TÉRMINOS DE CONFIDENCIALIDAD

Este documento es resultado del trabajo desarrollado por el área de tecnología de DATACENTER COLOMBIA S.A.S y para uso exclusivo de DATACENTER COLOMBIA Por razones de Confidencialidad de la información, las ideas, conceptos, definiciones, aplicaciones, planes de trabajo y en general las soluciones contenidas en esta línea base de seguridad de la información, no debe ser revelado, usado, duplicado o publicado total o parcialmente, fuera de la compañía u organización, sin una autorización expresa escrita de DATACENTER COLOMBIA

Manual de la Política de Seguridad

Versión 9.0

Cumplimiento al Numeral 5.1 Política de la Norma ISO 27001:2022

CONTROL DE CAMBIOS

Versión	Fecha	escripción	Responsable
1.0	15/05/2015	Versión inicial	Ivonne Martínez
2.0	19/08/2016	Actualización tipos de datos personales ley 1581 2012.	Ricardo Velasco
3.0	15/08/2018	Actualización nuevo esquema de trabajo con SIG.	Ivonne Martínez
4.0	25/10/2019	Actualización numeral 4.8.1. Normas para la política de control de acceso	Jorge Retamozo Ruiz
5.0	15/11/2019	Se actualiza el numeral 4.8.1 con respecto a la complejidad de contraseñas en la organización.	Jorge Retamozo Ruiz
6.0	11/03/2021	Se actualizar el numero 4.11 con respecto al uso de cámaras fotográficas.	Carlos Arturo Vesga Pedraza
7.0	28/12/2022	Actualización de roles responsables.	Ivonne Martinez
8.0	12/11/2024	Alineación a la ISO 27001:2022 controles identidad y administración de accesos	Carlos Arturo Vesga Pedraza
9.0	29/08/2025	Se adiciona el literal e) en el numeral 5.1.14.1 “Normas para la política de seguridad en las operaciones”, donde se establece explícitamente que las políticas de navegación segura y filtrado web aplicadas mediante Sophos Endpoint se mantienen vigentes y consistentes en todo entorno de conexión (corporativo y remoto). Se adicionan los numerales **5.1.18** "Política de uso de criptografía" y **5.1.19** "Política de desarrollo seguro y gestión de ambientes", alineadas con los controles A.8.24 a A.8.31 de la ISO/IEC 27002:2022.	Ivonne Martinez Carlos Arturo Vesga Pedraza

Elaborado Por:	Revisado Por:	Aprobado Por:
Carlos Vesga Coordinador de Seguridad de la información y Ciberseguridad Datacenter Colombia	**Heriberto Delgado** Gerente de Operaciones Datacenter Colombia	**Álvaro Delgado** Gerente General Datacenter Colombia

Tabla de Contenido

1. PROPÓSITO 6
2. ALCANCE 6
3. DEFINICIONES 6
4. POLÍTICA GENERAL 10
4.1. Política Global de Seguridad de la Información A.5.1 10
4.1.1. Normas para la política global de seguridad de la información 10
5. POLÌTICAS ESPECÌFICAS 11
5.1. Controles Organizacionales 12
5.1.1. Política para la organización de la seguridad de la información (A.5.2) 12
5.1.2. Política de Segregación de funciones (A.5.3) 13
5.1.3. Responsabilidades de la dirección (A.5.4) 14
5.1.4. Contacto con las autoridades y Contacto con grupos de interés especial (A5.5, A5.6) 14
5.1.5. Política de Clasificación y Gestión de Activos de Información (A.5.9, A.5.12, A.5.13) 15
5.1.6. Política Para Uso aceptable de la información y otros Activos asociados (A.5.10- A.5.11) 17
5.1.7. Política de Transferencia de Información (A.5.14) 18
5.1.8. Política de Control de Acceso (A.5.15-A.5.18, A.8.1-A.8.5) 19
5.1.9. Política de Enmascaramiento de Datos (A.8.11) 21
5.1.10. Política de Relación con Proveedores (A.5.19, A.5.20, A.5.21, A.5.22) 21
5.1.11. Política de Seguridad de la información para el uso de servicios en la nube (A.5.23) 22
5.1.12. Política Derechos de propiedad intelectual (A.5.32) 23
5.1.13. Política de Protección de registros (A.5.33- A.8.15) 24
5.1.14. Política Privacidad y protección de PII (A.5.34) 24
5.1.15. 4.1.6 Política de Seguridad en las operaciones (A.5.37) 25
5.1.16. Política para la Gestión de Incidentes de Seguridad de la Información (A.5.24-A.5.28) 26
5.1.17. Política de Continuidad del Negocio (A.5.29, A.5.30) 27
5.1.18. Política de Cumplimiento (A.5.31- A.5.37) 28
5.2. Controles de Personas 29
5.2.1. Política de Seguridad para los recursos humanos (A.6) 29
5.2.2. Trabajo a distancia (A.6.7) 30
5.3. Controles Físicos 31
5.3.1. Política de Seguridad Física y del entorno (A.7.1-A.7.6) 31
5.3.2. Política Entrada Física 32
5.3.3. Escritorio y pantalla limpia (A.7.7) 32
5.3.4. Política de Medios de Almacenamiento (A.7.10) 33
5.4. Tecnología 34
5.4.1. Política de Dispositivos de punto final de usuario (A.8.1) 34
5.4.2. Política Gestión de vulnerabilidades técnicas (A.8.8) 35
5.4.3. Política para la Eliminación de información (A.8.10) 35
5.4.4. Política Copias de Respaldo (A.8.13) 36
5.4.5. Política de Uso de Criptografía (A.8.24) 37
5.4.6. Política para la seguridad de redes y los servicios de red (A.8.20-A.8.22) 39
5.4.7. Política de Desarrollo Seguro (A.8.25, A.8.26, A.8.27, A.8.28, A.8.29, A.8.30, A.8.31) 41
6. ANEXOS 42

1. PROPÓSITO

Presentar en forma clara y coherente un conjunto de directrices que conforman la política de seguridad de la información de Datacenter Colombia S.A.S., estableciendo medidas organizacionales, tecnológicas, físicas y legales necesarias para proteger los activos de información de la compañía y de sus clientes.

2. ALCANCE

Las Políticas de Seguridad de la Información son aplicables para todos los aspectos administrativos y de control que deben ser cumplidos por los gerentes, directivos, coordinadores, funcionarios, contratistas, clientes, socios estratégicos y terceros que presten sus servicios o tengan algún tipo de relación con las operaciones de Datacenter Colombia o de los servicios prestados.

3. DEFINICIONES

A continuación, se presentan las principales definiciones aplicables para la correcta interpretación de las políticas de Datacenter:

Activo de información
Cualquier cosa que tenga un valor de importancia relevante para los procesos de la organización. Entre los activos de información más relevantes de una organización se encuentra hardware, software, documentos electrónicos o físicos, infraestructura, servicios, personal, entre otros. El término Activo es sinónimo de Activo de Información.

Amenaza
Es una fuente generadora de eventos o acciones que puede producir o causar un daño representativo al activo de información, generando un factor o escenario de riesgo que originaría a la organización pérdidas por riesgo de seguridad de la información. La amenaza es un contexto de seguridad de la información que se manifiesta a través de actos deliberados, intencionados o impredecibles y que pueden ser provocados por las personas la tecnología, la infraestructura, acontecimientos externos entre otros.

Acuerdo de Confidencialidad
Es un convenio que genera obligaciones a una o a ambas partes que intervienen, con respecto al uso, manejo y divulgación de la información, con el propósito de preservar la confidencialidad, integridad y disponibilidad de la misma, como parte de una relación contractual o comercial.

Confidencialidad
Propiedad de salvaguardar el activo de información de personas, individuos, procesos o entidades no autorizados.

Controles
Medidas de protección o salvaguardas dispuestas para reducir el nivel de riesgo. Las cuales pueden ser políticas, procedimientos, directrices, prácticas, estructuras de la organización, soluciones tecnológicas, entre otras.

Custodio
Se refiere al responsable de la custodia o protección del activo de información utilizado para el desarrollo de las operaciones del negocio. El custodio tiene la misión de preservar la seguridad de este; por lo tanto, el propietario de la información tiene el rol de custodio del activo de información a cargo.

Dato público
Son aquellos datos que las normas y la Constitución han determinado expresamente como públicos, cuya recolección y tratamiento, no requiere autorización del titular de la información. (Ej. Datos contenidos en sentencias judiciales ejecutoriadas, datos sobre el estado civil de las personas, entre otros., que no estén sometidos a reserva y los relativos al estado civil de las personas.

Dato semiprivado
Es el dato que no tiene naturaleza íntima, reservada ni pública y cuyo conocimiento o divulgación puede interesar no solo a su titular sino a cierto sector o grupo de personas o a la sociedad en general, como el dato financiero y crediticio de actividad comercial o de servicios. Para su tratamiento se requiere la autorización expresa del titular de la información y deben ser tratados conforme a los fines y propósitos de la autorización impartida por su titular. (Ej. Dato financiero y crediticio, Dirección, teléfono, nivel escolaridad).

Dato Privado o sensible
Es el dato que por su naturaleza íntima o reservada solo es relevante para el titular. No puede ser objeto de tratamiento a menos que sea requerido para salvaguardar un interés vital del titular y este se encuentre incapacitado, o en los casos que haya sido autorizada expresamente. (Ej. Origen racial o étnico, orientación política, convicciones religiosas, datos biométricos, relativos a la salud, orientación sexual).

Disponibilidad
Propiedad de garantizar que el activo de información sea accesible y utilizable en el momento que se requiera, por parte de las personas, procesos o entidades autorizadas.

Dueño del riesgo
Responsable de hacer seguimiento a la mitigación de los riesgos a los que están expuestos los activos de información de sus procesos.

Evento de seguridad de la información
Es la ocurrencia identificada de un estado del activo de información (sistema, servicio, red, etc.) que indica un posible incumplimiento de la política de seguridad de la información, una

falla de controles existentes, o una situación desconocida que puede ser pertinente para la seguridad (ISO/IEC 27000).

Incidente de seguridad de la información
Se define como un evento o una serie de eventos indeseados o inesperados, que tienen una probabilidad significativa de comprometer las operaciones de negocio y de amenazar las propiedades de la información “Confidencialidad, Integridad y Disponibilidad” (ISO/IEC 27000).

Información
Conjunto de datos ordenados con el objetivo específico de generar conocimiento. Tipo de activo de información que se puede materializar en diferentes formas. La información puede estar impresa o escrita en papel, almacenada electrónicamente, transmitida por correo o utilizando medios electrónicos, presentada en imágenes, o expuesta en una conversación. Cualquiera sea la forma que adquiere la información, o los medios por los cuales se distribuye o almacena, siempre debe ser protegida en forma adecuada. La información electrónica, siempre se encuentra asociada a un activo de información determinado.

