un conjunto de lineamientos y/o políticas administrativas, humanas y técnicas de administración de la información. El concepto lo usan diferentes estándares, principalmente la ISO/IEC 27001. En cuanto al Programa Integral de Gestión de Datos Personales PIGDP consiste en implementar al interior de la organización las medidas apropiadas y efectivas para cumplir con las obligaciones establecidas en la Ley 1581 de 2012. Para lo cual el Decreto 1074 en su sección 6 desarrolla el principio de responsabilidad demostrada frente al tratamiento de datos personales y la Superintendencia de Industria y Comercio publicó la guía para la implementación del principio de responsabilidad demostrada

(Accountability) en las organizaciones, publicado en la página web de la SIC www.sic.gov.co. Por medio del SGSI o de un PIGDP, la organización realiza el diseño, implantación, mantenimiento de un conjunto de procesos para gestionar de manera eficiente el acceso y uso de la información en general con base en los principios de la seguridad de esta que son la confidencialidad, integridad y disponibilidad, para de esta manera minimizar los riesgos asociados al tratamiento de la información, de acuerdo con su clasificación y naturaleza de los datos. **(Tabla 1: A.1.)**

7.1.1.1.3. SEGURIDAD DE LA INFORMACIÓN PERSONAL EN TORNO AL RECURSO HUMANO

- Implementar controles de seguridad de la información personal para el recurso humano antes de la vinculación y una vez finalizado el contrato laboral

Políticas y controles relacionados con el recurso humano vinculado a la organización que tendrá acceso a la información personal, antes, durante y posterior al desempeño de las funciones. Por ejemplo, acuerdos de confidencialidad de la información, estudios de seguridad previos a la contratación, cierre y control para perfiles de acceso a la información una vez finalizada la relación contractual, etc. **(Tabla 1: A.5.)**

7.1.1.1.4. CONTROL DE ACCESO A LA INFORMACIÓN PERSONAL (Tabla 1: B.8)

- Definir una política de control de acceso a la información personal, tanto en las instalaciones físicas como a nivel tecnológico

Se deben implementar medidas o controles para regular el acceso a la información personal, estas políticas deben contemplar tanto el acceso físico (a las instalaciones) como el acceso lógico (al software, aplicaciones, usuarios, IP´s, claves, etc.). Esto es definir quién tiene permisos sobre la información personal y qué puede hacer exactamente con los datos personales. **(Tabla 1: AP.4.)**

- Definir un procedimiento para la gestión de usuarios con acceso a la información personal

Es complemento del control de acceso a la información personal. Está relacionado con las políticas para el control de los usuarios que tienen acceso a los datos personales. Esto es definir quién es el responsable de crear los usuarios, autorizaciones, seguridad en cuanto a claves, notificaciones, eliminación, perfiles de acceso, permisos, entre otros. **(Tabla 1: APT.1.)**

- Implementar una política específica para el acceso a la información personal de las bases de datos con información personal sensible

Se relaciona con la política para regular el acceso a la información personal, pero donde se alude específicamente al tratamiento de los datos sensibles (aquellos cuyo uso inadecuado puede generar discriminación), dentro de las políticas generales de acceso a la información o con políticas específicas para este tipo de datos. Estas políticas deben contemplar tanto el acceso físico (a las instalaciones) como el acceso lógico (al software, aplicaciones, usuarios, IP´s, claves, etc.), dentro de las cuales se define entre otros aspectos quién tiene permisos sobre dichos datos y qué puede hacer exactamente con ellos. **(Tabla1:AP.4.)**

- Definir una política implementada de copia de respaldo de la información personal

Hace referencia a si se tiene una política que indique a qué datos se les realiza una copia de seguridad, esto depende de la definición que la organización realice en cuanto a tipos de datos, tiempos de retención, datos a respaldar, medios de almacenamiento, ubicación de la copia, pruebas de restauración, disposición final, entre otros aspectos. **(Tabla 1: AP.3.)**

- Implementar política de protección para el acceso remoto a la información personal

Se refiere a las medidas de seguridad que se implementen para garantizar una forma confiable de consulta, uso o extracción de la información remota, desde dispositivos que no estén en la organización. Lo anterior teniendo en cuenta las posibilidades que hoy existen de consultar los datos que una empresa tenga en sus servidores, equipos, datacenter, etc., desde diferentes puntos como dispositivos móviles, agilizando procesos de consulta, promoción y venta, etc. es importante asegurar y controlar dichos accesos a la red de la Organización. **(Tabla 1: AP.2)**

7.1.1.1.5. SEGURIDAD EN LOS SISTEMAS DE INFORMACIÓN PERSONAL

- Implementar un procedimiento que contemple la definición de especificaciones y requisitos de seguridad de los sistemas de información personal

Es documentar los pasos y metodología utilizadas para definir las necesidades identificadas antes, durante y posterior al desarrollo de sistemas de información relacionados con el tratamiento de datos personales, en lo relativo a la seguridad de la información en cada etapa del ciclo del dato en el que apoye el sistema de información. **(Tabla 1: AP.10)**

- Implementar controles de seguridad de la información durante el mantenimiento (Control de cambios) de los sistemas de información personal

Se refiere a si existen controles implementados sobre la documentación sobre los cambios que requieran los sistemas de información o específicamente aquellos que incluyen el tratamiento de datos personales. **(Tabla 1: B.7)**

- Implementar un procedimiento implementado de auditoría de los sistemas de información que contengan datos personales
- Implementar procedimientos automatizados que permitan evaluar la eficiencia y suficiencia de los controles implementados a un sistema de información mediante el cual se traten datos personales para evitar su pérdida, uso o acceso no autorizado o fraudulento, de manera que se garantice la disponibilidad, integridad y confidencialidad de los datos personales. **(Tabla 1: APT.3.)**
- Definir un monitoreo de consulta sobre las bases de datos con información personal
- Permitir efectuar trazabilidad o seguimiento de cualquier consulta que realice sobre la base de datos con información personal. Lo cual se definirá dependiendo del riesgo a que esté expuesta esta información y la naturaleza de los datos que se estén tratando. **(Tabla 1: A.3.)**

7.1.1.1.6. PROCESAMIENTO DE INFORMACIÓN PERSONAL

- Definir una política implementada para el correcto tratamiento de la información personal en las diferentes etapas del ciclo de vida del dato (recolección, circulación y disposición final)

Está relacionado con la identificación de quién realiza qué y cómo lo hace en cada paso del tratamiento, para ello es importante elaborar una matriz de riesgo de los datos personales, identificar el ciclo del dato y en cada etapa, los riesgos asociados; una vez se realice esta tarea, se deben identificar los controles que se requieren para su gestión, demostrando así el correcto tratamiento en cada etapa. Definir un procedimiento implementado para la validación de datos de entrada y procesamiento de la información personal, para garantizar que los datos recolectados y procesados sean correctos y apropiados, como confirmación de tipos, formatos, longitudes, pertinencia, cantidad, uso, etc.

Está relacionado con la veracidad del dato, el cual se debe garantizar desde su recolección, por lo tanto, es necesario minimizar el riesgo de error o ataques por inyección de código, utilizando técnicas de validación de los datos de entrada y procesamiento, al confirmar tipos, formatos, longitudes, pertinencia, cantidad, uso, entre otros. **(Tabla 1: APT.5)**

- Implementar un control de seguridad de información para la validación de datos de salida.

Este control está relacionado con la veracidad e integridad del dato, las cuales se deben garantizar desde su recolección, procesamiento y busca tener resultados esperados. Los datos de salida son los datos esperados, que si se presume un campo con un tipo de dato definido sea ese el que se obtiene y no otro. La pertinencia de la información reportada según la finalidad. Esta es una manera de controlar la veracidad, calidad y acceso no autorizado a la información.

