CORPORACIÓN GILBERTO ECHEVERRI MEJÍA

POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Versión 3.1

2024

+(57) (4) 540 90 40 / 01 8000 413522
Edificio Estación Medellín - Ferrocarril de Antioquia
Carrera 52 nº 43 - 31, Oficinas 204 y 205, Medellín, Antioquia
www.corporaciongilbertoecheverri.gov.co

Contenido

1. INTRODUCCIÓN 5
2. OBJETIVO 5
3. BASE LEGAL Y ÁMBITO DE APLICACIÓN 6
4. ALCANCE 7
5. GLOSARIO 7
6. CLASIFICACIÓN DE LA INFORMACIÓN 12
7. MEDIDAS DE SEGURIDAD 12
   7.1. Medidas de seguridad comunes 13
      7.1.1. Gestión de documentos y soportes 13
      7.1.2. Control de acceso 13
      7.1.3. Ejecución del tratamiento fuera de las instalaciones 14
      7.1.4. Bases de datos temporales, copias y reproducciones 14
      7.1.5. Responsable de seguridad 14
      7.1.6. Auditorías 14
   7.2. Medidas de seguridad para bases de datos no automatizadas 15
      7.2.1 Archivo de documentos: 15
      7.2.2. Acceso a los documentos 16
   7.3. Medidas de seguridad para bases de datos automatizadas 16
      7.3.1. Identificación y autenticación. 16
      7.3.2. Entrada y salida de documentos o soportes 17
      7.3.3. Control de acceso físico 17
      7.3.4. Copias de respaldo y recuperación de datos 18
      7.3.5. Registro de acceso 18
      7.3.6. Redes de comunicaciones 19
      7.3.7. Consolidado medidas de seguridad 19
8. POLÍTICAS DE LA ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN 21
   8.1 POLÍTICA PARA USO DE DISPOSITIVOS MÓVILES 22
   8.2 Normas para uso de dispositivos móviles 22
   8.3. POLÍTICA PARA USO DE CONEXIONES REMOTAS 22
      8.3.1. Normas para uso de conexiones remotas 22

9. POLÍTICAS DE GESTIÓN DE ACTIVOS DE INFORMACIÓN 24
9.1. POLÍTICA DE RESPONSABILIDAD POR LOS ACTIVOS 24
9.1.1. Normas de responsabilidad por los activos 24
9.2. POLÍTICA DE CLASIFICACIÓN Y MANEJO DE LA INFORMACIÓN 25
9.2.1. Normas para la clasificación y manejo de la información 25
9.3. POLÍTICA PARA USO DE TOKENS DE SEGURIDAD 26
9.3.1. Normas para uso de tokens de seguridad 26
9.4. POLÍTICA PARA USO DE MULTIFACTOR 27
9.4.1. Normas para uso de tokens de MFA 27
9.5. POLÍTICA DE USO DE PERIFÉRICOS Y MEDIOS DE ALMACENAMIENTO 27
9.5.1. Normas uso de periféricos y medios de almacenamiento 27
10. POLÍTICAS DE CONTROL DE ACCESO 29
10.1. POLÍTICA DE ACCESO A REDES Y RECURSOS DE RED 29
10.1.1. Normas de acceso a redes y recursos de red 29
10.2. POLÍTICA DE CONTROL DE ACCESO A SISTEMAS Y APLICATIVOS 29
10.2.1. Normas de control de acceso a sistemas y aplicativos 30
11. POLÍTICAS DE SEGURIDAD FÍSICA 31
11.1. POLÍTICA DE ÁREAS SEGURAS 31
11.1.1. Normas de áreas seguras 31
11.2. POLÍTICA DE SEGURIDAD PARA LOS EQUIPOS INSTITUCIONALES 32
11.2.1. Normas de seguridad para los equipos institucionales 32
12. POLÍTICAS DE SEGURIDAD EN LAS OPERACIONES 33
12.1. POLÍTICA DE ASIGNACIÓN DE RESPONSABILIDADES OPERATIVAS 33
12.1.1. Normas de asignación de responsabilidades operativas 34
12.2. POLÍTICA DE PROTECCIÓN FRENTE A SOFTWARE MALICIOSO 34
12.2.1. Normas de protección frente a software malicioso 34
12.3. POLÍTICA DE COPIAS DE RESPALDO DE LA INFORMACIÓN 35
12.3.1. Normas de copias de respaldo de la información 35
12.4. POLÍTICA DE CONTROL AL SOFTWARE OPERATIVO 36
13. POLÍTICAS DE SEGURIDAD EN LAS COMUNICACIONES 37
13.1. POLÍTICA DE GESTIÓN Y ASEGURAMIENTO DE LAS REDES DE DATOS 37

13.1.1. Normas de gestión y aseguramiento de las redes de datos 38
13.2. POLÍTICA DE USO DEL CORREO ELECTRÓNICO 38
13.2.1. Normas de uso del correo electrónico 38
13.3. POLÍTICA DE USO ADECUADO DE INTERNET 39
13.3.1. Normas de uso adecuado de internet 39
14. POLÍTICAS DE ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN 40
14.1. POLÍTICA PARA EL ESTABLECIMIENTO DE REQUISITOS DE SEGURIDAD 40
14.1.1. Normas para el establecimiento de requisitos de seguridad 40
14.2. POLÍTICA DE DESARROLLO SEGURO, REALIZACIÓN DE PRUEBAS Y SOPORTE DE LOS SISTEMAS 41
14.2.1. Normas de desarrollo seguro, realización de pruebas y soporte de los sistemas .. 41
15. PROCEDIMIENTO DE NOTIFICACIÓN, GESTIÓN Y RESPUESTA ANTE INCIDENCIAS 43
16. POLÍTICAS DE CUMPLIMIENTO 44
16.1. FUNCIONES Y OBLIGACIONES DEL PERSONAL 44
17. BASES DE DATOS Y SISTEMAS DE INFORMACIÓN 46
18. MEDIDAS PARA EL TRANSPORTE, DESTRUCCIÓN Y REUTILIZACIÓN DE DOCUMENTOS Y SOPORTES 47
19. CUMPLIMIENTO 47
20. DISPOSICIÓN FINAL 47

1. Introducción

Las políticas de seguridad de información tienen por objeto establecer las medidas de índole técnica y de organización, necesarias para garantizar la seguridad de las tecnologías de información (equipos de cómputo, sistemas de información, redes (Voz y Datos) y personas que interactúan haciendo uso de los servicios asociados a ellos.