Datacenter Colombia S.A.S. considera información toda forma de comunicación o representación de conocimiento o datos digitales, escritos en cualquier medio, ya sea magnético, papel, visual generada por procesos administrativos o tecnológicos.

Información Pública
Es aquella información que ha sido declarada de conocimiento público por disposición de los dueños de procesos de Datacenter Colombia, obligación contractual, ley o norma jurídica, y por tanto puede ser publicada o entregada sin restricciones, sin implicar daños a terceros ni a Datacenter Colombia.

Información Confidencial
Es aquella información que Datacenter Colombia utiliza para la ejecución de su objeto económico o social, y debe ser accedida solo por un grupo limitado de usuarios o personas autorizados. La divulgación de esta clase de información sin previa autorización de su propietario expone en riesgos extremos Datacenter Colombia, sus clientes, proveedores y terceros.

Información Uso Interno
Es aquella información que Datacenter Colombia utiliza para la ejecución de su objeto económico o social, y puede ser accedida por usuarios o personas autorizadas, para el desarrollo exclusivo de sus actividades diarias en cumplimiento de las funciones de su cargo o labor contractual acordada con la organización. La divulgación de esta clase de información al interior de las áreas de Datacenter Colombia, está sujeta al criterio de su propietario. Su divulgación sin previa autorización del propietario expone en riesgos leves o moderados a Datacenter Colombia.

Información personal
Todo dato o contenido asociado a la persona o individuo, que lo identifique o tenga relación directa con éste (documentos personales, contactos familiares, información familiar o círculos de amistad personal que no tenga que ver con los procesos y actividades de Datacenter Colombia, entre otros).

Integridad
Propiedad de salvaguardar la exactitud y estado completo del activo de información.

Mejora del SGSI
Mejora continua, acciones correctivas y acciones preventivas requeridas con el fin de minimizar impactos a todo nivel para la organización.

Partes Interesadas
Hace referencia a los empleados, clientes, usuarios, proveedores, socios estratégicos, accionistas, grupos u organizaciones que forman parte activa o pasiva de la organización.

Proteger la organización
Reducción del riesgo a través de la implementación de acciones o medidas de control dirigidas a disminuir el impacto o severidad de las consecuencias del riesgo si éste se materializa.

Procesamiento de Información
Es la capacidad que tiene un sistema de información de efectuar cálculos con base a una secuencia de operaciones preestablecidas, permitiendo la transformación de datos fuentes en información para ser utilizada en la toma de decisiones.

Riesgo
Se entiende por riesgo, la posibilidad de incurrir en pérdidas económicas, operativas, legales o de imagen para la organización por deficiencias, fallas o al no adecuado uso y/o manejo del activo de información, a causa de amenazas o vulnerabilidades que le altere su correcto funcionamiento u operatividad.

Seguridad de la información
Preservación de la confidencialidad, integridad y disponibilidad del activo de información, adicionalmente se deben preservar otros criterios o propiedades tales como la autenticidad, no repudio, confiablidad, propiedad y/o responsabilidad, entre otros.

SGSI
Sistema de gestión global, fundamentado en la orientación al riesgo del negocio a través de los procesos críticos y activos de información para establecer, implementar, operar, monitorear, revisar, mantener y mejorar la seguridad de la información en la organización tomando como base el modelo ISO/IEC 27001.

Tratamiento del riesgo
Proceso de selección e implementación de controles o acciones para ajustar el nivel de riesgo del activo a los niveles aceptables para la organización.

Vulnerabilidad
Es la debilidad o incapacidad de resistencia de un activo de información frente a una amenaza.

Sistema de Información
Disposición de personas, actividades o procedimientos y recursos tecnológicos integrados entre sí, para apoyar y mejorar las operaciones diarias de la organización, con la finalidad de satisfacer las necesidades de información a nivel general y facilitar la toma de decisiones por parte de los directivos de la organización. Los ejemplos aplicados más representativos: sistemas de automatización de oficina, sistemas de procesamiento de transacciones y sistemas de información de gestión.

Ente externo
Entidad que vigila o audita las actividades de una compañía bajo los lineamientos establecidos en un contrato o licitación suscrito por el mismo.

4. POLÍTICA GENERAL

4.1. Política Global de Seguridad de la Información A.5.1

Proteger, preservar y administrar la Información de los procesos del negocio de Datacenter Colombia S.A.S, clientes y socios estratégicos frente a amenazas internas o externas, accidentales o deliberadas, asegurando la Confidencialidad, Integridad y Disponibilidad de la información; en pro de la correcta ejecución de un Gobierno de Seguridad de la Información con enfoque en la norma ISO/IEC 27001:2022.

4.1.1. Normas para la política global de seguridad de la información

Para dar cumplimiento a la política, Datacenter Colombia S.A.S ha definido los siguientes compromisos para las áreas que la conforman.

La gerencia general demuestra su apoyo ante el sistema de gestión de seguridad de la información revisando y aprobando el manual de políticas de seguridad. Y designando las herramientas y recursos necesarios para el cumplimiento de este.

a) La gerencia general facilitará la divulgación de cada una de las políticas aprobadas en este documento a todas las áreas de la compañía, como también a los clientes y entes externos según aplique.

b) El Sistema Integral de Gestión (SIG) diseña, programa y ejecuta los programas de auditoría internas del sistema de gestión de seguridad de la información.

c) Los gerentes de procesos deben asegurarse de que todos los procedimientos de seguridad de la información dentro de su área de responsabilidad se realizan correctamente para fomentar un ambiente seguro en la compañía y lograr el cumplimiento de las políticas y estándares de seguridad de la información de Datacenter Colombia S.A.S.

d) Todas las áreas deben proteger los activos de información frente a incidentes de seguridad ocasionados por situaciones accidentales o deliberadas, materializadas sobre el hardware, software, fallas de la red corporativa o el tratamiento no adecuado de la información del negocio.

e) La gerencia general y/o el coordinador de seguridad de la información y ciberseguridad, revisarán las políticas anualmente o cuando se presenten cambios significativos en la organización para asegurar su coherencia con los objetivos del negocio y su eficacia.

Todas las áreas deben monitorear cambios significativos en los riesgos que afectan a los recursos de información frente a las amenazas más importantes.

5. POLÌTICAS ESPECÌFICAS

En el contexto de la ISO 27001:2022, las Políticas Específicas son una piedra angular del Sistema de Gestión de Seguridad de la Información (SGSI), proporcionando directrices claras para salvaguardar la confidencialidad, integridad y disponibilidad de la información en una organización. Estas políticas se enfocan en áreas específicas de seguridad y son cruciales para establecer un entorno robusto de protección cibernética. De esta manera abordamos las siguientes categorías:

- **Controles Organizacionales**: Establecen la estructura, roles y responsabilidades dentro de la organización, incluyendo la gestión de riesgos y la concienciación del personal.

- **Controles de Personas:** Regulan el comportamiento y las acciones de los individuos, desde la capacitación en seguridad hasta la gestión de accesos.

- **Controles Físicos**: Se centran en la protección física de los activos de información, abarcando el control de acceso y la seguridad de los equipos.

- **Controles Tecnológicos:** Relacionados con la seguridad de los sistemas y la infraestructura tecnológica, incluyendo la gestión de parches y la seguridad de redes.

Juntas, estas políticas forman un marco sólido que fortalece la resiliencia cibernética, protege los datos y aumenta la confianza de los Stakeholders en la seguridad de la organización. A continuación, procederemos a explorar detalladamente cada una de estas políticas específicas, para una implementación efectiva dentro del marco de la ISO 27001:2022.

5.1. Controles Organizacionales

5.1.1. Política para la organización de la seguridad de la información (A.5.2)

Definir, coordinar y controlar la gestión necesaria para mitigar los riesgos asociados a la seguridad de la información en Datacenter Colombia S.A.S y reportar al área de seguridad informática, quienes deben contar con la presencia de personal clave y claramente definido, con el objeto de cumplir y soportar las actividades de Seguridad de la Información.

5.1.1.1. Normas para la política de la organización de la seguridad de la información

Para dar cumplimiento a la política, Datacenter Colombia S.A.S ha definido los siguientes compromisos para las áreas que la conforman.

a) Promover iniciativas para incrementar la seguridad de la información, de acuerdo con las competencias y responsabilidades asignadas a cada área.

b) Garantizar que la seguridad sea parte del proceso de planificación informática, documental y normativa en el desarrollo de los proyectos de la organización.

c) Se debe definir los privilegios de acceso a los activos de información que debe tener cada área de acuerdo con su función dentro de la organización para evitar la modificación no autorizada o uso indebido de la información.

d) La gerencia y el área administrativa debe tener disponible los contactos con las autoridades competentes tanto en el marco legal como normativo.

e) Promover procedimientos de control para comprobar el grado de cumplimiento al Sistema de Seguridad de la Información.

f) Promover la difusión y apoyo a la Política de Seguridad de la Información de Datacenter Colombia S.AS.

g) Delimitar las responsabilidades de todo el personal involucrado, incluyendo colaboradores y terceras partes.

h) Aprobar los acuerdos de confidencialidad a utilizar en las relaciones con terceros, ya sean proveedores de servicio, de personal, entre otros.

i) Coordinar todos los proyectos de mejora o cambio, respecto a la seguridad de la información en aplicaciones o sistemas de información.

j) Garantizar que los procesos de adquisición, uso, gestión y salida de los servicios en la nube deben establecerse de acuerdo con los requisitos de seguridad de la información de Datacenter Colombia S.A.S

k) Datacenter Colombia S.A.S. está comprometida a identificar, evaluar y gestionar los riesgos de seguridad de la información, garantizando que los propietarios de riesgos acepten y gestionen los riesgos residuales.

l) Datacenter Colombia S.A.S asegura que todo el personal, incluidos colaboradores externos, tenga las competencias necesarias y reciba formación continua para cumplir con sus responsabilidades en materia de seguridad de la información.

m) El área de seguridad de la información de Datacenter Colombia S.A.S pueden delegar tareas, pero mantendrán la responsabilidad final de asegurar que se ejecuten correctamente. Se implementarán controles para supervisar y auditar las tareas delegadas.

5.1.2. Política de Segregación de funciones (A.5.3)

Datacenter Colombia S.A.S establece directrices para la segregación de funciones, con el fin de evitar conflictos de interés y garantizar un control efectivo sobre las operaciones, protegiendo la confidencialidad, integridad y disponibilidad de la información.