- Definir una política implementada para el intercambio físico o electrónico de datos (como por ejemplo durante el comercio electrónico para la compra y venta de productos o servicios), transporte y/o almacenamiento de información personal.

Se refiere a si existen medidas de seguridad que se apliquen para minimizar los riesgos asociados al intercambio de datos personales bien sea de manera física o electrónica, como interceptación, consulta no autorizada, fraude, pérdida o robo de la información.

- Definir un procedimiento o control implementado para la disposición final de la información personal (supresión, archivo, destrucción, etc.).

Una vez identificados los riesgos asociados al tratamiento de datos en cada una de las etapas, debe implementar controles coherentes en cuanto a lo que se decida hacer finalmente con dicha información, que puede ser eliminación (borrado seguro), destrucción o conservación, de manera que nunca se expongan los datos a un uso no autorizado o fraudulento que conlleve a la materialización de un riesgo tanto para el titular como para el responsable del tratamiento. **(Tabla 1: APT.6)**

7.1.1.1.7. GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN PERSONAL

- Definir una política y procedimientos implementados de gestión de incidentes de seguridad de la información personal.

Teniendo en cuenta que un Incidente de seguridad de datos personales se refiere a la violación de los códigos de seguridad o la pérdida, robo y/o acceso no autorizado de datos personales bien sea en manos del responsable del tratamiento o de su encargado, se refiere a la documentación de los pasos a seguir una vez se detecte la comisión del incidente, tanto a nivel correctivo como preventivo. Dentro de los cuales se deben determinar tiempos, roles y responsabilidades. **(Tabla 1: APT.7)**

- Implementar una política para mejorar la seguridad de la información personal a partir de los incidentes o vulnerabilidades detectados.

Una vez se han determinado las causas e impacto del incidente detectado relacionado con datos personales, es importante identificar oportunidades de mejora e implementar controles que redunden en la prevención de la ocurrencia de otros hechos relacionados con las vulnerabilidades detectadas. **(Tabla 1: AP.7.)**

7.1.1.1.8. AUDITORIAS DE SEGURIDAD DE LA INFORMACIÓN PERSONAL

- Definir una política de auditorías de seguridad de la información personal.

Definir una política de auditoría de seguridad de la información personal o en general, que permita evaluar el cumplimiento, resultados y documentación de acciones correctivas o preventivas relacionadas con el tratamiento de datos personales. **(Tabla 1: AP.8.)**

- Dentro de las auditorías de seguridad de información personal, tiene en cuenta el cumplimiento de requisitos, políticas y normas que específicamente le apliquen a la base de datos.

- Implementar una política de auditoría de seguridad de la información personal o en general (de toda la información), que permita evaluar el cumplimiento, resultados y la documentación de acciones correctivas y/o preventivas, sobre tratamiento de datos personales, donde sea posible evaluar el cumplimiento de requisitos, políticas y normas que específicamente le apliquen a la base de datos con información personal que está registrando. **(Tabla 1: AP.8)**

- Gestión de derechos de acceso de usuarios privilegiados.

  Se trata de administrar niveles de acceso privilegiados, más altos y estrictos. La asignación y el uso de los derechos de acceso privilegiado deben controlarse estrictamente, dados los derechos adicionales que se transmiten sobre los activos de información y los sistemas que los controlan. **(Tabla 1: A.2)**

- Política de Reporte BD - DP ante la SIC

  De conformidad con la Circular Única de la Superintendencia de Industria y Comercio, todas las sociedades y entidades sin ánimo de lucro que tengan activos totales superiores

a 100.000 Unidades de Valor Tributario (UVT), lo cual equivale a aproximadamente COP$ 4,241,200,000 para el 2023, y todas las personas Jurídicas de naturaleza pública, que traten datos personales en calidad de Responsables bajo el ámbito de aplicación de la Ley 1581 de 2012, están obligadas a registrar sus bases de datos ante el Registro Nacional de Bases de Datos ("RNBD").

Antes de registrar las bases de datos es preciso realizar el inventario de las bases de datos con información personal a cargo del responsable del tratamiento, bien sea en medio físico (papel) o electrónico (listas o archivos en cualquier formato, bases de datos relacionales, etc.).

Al efectuar este inventario se debe obtener la siguiente información:

- Cantidad de bases de datos con información personal.
- Cantidad de titulares por cada base de datos.
- Información detallada de los canales o medios que se tienen previstos para atender a los titulares.
- Tipo de datos personales contenidos en cada base de datos a los que se realiza tratamiento, como: datos de identificación, ubicación, socioeconómicos, sensibles u otros.
- Ubicación física de las bases de datos. Al respecto se preguntará si la base de datos se encuentra almacenada en medios propios, por ejemplo, archivadores o servidores (dependiendo de si se trata de un archivo físico o una base de datos electrónica), internos o externos a las instalaciones físicas del responsable.
- Cuando el tratamiento de los datos personales se realice a través de un (unos) encargado (s) del tratamiento, se solicitarán los datos de identificación y ubicación de ese (esos) encargado (s). ✓ Medidas de seguridad y/o controles implementados en la base de datos para minimizar los riesgos de un uso no adecuado de los datos personales tratados.
- Información sobre si se cuenta con la autorización de los titulares de los datos contenidos en las bases de datos.
- Forma de obtención de los datos (directamente del titular o mediante terceros).
- Cuando se ha realizado transferencia o transmisión internacional de la base de datos, se solicitará la información básica del destinatario.
- Si la base de datos se ha cedido, se solicitará se solicitará la información básica del cesionario.

(Tabla 1: AP.6)

7.1.2. CONTROLES TÉCNICOS

7.1.2.1. AUTENTICACIÓN DE USUARIOS (usuario, redes, soporte y aplicación)

Controles básicos

- Definir un identificador único por usuario y prohibir cuentas compartidas entre varios usuarios. Si es inevitable utilizar identificadores genéricos o compartidos, exigir una validación de jerarquía, implementar medidas para registrar las acciones asociadas con estos y renovar la contraseña cuando una persona ya no necesite acceder a la cuenta.

- En el caso de autenticación de usuario basada en contraseña, se deben aplicar las siguientes reglas:

    - Almacenar únicamente las huellas dactilares de las contraseñas, obtenidas mediante técnicas de última generación;
    - Solicitar una renovación periódica de las contraseñas para usuarios simples y usuarios administradores;
    - Cuando inicia sesión por primera vez, solicitar al usuario que cambie cualquier contraseña atribuida automáticamente o por un administrador al crear la cuenta o restablecer la contraseña;
    - Imponer complejidad de contraseña como mínimo de 14 caracteres, con bloqueo después de 3 fallos.

- Favorecer la autenticación multifactor siempre que sea posible, especialmente cuando se puede acceder a la conexión desde fuera de la red de la organización.

- Limitar el número de intentos de acceso a cuentas de usuario en estaciones de trabajo y bloquear el acceso a la cuenta temporalmente o no, cuando se alcance su límite. (**Tabla 1: C.2)**

- Exigir a los administradores que utilicen contraseñas complejas y que las renueven con una frecuencia razonable y relevante.

- Implementar medidas técnicas para hacer cumplir las reglas de autenticación (por ejemplo, bloquear el acceso de un administrador, si la contraseña no está actualizada).

- Si es posible, evite hacer que los identificadores (o inicios de sesión) de usuarios y administradores sean los mismos que las cuentas definidas por defecto por las compañías de software y desactive las cuentas predeterminadas.

- Almacenar contraseñas de forma segura, procesadas con una función (hash) diseñada específicamente para este fin y siempre usando una llave. Una clave no debe ser almacenados en la misma base de datos que las huellas digitales de las contraseñas.

7.1.2.2. GESTION DE ACCESO

Controles básicos

- Definir perfiles de autorización en los sistemas separando los privilegios, para restringir el acceso de los usuarios solo a los datos necesarios para cumplir sus responsabilidades.