En una organización la gestión de seguridad puede tornarse compleja y difícil de realizar, esto no solo por razones técnicas, sino también por razones organizativas que comprenden la coordinación de todos los esfuerzos encaminados al aseguramiento de un entorno informático institucional. Lo anterior es posible mediante la administración de recurso humano y tecnológico, donde se requiere un adecuado control que integre los esfuerzos y conocimiento humano con las técnicas depuradas de mecanismos automatizados para que no se convierta en un ambiente desordenado y confuso; se hace necesario entonces, emplear mecanismos reguladores de las funciones y actividades desarrolladas por cada una de las personas vinculadas con La Corporación Gilberto Echeverri Mejía.

Este documento describe las políticas y normas de seguridad de la información definidas por La Corporación Gilberto Echeverri Mejía. Para la elaboración de este, se toman como base las leyes y demás regulaciones aplicables, la estrategia de gobierno en línea de Colombia, la norma ISO 27001:2022/Chor 2:2015 y las recomendaciones del estándar ISO 27002:2022/Cor 2:2015

Las políticas incluidas en este documento se constituyen como parte fundamental del plan de seguridad de la información de La Corporación Gilberto Echeverri Mejía y se convierten en la base para la implantación de los controles, procedimientos y estándares definidos.

La seguridad de la información es una prioridad para la Corporación y por tanto es responsabilidad de todos velar por que no se realicen actividades que contradigan la esencia y el espíritu de cada una de estas políticas.

2. Objetivo

La presente política tiene como propósito dar a conocer cuáles son los requisitos básicos de seguridad de la información para establecer controles efectivos sobre todas las actividades que se desarrollan en La Corporación Gilberto Echeverri Mejía, con el fin de que todos los involucrados en la operación o que prestan servicios garanticen el buen uso de los sistemas, herramientas, recursos e información a la que tienen acceso.

Así como, presentar los lineamientos de control para todos los empleados, terceros y entes que tengan acceso a la información de La Corporación Gilberto Echeverri Mejía, para garantizar su seguridad a través de los principios de confidencialidad, integridad y disponibilidad, estableciendo las políticas de seguridad que se aplican a todos los sistemas de información, la red, así como, a todas las instalaciones en las que procesan, almacenan, o transmiten información.

Enmarcado en las buenas prácticas y disposiciones legales como son los estándares internacionales de seguridad (ISO 27001:2022/Cor 2:2015), la Ley 1581 de 2012 y los aspectos establecidos por la Superintendencia de Industria y Comercio mediante la Guía de para la Implementación del Principio de Responsabilidad Demostrada (Accountability).

Lo anterior, teniendo en cuenta que la organización se enfrenta a amenazas relativas a la seguridad, en especial relacionados con el fraude asistido por computadores, como también a las acciones de personas, los cuales cada vez se han vuelto más comunes, ambiciosos y sofisticados. A continuación, se describen los principales objetivos específicos:

- ✓ Minimizar los incidentes de seguridad de la información presentados en La Corporación Gilberto Echeverri Mejía.
- ✓ Mantener los sistemas y los recursos tecnológicos adecuados, que fortalezcan la seguridad de la información.
- ✓ Establecer los fundamentos para el desarrollo y la implantación de un Modelo de Seguridad de la información.
- ✓ Definir la conducta a seguir en lo relacionado con el acceso, uso, manejo y administración de los recursos de información.
- ✓ Establecer y comunicar la responsabilidad en el uso de los activos de información, que soportan los procesos y sistemas del negocio.

3. Base legal y ámbito de aplicación

La Corporación Gilberto Echeverri Mejía, con objeto de garantizar el adecuado cumplimiento de la Ley Estatutaria 1581 de 2.012 de Protección de Datos (LEPD) y del Decreto 1074 de 2015, adopta estas políticas de seguridad de la información donde se recogen las medidas técnicas, humanas y administrativas necesarias para otorgar seguridad a los registros con el fin de impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento, de acuerdo con el principio de seguridad recogido en el artículo 4 literal g) de la LEPD.

Para todos los efectos del presente documento, entiéndase la abreviatura LEPD como Ley estatutaria de protección de datos personales 1581 de 2.012.

Domicilio: Edificio estación Medellín – Ferrocarril de Antioquia, Carrera 52 N° 43 – 31 Oficina 204 – 205, Medellín- Antioquia.

Teléfono: 6045409040 o 018000413522

Correo electrónico: contacto@corporaciongilbertoecheverri.gov.co

Página web: www.corporaciongilbertoecheverri.gov.co

Las disposiciones de este documento se aplican a las bases de datos objeto de responsabilidad de La Corporación Gilberto Echeverri Mejía, así como a los sistemas de información, soportes y equipos empleados en el tratamiento de los datos, que deban ser protegidos de acuerdo con la normativa vigente, a las personas que participan en el tratamiento y a los lugares donde se ubican dichas bases de datos.

4. Alcance

Las políticas de seguridad de la información cubren todos los aspectos administrativos y de control que deben ser cumplidos por los directivos, vinculados y terceros que laboren o tengan relación con la Corporación, para conseguir un adecuado nivel de protección de las características de seguridad y calidad de la información relacionada.

5. Glosario

- ✓ **Acceso autorizado:** Autorización concedida a un usuario para el uso de determinados recursos. En dispositivos automatizados es el resultado de una autentificación correcta, generalmente mediante el ingreso de usuario y contraseña.
- ✓ **Activo de información:** Cualquier componente (humano, tecnológico, software, documental o de infraestructura) que soporta uno o más procesos de negocios del instituto y, en consecuencia, debe ser protegido.
- ✓ **Activo:** Es el conjunto de los bienes y derechos tangibles e intangibles de propiedad de una persona natural o jurídica que por lo general son generadores de renta o fuente de beneficios, en el ambiente informático llámese activo a los bienes de información y procesamiento, que posee la Corporación. Recurso del sistema de información o relacionado con éste, necesario para que la organización funcione correctamente y alcance los objetivos propuestos.
- ✓ **Acuerdo de Confidencialidad:** Es un documento en el que los vinculados y contratistas manifiestan su voluntad de mantener la confidencialidad de la información de la Corporación, comprometiéndose a no divulgar, usar o explotar la información confidencial a la que tengan acceso en virtud de la labor que desarrollan dentro de la misma.
- ✓ **Amenaza**: Es un evento que puede desencadenar un incidente en la organización, produciendo daños materiales o pérdidas inmateriales en sus activos.
- ✓ **Archivo log:** Ficheros de registro o bitácoras de sistemas, en los que se recoge o anota los pasos que dan (lo que hace un usuario, como transcurre una conexión, horarios de conexión, terminales o Ips involucradas en el proceso, etc.)
- ✓ **Ataque:** Evento, exitoso o no, que atenta sobre el buen funcionamiento del sistema.
- ✓ **Autenticación:** Es el procedimiento de comprobación de la identidad de un usuario o recurso tecnológico al tratar de acceder a un recurso de procesamiento o sistema de información.
- ✓ **Autorización:** Consentimiento previo, expreso e informado del Titular para llevar a cabo el Tratamiento de datos personales.
- ✓ **Base de Datos:** Conjunto organizado de datos personales que sea objeto de Tratamiento.