5.1.2.1. Normas para la política de Segregación de funciones

a) Se asignarán funciones específicas a diferentes personas para evitar que una sola persona tenga control sobre procesos críticos o sensibles.

b) Los sistemas de control de acceso basados en roles serán configurados para evitar que se asignen roles conflictivos a un mismo individuo.

c) Esta política será revisada anualmente o cuando existan cambios significativos en los procesos o en la estructura de la organización, asegurando su efectividad y alineación con los principios de seguridad de la información.

d) Se deberán revisar los accesos a sistemas de manera periódica para garantizar que ningún usuario tenga roles conflictivos.

e) La dirección administrativa deberá reporta cualquier novedad (desvinculación, cambio de cargo y/o área) del trabajador o proveedor a cargo para que sean generados los requerimientos de modificación y/o inhabilitación de los usuarios bajo un respectivo caso en la herramienta de Gestión cada área los requerimientos correspondientes.

5.1.3. Responsabilidades de la dirección (A.5.4)

Datacenter Colombia S.A.S asegura que la alta dirección este comprometida y apoye las iniciativas de seguridad de la información, garantizando que todo el personal esté alineado con las responsabilidades y controles en materia de seguridad de la información.

5.1.3.1. Responsabilidades de la dirección

a) La alta dirección de Datacenter Colombia S.A.S es responsable de apoyar las políticas y procedimientos de seguridad de la información, asegurando su correcta implementación y cumplimiento.

b) La alta dirección se compromete a apoyar al área de Seguridad de la Información de Datacenter Colombia S.A.S para que el personal acceda a la información o activos asociados, reciban una inducción sobre sus roles y responsabilidades en seguridad de la información, así como la documentación relacionada.

c) La alta dirección debe asegurarse de que sus equipos comprendan sus responsabilidades en cuanto a seguridad de la información y se mantengan informados y actualizados en temas relacionados con su rol

d) Todo funcionario de Datacenter Colombia S.A.S debe cumplir con las políticas de seguridad de la información, políticas específicas y procedimientos establecidos, así como con los términos y condiciones de su empleo, contrato o acuerdo.

e) Se fomentará el desarrollo continuo de las competencias en seguridad de la información a través de programas de capacitación y actualización para todo el personal relevante.

f) Se implementará un canal para que los funcionarios puedan reportar violaciones de las políticas de seguridad de la información o incidentes.

5.1.4. Contacto con las autoridades y Contacto con grupos de interés especial (A5.5, A5.6)

Datacenter Colombia S.A.S establece la directriz para asegúrese de contar con un plan para comunicarse con las personas adecuadas cuando haya un problema con la seguridad de la información. Esto incluye autoridades policiales, agencias reguladoras, autoridades

supervisoras y grupos de intereses especiales como asociaciones profesionales y organismos certificadores. Esta política garantiza que compartamos información de forma rápida y correcta, para que podamos seguir las reglas y mantener nuestra información segura.

5.1.4.1. Normas para la política Contacto con las autoridades y Contacto con grupos de interés especial

El contacto con las autoridades será realizado por la Gerencia General de DCSAS o el Área de Seguridad de la Información y Ciberseguridad de DCSAS, en coordinación con la Gerencia de Operaciones de DCSAS. Si el incidente afecta a un cliente, se notificará al área de Seguridad de la Información del cliente para que gestione la comunicación.

Proceso de comunicación:

a) Ante la identificación de un incidente, el área de Seguridad de la Información determinará la necesidad de contactar a las autoridades y la información que debe compartirse.

b) La comunicación debe realizarse de manera oportuna y por los canales adecuados, cumpliendo con los acuerdos de confidencialidad y protección de datos.

c) Se mantendrá un registro detallado de todos los contactos realizados con las autoridades, para su revisión y auditoría.

d) Datacenter Colombia S.A.S identificará y mantendrá relaciones con grupos de interés especial relevantes, tales como:

   a. Grupos de respuesta a incidentes (CERT, CSIRT).
   b. Asociaciones profesionales de ciberseguridad.
   c. Foros y comunidades de seguridad de la información.
   d. Relación continua con las autoridades:

Datacenter Colombia S.A.S mantendrá un contacto regular con las autoridades para asegurar el cumplimiento de las normativas vigentes y entender las expectativas actuales y futuras al igual con autoridades y grupos de interés especial.

5.1.5. Política de Clasificación y Gestión de Activos de Información (A.5.9, A.5.12, A.5.13)

Datacenter Colombia S.A.S. es propietario de la información física como también de la información generada, procesada, almacenada y transmitida a través de su plataforma de tecnología por lo cual identificará los activos y la información de la organización, y definirá las responsabilidades y directrices que regulen el uso adecuado de estos.

Todos los activos de información de Datacenter Colombia S.A.S serán clasificados de acuerdo con su sensibilidad y criticidad, los controles de seguridad serán implementados de acuerdo con su importancia en la organización garantizando la confidencialidad, integridad y disponibilidad de los activos de información.

La infraestructura de Datacenter Colombia S.A.S que procese, almacene y transmita información de sus clientes podrá ser ajustada a los lineamientos de seguridad de estos.

5.1.5.1. Normas para la política de seguridad de Clasificación y Gestión de Activos de Información

Para dar cumplimiento a la política, Datacenter Colombia S.A.S ha definido los siguientes compromisos para las áreas que la conforman.

a) Todas las áreas deberán alinearse a procediendo de gestión de activos para el manejo de toda la información de Datacenter Colombia S.A.S.

b) Las gerencias adoptaran la clasificación de la información en los procesos que manejan.

c) Datacenter Colombia S.A.S mantendrá un inventario de sus activos de información y cada gerencia declarará sus activos en el documento “Inventario de activos de información” y deberá asegurar su actualización para lo cual informará al área de servicios si presenta algún cambio.

d) Las áreas tienen la potestad de llevar un control adicional de sus activos de acuerdo con la información que requieran.

e) La gerencia de infraestructura definirá los métodos y herramientas de cifrado de la información de Datacenter Colombia S.A.S. de acuerdo con el nivel de clasificación de los activos, estándares de cifrado y capacidad de la infraestructura de IT.

f) Las gerencias de servicios e infraestructura deberán efectuar la eliminación segura de la información a través de herramientas apropiadas en los casos de dada de baja o cambio de usuarios de los activos.

g) La información o documentos físicos estará custodiada en el archivo centralizado de Datacenter Colombia S.A.S administrado por el área de archivo de GELSA. Quienes también realizaran la destrucción de esta cumplido los tiempos de retención establecidos con las áreas de apoyo de Datacenter Colombia S.A.S.

h) Para la información compartida en servidores de archivos la gerencia de infraestructura deberá garantizar e implementar los controles de acceso de acuerdo con la clasificación de esta.

i) Para el repositorio documental el área del SIG deberá definir la estructura de este y la gerencia de infraestructura deberá garantizar e implementar los controles de acceso de acuerdo con la clasificación de la información definida por las áreas de Datacenter Colombia S.A.S.

j) Determinar las categorías y datos sensibles que deberán ser enmascarados para garantizar el cumplimiento de la normatividad sobre la privacidad y protección de la información.

k) Implementar un control para el borrado de información en donde se establezca cómo, cuándo y dónde se eliminen los datos cuando ya no sean necesarios, con el fin de evitar la fuga de información sensible y permitir el cumplimiento de la privacidad y otros requisitos (podría incluir la eliminación dentro de los sistemas TI, medios extraíbles o servicios en la nube).

l) Aplicar medidas contra la fuga de datos para evitar la divulgación no autorizada de información sensible, incluyendo la información dentro de los sistemas informáticos, redes o cualquier dispositivo. Este control se establece en medida de la sensibilidad y clasificación de la información y evaluación de los riesgos.

5.1.6. Política Para Uso aceptable de la información y otros Activos asociados (A.5.10- A.5.11)

Lograr y mantener la protección adecuada de los activos de información mediante la implementación de normas y buenas prácticas para el uso de estos y la adecuada asignación de éstos a los usuarios finales que deban administrarlos de acuerdo con sus roles y funciones.

5.1.6.1. Normas para la política de usos de los activos

Para dar cumplimiento a la política, Datacenter Colombia S.A.S ha definido los siguientes compromisos para las áreas que la conforman.

a) Gestión del servicio pone al servicio de los colaboradores el uso de los medios necesarios para el normal desarrollo de las labores propias de sus respectivos cargos, para lo cual adopta y comunica las políticas de uso aceptable, controles y medidas dirigidas a garantizar la seguridad y continuidad del servicio que presta.

b) Todos los requerimientos de aplicativos, sistemas y equipos informáticos deben ser solicitados a través de la herramienta de gestión con su correspondiente justificación para su respectiva viabilidad.

c) Los usuarios no podrán efectuar ninguna de las siguientes labores sin previa autorización del área de Infraestructura de Datacenter Colombia:

- Instalar software en cualquier equipo de Datacenter;
- Bajar o descargar software de Internet u otro servicio en línea en cualquier equipo de Datacenter;
- Modificar, revisar, transformar o adaptar cualquier software propiedad de Datacenter Colombia S.A.S.
- Descompilar o realizar ingeniería inversa en cualquier software de propiedad de Datacenter.
- Copiar o distribuir cualquier software de propiedad de Datacenter Colombia S.A.S.

Nota: Para los casos en que los equipos hagan parte del inventario de los clientes, cualquiera de las anteriores actividades deberá contener autorización del área o departamento del cliente responsable por ellos.

5.1.7. Política de Transferencia de Información (A.5.14)

Datacenter Colombia S.A.S asegurará la protección de la información en el momento de ser transferida o intercambiada internamente o con otras entidades y establecerá los procedimientos y controles necesarios para el intercambio de información; así mismo, se establecerán Acuerdos de Confidencialidad y/o de Intercambio de Información con las terceras partes con quienes se realice dicho intercambio.