- Obtener todas las solicitudes de autorización validadas y aprobadas por un gerente (por ejemplo: gerente de línea, gerente de proyecto).
- Retirar el derecho de acceso de los usuarios tan pronto como ya no estén autorizados a acceder a un recurso informático (por ejemplo, cambio de misión o puesto), así como al final de su contrato.
- Realizar una revisión periódica, al menos semestralmente, de las autorizaciones con el fin de identificar y eliminar cuentas no utilizadas y realinear los derechos otorgados a las responsabilidades de cada usuario. Los directivos deberían participar en esta revisión para que puedan garantizar la legitimidad operativa de los derechos concedidos.
- Establecer, documentar y revisar periódicamente una política de control de acceso en relación con las operaciones de tratamiento de datos personales, que incluya:
    - Los procedimientos que se aplicarán automáticamente a la llegada y salida o cambio de rol de una persona con acceso a datos personales;
    - Las consecuencias previstas para las personas con acceso legítimo a los datos en caso de no-cumplimiento de medidas de seguridad (por ejemplo: uso indebido de un derecho de acceso legítimo);
    - Las medidas que permiten restringir y controlar la concesión y el uso del acceso al procesamiento. **(Tabla 1: B.8)**

7.1.2.3. CONTROLES EN ESTACIONES DE TRABAJO (Tabla 1: C.2)

Controles básicos.

- Proporcionar un mecanismo de bloqueo automático de sesión activa cuando la estación de trabajo no se ha usado durante un tiempo determinado.
- Instalar un software firewall en la estación y restringir la apertura de puertos de comunicación a aquellos estrictamente necesarios para el correcto funcionamiento de las aplicaciones instaladas en la estación de trabajo. **(Tabla 1: C.9)**
- Utilizar un antivirus actualizado periódicamente. **(Tabla 1: C.15)**
- Instalar los parches para prevenir las brechas de seguridad con las actualizaciones de seguridad apropiadas tan pronto como sea posible después de probarlas. Las actualizaciones que corrijan fallas críticas divulgadas públicamente deben instalarse sin demora. **(Tabla 1: B.9)**
- Mantener los derechos de los usuarios al mínimo estricto en función de sus necesidades para el uso de sus estaciones de trabajo.
- Permitir y promover el almacenamiento de los datos de los usuarios en un espacio de almacenamiento en línea respaldado periódicamente y accesible a través de la red interna de la organización en lugar de en las estaciones de trabajo reales. Si los datos se almacenan

localmente, proporcione medios de sincronización o respaldo a los usuarios y capacítelos para usarlos.

- Borre de forma segura los datos de cualquier estación de trabajo antes de reasignarlos a otra persona.
- Respecto a soportes extraíbles (ej.: memorias USB, discos duros externos):
    - Sensibilizar a los usuarios sobre los riesgos asociados a los dispositivos extraíbles, especialmente si proceden del exterior;
    - Restringir la conexión de medios extraíbles a lo estrictamente necesario;
    - Deshabilite la “ejecución automática” desde medios extraíbles.
- Para asistencia en estaciones de trabajo:
    - Las herramientas de administración remota deben obtener el consentimiento del usuario antes de cualquier intervención en su puesto (por ejemplo: cada vez que se acuerda una cita, mostrando un mensaje al usuario que debe aceptar);
    - El usuario también debe poder distinguir si el control remoto todavía está en curso y si finalizó (por ejemplo: mostrando un mensaje en la pantalla).
- Restringir los privilegios de administración, tanto local como en red, a usuarios cuyo puesto no lo requiera.
- Permitir únicamente la ejecución de aplicaciones descargadas de fuentes seguras (lista blanca).
- Restringir el uso de aplicaciones que requieran derechos de administrador para su ejecución.
- Proporcionar un entorno seguro mediante un entorno de escritorio virtual que se ejecuta en un servidor central y al que los usuarios pueden acceder de manera remota a través de una red desde cualquier dispositivo, permitiendo que los administradores pueden controlar el acceso, la seguridad y las políticas de los usuarios finales, protegiendo los datos, los sistemas y el software de la empresa.
- Configurar una solución para analizar y descontaminar medios extraíbles antes de cada uso.
- Ante el compromiso de un puesto de trabajo, buscar el origen y cualquier rastro de intrusión en el sistema de información de la organización para detectar el compromiso de otros elementos.
- Implementar actualizaciones críticas en los sistemas operativos sin demora (si corresponde, después de probarlas) programando una verificación automática semanal.
- Fijar los puestos de trabajo a muebles específicos o de difícil traslado (ej.: utilizar cables antirrobo).

- Hay que asegurar que todos los usuarios estén bien informados sobre las acciones a tomar y la lista de personas con las que se debe contactar en caso de un incidente de seguridad o un evento inusual que afecte a los sistemas de información y comunicación de la organización.

7.1.2.4. CONTROLES EN DISPOSITIVOS MOVILES

Controles básicos

- Sensibilizar a los usuarios sobre los riesgos específicos asociados con el uso de herramientas informáticas móviles (por ejemplo, robo de equipos, conexión a redes no controladas y riesgos de equipos, en particular equipos públicos, uso de equipos personales) y los procedimientos para restringirlos.
- Proporcionar control de acceso a través de dispositivos de autenticación adecuados Todos los flujos de información deben estar cifrados (por ejemplo, VPN para acceso externo). **(Tabla 1: B.7)**
- Proporcionar a los usuarios espacios de almacenamiento compartido a los que se pueda acceder de forma remota, para almacenar allí todos sus datos para mitigar los daños causados por la pérdida o robo de sus dispositivos.
- Implementar o integrar una solución de cifrado para dispositivos de almacenamiento extraíbles (por ejemplo: computadora portátil, unidad USB, disco duro externo, CD-R, DVD-RW) como:
    - Cifrado del disco duro (muchos sistemas operativos admiten esta funcionalidad);
    - Cifrado archivo por archivo;
    - Creación de contenedores cifrados (carpeta que puede contener varios archivos) **(Tabla 1: C.10)**
- Para los smartphones, además del uso del PIN de la tarjeta SIM, habilitar el bloqueo automático de esta.
- Hay que asegurar que los usuarios reciban los datos de contacto adecuados del empleado a cargo en caso de pérdida o robo de sus dispositivos.
- Evaluar y abordar los riesgos asociados con el uso de equipos personales por parte de los usuarios (traiga su propio dispositivo o BYOD) y autorícelos solo respecto de aquellos riesgos identificados. En consecuencia, se restringirá el acceso a los datos y aplicaciones de dichos dispositivos que no estén controlados por la organización en lo que respecta a su criticidad. Asegúrese de que la política de Seguridad de la información cubra y formalice las responsabilidades de todos los involucrados, así como las precauciones que deben seguirse.
- Establecer un sistema de gestión de dispositivos móviles (MDM), incluidos los personales utilizados en el contexto profesional (BYOD), si la práctica está permitida, para estandarizar

las configuraciones y controlar el nivel de garantía de seguridad de los dispositivos conectados a la red de la organización.