- ✓ **Centro de cómputo**: Es una zona específica para el almacenamiento de múltiples computadores para un fin específico, los cuales se encuentran conectados entre sí a través de una red de datos.
- ✓ **Cifrado**: Es la transformación de los datos mediante el uso de la criptografía para producir datos ininteligibles (cifrados) y asegurar su confidencialidad. El cifrado es una técnica muy útil para prevenir la fuga de información, el monitoreo no autorizado e incluso el acceso no autorizado a los repositorios de información.
- ✓ **Confidencialidad**: Es la garantía de que la información no está disponible o divulgada a personas, entidades o procesos no autorizados.
- ✓ **CONPES 3854 Ciberseguridad del 11 de abril de 2016**: Este documento busca generar lineamientos de política en ciberseguridad y ciberdefensa orientados a desarrollar una estrategia nacional que contrarreste el incremento de las amenazas informáticas que afectan significativamente al país. Adicionalmente, recoge los antecedentes nacionales e internacionales, así como la normatividad del país en torno al tema.
- ✓ **Contraseña**: Seña secreta que permite el acceso a dispositivos, información o bases de datos antes inaccesibles. Se utiliza en la autentificación de usuarios que permite el acceso autorizado.
- ✓ **Control de acceso**: Mecanismo que permite acceder a dispositivos, información o bases de datos mediante la autentificación.
- ✓ **Control**: Es toda actividad o proceso encaminado a mitigar o evitar un riesgo. Incluye políticas, procedimientos, guías, estructuras organizacionales y buenas prácticas, que pueden ser de carácter administrativo, tecnológico, físico o legal.
- ✓ **Copia de respaldo**: Copia de los datos de una base de datos en un soporte que permita su recuperación.
- ✓ **Corriente eléctrica regulada**: Se utiliza para regular o mantener el voltaje de la red eléctrica para que no afecte el funcionamiento de los recursos TIC de la corporación.
- ✓ **Criptografía**: Es la disciplina que agrupa a los principios, medios y métodos para la transformación de datos con el fin de ocultar el contenido de su información, establecer su autenticidad, prevenir su modificación no detectada, prevenir su repudio, y/o prevenir su uso no autorizado.
- ✓ **Cuenta**: Mecanismo de identificación de un usuario, llámese de otra manera, al método de acreditación o autenticación del usuario mediante procesos lógicos dentro de un sistema informático.
- ✓ **Dato personal**: Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables.
- ✓ **Dato público**: Es el dato que no sea semiprivado, privado o sensible. Son considerados datos públicos, entre otros, los datos relativos al estado civil de las personas, a su profesión u oficio y a su calidad de comerciante o de servidor público. Por su naturaleza, los datos públicos pueden estar contenidos, entre otros, en registros públicos, documentos públicos, gacetas y boletines oficiales y sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva.
- ✓ **Datos sensibles**: Se entiende por datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido

político o que garanticen los derechos y garantías de partidos políticos de oposición, así como los datos relativos a la salud, a la vida sexual, y los datos biométricos.

- ✓ **Decreto 1078 de 2015**. Decreto por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones
- ✓ **Derechos de autor**: Es el conjunto de normas que protegen al autor como creador de una obra en el campo literario y artístico, entendida ésta, como toda expresión humana producto del ingenio y del talento que se ve materializada de cualquier forma perceptible por los sentidos y de manera original.
- ✓ **Encargado del Tratamiento**: Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el Tratamiento de datos personales por cuenta del responsable del Tratamiento.
- ✓ **Equipo de cómputo**: Dispositivo electrónico capaz de recibir un conjunto de instrucciones y ejecutarlas realizando cálculos sobre los datos numéricos, o bien compilando y correlacionando otros tipos de información.
- ✓ **Identificación**: Proceso de reconocimiento de la identidad de los usuarios.
- ✓ IEC: (Comisión Electrotécnica Internacional) Junto a la ISO, desarrolla estándares que son aceptados a nivel internacional.
- ✓ **Impacto**: Consecuencia de la materialización de una amenaza.
- ✓ **Incidente de seguridad**: Es un evento adverso, confirmado o bajo sospecha, que haya vulnerado la seguridad de la información o que intente vulnerarla, sin importar la información afectada, la plataforma tecnológica, la frecuencia, las consecuencias, el número de veces ocurrido o el origen (interno o externo).
- ✓ **Incidente**: Cualquier evento que no forma parte del desarrollo habitual del servicio y que causa, o puede causar una interrupción del mismo o reducción de la calidad del servicio.
- ✓ **Información sensible**: Es la tipificación que recibe la información que no se considera de acceso público como por ejemplo ciertos datos personales y bancarios, contraseñas de correo electrónico e incluso el domicilio en algunos casos. Aunque lo más común es usar este término para designar datos privados relacionados con Internet o la informática, sobre todo contraseñas, tanto de correo electrónico, conexión a Internet, IP privada, sesiones del PC, etc.
- ✓ **Inventario de activos de información**: Es una lista ordenada y documentada de los activos de información pertenecientes a la corporación.
- ✓ **ISO/IEC 27001:2022/Cor 2:2015**: Information technology – Security techniques - Information security management systems – Requirements. Esta norma es certificable y especifica los requisitos necesarios para establecer, implantar, mantener y mejorar un Sistema de Gestión de la Seguridad de la Información según el famoso “Círculo de Deming”: PDCA - acrónimo de Plan, Do, Check, Act (Planificar, Hacer, Verificar, Actuar). Es consistente con las mejores prácticas descritas en ISO/IEC 17799 y tiene su origen en la norma británica British Standard BS 7799-2 publicada por primera vez en 1998 y elaborada con el propósito de poder certificar los Sistemas de Gestión de la Seguridad de la Información implantados en las organizaciones y por medio de un proceso formal de auditoría realizado por un tercero.
- ✓ **ISO/IEC 27002:2022/Cor 2:2015**: Information technology – Security techniques. Code of practice for information security management. También conocida como ISO/IEC 17799, proporciona

recomendaciones de las mejores prácticas en la gestión de la seguridad de la información a todos los interesados y responsables en iniciar, implantar o mantener sistemas de gestión de la seguridad de la información. La seguridad de la información se define en el estándar como "la preservación de la confidencialidad (asegurando que sólo quienes estén autorizados pueden acceder a la información), integridad (asegurando que la información y sus métodos de proceso son exactos y completos) y disponibilidad (asegurando que los usuarios autorizados tienen acceso a la información y a sus activos asociados cuando lo requieran)".