5.1.7.1. Normas para la política de transferencia de información

Para dar cumplimiento a la política, Datacenter Colombia S.A.S ha definido los siguientes compromisos para las áreas que la conforman.

a) La Gerencia de Infraestructura de Datacenter Colombia S.A.S debe garantizar la integridad y confidencialidad de la información del negocio de extremo a extremo al ser transferida por canales dedicados o por internet. En este sentido no se debe hacer uso de protocolos de transferencia de información catalogados como inseguros (ftp, telnet, http, etc) y se debe asegurar con protocolos o técnicas de cifrado robusto el canal de comunicación implementado para tal fin.

b) La Gerencia de Infraestructura de Datacenter Colombia S.A.S deberá establecer procedimientos y controles para proteger la transferencia de información abarcando la detección y protección contra malware o amenazas avanzadas transmitidas a través de los canales de comunicaciones.

c) Datacenter Colombia S.A.S velará por la protección de la información, sin embargo, el contenido de los archivos enviados a través del canal de Internet de la compañía será directamente responsabilidad del funcionario y/o contratista.

d) La Gerencia de Infraestructura de Datacenter Colombia S.A.S y la Gerencia de Soluciones debe definir estrategias para la correcta gestión e intercambio seguro de

información con entidades externas, lo anterior de la mano con el diseño, establecimiento y aplicación de acuerdos en los cuales se definan las responsabilidades en el intercambio de información de las partes que interactúen en el mismo.

e) Los administradores de los activos de información tecnológicos y recursos informáticos deben aplicar los controles necesarios que garantizan la disponibilidad, confidencialidad e integridad de la información transmitida electrónicamente por medio de recursos tecnológicos de propiedad o provistos por Datacenter Colombia S.A.S, según necesidad o el nivel de criticidad de esta.

f) A través de los planes de auditoría interna se debe identificar, revisar regularmente y documentar los requisitos para los acuerdos de confidencialidad o no divulgación que reflejen las necesidades de la organización para la protección de la información.

g) Toda información sensible y catalogada como privada para el negocio a transferir a través correo electrónico debe estar cifrada sea directamente la información o el correo electrónico.

h) Gestionar las páginas web a las que acceden los usuarios por medio del filtrado web, protegiendo así los sistemas informáticos, equipos, redes y usuarios, y previniendo cualquier tipo de compromiso por código malicioso o amenaza en la red.

i) Para proteger la integridad y confidencialidad de la información en tránsito, se prohíbe el uso de protocolos de transferencia no seguros, como FTP y HTTP sin cifrado. En su lugar, deben emplearse protocolos seguros, tales como SFTP, FTPS, HTTPS o VPN, que garanticen el cifrado de extremo a extremo en las comunicaciones.

5.1.8. Política de Control de Acceso (A.5.15-A.5.18, A.8.1-A.8.5)

Definir las pautas generales para asegurar un acceso controlado, físico o lógico, a la información de la plataforma informática de Datacenter Colombia S.A.S a través de medidas de control de acceso con el fin de evitar la adulteración, pérdida, fuga, consulta, uso o acceso no autorizado o fraudulento, impactando la Confidencialidad, Integridad y Disponibilidad de la información.

5.1.8.1. Normas para la política de control de acceso

Para dar cumplimiento a la política, Datacenter Colombia S.A.S ha definido los siguientes compromisos para las áreas que la conforman.

Datacenter Colombia S.A.S establecerá procedimientos formales para controlar la definición de perfiles y la asignación de derechos de acceso a los usuarios, previamente definidos por el coordinador de seguridad de la información y ciberseguridad. Dichos procedimientos

deben cubrir todas las etapas del ciclo de vida del usuario, desde su registro inicial hasta la eliminación o desactivación del registro a quienes no necesiten el acceso.

a) Datacenter Colombia S.A.S suministrará a los usuarios y las claves respectivas para el acceso a los servicios de red y sistemas de información a los que hayan sido autorizados, las claves son de uso personal e intransferible.

b) La contraseña de acceso para: equipos de cómputo, servidores, base de datos, equipos de telecomunicaciones deberá tener mínimo ocho caracteres con la siguiente estructura: una letra minúscula, una letra mayúscula, un número.

c) La contraseña de acceso para las soluciones tecnológicas que desarrolla Datacenter deberá contener la siguiente estructura:

    a. Tener mínimo 8 caracteres con una combinación de caracteres alfanuméricos y un carácter especial.
    b. Tener mínimo 6 caracteres con una combinación de caracteres alfanuméricos.

d) Cada funcionario es responsable por las acciones realizadas sobre cualquier recurso de Información de Datacenter Colombia S.A.S a través del usuario que le ha sido asignado. Por lo tanto, la identidad de cada funcionario se encuentra establecida de una manera única. Este usuario de ninguna manera o por ninguna circunstancia podrá ser compartido. El sobrepaso a esta directriz será tratado como una violación a la seguridad de la información.

e) Para el acceso a los servicios de información el gerente de proceso de cada dependencia deberá realizar la solicitud a la mesa de servicio, especificando los datos exactos de la persona, a que servicios debe darse acceso y por cuanto tiempo

f) Otorgar acceso a los usuarios sobre los servicios y/o activos necesarios para soportar el servicio específico requerido. Se deben fortalecer los controles de acceso a nivel de objeto o aplicación, de manera que un usuario legítimo, una vez otorgado el acceso, no pueda alterar datos no requeridos por el servicio solicitado.

g) Únicamente se debe proporcionar a los colaboradores el acceso a los servicios para los que específicamente se les haya autorizado su uso. Se deben utilizar métodos apropiados de autenticación para el control de acceso a los usuarios remotos. Se deben implantar controles adicionales para el acceso por redes inalámbricas. Se debe establecer una adecuada segregación de redes, separando los entornos de red de usuarios y los servicios.

h) Definir quién o quiénes pueden acceder al tipo de datos enmascarados o no enmascarados, limitando la exposición de información sensible, principalmente a los datos personales y también otras categorías de datos sensibles.

5.1.9. Política de Enmascaramiento de Datos (A.8.11)

Datacenter Colombia S.A.S establece que todos los datos sensibles gestionados en sus sistemas de información deben contar con mecanismos de enmascaramiento que aseguren su confidencialidad, integridad y disponibilidad, en cumplimiento con los requisitos normativos, contractuales y legales aplicables. Esta política busca prevenir accesos no autorizados y reducir el riesgo de exposición indebida de información crítica, aplicando controles técnicos y procedimentales en bases de datos, aplicaciones y desarrollos internos, conforme a los lineamientos del SGSI y de las áreas responsables.

5.1.9.1. Normas para la política de Enmascaramiento de Datos

Para dar cumplimiento a esta política, Datacenter Colombia S.A.S ha definido los siguientes compromisos para las áreas responsables:

a) Todos los campos identificados como datos sensibles (ej. datos personales, financieros, credenciales, información regulada) deben ser enmascarados en su visualización y manipulación, conforme al inventario de activos de información.
b) En ausencia de herramientas específicas de *data masking*, el enmascaramiento se aplicará mediante lógica de aplicación o codificación segura, asegurando que los datos sensibles no se expongan en interfaces de usuario, pruebas o ambientes no productivos.
c) El área de Soluciones Tecnológicas será responsable de implementar enmascaramiento en aplicaciones y desarrollos, siguiendo las directrices de codificación segura (GST-DG-07) y gestión de seguridad en aplicaciones (SGSI-DG-06).
d) El área de DBA/Infraestructura deberá validar que en las bases de datos bajo su gestión se apliquen mecanismos de cifrado o enmascaramiento cuando la tecnología lo permita, y que dichos registros estén debidamente documentados.
e) Se prohíbe el uso de datos sensibles reales en ambientes de desarrollo o prueba sin aplicar enmascaramiento o anonimización previa.
f) El Coordinador del SGSI será responsable de supervisar la correcta aplicación de esta política, actualizar la Declaración de Aplicabilidad y coordinar las revisiones periódicas para verificar su cumplimiento.

5.1.10. Política de Relación con Proveedores (A.5.19, A.5.20, A.5.21, A.5.22)

Garantizar la protección de los activos de la organización que sea accesible por los proveedores.

5.1.10.1. Normas para la política con proveedores

Para dar cumplimiento a la política, Datacenter Colombia S.A.S ha definido los siguientes compromisos para las áreas que la conforman.

a) Se deben establecer acuerdos documentados con todos los proveedores de servicios internos y externos.

b) Se deben adoptar medidas con los proveedores de servicios de comunicaciones, alojamiento de servidores, mantenimiento o bajo el modelo de infraestructura tecnológica como servicio, para hacer frente a problemas de seguridad de la información a través de un punto de contacto definido y de una persona que sea competente para tratar los problemas de seguridad de la información de manera eficaz.

c) Se deben adoptar medidas con los proveedores de servicios logísticos y administrativos que apoyan la operación y que pueden afectar la disponibilidad de las plataformas tecnológicas y por tanto la prestación del servicio.

d) Las gerencias deben hacer seguimiento, revisar y auditar de ser posible con regularidad la prestación de servicios de los proveedores a cargo.

5.1.11. Política de Seguridad de la información para el uso de servicios en la nube (A.5.23)

Garantizar la protección de la confidencialidad, integridad y disponibilidad de los activos de información gestionados en servicios en la nube, alineándose con estándares de seguridad aplicables y asegurando que los proveedores cumplen con las prácticas de protección de datos y resiliencia operacional adecuadas

5.1.11.1. Normas para la Política de Seguridad de la información para el uso de servicios en la nube (A.5.23)

a) Identificar y evaluar riesgos específicos asociados con el uso de la nube, como la transferencia de datos entre ubicaciones, acceso por terceros y dependencia de conectividad.
b) Verificar que el servicio en la nube se adapte a los requisitos y controles del Sistema de Gestión de Seguridad de la Información (SGSI) de la empresa, considerando su nivel de madurez.
c) Exigir al proveedor certificaciones vigentes (ISO 27001, 27017, 27018, entre otras) y evidencia de auditorías recientes que demuestren el cumplimiento de las prácticas de seguridad en la nube.
d) Revisar que el proveedor cuente con un protocolo de respuesta a incidentes que garantice una rápida recuperación y notificación de eventos de seguridad.
e) Establecer que el proveedor implemente control de acceso basado en roles (RBAC) o control de acceso basado en atributos (ABAC) para limitar el acceso según necesidades específicas.
f) Asegurar que el proveedor mantenga políticas de respaldo y recuperación que incluyan pruebas periódicas de recuperación ante desastres, garantizando la disponibilidad de la información.

g) Exigir que el proveedor gestione las configuraciones de seguridad de forma segura y documentada, aplicando principios de configuración segura y manteniendo un registro de cambios en la infraestructura en la nube.
h) Asegurarse de que el proveedor gestione los riesgos de entornos multicliente, evitando configuraciones que puedan exponer los datos de la empresa.

5.1.12. Política Derechos de propiedad intelectual (A.5.32)

Proteger los derechos de propiedad intelectual de Datacenter Colombia S.A.S. y garantizar que los activos desarrollados, tanto interna como externamente, sean gestionados de acuerdo con los requisitos de confidencialidad, integridad y disponibilidad.