- Sensibilizar sobre malas prácticas en lugares públicos:
    - No dejar equipos o documentos desatendidos;
    - No comparta información confidencial (por ejemplo: datos personales, información que pueda revelar violaciones de seguridad).
- Restringir el almacenamiento de datos locales en estaciones de trabajo a lo estrictamente necesario, en particular para equipos personales, y posiblemente prohibirlo cuando se viaje al extranjero.
- Protéjase contra robos (por ejemplo: cable de seguridad, marcado visible de equipos) y mitigue los impactos (por ejemplo: bloqueo automático, cifrado, eliminación remota). Si se va a utilizar un mecanismo de eliminación en un dispositivo personal (BYOD), se deben incorporar las condiciones de uso. **(Tabla 1: C.10)**

7.1.2.5. PROTECCION DE LA RED (Tabla 1: C.4)

Controles básicos

- Limitar el acceso a Internet bloqueando servicios innecesarios (por ejemplo, VoIP, peer to peer).
- Administrar redes Wi-Fi. Deben utilizar cifrado de última generación (WPA3 o WPA2). Las redes abiertas a invitados deben estar separadas de la red interna. **(Tabla 1: C.10)**
- Hacer cumplir el uso de VPN para el acceso remoto implementando, si es posible, una autenticación de usuario sólida (por ejemplo: contraseña de un solo uso basada en el tiempo (TOTP).
- Hay que asegurar que ninguna interfaz de administración esté directamente a través de Internet. Las operaciones de administración y mantenimiento deben realizarse a través de una VPN.
- Para fines de administración de red, la mejor práctica es configurar e implementar (correctamente) el protocolo SSH o acceder físicamente al equipo.
- Limitar los flujos de red filtrando los flujos entrantes/salientes en los equipos (firewalls, servidores proxy). Por ejemplo, si un servidor web está en modo solo HTTPS, solo debe permitir flujos entrantes en esa máquina en el puerto 443 y bloquear todos los demás puertos. **(Tabla 1: C.9)**
- Particionar la red para mitigar los posibles impactos de las violaciones de seguridad. Implementar al menos dos áreas de red diferenciadas: una red interna donde no se permite conexión a Internet y una DMZ (zona desmilitarizada) accesible desde Internet, separada por puertas de enlace.

- Las operaciones de administración y mantenimiento deberán realizarse desde equipos bajo el control exclusivo del responsable del tratamiento o de sus subcontratistas.
- La identificación automática de hardware se puede implementar configurando la autenticación de hardware (protocolo 802.1X) o, al menos, definiendo una lista blanca de identificadores actualizados de controladores de interfaz de red (direcciones MAC) para restringir una conexión de dispositivo no listada.
- Evaluar e implementar sistemas de detección de intrusiones (IDS), prevención de intrusiones (IPS) y sistema de prevención de perdida de datos (DLP) que pueden analizar el tráfico de la red para detectar e incluso responder a algunos ataques y prevenir divulgación de información de datos personales. **(Tabla 1: C.11, Tabla 1: C.12)**
- Seguir las buenas prácticas para de cómo definir la interfaz para conectar un sistema de información a Internet, la elección de los cortafuegos31 o el despliegue del protocolo 802.1X.

7.1.2.6. SEGURIDAD DE SERVIDORES (Tabla 1: C.5)

Controles básicos

- Desinstalar o desactivar servicios e interfaces innecesarios.
- Restringir el acceso a las herramientas e interfaces de administración únicamente al personal autorizado. Utilice cuentas de usuario sin privilegios para operaciones de rutina.
- Adoptar una política de contraseñas específica para administradores.
- Cambiar las contraseñas, al menos, durante cada salida de un administrador y en caso de sospecha de compromiso.
- Instalar actualizaciones críticas sin demora (si corresponde después de probarlas), en particular parches de seguridad, ya sea para sistemas operativos o aplicaciones, programando un chequeo automático semanal. **(Tabla 1: B.9)**
- Utilizar software de detección y eliminación de malware (por ejemplo, antivirus) y actualícelos periódicamente. **(Tabla 1: C.15)**
- Utilizar cuentas registradas para acceder a bases de datos y crear cuentas técnicas específicas de la aplicación.
- Realizar copias de seguridad y compruebe periódicamente la integridad de los archivos de copia de seguridad y la posibilidad de restaurarlos
- Implementar un protocolo fuerte que garantice el cifrado y la autenticación, al menos para cualquier intercambio de datos en Internet, y compruebe su correcta implementación mediante herramientas adecuadas. **(Tabla 1: C.10)**
- Restringir el uso de algoritmos de cifrado obsoletos para las comunicaciones del servidor. **(Tabla 1: C.10)**
- Establecer un sistema de registro de eventos. **(Tabla 1: C.16)**

- Cualquier sistema que procese datos personales confidenciales debe implementarse en un entorno dedicado (lógicamente aislado).
- Las operaciones de administración del servidor deben llevarse a cabo a través de una red dedicada y aislada, con un fuerte acceso de autenticación para mejorar la trazabilidad.
- Además de los flujos externos, los flujos internos se cifrarán tanto como sea posible con protocolos fuertes.
- Aislar servidores obsoletos pero esenciales (si aplica) y limitar el procesamiento de datos personales en ellos pendientes su sustitución por sistemas más modernos.
- En cuanto al software que se ejecuta en servidores, utilice herramientas de detección de vulnerabilidades (software de vulnerabilidad escaneos como nmap, nessus) o confiar en auditorías para el procesamiento más crítico para detectar posibles vulnerabilidades de seguridad. También se pueden utilizar sistemas de detección y prevención de ataques a sistemas o servidores críticos.
- Restringir el acceso físico y prohibir el acceso lógico remoto al diagnóstico y a la configuración de puertos.

7.1.2.7. SEGURIDAD DE SITIOS WEB (Tabla 1: C.6)

Controles básicos

- Flujos de intercambio de datos seguros mediante el uso de TLS:
    - Obtener certificados en los niveles apropiados (dominio, organización o extendido) de una autoridad certificadora y gestionarlos adecuadamente;
    - Implementar un protocolo fuerte en todos los sitios web, utilizando solo las últimas versiones y verificando su correcta implementación. Hacer obligatorio su uso en todas las páginas de autenticación o páginas en las que se muestran o transmiten datos personales.
- Limitar los puertos de comunicación a los estrictamente necesarios para el correcto funcionamiento de las aplicaciones instaladas. Si el acceso a un servidor web se realiza solo a través de HTTPS, debe permitir el tráfico de red IP entrante para esa máquina en el puerto 443 y bloquear todos los demás puertos.
- Restringir el acceso a herramientas e interfaces administrativas únicamente al personal autorizado. En particular, restrinja el uso de cuentas de administrador a los equipos de TI internos y solo para acciones administrativas que las requieran.
- Implementar las opciones “HttpOnly” y “secure” para todas las cookies utilizadas.
- Si se usan cookies que no son necesarias para el servicio, obtener el consentimiento del usuario tras informarle y antes de almacenarla.

- Limite el número de componentes utilizados, supervíselos periódicamente y actualícelos.
- Limitar la información devuelta al crear una cuenta de usuario o al restablecer una contraseña, para no informar a un atacante sobre la existencia – o no – de una cuenta asociada con un identificador (por ejemplo, dirección de correo electrónico). **(Tabla 1: C.14)**
- En particular, protéjase contra los ataques más comunes a los sitios web referidos en OWASP Top 10 (inyecciones SQL, inyecciones XSS, manipulaciones de URL).
- Implementar un procedimiento de gestión de Vulnerabilidades.