- ✓ **ISO**: (Organización Internacional de Estándares) Corporación mundialmente reconocida y acreditada para normar en temas de estándares en una diversidad de áreas, aceptadas y legalmente reconocidas.
- ✓ **Ley 23 de 1982 Derecho de Autor**: De conformidad con el artículo 9, la protección que esta otorga tiene como título originario la creación intelectual, sin que se requiera registro alguno. Las formalidades que en ella se establecen son para la mayor seguridad Jurídica de los titulares de los derechos que se protegen.
- ✓ **Licencia de software**: Es un contrato en donde se especifican todas las normas y cláusulas que rigen el uso de un determinado producto de software, teniendo en cuenta aspectos como: alcances de uso, instalación, reproducción y copia de estos productos.
- ✓ **Medio removible**: Es cualquier componente extraíble de hardware que sea usado para el almacenamiento de información; los medios removibles incluyen cintas, discos duros removibles, CDs, DVDs y unidades de almacenamiento USB, entre otras.
- ✓ **MFA:** La autenticación multifactor (multi factor authentication o MFA) es una tecnología de seguridad que requiere múltiples métodos de autenticación de categorías independientes de credenciales para verificar la identidad de un usuario para un inicio de sesión u otra transacción.
- ✓ **Perfil de usuario**: Grupo de usuarios a los que se da acceso.
- ✓ **Perfiles de usuario**: Son grupos que concentran varios usuarios con similares necesidades de información y autorizaciones idénticas sobre los recursos tecnológicos o los sistemas de información a los cuales se les concede acceso de acuerdo con las funciones realizadas. Las modificaciones sobre un perfil de usuario afectan a todos los usuarios cobijados dentro de él.
- ✓ **Política de seguridad**: Es el documento de normas y lineamientos de seguridad de la información que define la corporación para evitar que surja vulnerabilidades que puede afectar el negocio.
- ✓ **Propiedad intelectual**: Hace referencia a toda creación del intelecto humano. Las obras literarias, artísticas y científicas; las interpretaciones de los artistas intérpretes y las ejecuciones de los artistas ejecutantes, los fonogramas y las emisiones de radiodifusión; las invenciones en todos los campos de la actividad humana; los descubrimientos científicos; los dibujos y modelos industriales; las marcas de fábrica, de comercio y de servicio, así como los nombres y denominaciones de origen; y todos los demás derechos relativos a la actividad intelectual en los terrenos industrial, científico, literario y artístico. Los derechos de Propiedad Intelectual se dividen en dos ramas que protegen los intereses de los creadores al ofrecerles ventajas en relación con sus creaciones: La propiedad Industrial y La Protección a Derechos de Autor
- ✓ **Proveedores**: Negocio o empresa que ofrece servicios a otras empresas o particulares. Ejemplos de estos servicios incluyen: acceso a internet, operador de telefonía móvil, etc.

- ✓ **Recurso protegido**: Cualquier componente del sistema de información, como bases de datos, programas, soportes o equipos, empleados para el almacenamiento y tratamiento de datos personales.
- ✓ **Recursos tecnológicos**: Son aquellos componentes de hardware y software tales como: servidores (de aplicaciones y de servicios de red), estaciones de trabajo, equipos portátiles, dispositivos de comunicaciones y de seguridad, servicios de red de datos y bases de datos, entre otros, los cuales tienen como finalidad apoyar las tareas administrativas necesarias para el buen funcionamiento y la optimización del trabajo al interior de La Corporación Gilberto Echeverri Mejía.
- ✓ **Requerimiento**: Necesidad de un servicio TIC que el usuario solicita a través del mecanismo definido por la organización en los procedimientos normalizados.
- ✓ **Responsable de seguridad**: Una o varias personas designadas por el responsable del tratamiento para el control y la coordinación de las medidas de seguridad.
- ✓ **Responsable del Tratamiento**: Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre la base de datos y/o el Tratamiento de los datos.
- ✓ **SGSI**: Sistema de Gestión de Seguridad de la Información.
- ✓ **Sistema de información**: Es un conjunto organizado de datos, operaciones y transacciones que interactúan para el almacenamiento y procesamiento de la información que, a su vez, requiere la interacción de uno o más activos de información para efectuar sus tareas. Un sistema de información es todo componente de software ya sea de origen interno, es decir desarrollado por La Corporación Gilberto Echeverri Mejía o de origen externo ya sea adquirido por la entidad como un producto estándar de mercado o desarrollado para las necesidades de ésta.
- ✓ **Software malicioso**: Es una variedad de software o programas de códigos hostiles e intrusivos que tienen como objeto infiltrarse o dañar los recursos tecnológicos, sistemas operativos, redes de datos o sistemas de información.
- ✓ **Soporte Técnico**: Personal designado o encargado de velar por el correcto funcionamiento de las estaciones de trabajo, servidores, o equipo de oficina dentro de la Corporación.
- ✓ **Soporte**: Material en cuya superficie se registra información o sobre el cual se pueden guardar o recuperar datos, como el papel, la cinta de video, el CD, el DVD, el disco duro, etc.
- ✓ **TIC**: Las Tecnologías de la Información y la Comunicación, también conocidas como TIC, son el conjunto de tecnologías desarrolladas para gestionar información y enviarla de un lugar a otro. Abarcan un abanico de soluciones muy amplio. Incluyen las tecnologías para almacenar información y recuperarla después, enviar y recibir información de un sitio a otro, o procesar información para poder calcular resultados y elaborar informes.
- ✓ **Titular**: Persona natural cuyos datos personales sean objeto de Tratamiento.
- ✓ **Transferencia**: La transferencia de datos tiene lugar cuando el responsable y/o Encargado del Tratamiento de datos personales, ubicado en Colombia, envía la información o los datos personales a un receptor, que a su vez es Responsable del Tratamiento y se encuentra dentro o fuera del país.
- ✓ **Tratamiento**: Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión.
- ✓ **Usuario**: Defínase a cualquier persona jurídica o natural, que utilice los servicios informáticos de la red institucional y tenga una especie de vinculación con la Corporación.

- ✓ **Usuario**: Sujeto autorizado para acceder a los datos o recursos, o proceso que accede a los datos o recursos sin identificación de un sujeto.
- ✓ **Vulnerabilidades**: son las debilidades, hoyos de seguridad o flaquezas inherentes a los activos de información que pueden ser explotadas por factores externos y no controlables por la corporación (amenazas), las cuales se constituyen en fuentes de riesgo.