5.1.12.1. Normas para la Política de Derechos de propiedad intelectual (A.5.32)

a) Todos los activos de propiedad intelectual desarrollados por Datacenter Colombia S.A.S., incluyendo software, documentación técnica, y cualquier creación intelectual derivada de las actividades de la empresa, serán de propiedad exclusiva de Datacenter Colombia S.A.S., salvo acuerdo contractual en contrario.

b) Los contratos de desarrollo realizados por proveedores y contratistas deben incluir una cláusula de transferencia de propiedad intelectual hacia Datacenter Colombia S.A.S. de todos los materiales, códigos y productos generados en el marco del contrato.

c) Todo desarrollo de propiedad intelectual clasificado como confidencial o reservado debe contar con medidas de protección adecuadas, tales como cifrado y acceso restringido, para evitar su divulgación o uso no autorizado.

d) Los activos de propiedad intelectual deben registrarse y actualizarse periódicamente en el inventario de activos de Datacenter Colombia S.A.S., indicando su nivel de sensibilidad y aplicando controles específicos según el tipo de información.

e) La eliminación o destrucción de cualquier activo de propiedad intelectual debe realizarse conforme a los procedimientos de eliminación segura, asegurando que no se conserve ningún registro o copia sin autorización.

f) El acceso a los activos de propiedad intelectual estará limitado a personal autorizado de Datacenter Colombia S.A.S. y será revisado y actualizado en caso de cambios en las responsabilidades del personal.

g) En caso de incidentes que impliquen el uso no autorizado o la pérdida de activos de propiedad intelectual, se activará el procedimiento de respuesta a incidentes de seguridad, y se tomarán las medidas correctivas pertinentes para prevenir futuras ocurrencias.

5.1.13. Política de Protección de registros (A.5.33- A.8.15)

Asegurar la protección, integridad y disponibilidad de los registros críticos de Datacenter Colombia S.A.S., aplicando controles de acceso, almacenamiento y eliminación segura para evitar la pérdida o el uso no autorizado de la información.

5.1.13.1. Normas para la Política de Protección de registros (A.5.33 – A.8.15)

a) Todos los registros que contengan información confidencial o crítica de Datacenter Colombia S.A.S. deberán ser almacenados en medios seguros y protegidos contra accesos no autorizados mediante el uso de controles físicos y lógicos.
b) Los registros digitales se almacenarán en sistemas de almacenamiento seguros, aplicando mecanismos de cifrado en función de su nivel de sensibilidad, y se realizará un respaldo periódico para garantizar su disponibilidad.
c) Los registros físicos deberán ser resguardados en áreas designadas y protegidas, como archivadores con acceso controlado o espacios de almacenamiento seguro, y solo personal autorizado podrá acceder a ellos.
d) Los registros deben mantenerse de acuerdo con el periodo de retención definido por Datacenter Colombia S.A.S., cumpliendo con las normativas legales y contractuales aplicables, y serán eliminados de forma segura una vez finalizado dicho periodo.
e) La eliminación de registros, tanto en formato físico como digital, debe realizarse mediante procedimientos seguros, asegurando la destrucción completa para prevenir cualquier recuperación no autorizada de la información.
f) Todos los accesos a registros electrónicos sensibles deben ser registrados y auditados regularmente para asegurar que no haya accesos no autorizados o uso indebido de la información.
g) En caso de una posible pérdida, alteración o acceso no autorizado a los registros, se activará el protocolo de respuesta a incidentes de seguridad para investigar y mitigar el impacto en la operación.

5.1.14. Política Privacidad y protección de PII (A.5.34)

Proteger la privacidad y la seguridad de los datos personales procesados por Datacenter Colombia S.A.S., garantizando que la recolección, almacenamiento, uso y eliminación de la información de identificación personal (PII) cumpla con las normativas de protección de datos y los estándares de seguridad de Datacenter Colombia S.A.S.

5.1.14.1. Normas para la política de Privacidad y protección de PII (A.5.34)

a) Toda recolección de datos personales debe estar respaldada por una base legal y contar con el consentimiento informado del titular de la información, salvo en los casos permitidos por la ley.

b) Los datos personales se almacenarán en sistemas seguros, aplicando cifrado y control de acceso para evitar accesos no autorizados y mantener la confidencialidad de la información.
c) El acceso a la PII estará restringido únicamente al personal autorizado que requiera dicha información para el desarrollo de sus funciones, aplicando el principio de minimización de acceso.
d) Los datos personales serán conservados únicamente durante el período necesario para cumplir con los fines para los cuales fueron recolectados o según lo exijan las normativas legales y contractuales aplicables.
e) La eliminación de datos personales deberá realizarse de manera segura y completa una vez que hayan cumplido su propósito o expirado el periodo de retención, previniendo cualquier recuperación no autorizada.
f) En caso de detectar un incidente de seguridad que afecte la PII, se activará el protocolo de respuesta a incidentes, notificando a los titulares y autoridades competentes según los requisitos legales aplicables.
g) Se revisarán y actualizarán periódicamente las medidas de protección de la PII para asegurar su adecuación a cambios en las normativas de privacidad y en los procesos internos de Datacenter Colombia S.A.S.

5.1.15. 4.1.6 Política de Seguridad en las operaciones (A.5.37)

Asegurar operaciones correctas y seguras de las instalaciones de procesamiento de información.

5.1.15.1. Normas para la política de seguridad en las operaciones

Para dar cumplimiento a la política, Datacenter Colombia S.A.S ha definido los siguientes compromisos para las áreas que la conforman.

a) Datacenter Colombia S.A.S asignará funciones específicas a sus funcionarios, quienes deben efectuar la operación y administración de los recursos tecnológicos, manteniendo y actualizando la documentación de los procesos operativos para la ejecución de las actividades.

b) Se debe garantizar la correcta planificación, documentación y actualización de los procedimientos relacionados con la operación y administración de la plataforma tecnológica que apoya los procesos de negocio de Datacenter Colombia S.A.S, entre los principales se encuentran la ***gestión de cambios, la gestión de la capacidad y la separación de ambientes***. Así mismo, deberán ser puestos a disposición de los usuarios que los necesitan.

c) Datacenter Colombia S.A.S debe proveer a los funcionarios encargados de la operación de manuales de configuración y operación de los sistemas operativos, servicios de red, bases de datos y sistemas de información (comunicaciones y servicios como correo,

intranet, WEB) así como todos los componentes de la plataforma tecnológica de la entidad.

d) Datacenter Colombia S.A.S se encarga de gestionar todo el ciclo de configuración de seguridad tecnológica, garantizando así un nivel adecuado de seguridad y evitando cualquier cambio no autorizado dentro de los sistemas de información. Esto incluye la definición, documentación, implementación, monitoreo y revisión de la configuración (incluyendo software, hardware, servicios y redes).

e) Datacenter Colombia S.A.S garantiza que las políticas de navegación segura y filtrado web aplicadas a través de las soluciones de seguridad (ej. Sophos Endpoint) se mantienen vigentes y consistentes en todo entorno de conexión, incluyendo la red corporativa, accesos remotos y conexiones externas, con el fin de prevenir accesos a sitios maliciosos, inapropiados o no autorizados.

5.1.16. Política para la Gestión de Incidentes de Seguridad de la Información (A.5.24-A.5.28)

Establecer lineamientos generales para gestionar los incidentes de seguridad de la información, con el fin de prevenir y mitigar el impacto de estos sobre las operaciones del negocio.

5.1.16.1. Normas para la política de gestión de incidentes de seguridad de la información

Para dar cumplimiento a la política, Datacenter Colombia S.A.S ha definido los siguientes compromisos para las áreas que la conforman.

a) Disponer los recursos necesarios a fin de brindar una apropiada gestión de los incidentes de seguridad de la información, mediante la designación de un equipo responsable por la gestión de incidentes de seguridad de la información.

b) Registrar y revisar eventos y actividades críticas llevadas a cabo por los usuarios en los sistemas.

c) Definir un procedimiento adecuado para hacer el registro de los incidentes de manera que estos queden consignados de forma centralizada y tengan el tratamiento adecuado dependiendo su criticidad.

d) Todos los funcionarios, clientes, socios estratégicos, proveedores de Datacenter Colombia S.A.S y cualquier tercero que interactúe con los sistemas de información de la compañía tienen el deber de reportar cualquier incidente de seguridad o actividad

sospechosa que detecten sobre los sistemas de información al líder de seguridad informática y perimetral de Datacenter Colombia S.A.S.

e) Dar cumplimiento a la presente política, independiente del cargo que desempeñe y de su situación contractual.

f) Concientizar a los usuarios respecto de su responsabilidad frente a la mitigación de los incidentes y los beneficios que trae consigo mantener el bueno uso de los activos y comunicar cualquier evento que pueda suponer un mal funcionamiento.

g) Revisar y analizar los incidentes de seguridad de la información.

5.1.17. Política de Continuidad del Negocio (A.5.29, A.5.30)

Asegurar que la organización no experimente interrupciones inaceptables en cualquiera de sus operaciones esenciales, ante la eventualidad de una falla parcial o total de los servicios que se encuentran bajo la administración directa de la Gerencia de Infraestructura, de manera que permita gestionar los riesgos, proteger la información de los procesos críticos y mantener la habilidad de la organización para resistir incidentes catastróficos.

5.1.17.1. Normas para la política de continuidad del negocio

Para dar cumplimiento a la política, Datacenter Colombia S.A.S ha definido los siguientes compromisos para las áreas que la conforman.

a) Evaluar el impacto de eventos que afectan los procesos de la organización que tienen soporte en la infraestructura tecnológica que ésta administra.

b) Definir niveles de impacto sobre la operación del negocio.

c) Se debe planear, desarrollar e implantar un Plan de Continuidad del negocio para asegurar que los procesos de negocio de Datacenter Colombia S.A.S puedan ser restaurados dentro de escalas de tiempo razonables, minimizando el impacto y con los niveles de seguridad adecuados para proteger la información.

d) Desarrollar un plan de contingencia para aquellos servicios de TI que son críticos para Datacenter Colombia S.A.S. Los planes deben considerar medidas tanto técnicas como administrativas y de vínculo con entidades externas. El plan de contingencia se debe someter a pruebas de forma controlada dos veces al año, para verificar su eficacia y capacidad de respuesta a eventos inesperados.

e) Suministrar los recursos suficientes para proporcionar una respuesta efectiva de funcionarios y procesos en caso de contingencia o eventos catastróficos que se presenten en Datacenter Colombia S.A.S y que afecten la continuidad de su operación.

f) Adoptar medidas para asegurar la prestación continua de los servicios críticos de la red en caso de una prolongada falta de disponibilidad de:
   - el centro de operaciones de la red
   - los equipos de red críticos
   - los enlaces de red en las instalaciones de la empresa
   - el software de comunicaciones, los datos de control y la documentación

g) Definir las acciones a seguir en caso de situaciones no previstas que afecten la continuidad de los procesos críticos de Datacenter.