7.1.2.8. GESTION DE DESARROLLO - SDLC

Controles básicos

- Integrar la protección de datos, incluidos sus requisitos de seguridad de datos, desde el diseño de la aplicación o servicio. Estos requisitos pueden dar lugar a una variedad de opciones de arquitectura (descentralizada o centralizada), de funcionalidades (por ejemplo: anonimización realizada poco después de la recopilación, minimización de datos), de tecnologías (por ejemplo: cifrado de comunicaciones), etc. **(Tabla 1: C.9)**
- Implementar medidas contra ataques comunes dirigidos a bases de datos (por ejemplo: inyecciones de código SQL, scripts).
- Para cualquier desarrollo dirigido al público en general, considerar cuidadosamente los parámetros que afectan la privacidad y su cumplimiento, en particular la configuración predeterminada.
- Definir pruebas integrales (por ejemplo: pruebas unitarias, de integración, funcionales y de seguridad) antes de que un producto esté disponible o se actualice. Durante una actualización, asegúrese de que las pruebas utilizadas sean siempre apropiadas.
- Llevar a cabo desarrollos y pruebas informáticas en un entorno informático distinto al de producción. (por ejemplo, en diferentes ordenadores o máquinas virtuales) y en datos ficticios o anonimizados.
- Realizar una prueba de no regresión y/o una revisión del código antes de que cualquier actualización entre en producción, para evitar la aparición de fuentes de violación de datos personales.
- Establecer una defensa en profundidad de los sistemas, es decir, una combinación de varias medidas y controles de seguridad (por ejemplo, controlar los datos ingresados en un formulario en línea, pero también proteger las consultas de bases de datos). En particular, las medidas implementadas en la parte “Frontend” de una aplicación pueden eludirse y deberían reforzarse con medidas en la parte “Backend”.
- El desarrollo debe imponer formatos de entrada y registro de datos que minimicen los datos recopilados. Si solo se recopila el año de nacimiento de una persona, el campo del formulario

correspondiente no debe permitir el ingreso del mes y día de nacimiento. Esto puede significar, en particular, la implementación de un menú desplegable que limite las opciones para un campo de formulario.

- Definir reglas de codificación y documentación para mantener la aplicación o servicio a lo largo del tiempo sin introducir nuevas vulnerabilidades y para corregir eficazmente los fallos de funcionamiento.
- La creación y gestión de perfiles de usuario con derechos de acceso a datos variables según las categorías de usuarios debe integrarse desde la fase de diseño.
- Las pruebas realizadas con datos ficticios o anonimizados a veces no son suficientes para garantizar que un nuevo servicio o característica funcione correctamente. Entonces es posible realizar pruebas en un entorno de preproducción con datos reales. El entorno de preproducción debe estar configurado y asegurado al mismo nivel que el propio entorno de producción y el nuevo servicio o su actualización debe haber pasado ya por todas las pruebas (unitarias, de integración y funcionales) en los entornos de desarrollo y pruebas.

7.1.2.9. PROTECCION FISICA (Tabla 1: C.1)

Controles básicos

- Restringir el acceso a las instalaciones mediante puertas cerradas con llave.
- Instalar alarmas de intrusión y comprobar periódicamente su correcto funcionamiento.
- Instalar detectores de humo y equipos contra incendios e inspeccionarlos anualmente.
- Proteger las llaves de acceso a las instalaciones, así como los códigos de alarma.
- Distinguir las áreas del edificio según el riesgo (por ejemplo: proporcionar un control de acceso exclusivo para la sala de computadoras).
- Mantener una lista actualizada de personas o categorías de personas autorizadas a ingresar a cada área y revisar periódicamente esta lista.
- Establecer normas y medios para controlar el acceso de visitantes, al menos haciendo que los visitantes sean acompañados fuera de las zonas de recepción pública por una persona perteneciente a la organización.
- Proteja el acceso a la red (por ejemplo: enchufes de oficina, bahías de conexión) y permita que solo el equipo autorizado conectarse a ellos.
- Proteger físicamente los equipos informáticos con medidas específicas (por ejemplo: sistema dedicado contra incendios, elevación contra posibles inundaciones, redundancia del suministro eléctrico, redundancia del sistema de aire acondicionado).

- Mantener un registro de los accesos a salas u oficinas que puedan contener material que procese datos personales y que, en caso de incidente, pueda tener un impacto negativo grave en los interesados.
- Hay que asegurar que solo personal autorizado admita en las áreas de acceso restringido. Por ejemplo: – dentro de las zonas reguladas, exigir que todas las personas lleven un medio de identificación visible (por ejemplo, una placa);
    - Los visitantes (por ejemplo: personal de soporte técnico) solo deben tener acceso limitado. La fecha y hora de su se deben registrar la llegada y la salida;
    - Revisar y actualizar periódicamente los permisos de acceso a áreas seguras y eliminarlos si es necesario.

7.1.2.10. CONTROLES EN EL INTERCAMBIO DE INFORMACION (Tabla 1: APT.4)

Controles básicos

- Cifrar los datos antes de almacenarlos en un medio físico para transmitirlos a un tercero (por ejemplo, unidad USB, disco duro portátil, disco óptico). **(Tabla 1: C.10)**
- Al enviar a través de una red:
    - Cifrar las partes sensibles que se van a transmitir.
    - Utilizar un protocolo que garantice la confidencialidad y autenticación del servidor de destino del archivo transferencias (por ejemplo, SFTP o HTTPS), utilizando las versiones más recientes de los protocolos;
- Recomendar abrir un archivo recibido desde fuera solo si conoce al remitente y después de realizar un análisis antivirus. **(Tabla 1: C.15)**
- Utilizar algoritmos de clave pública, cuando diferentes actores hayan implementado una infraestructura de gestión de clave pública para garantizar la confidencialidad e integridad de las comunicaciones, así como la autenticación del emisor.
- Exigir que los datos sean firmados electrónicamente por el emisor antes de su envío para garantizar que él o ella es el originador de la transmisión.
- Usar un servidor de almacenamiento de archivos temporal. En este caso, asegúrese de:
    - Establecer un tiempo limitado para que los archivos estén disponibles;
    - Restringir el acceso a los archivos únicamente a destinatarios debidamente autorizados;
    - Cifrar archivos antes de cargarlos en el servicio si la solución utilizada no lo permite posibilidad de forma integrada.
- Para los sistemas más sensibles, limitar los archivos del exterior a áreas aisladas del resto del sistema.

7.1.2.11. CONTROLES EN ENCARGADOS DE TRATAMIENT0 DE DATOS PERSONALES

Controles básicos

- Utilizar solo proveedores con garantías suficientes (especialmente en cuanto a conocimiento especializado, confiabilidad y recursos).
- Definir un contrato con los proveedores, que contenga el objeto, la duración, el propósito del procesamiento, así como las obligaciones de las partes, en particular en términos de seguridad. Asegúrese de que contenga, en particular, disposiciones que establezcan:
    - La división de responsabilidades y obligaciones relativas a la confidencialidad de los datos personales confiado;
    - Requisitos mínimos de autenticación de usuario;
    - Las condiciones de devolución y destrucción de los datos al final del contrato;
    - Las normas de gestión y notificación de incidencias. Estas deberían incluir informar al responsable del tratamiento en caso de que se descubra una violación o incidente de seguridad, y esto debería hacerse lo antes posible. en caso de violación de datos personales;
    - Asistencia que debe prestarse al encargado del tratamiento para garantizar el cumplimiento de las obligaciones de seguridad;
    - La revisión periódica de las medidas de seguridad y, en su caso, de las condiciones para su revisión.
- Proporcionar los medios para verificar la eficacia de las garantías de protección de datos ofrecidas por el proveedor (por ejemplo: auditorías de seguridad, visitas al sitio). Dichas garantías incluyen, entre otras:
    - El cifrado de los datos según su sensibilidad o, en su defecto, la existencia de procedimientos que garanticen que la empresa de servicios no tenga acceso a los datos que se le confían si no es necesario para la ejecución de su contrato; **(Tabla 1: C.9)**
    - Cifrado de transmisiones de datos (por ejemplo: conexión HTTPS, implementación de VPN); **(Tabla 1: C9)**
    - Garantías para proteger la red, trazabilidad, gestión de autorizaciones, autenticación, prácticas de administrador, auditorías, etc.
- Considerar los riesgos de la subcontratación que pueda generar el proveedor en la prestación del servicio.
- Exigir una certificación de seguridad de la información para evaluar su fiabilidad. Por ejemplo, la norma internacional ISO/IEC 27001 requiere medidas organizativas y técnicas para el

establecimiento de un Sistema de Gestión de Seguridad de la Información (SGSI), mientras que ISO/IEC 27701 cubre Sistemas de Gestión de Privacidad