6. Clasificación de la información

- ✓ **Publica**: Información que puede ser conocida por todos los miembros enmarcados en el alcance y el público en general. Son considerados datos públicos, entre otros, los datos relativos al estado civil de las personas, a su profesión u oficio y a su calidad de comerciante o de servidor público. Por su naturaleza, los datos públicos pueden estar contenidos, entre otros, en registros públicos, documentos públicos, gacetas y boletines oficiales y sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva.
- ✓ **Interna**: Información que requiere la entidad para la ejecución de su objeto social y puede ser accedida por el personal de La Corporación Gilberto Echeverri Mejía para el cumplimiento de las actividades diarias, alineadas a las funciones y responsabilidades del cargo o de la prestación de servicios de terceros y su conocimiento es de carácter general. Su disponibilidad a terceros es únicamente mediante un acuerdo contractual que exprese la necesidad de su uso para efectos del cumplimiento de este y para lo cual se debe comprometer a no divulgarla.
- ✓ **Confidencial**: Información propia que solo está disponible para los colaboradores de La Corporación Gilberto Echeverri Mejía en función de sus labores y que no puede ser conocida por otros empleados o terceros sin autorización del responsable de administrar la base de datos. También se refiere a un dato personal que por su naturaleza íntima o reservada solo interesa a su titular y para su tratamiento requiere de su autorización previa, informada y expresa. Bases de datos que contengan datos como Números telefónicos y correos electrónicos personales; datos laborales, sobre infracciones administrativas o penales, administrados por administraciones tributarias, entidades financieras y entidades gestoras y servicios comunes de la Seguridad Social, bases de datos sobre solvencia patrimonial o de crédito, bases de datos con información suficiente para evaluar la personalidad del titular, bases de datos de los responsables de operadores que presten servicios de comunicación electrónica.
- ✓ **Reservada**: Información que solo debe tener acceso personal específico y la revelación al público puede causar daño a la reputación, marca o estrategias de organización. También, hace referencia a aquellos datos privados que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición así como los datos relativos a la salud, a la vida sexual y los datos biométricos

7. Medidas de seguridad

Las bases de datos son accesibles únicamente por las personas designadas por La Corporación Gilberto Echeverri Mejía, y referidas en el "Anexo 2. Roles y Responsabilidades" de este documento.

Los responsables de seguridad de La Corporación Gilberto Echeverri Mejía, señalados en el "Anexo 2. Roles y Responsabilidades", se encargan de gestionar los permisos de acceso a los usuarios, el procedimiento de asignación y distribución que garantiza la confidencialidad, integridad y almacenamiento de las contraseñas, durante su vigencia, así como la periodicidad con la que se cambian.

A continuación, se enumeran y detallan las medidas de seguridad implementadas por La Corporación Gilberto Echeverri Mejía.

7.1. Medidas de seguridad comunes
7.1.1. Gestión de documentos y soportes

Los encargados de vigilar y controlar que personas no autorizadas no puedan acceder a los documentos y soportes con datos personales son los usuarios autorizados para acceder a estos. Los usuarios autorizados están referidos en el numeral "Anexo 2. Roles y Responsabilidades" sobre bases de datos y sistemas de información del presente en esta política.

Los documentos y soportes deben clasificar los datos según el tipo de información que contienen, ser inventariados y ser accesibles solo por el personal autorizado, salvo que las características de estos hagan imposible la identificación referida, en cuyo caso se dejará constancia motivada en el registro de entrada y de salida de documentos y en esta política.

La identificación de los documentos y soportes de contengan datos personales sensibles debe realizarse utilizando sistemas de etiquetado comprensibles y con significado que permita a los usuarios autorizados identificar su contenido y que dificulten la identificación para el resto de las personas.

La salida de documentos y soportes que contengan datos personales fuera de los lugares que están bajo el control del responsable del tratamiento debe ser autorizada por este último. Este precepto también es aplicable a los documentos o soportes anexados y enviados por correo electrónico.

7.1.2. Control de acceso

El personal de La Corporación Gilberto Echeverri Mejía solamente debe acceder a aquellos datos y recursos necesarios para el desarrollo de sus funciones y sobre los cuales se encuentren autorizados por el responsable del tratamiento en esta política.

La modificación sobre algún dato o información, así como la concesión, alteración, inclusión o anulación de los accesos autorizados y de los usuarios recogidos en la lista actualizada mencionada en el párrafo anterior, corresponde de manera exclusiva al personal autorizado.

Cualquier persona ajena a La Corporación Gilberto Echeverri Mejía, que, de forma autorizada y legal, tenga acceso a los recursos protegidos, estará sometido a las mismas condiciones y tendrá las mismas obligaciones de seguridad que el personal propio.

7.1.3. Ejecución del tratamiento fuera de las instalaciones

El almacenamiento de datos personales del responsable del tratamiento o encargado del tratamiento en dispositivos portátiles y su tratamiento fuera de los lugares requiere una autorización previa por parte de La Corporación Gilberto Echeverri Mejía, y el cumplimiento de las garantías de seguridad correspondientes al tratamiento de este tipo de datos.

La información que se requiere para el uso diario en la corporación; así como la información importante y susceptible, debe ser almacenada y trabajada desde el OneDrive asignado al correo a cada una de las personas

7.1.4. Bases de datos temporales, copias y reproducciones

Las bases de datos temporales o copias de documentos creadas para trabajos temporales o auxiliares deben cumplir con el mismo nivel de seguridad que corresponde a las bases de datos o documentos originales. Una vez que dejan de ser necesarias, estas bases de datos temporales o copias son borradas o destruidas, impidiéndose así el acceso o recuperación de la información que contienen.

7.1.5. Responsable deseguridad

La Corporación Gilberto Echeverri Mejía, ha designado a los responsables de seguridad encargados de coordinar y controlar las medidas de seguridad contenidas en la presente política. Sus datos se señalan en el "Anexo 2. Roles y Responsabilidades".

De acuerdo con la normativa sobre protección de datos, la designación de los responsables de seguridad no exonera de responsabilidad al responsable del tratamiento o encargado del tratamiento.

7.1.6. Auditorías

Las bases de datos que contengan datos personales, objeto de tratamiento por La Corporación Gilberto Echeverri Mejía, clasificadas con nivel de seguridad sensible o privado, se han de someter, se elevaran auditorias aleatorias según los riesgos establecidos o al menos cada dos (2) años, a una auditoría interna o externa que verifique el cumplimiento de las medidas de seguridad contenidas en esta política.