5.1.18. Política de Cumplimiento (A.5.31- A.5.37)

Velar por la identificación, documentación y cumplimiento de la legislación relacionada con la seguridad de la información, entre ella la referente a la protección de datos personales, los derechos de autor y propiedad intelectual, razón por la cual propenderá porque el software instalado en los recursos de la plataforma tecnológica cumpla con los requerimientos legales y de licenciamiento aplicables.

5.1.18.1. Normas para la política de cumplimiento

Para dar cumplimiento a la política, Datacenter Colombia S.A.S ha definido los siguientes compromisos para las áreas que la conforman.

a) El coordinador de seguridad de información y ciberseguridad definirá y documentará claramente todos los requisitos normativos y contractuales pertinentes para cada sistema de información. Del mismo modo se definirá y documentará los controles específicos y las responsabilidades y funciones individuales para cumplir con dichos requisitos.

b) Se debe establecer en los contratos de trabajo de empleados y en los contratos de desarrollo realizados por proveedores y contratistas, cláusulas respecto a la propiedad intelectual de Datacenter Colombia S.A.S, al material y productos generados en el desarrollo del negocio.

c) Los diferentes aspectos contemplados en este Manual son de obligatorio cumplimiento para todos los funcionarios, contratistas y otros colaboradores de Datacenter Colombia S.A.S. En caso de que se violen las políticas de seguridad ya sea de forma intencional o por negligencia, Datacenter Colombia S.A.S tomará las acciones disciplinarias y legales correspondientes.

d) Se debe implementar controles para asegurar la privacidad y la protección de la información de datos personales, como se exige en la legislación y la reglamentación pertinente. Cuando sea aplicable.

e) El coordinador de seguridad de la información y ciberseguridad en conjunto con las gerencias deberá revisar independientemente a intervalos planificados o cuando ocurran cambios significativos, el enfoque de la organización para la gestión de la seguridad de la información y su implementación (objetivos de control, controles, política, procesos y procedimientos para la seguridad de la información)

5.2. Controles de Personas

5.2.1. Política de Seguridad para los recursos humanos (A.6)

Datacenter Colombia S.A.S asegurará que los gerentes, directores, colaboradores, proveedores y demás recursos que se encuentren asociados a las actividades de la compañía, entiendan sus responsabilidades y las funciones de sus roles, con el fin de reducir el riesgo de hurto, fraude, filtraciones o uso inadecuado de la información y de las instalaciones tanto de Datacenter Colombia S.A.S. como de sus clientes.

Datacenter Colombia S.A.S delega la responsabilidad a un tercero para manejar los procesos asociados a la selección, términos y condiciones de empleo (Antes de asumir el empleo A7.1).

5.2.1.1. Normas para la política de seguridad de los recursos humanos

Para dar cumplimiento a la política, Datacenter Colombia S.A.S ha definido los siguientes compromisos para las áreas que la conforman.

a) Para toda persona que ingrese a la compañía, la dirección administrativa debe asegurar las responsabilidades sobre seguridad de manera previa a la contratación. Esta tarea debe reflejarse en una adecuada descripción del cargo y en los términos y condiciones de la contratación. Así mismo, asegurará que los colaboradores conozcan sus roles y responsabilidades con respecto a su rol dentro de la organización.

b) La dirección administrativa debe garantizar que todos los empleados de Datacenter Colombia S.A.S y terceros reciban la educación y la formación en toma de conciencia apropiada y actualización regulares sobre las políticas y procedimientos pertinentes a su cargo.

c) Todos los gerentes, directores, colaboradores, proveedores y demás recursos asociados a las actividades de la compañía deberán conducirse conforme a los principios de confidencialidad y uso adecuado de los recursos informáticos y de información de Datacenter Colombia S.A.S, así como comprometerse a cumplir con lo establecido en el Manual de la Política de Seguridad de Datacenter.

d) Los colaboradores deben firmar un acuerdo de confidencialidad y un documento de aceptación de Políticas de seguridad de la información antes que se les otorgue acceso

a las instalaciones de procesamiento y/o acceso a la información de Datacenter Colombia S.A.S o de terceros. El área administrativa es responsable de garantizar que esta norma se cumpla.

e) La alta gerencia debe definir y establecer el procedimiento disciplinario ante alguna falta a las políticas de seguridad y normas por parte de los colaboradores y terceros. El área administraba velará por la comunicación de este.

f) El coordinador de Seguridad de la información y ciberseguridad deberá diseñar y ejecutar de forma permanente un programa de concienciación en seguridad de la información a fin de apoyar el cumplimiento de las políticas de seguridad de la información durante la vinculación y desvinculación de los colaboradores.

g) El gerente de cada área debe reportar a la dirección administrativa cualquier novedad (desvinculación, cambio de cargo y/o área) del trabajador o proveedor a cargo para que sean generados los requerimientos de modificación y/o inhabilitación de los usuarios de acceso a las plataformas que información al área de servicio quienes escalaran a cada área los requerimientos correspondientes.

5.2.2. Trabajo a distancia (A.6.7)

Establecer restricciones para el uso de dispositivos móviles y portátiles; autorizando, monitoreando y controlando el acceso de estos a los sistemas de información.

5.2.2.1. Normas para la política de Trabajo a distancia (A.6.7)

Para dar cumplimiento a la política, Datacenter Colombia S.A.S ha definido los siguientes compromisos para las áreas que la conforman

a) El uso de los equipos portátiles fuera de las instalaciones de Datacenter Colombia S.A.S. únicamente se permitirá a usuarios autorizados por las Gerencias de proceso, previa solicitud de la dependencia respectiva, y éstos se protegerán mediante el uso de controles tecnológicos.

b) Cualquier funcionario de Datacenter Colombia S.A.S autorizado por la Gerencia, que requiera tener acceso a la información de la organización desde redes externas, podrá acceder remotamente mediante el debido proceso de autenticación y uso de conexiones seguras. Lo anterior asegurando el cumplimiento de requisitos de seguridad de los equipos desde los que se accede.

5.3. Controles Físicos

5.3.1. Política de Seguridad Física y del entorno (A.7.1-A.7.6)

Evitar el acceso físico no autorizado, daños e interferencia para la información de la organización, definiendo normas y procedimientos para la protección física en las zonas donde se alojan los servicios de TI críticos de Datacenter Colombia S.A.S.

5.3.1.1. Normas para la política de seguridad física y del entorno

Para dar cumplimiento a la política, Datacenter Colombia S.A.S ha definido los siguientes compromisos para las áreas que la conforman.

a) Las áreas seguras se protegerán mediante controles de entrada adecuados para garantizar que se le permita el acceso únicamente al personal autorizado.

b) Los servidores que contengan información y servicios de Datacenter Colombia S.A.S deben ser mantenidos en un ambiente seguro y protegido por los menos con:
   - Controles de acceso y seguridad física.
   - Detección de incendio y sistemas de extinción de conflagraciones.
   - Controles de humedad y temperatura.
   - Bajo riesgo de inundación.
   - Sistemas eléctricos regulados y respaldados por fuentes de potencia ininterrumpida (UPS).

c) Los controles aquí mencionados deben ser monitoreados y revisados de manera permanente evitando la pérdida de información por cualquier causa “fuga, robo, destrucción o daño.

d) Se deben realizar mantenimientos preventivos y correctivos de los servidores, equipos de comunicaciones y de seguridad que conforman la plataforma tecnológica de Datacenter Colombia S.A.S.

e) Se deben tener en cuenta los procesos de instalación y retirada del equipo, de tal manera que estos se hagan de forma controlada y segura. La protección de los equipos, incluso cuando se utilizan fuera de la oficina, es necesaria para reducir el riesgo de acceso no autorizado a la información y para protegerlo contra pérdida o robo.

f) Este control permite que a las instalaciones sensibles de Datacenter Colombia S.A.S puedan ser monitoreadas de manera continua para detectar accesos físicos no autorizados.

5.3.2. Política Entrada Física

Regular el uso de cámaras filmadoras, fotográficas, dispositivos móviles dentro de las instalaciones de Datacenter Colombia S.A.S, así como los registros que deriven de las mismas (Video e Imágenes).

5.3.2.1. Normas para la política de controles físicas de entrada.

Para dar cumplimiento a la política, Datacenter Colombia S.A.S ha definido los siguientes compromisos para las áreas de que la conforman.

a) No está permitido el ingreso y uso de cámaras filmadoras, fotográficas, dispositivos móviles a las áreas seguras de Datacenter Colombia S.A.S (cuarto de telecomunicaciones, centros de datos) sin autorización previa del área de Seguridad de la información.

b) Cualquier toma fotográfica o filmación que se encuentre autorizada por el área de Seguridad de la Información de Datacenter Colombia S.A.S, estará supervisada por el responsable del área solicitante a fin de evitar el registro de imágenes que afecten la protección, la seguridad y la propiedad intelectual de Datacenter Colombia S.A.S.

5.3.3. Escritorio y pantalla limpia (A.7.7)

Garantizar que la información confidencial que se encuentra en los medios físicos, magnéticos, digitales, impresoras, escáner y equipos de cómputo, se proteja con el uso de contraseñas, protectores de pantalla; y los medios físicos que contienen información propia de la compañía, se encuentran resguardados en los escritorios de los funcionarios y diferentes áreas en que laboran en Datacenter Colombia S.A.S.

5.3.3.1. Normas para la política de escritorio y pantalla limpia

Para dar cumplimiento a la política, Datacenter Colombia S.A.S ha definido los siguientes compromisos para las áreas que la conforman.

a) Siempre que un funcionario se ausenta de su lugar de trabajo debe bloquear la sesión y guardar en un lugar seguro cualquier documento o medio magnético removible que contenga información de uso interno que se considere confidencial.

b) Los funcionarios son responsables de los equipos asignados a su cargo para el desarrollo de sus labores, por tanto, quienes tengan a su cargo equipos portátiles deben verificar que el equipo se encuentre seguro siempre que se ausenten de su lugar de trabajo.

c) Todos los escritorios o mesas de trabajo deben permanecer limpios para proteger documentos en papel y dispositivos de almacenamiento como CD, Memorias USB, y otros, con fin de reducir riesgos de acceso no autorizado, pérdida y daño de la información durante el horario normal de trabajo y fuera del mismo.

d) Todos los funcionarios deben dar el tratamiento adecuado a la documentación impresa, escaneada o física utilizada, con el fin de evitar el uso o perdida de documentación sensible que afecte la seguridad de Datacenter Colombia S.A.S y sus aliados.

e) En todas las áreas donde se procese información física a través de Impresoras, escáner, fax y multifuncionales no se debe dejar documentos que contengan información sensible para Datacenter Colombia S.A.S y sus aliados.

f) Al final de la jornada de trabajo el funcionario debe asegurar de limpiar su escritorio y guardar todos los papeles que contengan información confidencial.

g) La gerencia de infraestructura garantizará a través de Directorio Activo la política de escritorio limpio para las estaciones de trabajo asociadas a este.