7.1.2.12. REGISTRO DE ACTIVIDADES (Tabla 1: C.7)

Controles básicos

- Implementar un sistema de registro de las actividades de los usuarios (registros de aplicaciones), intervenciones técnicas (incluidas las de los administradores), anomalías y eventos relacionados con la seguridad (registros técnicos o del sistema).
- Conservar estos registros durante un período continúo adecuado
- Garantizar que los registros de creación, consulta, intercambio, modificación y eliminación de los datos contiene el identificador del autor, la fecha, la hora y la naturaleza de la operación, así como la referencia de los datos en cuestión (para evitar duplicación).
- Proteger el equipo de registro y la información registrada contra operaciones no autorizadas (por ejemplo, haciéndolos inaccesibles para las personas cuya actividad se registra), uso indebido por parte de cuentas autorizadas (por ejemplo: estableciendo una carta de uso o alertas específicas) y la destrucción de los registros generados.
- Garantizar el correcto funcionamiento del sistema de registro integrando el equipo en una herramienta de monitoreo y verificando periódicamente la presencia de registros explotables.
- Garantizar que los encargados del tratamiento estén obligados contractualmente a implementar el registro de acuerdo con estas recomendaciones y a notificar lo antes posible cualquier anomalía o incidente de seguridad al responsable del tratamiento.
- Analizar activamente, en tiempo real o en el corto plazo, los registros recopilados para poder detectar la ocurrencia de un incidente
- Involucrar al usuario en el seguimiento de las transacciones realizadas en su cuenta y sus datos (por ejemplo: proporcionar un resumen de las tres últimas conexiones).
- Establecer un sistema de recolección centralizando de registros de eventos en todo el sistema de información para para evitar cualquier alteración de este y efectuar correlación de los eventos registrados. **(Tabla 1: C.16)**

7.1.2.13. PLANES DE CONTINUIDAD (Tabla 1: A.4)

Controles básicos

- Redactar un plan de continuidad del servicio (BCP) y un plan de recuperación ante desastres (DRP). **(Tabla 1: A.4)**
- Garantizar que los usuarios, proveedores de servicios y subcontratistas sepan a quién alertar en caso de incidente.

- Probar periódicamente la restauración de copias de seguridad y la aplicación del plan de continuidad del negocio o plan de recuperación ante desastres.
- Contratar un seguro para proteger los equipos utilizados para tratamientos esenciales;
- Prever redundancia material de los equipos de almacenamiento (por ejemplo: utilizando tecnología RAID).

7.1.2.14. GESTION DE INCIDENTES

Controles básicos

- Establecer procedimientos que detallan los sistemas de generación y emisión de alertas de diferentes fuentes (ej.: automáticas, por parte de los usuarios), su procesamiento y las acciones a tomar en caso de un incidente comprobado (ej.: personas a contactar, acciones para limitar el incidente según a su naturaleza). Incluir la gestión de violaciones de datos en el proceso de gestión de incidentes. Definir criterios para clasificar un incidente como violación de datos.
- Analizar periódicamente los registros recopilados.
- Notificar al responsable del tratamiento, lo antes posible, en caso de anomalía o incidente de seguridad.
- Difundir a todos los usuarios, internos y externos, la conducta y la lista de personas con las que contactar si se produce un incidente de seguridad o un evento inusual que afecte a los sistemas de información y comunicación de la entidad. Concientizar a los usuarios sobre la importancia de reportar eventos sospechosos.
- Evaluar el riesgo que la violación supone para las personas, teniendo en cuenta la gravedad y probabilidad de las consecuencias que la violación pueda tener sobre sus derechos y libertades.
- Mantener un registro interno de todas las violaciones de datos personales.
- Realizar seguimiento automático de registros, junto con una configuración adecuada de alertas.
- Establecer capacitación obligatoria para todo el personal sobre cómo identificar y denunciar infracciones, así como sobre qué hacer en este caso.
- Definición de un área de ingeniería forense **(Tabla 1: A.8.)**

7.1.2.15. INTEGRIDAD DE LOS DATOS

Controles básicos

- Redactar un procedimiento que indique cómo se gestionarán las claves y certificados considerando los casos de olvido de contraseñas para su desbloqueo.
- Utilizar algoritmos reconocido y seguro, por ejemplo, los siguientes algoritmos:

- Aplicar recomendaciones de uso relevantes, específicas para el algoritmo elegido. Los errores de implementación tienen un impacto significativo en la seguridad del mecanismo criptográfico.
- Proteger las claves privadas, al menos mediante la implementación de derechos de acceso limitados y una contraseña segura.
- Al recibir un certificado electrónico, verificar que el mismo contenga una indicación de uso acorde a lo esperado, que sea válido y no revocado y que tenga una correcta cadena de confianza en todos los niveles.
- Utilizar software o bibliotecas criptográficas verificadas por terceros con experiencia comprobada.

7.1.2.16. COMPUTACION EN LA NUBE

Controles básicos

- Mantener actualizado el mapeo de los datos y el procesamiento en la nube. También mapee los servicios en la nube en uso (incluidas las aplicaciones SaaS). Identifique los recursos de la nube no utilizados o no monitoreados y, si corresponde, elimínelos.
- Evaluar las necesidades de seguridad para el procesamiento de datos implementado para elegir:
    - El método apropiado de despliegue del servicio (público, privado, híbrido, comunitario, Multinube);
    - El proveedor de servicios en la nube tras evaluar su nivel de seguridad garantizado (en particular para copias de seguridad, redundancia, cifrado, seguridad física, mantenimiento) según especificaciones de seguridad en la nube reconocidas. **(C.10)**
- Incluir los servicios en la nube en el análisis de riesgos.
- Asegurar que los requisitos de seguridad y la asignación de responsabilidad estén cubiertos por un contrato entre el proveedor y el cliente
- Asegurar que todas las partes involucradas en el suministro del servicio en la nube realmente mantengan el nivel de seguridad acordado (el propio proveedor y sus posibles subcontratistas).
- Configurar (si es el caso) las herramientas de seguridad proporcionadas por el proveedor (e.g.: cifrado, gestión de accesos e identidades, firewall, herramienta anti-DDoS) de acuerdo con la política interna de seguridad de los sistemas de información. **(Tabla 1: C.9, Tabla 1: C.10)**.
- Cifrar los datos inactivos, así como los datos en tránsito, y utilizar la gestión de claves criptográficas adecuada. Tenga en cuenta que utilizar los servicios de gestión de claves ofrecidos por el proveedor de servicios implica que el proveedor de servicios también tiene la capacidad de acceder a los datos;

- Asegurarse que solo se asignen al personal autorizado los derechos de acceso y permisos pertinentes para el acceso a los recursos (datos y aplicaciones) en la nube y aplicar el principio de menos privilegios
- Autenticar a los usuarios para acceder a los servicios en la nube y otorgar solo las autorizaciones necesarias
- Gestionar y configurar permisos de recursos de la nube;
- Realizar copias de seguridad y verificar que su proveedor realmente tenga varios centros de datos de respaldo que estén geográficamente distantes entre sí.
- Realizar auditorías periódicas de seguridad del proveedor.