Serán objeto de auditoría tanto los sistemas de información como las instalaciones de almacenamiento y tratamiento de datos.

La Corporación Gilberto Echeverri Mejía podrá realizar una auditoría siempre que se realicen modificaciones sustanciales en el sistema de información que puedan afectar al cumplimiento de las medidas de seguridad, con el fin de verificar la adaptación, adecuación y eficacia de estas.

Las auditorías concluirán con un informe de auditoría que contendrá:

- ✓ El dictamen sobre la adecuación de las medidas y controles a la normativa sobre protección de datos.
- ✓ La identificación de las deficiencias identificadas como: hallazgos observaciones y la sugerencia de medidas correctoras o complementarias necesarias.
- ✓ La descripción de los datos, hechos y observaciones en que se basen los dictámenes y las recomendaciones propuestas con sus respectivos planes de mejoramiento

El responsable de seguridad estudiará el informe y trasladará las conclusiones al responsable del tratamiento para que implemente las medidas correctoras. Los informes de auditoría serán adjuntados a las políticas de seguridad de la información y quedarán a disposición de la Autoridad de Control.

7.2. Medidas de seguridad para bases de datos no automatizadas

7.2.1 Archivo de documentos:

La Corporación Gilberto Echeverri Mejía, fija los criterios y procedimientos de actuación que se deben utilizar para el archivo de documentos que contengan datos personales conforme a la Ley. Los criterios de archivo garantizan la conservación, localización y consulta de los documentos y hacen posible los derechos de consulta y reclamo de los Titulares. Estos criterios y procedimientos se recogen en el “Anexo 1. Información de Bases de datos”.

Se recomienda que los documentos sean archivados considerando, entre otros, criterios como el grado de utilización de los usuarios con acceso autorizado a los mismos, la actualidad de su gestión y/o tratamiento y la diferenciación entre bases de datos históricas y de administración o gestión de la entidad.

Los dispositivos de almacenamiento de documentos deben disponer de llaves u otros mecanismos que dificulte su apertura, excepto cuando las características físicas de éstos lo impidan, en cuyo caso La Corporación Gilberto Echeverri Mejía, adoptará las medidas necesarias para impedir el acceso de personas no autorizadas.

Los dispositivos se identifican y describen en el “Anexo 1. Información de Bases de datos”.

Cuando los documentos que contienen datos personales se encuentren en proceso de revisión o tramitación y, por tanto, fuera de los dispositivos de almacenamiento, ya sea antes o después de su archivo, la persona que se encuentre a cargo de estos deben custodiarlos e impedir en todo caso que personas no autorizadas puedan acceder a ellos.

Los dispositivos de almacenamiento que contengan documentos con datos personales clasificados con nivel de seguridad sensible deben encontrarse en áreas o locales en las que el acceso esté protegido con puertas de acceso con sistemas de apertura de llave u otros mecanismos similares. Estas áreas deben permanecer cerradas cuando no se precise el acceso a dichos documentos. Si no fuera posible cumplir con lo anterior, La Corporación Gilberto Echeverri Mejía, podrá adoptar medidas alternativas debidamente motivadas que se incluirán en la presente política.

La descripción de las medidas de seguridad de almacenamiento se encuentra recogidas en el “Anexo 1. Información de Bases de datos”.

7.2.2. Acceso a los documentos

El acceso a los documentos ha de realizarse exclusivamente por el personal autorizado en el "Anexo 2. Roles y Responsabilidades", siguiendo los mecanismos y procedimientos definidos. Estos últimos deben identificar y conservar los accesos realizados a la documentación clasificada con nivel de seguridad sensible, tanto por usuarios autorizados como por personas no autorizadas tal y como se refleja en el numeral referido anteriormente.

El procedimiento de acceso a los documentos que contienen datos clasificados como sensibles implica el registro de accesos a la documentación, la identidad de quien accede, el momento en que se produce el acceso y los documentos a los que se han accedido. El acceso a documentos con este tipo de datos se realiza por personal autorizado; si se realiza por personas no autorizadas deberá supervisarse por algún usuario autorizado o por el responsable de seguridad de la información en la Corporación Gilberto Echeverri Mejía.

7.3. Medidas de seguridad para bases de datos automatizadas

7.3.1. Identificación y autenticación.

La Corporación Gilberto Echeverri Mejía, debe instalar un sistema de seguridad informática que permita identificar y autenticar de forma correcta a los usuarios de los sistemas de información, con el fin de garantizar que solo el personal autorizado pueda acceder a las bases de datos.

También ha de establecer un mecanismo que permita la identificación personalizada, única e inequívoca de todo usuario que intente acceder al sistema de información y que verifique si está autorizado. La identificación debe realizarse mediante un sistema único para cada usuario en todos los sistemas que requieran de acceso por contraseña en la organización que accede a la información teniendo en cuenta el nombre de usuario, la identificación de empleado, el nombre del departamento, etc. La nomenclatura utilizada para la asignación de nombres de usuario para acceder al sistema de información y el sistema de autenticación de los usuarios se recogen en el “Anexo 1. Información de Bases de datos”.

Cuando el sistema de autenticación esté basado en la introducción de contraseña, se ha de implantar un procedimiento de asignación, distribución y almacenamiento de contraseñas; para garantizar la

integridad y confidencialidad de estas últimas, se recomiendan que tengan un mínimo de nueve caracteres y contengan mayúsculas, minúsculas, números y letras. La política de contraseñas de La Corporación Gilberto Echeverri Mejía se encuentra en el "Anexo 1. Información de Bases de datos".

Cuando el sistema de autenticación esté basado en la introducción de contraseña. La Corporación Gilberto Echeverri Mejía, debe implementar un segundo método de autenticación de un solo uso que provea de robustes, garantice la autenticidad y presencia del usuario y control de acceso desautorizado en caso de robo o copia de la contraseña anteriormente implantada.

Por otra parte, La Corporación Gilberto Echeverri Mejía, debe vigilar que las contraseñas se cambien de forma periódica, nunca por un tiempo superior a 180 días. El periodo de vigencia de las contraseñas se recoge en el ya referido "Anexo 1. Información de Bases de datos".

La Corporación Gilberto Echeverri Mejía, también garantiza el almacenamiento automatizado, interno y cifrado, de las contraseñas mientras estén vigentes, y adoptará un mecanismo para limitar los intentos reiterados de accesos no autorizados, también detallado en el "Anexo 1. Información de Bases de datos".