5.3.4. Política de Medios de Almacenamiento (A.7.10)

El uso de periféricos y medios de almacenamiento en los recursos de la plataforma tecnológica de Datacenter Colombia S.A.S será reglamentado por el área de Infraestructura de TI, considerando las labores realizadas por los funcionarios y su necesidad de uso.

5.3.4.1. Normas para la política de medios de Almacenamiento

Para dar cumplimiento a la política, Datacenter Colombia S.A.S ha definido los siguientes compromisos para las áreas que la conforman.

a) Infraestructura implantará los controles que regulen el uso de periféricos y medios de almacenamiento en la plataforma tecnológica de Datacenter Colombia S.A.S, de acuerdo con los lineamientos y condiciones establecidas.

b) Gestión de servicios debe generar y aplicar lineamientos para la disposición segura de los medios de almacenamiento de Datacenter Colombia S.A.S, ya sea cuando son dados de baja o re-asignados a un nuevo usuario.

c) Los funcionarios y el personal externo deben acogerse a las condiciones de uso de los periféricos y medios de almacenamiento establecidos por Datacenter Colombia S.A.S. Así mismo, no deben modificar la configuración de periféricos y medios de almacenamiento establecidos por la compañía.

d) Los usuarios que requieran utilizar dispositivos de almacenamiento externo deben obtener aprobación formal e individual del coordinador de seguridad de la información y

ciberseguridad. Si los dispositivos son del cliente es necesario que remitan la aprobación por parte del área autorizada de sus empresas.

5.4. Tecnología

5.4.1. Política de Dispositivos de punto final de usuario (A.8.1)

Asegurar el uso adecuado y seguro de los dispositivos de punto final que acceden a los sistemas y recursos de Datacenter Colombia S.A.S., protegiendo la información contra accesos no autorizados, pérdida o daño.

5.4.1.1. Normas para la Política de Dispositivos de punto final de usuario (A.8.1)

a) Todos los dispositivos de punto final que accedan a sistemas o datos sensibles deben contar con autenticación segura, como contraseñas fuertes, autenticación biométrica o autenticación multifactor, para prevenir el acceso no autorizado.
b) La información clasificada como confidencial o sensible debe estar cifrada en dispositivos de punto final, tanto en reposo como en tránsito, para asegurar la protección de datos en caso de pérdida o robo del dispositivo.
c) Se deben instalar únicamente aplicaciones autorizadas y verificadas en los dispositivos de punto final para evitar el riesgo de software malicioso. Cualquier instalación adicional debe ser aprobada por el área de Seguridad de la Información.
d) Los dispositivos deben estar configurados para recibir y aplicar automáticamente actualizaciones de seguridad del sistema operativo y las aplicaciones, minimizando las vulnerabilidades y el riesgo de ataques.
e) Todos los dispositivos deben contar con software de protección contra malware y configurarse para realizar análisis periódicos de amenazas.
f) Solo se permitirá la conexión de dispositivos de punto final a redes internas de Datacenter Colombia S.A.S. si cumplen con las políticas de seguridad establecidas y están registrados en el inventario de activos autorizados.
g) Los dispositivos deben configurarse para bloquearse automáticamente después de un periodo corto de inactividad, y requerir autenticación para reanudar la sesión.
h) Los usuarios de dispositivos de punto final no deben almacenar información confidencial o crítica en dispositivos personales. Solo se permite almacenar esta información en dispositivos corporativos bajo los controles de seguridad establecidos.
i) Los datos críticos almacenados en dispositivos de punto final deben contar con un respaldo periódico, y los procesos de recuperación de información deben ser revisados regularmente.
j) Los usuarios deben reportar inmediatamente al área de Seguridad de la Información de Datacenter cualquier pérdida o robo de un dispositivo de punto final. El equipo de seguridad tomará las medidas necesarias para proteger la información contenida en el dispositivo y, cuando sea posible, desactivar o borrar la información de forma remota.

5.4.2. Política Gestión de vulnerabilidades técnicas (A.8.8)

Implementar un proceso continuo de identificación, evaluación y tratamiento de vulnerabilidades técnicas en los sistemas y redes de Datacenter Colombia S.A.S., con el fin de mitigar riesgos y proteger la integridad, disponibilidad y confidencialidad de la información.

5.4.2.1. Normas para la Política Gestión de vulnerabilidades técnicas (A.8.8)

a) La organización realizará evaluaciones periódicas de seguridad en todos sus sistemas y redes, incluyendo escaneos de vulnerabilidades, pruebas de penetración y revisiones de configuración, para identificar y priorizar vulnerabilidades técnicas. Las vulnerabilidades identificadas se clasificarán de acuerdo con su criticidad y el impacto potencial en los sistemas y operaciones, aplicando un enfoque de priorización para abordar primero aquellas con un mayor riesgo para la seguridad de la información.

b) El área de Infraestructura y Seguridad de la Información será responsable de implementar y mantener un inventario actualizado de todas las vulnerabilidades críticas que afecten a los activos de Datacenter Colombia S.A.S., estableciendo un plan de acción para su tratamiento o mitigación y definiendo los tiempos de remediación según el nivel de riesgo de cada vulnerabilidad. Los sistemas y aplicaciones deben configurarse para recibir y aplicar actualizaciones de seguridad y parches automáticamente cuando sea posible. En los casos en que no se puedan aplicar parches de manera inmediata, se definirán medidas compensatorias temporales hasta que la vulnerabilidad pueda ser mitigada o resuelta de forma completa.

c) La empresa garantizará que las fuentes confiables de inteligencia de amenazas y vulnerabilidades, como los reportes de fabricantes y alertas de seguridad, sean monitoreadas regularmente para detectar y abordar nuevas amenazas. Adicionalmente, las pruebas de seguridad y los escaneos de vulnerabilidades se realizarán tras cualquier cambio significativo en la infraestructura de TI, con el fin de asegurar que no se introduzcan nuevas vulnerabilidades en los sistemas.

d) El área de Infraestructura implementará procesos de auditoría y seguimiento para verificar la efectividad de las acciones de mitigación aplicadas y asegurar que las vulnerabilidades han sido gestionadas adecuadamente. Cualquier incidente derivado de una vulnerabilidad explotada será reportado y gestionado a través del protocolo de respuesta a incidentes, documentando las lecciones aprendidas y adoptando medidas correctivas para evitar futuros incidentes similares.

5.4.3. Política para la Eliminación de información (A.8.10)

Establecer los lineamientos para la eliminación segura y efectiva de la información en los sistemas y dispositivos de Datacenter Colombia S.A.S., asegurando que los datos sensibles

y confidenciales sean destruidos de forma irreversible, protegiendo así la confidencialidad y previniendo el acceso no autorizado.

5.4.3.1. Normas para la Política para la Eliminación de información (A.8.10)

a) La eliminación de información debe realizarse de manera segura, aplicando métodos que aseguren la destrucción completa e irreversible de los datos almacenados en medios digitales y físicos, incluyendo archivos, dispositivos de almacenamiento y documentos.

b) Los datos clasificados como confidenciales o sensibles serán eliminados mediante técnicas aprobadas, como el borrado seguro, el sobreescrito, el desmagnetizado o la destrucción física, según corresponda al tipo de medio y nivel de sensibilidad de la información.

c) El área de Infraestructura será responsable de implementar procedimientos de eliminación de información para cada tipo de dispositivo o medio de almacenamiento, incluyendo los sistemas de respaldo, dispositivos móviles y equipos obsoletos, asegurando que se apliquen controles de seguridad adecuados en cada proceso.

d) En el caso de proveedores o terceros que manejan información de Datacenter Colombia S.A.S., se incluirá en los contratos una cláusula de eliminación segura de datos al finalizar la relación contractual, estableciendo los métodos de destrucción que deberán aplicarse.

e) Toda eliminación de información debe ser registrada, especificando el tipo de datos eliminados, el método utilizado, la fecha y el personal responsable, y conservando estos registros según lo determine la política de retención de datos.

f) En caso de dispositivos reutilizables, se deben realizar procesos de borrado seguro y verificación antes de su reasignación o disposición, para asegurar que no contengan información residual que pueda ser recuperada.

5.4.4. Política Copias de Respaldo (A.8.13)

Garantizar que toda la configuración e información almacenada en los componentes de la plataforma tecnológica de Datacenter Colombia S.A.S, se encuentre debidamente respaldada con el fin de asegurar la disponibilidad de la información y dar continuidad a las operaciones de la organización.

5.4.4.1. Normas para la política de copias de respaldo

Para dar cumplimiento a la política, Datacenter Colombia S.A.S ha definido los siguientes compromisos para las áreas que la conforman.

a) De acuerdo con la evaluación de los activos las áreas deben garantizar copias de respaldo a aquellos catalogados como críticos y a los que ellos consideren alineados a las capacidades de almacenamiento.

b) Los archivos de respaldos deben tener un control de acceso lógico de acuerdo con la sensibilidad de sus datos, además de contar con protección física.

c) El área de Infraestructura debe asegurar la existencia de un procedimiento formal donde se especifiquen la periodicidad y procedimientos de generación, almacenamiento, retención y rotación de copias de respaldo.

d) Se debe definir un instructivo para la restauración de las copias de respaldo. Como también establecer un procedimiento de emergencia para dejar sin efecto los cambios efectuados y poder recuperar las versiones autorizadas anteriores.

e) Se deben realizar pruebas de restauración de las copias de respaldo de forma periódica para verificar la efectividad de estas.

f) Se deberá generar una copia de respaldo de toda la documentación del centro de cómputo, incluyendo el hardware, el software la cual deberá ser de acceso restringido y estar físicamente en un lugar distinto a los centros de procesamiento principales.

g) Los respaldos críticos deben mantenerse en ubicaciones fuera del sitio principal (offsite) para garantizar la recuperación en caso de desastres que afecten los centros de procesamiento principales. Asimismo, se deben definir y aplicar procedimientos de rotación segura para los medios de respaldo, garantizando su integridad y disponibilidad de acuerdo con las necesidades de recuperación de la organización.

5.4.5. Política de Uso de Criptografía (A.8.24)

Establecer los lineamientos para el uso adecuado de técnicas y controles criptográficos que protejan la confidencialidad, integridad y, cuando aplique, la autenticación y no repudio de la información procesada, almacenada o transmitida por Datacenter Colombia S.A.S., alineado con las mejores prácticas internacionales y la norma ISO/IEC 27001:2022.