7.1.2.17. INTERFACES DE PROGRAMACION DE APLICACIONES (API) (Tabla 1: C.22)

Controles básicos

- Identificar los actores y su rol funcional (titular de los datos, administrador de API) para organizar el perímetro de asignación de cada uno en términos de acceso a las API y a los datos.
- Para limitar el intercambio a datos necesarios, solo a personas físicas y para los fines previstos, según el principio de minimización.
- Crear una separación entre las llamadas a las funciones comunes de la API y aquellas dedicadas a su administración, para las cuales parece necesaria una autenticación robusta.
- Disponer de registros relevantes para realizar un seguimiento de los intercambios y para detectar y reaccionar en caso de uso indebido de la API, acceso ilegítimo a los datos, exceder la capacidad de acceso o cualquier otro comportamiento inusual
- Mantener la documentación actualizada. Esto debe incluir el formato de las consultas y los datos involucrados en el intercambio para limitar el riesgo de una mala interpretación.
- La implementación de la API debe estar de acuerdo con medidas de seguridad estándar como la implementación de un mecanismo de autenticación adecuado, la gestión periódica de autorizaciones o el cifrado de las comunicaciones. al estado del arte.
- Debería estar disponible una versión Sandbox de la API para permitir experimentos y probar los resultados esperados a partir de datos ficticios

7.1.2.18. CONTROLES DE MANTENIMIENTO Y FIN DE VIDA UTIL DEL HARDWARE Y SOFTWARE (Tabla 1: C.23)

Controles básicos

- Registrar las intervenciones de mantenimiento sobre la infraestructura tecnológica en un libro de registro.

- Abrir el acceso necesario para el mantenimiento remoto a petición del proveedor del servicio, durante un período de tiempo predefinido y adecuado a la intervención. Estos accesos deberán cerrarse nuevamente al finalizar este plazo.
- Incluir cláusulas de seguridad en los contratos de mantenimiento con proveedores de servicios para controlar su acceso a los sistemas de información.
- Garantizar que las intervenciones de terceros sean supervisadas por un responsable de la organización.
- Acompañar a los contratistas externos, especialmente en salas sensibles (por ejemplo, salas de servidores).
- Eliminar de forma segura los datos contenidos en los equipos antes de su eliminación, su envío para reparación a un tercero o al finalizar un contrato de alquiler.
- Redactar e implementar un procedimiento seguro de eliminación de datos.
- Utilizar software dedicado para eliminar datos sin destrucción física que haya sido calificado o certificado.
- Implementar herramientas de seguimiento en tiempo real para intervenciones de mantenimiento a distancia por parte de terceros.

7.1.2.19. CONTROL DE CAMBIOS (Tabla 1: B.7)

Controles básicos

- Definición y Documentación: Establecer y documentar una política clara y detallada de control de cambios que incluya los objetivos, alcance, roles y responsabilidades. **(Tabla 1: C.18)**
- Comunicación y Adopción: Asegurar que la política sea comunicada a todo el personal relevante y adoptada formalmente por la organización.
- Solicitud Formal de Cambio (RFC): Implementar un sistema formal para la solicitud de cambios, que incluya la documentación detallada del cambio propuesto, el impacto esperado, los riesgos asociados y el plan de implementación.
- Evaluación y Aprobación: Establecer un proceso de evaluación y aprobación que involucre a las partes interesadas clave, como el equipo de TI, el equipo de seguridad, y la alta dirección, según sea necesario.
- Análisis de Riesgos: Realizar un análisis de riesgos para cada cambio propuesto, identificando posibles impactos negativos en la seguridad, la funcionalidad y la disponibilidad del sistema.
- Evaluación de Impacto: Evaluar el impacto potencial del cambio en los usuarios, los procesos de negocio y otros sistemas dependientes.

- Plan de Implementación: Desarrollar un plan detallado de implementación que incluya las etapas del cambio, los recursos necesarios, el cronograma y las medidas de contingencia.
- Pruebas Preliminares: Realizar pruebas en un entorno de prueba aislado para validar que el cambio funciona según lo esperado y no introduce problemas adicionales.
- Control de Versiones: Utilizar sistemas de control de versiones para rastrear todas las modificaciones en el software, los sistemas y la configuración.
- Gestión de Configuraciones: Mantener una base de datos de gestión de configuraciones (CMDB) actualizada para documentar todas las configuraciones y versiones de los sistemas.
- Autorización Formal: Asegurar que todos los cambios sean autorizados formalmente por las partes responsables antes de la implementación.
- Documentación Detallada: Documentar todos los cambios aprobados, incluyendo los detalles del cambio, las pruebas realizadas, los resultados y las autorizaciones.
- Implementación Controlada: Implementar los cambios siguiendo el plan de implementación aprobado, asegurando que se sigan todos los procedimientos establecidos.
- Monitoreo Post-Implementación: Monitorear los sistemas después de la implementación del cambio para detectar cualquier problema o comportamiento inesperado.
- Planes de Contingencia: Preparar planes de contingencia y procedimientos de retroceso en caso de que el cambio cause problemas significativos.
- Gestión de Incidentes: Establecer procedimientos claros para la gestión de incidentes relacionados con la implementación de cambios, incluyendo la identificación, la resolución y la documentación de incidentes.
- Revisión Post-Implementación: Realizar revisiones post-implementación para evaluar el éxito del cambio y documentar cualquier lección aprendida.
- Auditoría de Cambios: Realizar auditorías periódicas del proceso de control de cambios para asegurar el cumplimiento con las políticas y procedimientos establecidos y para identificar áreas de mejora.
- Formación del Personal: Capacitar al personal relevante sobre el proceso de control de cambios, sus roles y responsabilidades, y la importancia de seguir los procedimientos establecidos. **(Tabla 1: C.18, Tabla 1: A.7)**
- Sensibilización Continua: Mantener programas de sensibilización continua para asegurar que todos los empleados entiendan la importancia del control de cambios y se mantengan actualizados sobre las mejores prácticas y políticas.

7.1.2.20. ESCRITORIO LIMPIO

Controles básicos

- Política Documentada: Crear una política formal de escritorio limpio que describa sus objetivos, alcance y las expectativas para todos los empleados. **(Tabla 1: AP.9.)**
- Difusión y capacitación: Comunicar la política a todos los empleados y contratistas para así proporcionar capacitación sobre su importancia y los procedimientos a seguir.
- Al final del día: Asegurar que todos los empleados limpien sus escritorios al final del día, guardando documentos en archivadores con llave y apagando o bloqueando sus computadoras.
- Ausencias prolongadas: Requerir que los empleados limpien sus escritorios cuando estén ausentes por períodos prolongados, como almuerzos o reuniones.
- Archivado seguro: Proveer gabinetes de archivo con cerradura y otros dispositivos de almacenamiento seguro para documentos confidenciales.
- Destrucción de documentos: Implementar procedimientos para la destrucción segura de documentos, como trituradoras de papel, para deshacerse de la información confidencial de manera segura.
- Bloqueo de pantalla: Configurar políticas de bloqueo automático de pantalla en las computadoras después de un período de inactividad.
- Almacenamiento seguro: Requerir que los dispositivos electrónicos como laptops y unidades USB se guarden en lugares seguros cuando no estén en uso.
- Inspecciones regulares: Realizar inspecciones periódicas de los escritorios para asegurar el cumplimiento de la política de escritorio limpio.
- Informes de cumplimiento: Documentar los resultados de las inspecciones y proporcionar retroalimentación a los empleados sobre el cumplimiento y las áreas de mejora.
- Cifrado de datos: Asegurar que los datos sensibles almacenados en dispositivos electrónicos estén cifrados. **(Tabla 1: C.10)**
- Almacenamiento en la nube: Fomentar el uso de almacenamiento seguro en la nube en lugar de almacenamiento local para documentos confidenciales.
- Acceso restringido: Limitar el acceso a áreas donde se manejen datos sensibles solo a personal autorizado.
- Sistema de identificación: Utilizar tarjetas de identificación y sistemas de control de acceso para monitorear y restringir el acceso físico a las instalaciones.
- Contenedores de seguridad: Proveer contenedores seguros para la disposición de documentos que contengan información confidencial.
- Recolección regular: Asegurar la recolección y destrucción regular de los residuos confidenciales por parte de personal autorizado.