7.3.2. Entrada y salida de documentos o soportes

La entrada de documentos o soportes debe registrarse indicando el tipo de documento o soporte, la fecha y hora, el emisor, el número de documentos o soportes incluidos en el envío, el tipo de información que contienen según el nivel de seguridad, la forma de envío y la persona responsable de la recepción. La salida o envío de documentos o soportes, debidamente autorizada, ha de registrarse indicando el tipo de documento o soporte, la fecha y hora, el receptor, el número de documentos o soportes incluidos en el envío, el tipo de información que contienen según el nivel de seguridad, la forma de envío y la persona responsable del envío.

7.3.3. Control de accesofísico

Los lugares que son sede de los sistemas de información que contienen datos personales deben estar debidamente protegidos con el fin de garantizar la integridad y confidencialidad de dichos datos; asimismo, han de cumplir con las medidas de seguridad físicas correspondientes al documento o soporte donde incluyen los datos.

La Corporación Gilberto Echeverri Mejía, tiene el deber de poner en conocimiento de su personal las obligaciones que les competen con el objetivo de proteger físicamente los documentos o soportes en los que se encuentran las bases de datos, no permitiendo su manejo, utilización o identificación por personas no autorizadas en la presente política. Los lugares e instalaciones donde se ubican las bases de datos, especificando sus características físicas y las medidas de seguridad física existentes se señalan en el "Anexo 1. Información de Bases de datos".

Solamente el personal autorizado puede tener acceso a los lugares donde estén instalados los equipos que dan soporte a los sistemas de información, de acuerdo con lo dispuesto en numeral antes referido.

7.3.4. Copias de respaldo y recuperación de datos

La Corporación Gilberto Echeverri Mejía, ha llevado a cabo los procedimientos de actuación necesarios para realizar copias de respaldo, al menos una vez a la semana, excepto cuando no se haya producido ninguna actualización de los datos durante ese periodo. Todas las bases de datos deben tener una copia de respaldo a partir de las cuales se puedan recuperar los datos.

De igual modo, ha establecido procedimientos para la recuperación de los datos con el objetivo de garantizar en todo momento la reconstrucción al estado en el que éstos se encontraban antes de su pérdida o destrucción. Cuando la pérdida o destrucción afecte a bases de datos parcialmente automatizadas se grabarán manualmente los datos dejando constancia de ello.

La Corporación Gilberto Echeverri Mejía, se encargará de controlar el correcto funcionamiento y aplicación de los procedimientos de realización de copias de respaldo y recuperación de los datos cada treinta (30) días.

Los procedimientos de copia y respaldo se recogen en el “Anexo 1. Información de Bases de datos”.

La Corporación Gilberto Echeverri Mejía, debe conservar una copia de respaldo de los datos y de los procedimientos de recuperación de los mismos, para nuestro caso se cuenta con AWS como proveedor de servicio de nube, adicionalmente se cuenta con el servicio de Amazon Machine Image (AMI), para la realización y almacenamiento de los backups. Este lugar deberá cumplir en todo caso las mismas medidas de seguridad exigidas para los datos originales.

7.3.5. Registro de acceso

De los intentos de acceso a los sistemas de información La Corporación Gilberto Echeverri Mejía, guardará como mínimo, la identificación del usuario, la fecha y hora en que se lleva a cabo, la base de datos a la que se accede, el tipo de acceso y si ese acceso ha sido autorizado o no autorizado.

En caso de que el registro haya sido autorizado, se guarda la información que permita identificar el registro consultado.

Los responsables de seguridad de las bases de datos automatizadas se encargan de controlar los mecanismos que permiten el registro de acceso, revisar con carácter mensual la información de control registrada y elaborar un informe de las revisiones realizadas y los problemas detectados. Además, deben impedir la manipulación o desactivación de los mecanismos que permiten el registro de acceso.

Los datos que contiene el registro de acceso deben conservarse, al menos, durante un (1) año.

No será necesario el registro de acceso cuando el responsable del tratamiento sea una persona natural y garantice que solamente él tiene acceso y trata los datos personales. Estas circunstancias deben hacerse constar expresamente.

7.3.6. Redes de comunicaciones

El acceso a datos personales a través de redes de comunicaciones, públicas o privadas, debe someterse a medidas de seguridad equivalentes al acceso local de datos personales.

La transmisión de datos personales mediante redes públicas o inalámbricas de comunicaciones electrónicas se tiene que llevar a cabo cifrando dichos datos, o utilizando otro mecanismo similar que garantice que la información no sea inteligible ni manipulada por terceras personas.

7.3.7. Consolidado medidas de seguridad

MEDIDAS DE SEGURIDAD

TABLA I: Medidas de seguridad comunes para todo tipo de datos (públicos, semiprivados, privados, sensibles) y bases de datos (automatizadas, no automatizadas)

Gestión de documentos y soportes	Control de acceso	Incidencias	Personal	Política de seguridad de la información
1. Medidas que eviten el acceso indebido o la recuperación de los datos que han sido descartados, borrados o destruidos. 2. Acceso restringido al lugar donde se almacenan los datos. 3. Autorización del responsable para la salida de documentos o soportes por medio físico o electrónico. 4. Inventario de soportes	1. Acceso de usuarios limitado a los datos necesarios para el desarrollo de sus funciones. 2. Lista actualizada de usuarios y accesos autorizados. 3. Mecanismos para evitar el acceso a datos con derechos distintos de los autorizados. 4. Concesión, alteración o anulación de permisos por el personal autorizado	1. Registro de incidencias: tipo de incidencia, momento en que se ha producido, emisor de la notificación, receptor de la notificación, efectos y medidas correctoras. 2. Procedimiento de notificación y gestión de incidencias.	1. Definición de las funciones y obligaciones de los usuarios con acceso a los datos 2. Definición de las funciones de control y autorizaciones delegadas por el responsable del tratamiento. 3. Divulgación entre el personal de las normas y de las consecuencias del incumplimiento de estas	1. Elaboración e implementación la política de obligado cumplimiento para el personal. 2. Contenido mínimo: ámbito de aplicación, medidas y procedimientos de seguridad, funciones y obligaciones del personal, descripción de las bases de datos, procedimiento ante incidencias, identificación de los encargados del tratamiento.

TABLA II: Medidas de seguridad comunes para todo tipo de datos (públicos, semiprivados, privados, sensibles) según el tipo de bases de datos				
Bases de datos no automatizadas			Bases de datos automatizadas	
Archivo	Almacenamiento de documentos	Custodia de documentos	Identificación y autenticación	Telecomunicaciones
1. Archivo de documentación siguiendo procedimientos que garanticen una correcta conservación, localización y consulta y permitan el ejercicio de los derechos de los Titulares.	1. Dispositivos de almacenamiento con mecanismos que impidan el acceso a personas no autorizadas.	1. Deber de diligencia y custodia de la persona a cargo de documentos durante la revisión o tramitación de los mismos.	1. Identificación personalizada de usuarios para acceder a los sistemas de información y verificación de su autorización. 2. Mecanismos de identificación y autenticación; Contraseñas: asignación, caducidad y almacenamiento cifrado.	1. Acceso a datos mediante redes seguras.