5.4.5.1. Normas para la política de uso de Criptografía

Para dar cumplimiento a la política, Datacenter Colombia S.A.S ha definido los siguientes compromisos para las áreas que la conforman.

a) Protección de datos en tránsito y en reposo

El área de Infraestructura de Datacenter Colombia S.A.S. debe garantizar que todo sistema

de información o aplicativo que procese o transmita información confidencial o reservada, utilice mecanismos robustos de cifrado extremo a extremo. Esta norma aplica tanto para la transmisión como para la recepción de información desde o hacia terceros, incluidos clientes y proveedores.

b) Desarrollo seguro con controles criptográficos

El área de Gestión de Soluciones Tecnológicas deberá garantizar que todo producto desarrollado internamente que maneje información sensible incorpore algoritmos de cifrado adecuados a los niveles de riesgo identificados. Estos controles criptográficos deben cumplir con los estándares internacionales vigentes (ej. AES-256, TLS 1.3, etc.).

c) Seguridad en almacenamiento de información cifrada

Infraestructura tecnológica debe implementar controles que aseguren la disponibilidad y confiabilidad de los sistemas de almacenamiento donde se alojan datos cifrados, previniendo accesos no autorizados o pérdida de integridad.

d) Gestión de claves criptográficas

Se desarrollarán lineamientos específicos sobre el ciclo de vida de las claves criptográficas, que incluyan:

- Generación segura de claves
- Distribución y almacenamiento protegidos
- Recuperación en caso de pérdida o compromiso
- Reemplazo planificado o de emergencia
- Eliminación segura al final de su vida útil

e) Rotación periódica de claves y revisión de controles

El área de Infraestructura debe implementar un plan de rotación periódica de claves de cifrado, basado en el nivel de criticidad de la información y el riesgo asociado. Además, se deben realizar auditorías regulares para verificar el cumplimiento de los algoritmos, longitudes de clave, protocolos de cifrado y políticas asociadas, garantizando su alineación con los requisitos de seguridad vigentes y las normativas aplicables.

f) Servicios a clientes

En los servicios ofrecidos a clientes, las áreas de Gestión de Soluciones e Infraestructura deberán alinear sus prácticas a los requerimientos contractuales y normativos de cifrado que apliquen, garantizando una protección adecuada de los datos de terceros.

5.4.6. Política para la seguridad de redes y los servicios de red (A.8.20-A.8.22)

La gerencia de Infraestructura de Datacenter Colombia S.A.S, como responsable de las redes de datos y los servicios de red de la organización, debe asegurar la debida protección contra accesos no autorizados a través de mecanismos de control de acceso lógico.

5.4.6.1. Normas para la política de redes y los servicios de red

Para dar cumplimiento a la política, Datacenter Colombia S.A.S ha definido los siguientes compromisos para las áreas que la conforman.

a) Datacenter Colombia S.A.S deberá proveer la infraestructura de red y seguridad para garantizar los servicios de red y seguridad de la información que transita a través de esta.

b) La Gerencia de Infraestructura de Datacenter Colombia S.A.S debe contar con personal idóneo para la gestión, control y protección de los equipos de red a fin de proteger la información en los sistema y aplicaciones.

c) La Gerencia de Infraestructura de Datacenter Colombia S.A.S debe establecer responsabilidades y procedimientos para la administración de los equipos de red.

d) La Gerencia de Infraestructura de Datacenter Colombia S.A.S debe garantizar una segmentación de red a fin de independizar el tráfico entre las diferentes áreas de la compañía y sus clientes. El equipo administrador de infraestructura deberá está en un segmento de red separado al de los ambientes de pruebas, preproducción y producción.

e) La Gerencia de Infraestructura de Datacenter Colombia S.A.S deberá implementar controles de seguridad robustos para salvaguardad la confidencialidad e integridad de la información que pasa a través de la red pública o redes inalámbricas y que se conectan con los sistemas y aplicaciones de la compañía y de nuestros clientes.

f) La Gerencia de Infraestructura de Datacenter Colombia S.A.S deberá establecer las restricciones entre los diferentes segmentos de red y aplicaciones. De la misma forma garantizar la restricción al equipo de trabajo que presta el servicio de red garantizando una correcta segregación de roles para los admiradores y auditores de la infraestructura, solo los administradores de las plataformas deberán tener permisos totales sobre esta.

g) La Gerencia de Infraestructura de Datacenter Colombia S.A.S deberá garantizar la disponibilidad de la red como también determinar y regular el monitoreo de la infraestructura que soporta el servicio.

h) La Gerencia de Infraestructura de Datacenter Colombia S.A.S debe asegurar que las redes inalámbricas de la organización cuenten con mecanismos de autenticación que evite accesos no autorizados.

i) La Gerencia de Infraestructura de Datacenter Colombia S.A.S debe establecer controles para la identificación y autenticación de los usuarios provistos por terceras partes en las redes o recursos de red de Datacenter Colombia S.A.S, así como velar por la aceptación de las responsabilidades de los mencionados terceros. De igual forma, se debe formalizar la aceptación de las Políticas de Seguridad de la Información por parte de estos.

j) La Gerencia de Infraestructura de Datacenter Colombia S.A.S deberá garantizar la diagramación de las topologías de red, físico-lógico, para las conexiones internas, contra terceros-aliados, centros de datos y todas aquellas que ayuden a la compresión de la interconectada y el servicio de networking. De igual manera deberá consolidar el inventario de redes y vlan y configuración de protocolos de enrutamiento para cada uno de los equipos que lo administren.

k) El coordinador de seguridad de la información y ciberseguridad debe autorizar la creación o modificación de las cuentas de acceso a las redes o recursos de red de Datacenter Colombia S.A.S por parte de terceros.

l) El coordinador de seguridad de la información y ciberseguridad debe verificar periódicamente los controles de acceso para los usuarios provistos por terceras partes, con el fin de revisar que dichos usuarios tengan acceso permitido únicamente a aquellos recursos de red y servicios de la plataforma Tecnológica para los que fueron autorizados

m) Todo equipo que se conecte a la red de datos de Datacenter Colombia S.A.S, deberá acatar y aplicar la política de seguridad de la información y cada uno de sus lineamientos.

n) Se deben garantizar las actividades de supervisión como un control para el monitoreo proactivo dentro de los sistemas de TI, redes, herramientas y aplicaciones; y que permitan el reconocimiento de actividades inusuales dentro de los sistemas de información para la activación de respuestas inmediatas.

o) Para asegurar un nivel adecuado de protección en el acceso a redes y servicios críticos, se debe implementar **autenticación multifactor (MFA)** en todos los accesos remotos y para usuarios con permisos elevados o administrativos. Este control adicional permite verificar la identidad del usuario mediante al menos dos factores de autenticación distintos, tales como una contraseña y un token de seguridad, una clave de un solo uso (OTP) enviada a un dispositivo móvil autorizado, o una autenticación biométrica. La autenticación multifactor debe ser configurada y revisada periódicamente para asegurar su eficacia y cumplimiento con las políticas de seguridad de Datacenter Colombia S.A.S.

5.4.7. Política de Desarrollo Seguro (A.8.25, A.8.26, A.8.27, A.8.28, A.8.29, A.8.30, A.8.31)

Asegurar que el desarrollo de software, ya sea interno o contratado externamente, cumpla con los requerimientos funcionales y de seguridad de la información, y que se implementen buenas prácticas de desarrollo seguro, pruebas, gestión de cambios y separación adecuada de entornos, alineados con la norma ISO/IEC 27002:2022.

5.4.7.1. Normas para la política de desarrollo seguro

Para dar cumplimiento a la política, Datacenter Colombia S.A.S ha definido los siguientes compromisos para las áreas que la conforman.

a) Seguridad en el ciclo de vida del desarrollo (A.8.25)

Todo sistema de información que apoye las operaciones propias o de los clientes debe ser desarrollado bajo una metodología formal que contemple desde su concepción los principios de desarrollo seguro. Esta metodología debe incluir lineamientos, buenas prácticas, plantillas, artefactos de control y actividades para mitigar riesgos y asegurar la calidad.

b) Requisitos de seguridad en las aplicaciones (A.8.26)

Los requisitos de seguridad deben estar definidos desde el inicio del proyecto, documentados y aprobados. Gestión de Soluciones debe verificar que estos se implementen correctamente y sean parte del criterio de aceptación previo a producción.

c) Principios de arquitectura segura (A.8.27)

La arquitectura de software debe incluir principios de mínimo privilegio, defensa en profundidad, separación de funciones y control de superficie de exposición, asegurando la confidencialidad e integridad de los datos y la resiliencia del sistema.

d) Codificación segura (A.8.28)

Se deben aplicar prácticas de codificación segura reconocidas (OWASP, SANS, etc.), así como revisiones sistemáticas de código fuente. Estas revisiones deben identificar y mitigar vulnerabilidades antes de que el código se promueva a producción.

e) Pruebas de seguridad y aceptación (A.8.29)

Gestión de Soluciones debe realizar pruebas funcionales y de seguridad en cada desarrollo, incluyendo pruebas automatizadas, revisión de vulnerabilidades y documentación de resultados. Toda implementación debe estar respaldada por evidencia de pruebas y validación formal.

f) Desarrollo subcontratado (A.8.30)

Cuando se subcontraten servicios de desarrollo, estos deben ajustarse a los mismos lineamientos de seguridad exigidos internamente. Se debe establecer seguimiento activo a su cumplimiento y cláusulas contractuales de confidencialidad, seguridad, propiedad y entrega del código.

g) Separación de entornos (A.8.31)

La Gerencia General debe garantizar la existencia de entornos separados de desarrollo, prueba y producción. Toda migración entre ambientes debe estar documentada, aprobada por el administrador de configuración y ejecutada bajo procedimientos formales.

✦ Controles complementarios definidos por la organización

h) Se debe contar con sistemas de control de versiones para gestionar adecuadamente los cambios en el código fuente de los sistemas de información.

i) Los cambios en los sistemas deben pasar por procedimientos formales de control de cambios, con aprobación previa, trazabilidad y documentación.

j) Los datos de prueba deben ser seleccionados, protegidos y controlados. Cuando se requiera el uso de datos reales o similares a los productivos, se debe contar con autorización formal del cliente.

k) Se deben implementar tecnologías de enmascaramiento de datos que limiten la exposición de información sensible en entornos no productivos.

l) Se debe monitorear continuamente el estado de seguridad del software en uso, aplicando parches o actualizaciones ante vulnerabilidades detectadas en el menor tiempo posible.

m) Gestión de Soluciones e Infraestructura deben implementar mecanismos criptográficos dentro del desarrollo cuando sea necesario, para asegurar la integridad de la información y mitigar riesgos de repudio.

n) Debe establecerse un plan de revisiones periódicas a los entornos y componentes del software, con foco en vulnerabilidades y cumplimiento de los lineamientos de esta política.

6. ANEXOS

- N. A