- Programas de sensibilización: Desarrollar programas de concienciación continua para mantener a los empleados informados sobre la importancia de un escritorio limpio.
- Responsabilidad individual: Fomentar la responsabilidad individual de los empleados en mantener sus áreas de trabajo libres de información confidencial expuesta.
- Sanciones por incumplimiento: Definir y comunicar las sanciones por incumplimiento de la política de escritorio limpio.
- Recompensas y reconocimientos: Implementar un sistema de recompensas para empleados que demuestren consistentemente buenas prácticas de escritorio limpio.

7.1.2.21. TRABAJO EN CASA (Tabla 1: C.20)

Controles básicos

- Políticas de trabajo en casa y Seguridad de la Información: Establecer políticas claras y detalladas que regulen el trabajo en casa, incluyendo el manejo seguro de datos y dispositivos.
- Definir responsabilidades y expectativas para los empleados que trabajan de forma remota.
- Implementar la autenticación Multifactor (MFA) para garantizar que los usuarios remotos sean autenticados de manera segura antes de acceder a los sistemas y datos.
- Utilizar conexiones VPN (Red Privada Virtual) para cifrar el tráfico entre los dispositivos remotos y la red corporativa, protegiendo la información de posibles interceptaciones.
- Mantener actualizados los sistemas y software utilizados en el teletrabajo para mitigar vulnerabilidades conocidas y posibles ataques.
- Encriptar dispositivos como laptops y dispositivos USB para proteger la información en caso de pérdida o robo.
- Utilizar el cifrado de extremo a extremo para proteger los datos transmitidos durante el trabajo remoto. **(Tabla 1: C.10)**
- Limitar el acceso a información confidencial solo a los empleados autorizados, basado en roles y privilegios.
- Implementar controles de acceso para evitar la divulgación de datos a personas no autorizadas.
- Establecer políticas de gestión de dispositivos para garantizar que los dispositivos personales utilizados para el teletrabajo cumplan con los requisitos de seguridad.
- Implementar soluciones de gestión de dispositivos móviles (MDM) para monitorear y gestionar los dispositivos utilizados para el trabajo remoto.
- Ofrecer formación regular sobre seguridad de la información y buenas prácticas de teletrabajo a los empleados.

- Sensibilizar sobre los riesgos asociados con el trabajo remoto, como el phishing y el malware, y cómo evitarlos.
- Realizar auditorías periódicas de los dispositivos y sistemas utilizados para el teletrabajo para detectar posibles vulnerabilidades y garantizar el cumplimiento de las políticas de seguridad.
- Supervisar el acceso y el uso de la información confidencial para detectar actividades sospechosas. **(Tabla 1: C.8)**
- Desarrollar planes de respuesta a incidentes específicos para el teletrabajo, incluyendo procedimientos para la notificación y mitigación de brechas de seguridad.
- Capacitar al personal sobre cómo informar de manera adecuada sobre incidentes de seguridad y cómo actuar en caso de sospecha de compromiso de datos.
- Implementar estos controles de seguridad de la información en entornos de teletrabajo ayuda a mitigar los riesgos asociados con el acceso remoto a los sistemas y datos corporativos, protegiendo así la información confidencial de la universidad.

7.1.2.22. RESTRICCION DE ACCESO A INFORMACION (Tabla 1: C.25)

- Implementar autenticación Multifactor (MFA) para garantizar que los usuarios proporcionen múltiples formas de identificación antes de acceder a la información.
- Asignar permisos y privilegios de acceso según los roles y responsabilidades de los usuarios para limitar el acceso a la información solo a aquellos que lo necesitan para realizar sus tareas. **(Tabla 1: C.18)**
- Establecer políticas claras de acceso que especifiquen quién tiene acceso a qué información y bajo qué circunstancias.
- Encriptar la información confidencial tanto en reposo como en tránsito para protegerla de accesos no autorizados.
- Implementar registros de auditoría para registrar y supervisar las actividades de acceso a la información, permitiendo la detección de cualquier actividad sospechosa. **(Tabla 1: C.8)**
- Limitar el acceso físico a los sistemas y dispositivos que almacenan información sensible mediante medidas de seguridad física como cerraduras, sistemas de acceso con tarjetas y cámaras de vigilancia.
- Utilizar sistemas de gestión de identidades y accesos para administrar y controlar de manera centralizada el acceso de los usuarios a los recursos de información.
- Implementar firewalls y otros dispositivos de seguridad de red para controlar y filtrar el tráfico de red, bloqueando accesos no autorizados a la información. **(Tabla 1: C.9)**
- Proporcionar formación regular sobre políticas de seguridad de la información y mejores prácticas de acceso para concienciar al personal sobre la importancia de proteger la información.

- Revisar y actualizar regularmente los controles de seguridad de acceso para asegurar que estén alineados con las necesidades y riesgos cambiantes de la organización.
- Al implementar estos controles de seguridad de la información, se puede restringir eficazmente el acceso a la información sensible, reduciendo así el riesgo de exposición y pérdida de datos.

7.1.2.23. USO ACEPTABLE DE INFORMACION

Controles básicos

- Establecer políticas claras y detalladas que determinen un uso aceptable de la información en la organización, incluyendo el acceso, almacenamiento, transmisión y uso de los datos.
- Proporcionar formación regular sobre las políticas de uso aceptable de la información y las mejores prácticas de seguridad de datos a todos los empleados, para asegurar su comprensión y cumplimiento.
- Realizar campañas de concienciación regular para educar a los empleados sobre los riesgos de seguridad de la información y la importancia de seguir las políticas de uso aceptable.
- Requerir que todos los empleados firmen un acuerdo de uso aceptable de la información, en el que se comprometan a cumplir con las políticas y procedimientos establecidos.
- Implementar un sistema de control de acceso basado en roles para garantizar que los usuarios solo tengan acceso a la información necesaria para realizar sus funciones laborales. **(Tabla 1: B.8).**
- Realizar auditorías periódicas de acceso para supervisar y registrar las actividades de los usuarios, identificar posibles violaciones de las políticas de uso aceptable y tomar medidas correctivas cuando sea necesario. **(Tabla 1: C.8).**
- Utilizar herramientas de filtrado de contenido y monitoreo de tráfico para detectar y prevenir el acceso a sitios web maliciosos o inapropiados, así como para evitar la transferencia de datos sensibles fuera de la red corporativa.
- Encriptar la información confidencial tanto en reposo como en tránsito para protegerla de accesos no autorizados, utilizando algoritmos de cifrado robustos y certificados de seguridad. **(Tabla 1: C.10).**
- Establecer políticas claras para el uso de dispositivos personales en el lugar de trabajo, incluyendo requisitos de seguridad y acceso a la red, para mitigar los riesgos asociados con el uso de dispositivos no gestionados.
- Revisar y actualizar regularmente las políticas y controles de seguridad de la información para asegurar su relevancia y efectividad en la protección de los datos de la Universidad Distrital.

7.1.2.24. CAPACITACION (Tabla 1: A.7)

Definir un programa de sensibilización y capacitación de datos personales

7.1.2.25. IDENTIFICACION DE BASES DE DATOS QUE CONTIENEN DATOS PERSONALES

Definir una política, procedimiento, o instructivo que permita realizar la gestión de la identificación, actualización y reporte de nuevas bases de datos con información personal a la SIC.

Control de Cambios			
Versión	**Descripción y justificación**	**Responsable**	**Fecha**
1	Creación del documento.	CPS Oficina Asesora de Tecnologías e Información	4/11/2024

Responsabilidades		
	NOMBRE	**CARGO**
CREACIÓN	Oscar Sanabria	CPS OATI
REVISÓ	Sebastián Vanegas	CPS OATI
APROBÓ	Alejandro Paolo Daza Corredor	Jefe OATI