TABLA III: Medidas de seguridad para datos privados según el tipo de bases de datos						
Bases de datos automatizadas y no automatizadas			Bases de datos automatizadas			
Auditoría	Responsable de seguridad	Política de seguridad de la información	Gestión de documento y soportes	Control de acceso	Identificación y autenticación	Incidencias
1. Auditoría ordinaria (interna o externa) cada año 2. Auditoría extraordinaria por modificaciones sustanciales en los sistemas de información. 3. Informe de detección de deficiencias y propuesta de correcciones. 4. Análisis y conclusiones del responsable de seguridad y del responsable del tratamiento.	1.Designación de uno o varios responsables de administrar las bases de datos. 2.Designación de uno o varios encargados del control y la coordinación de las medidas de la Política de seguridad de la información 3. Prohibición de delegación de la responsabilidad del responsable del tratamiento en los responsables de administrar	1. Controles periódicos de cumplimiento	1. Registro de entrada y salida de documentos y soportes: fecha, emisor y receptor, número, tipo de información, forma de envío, responsable de la recepción o entrega	1. Control de acceso al lugar o lugares donde se ubican los sistemas de información.	1. Mecanismo que limite el número de intentos reiterados de acceso no autorizados.	1. Registro de los procedimientos de recuperación de los datos, persona que los ejecuta, datos restaurados y datos grabados manualmente. 2. Autorización del responsable del tratamiento para la ejecución de los procedimientos de recuperación.

TABLA III: Medidas de seguridad para datos privados según el tipo de bases de datos						
Bases de datos automatizadas y no automatizadas			Bases de datos automatizadas			
Auditoría	Responsable de seguridad	Política de seguridad de la información	Gestión de documento y soportes	Control de acceso	Identificación y autenticación	Incidencias
	las bases de datos.					

TABLA IV: Medidas de seguridad para datos sensibles según el tipo de bases de datos						
Bases de datos no automatizadas			Bases de datos automatizadas			
Control de acceso	Almacenamiento de documentos	Copia o reproducción	Traslado de documentación	Gestión de documentos y soportes	Control de acceso	Telecomunicaciones
1. Acceso solo para personal autorizado. 2. Mecanismo de identificación de acceso. 3. Registro de accesos de usuarios no autoriza-dos	1. Archivadores, armarios u otros ubicados en áreas de acceso protegidas con llaves u otras medidas.	1. Solo por usuarios autoriza-dos. 2. Destrucción que impida el acceso o recuperación de los datos.	1. Medidas que impidan el acceso o manipulación de documentos	1. Definición de perfiles de usuarios acordes con su función. 2. Cifrado de datos. 3. Cifrado de dispositivos portátiles cuando se encuentren fuera.	1. Registro de accesos: usuario, hora, base de datos a la que accede, tipo de acceso, registro al que accede. 2. Control mensual del registro de accesos por el responsable de administrar las bases de datos.	1. Transmisión de datos mediante redes electrónicas cifradas.

8. Políticas de la organización de la seguridad de la información

En la Corporación la información es un activo fundamental para la prestación de sus servicios y la toma de decisiones eficientes, razón por la cual existe un compromiso expreso de protección de sus propiedades más significativas como parte de una estrategia orientada a la continuidad del negocio, la administración de riesgos y la consolidación de una cultura de seguridad.

Los vinculados, contratistas, personal externo, proveedores y todos aquellos que tengan responsabilidades sobre las fuentes, repositorios y recursos de procesamiento de la información de la Corporación, deben

adoptar los lineamientos contenidos en el presente documento y en los documentos relacionados con él, con el fin de mantener la confidencialidad, la integridad y asegurar la disponibilidad de la información.

8.1 Política para uso de dispositivos móviles

La Corporación, proveerá las condiciones para el manejo de los dispositivos móviles (teléfonos inteligentes y tabletas, entre otros) institucionales. Así mismo, velará porque las personas hagan un uso responsable de los servicios y equipos proporcionados por la entidad.

8.2 Normas para uso de dispositivos móviles

Normas dirigidas a: Profesional universitario Oficina TIC.

- ✓ El Profesional universitario Oficina TIC deben investigar y probar las opciones de protección de los dispositivos móviles institucionales que hagan uso de los servicios provistos por la corporación.
- ✓ El Profesional universitario Oficina TIC deben establecer las configuraciones aceptables para los dispositivos móviles institucionales que hagan uso de los servicios provistos por La Corporación Gilberto Echeverri Mejía.
- ✓ El Profesional universitario Oficina TIC deben establecer un método de bloqueo (por ejemplo, contraseñas, biométricos, patrones, reconocimiento de voz) para los dispositivos móviles institucionales que serán entregados a los usuarios. Se debe configurar estos dispositivos para que pasado un tiempo de inactividad pasen automáticamente a modo de suspensión y, en consecuencia, se active el bloqueo de la pantalla el cual requerirá el método de desbloqueo configurado.

Normas dirigidas a: Todos los usuarios.

- ✓ Los usuarios deben evitar usar los dispositivos móviles institucionales en lugares que no les ofrezcan las garantías de seguridad física necesarias para evitar pérdida o robo de estos.
- ✓ Los usuarios deben, cada vez que el sistema de sus dispositivos móviles institucionales notifique de una actualización disponible, aceptar y aplicar la nueva versión.
- ✓ Los usuarios deben evitar conectar los dispositivos móviles institucionales asignados por puerto USB a cualquier computador público, de hoteles o cafés internet, entre otros.
- ✓ Los usuarios no deben almacenar videos, fotografías o información personal en los dispositivos móviles institucionales asignados.

8.3. Política para uso de conexiones remotas

La Corporación Gilberto Echeverri Mejía establecerá las circunstancias y requisitos para el establecimiento de conexiones remotas a la plataforma tecnológica de la corporación; así mismo, suministrará las herramientas y controles necesarios para que dichas conexiones se realicen de manera segura.

8.3.1. Normas para uso de conexiones remotas

Normas dirigidas a: Profesional universitario Oficina TIC.

- ✓ El Profesional universitario Oficina TIC deben analizar y aprobar los métodos de conexión remota a la plataforma tecnológica de la Corporación.
- ✓ El Profesional universitario Oficina TIC deben implantar los métodos y controles de seguridad para establecer conexiones remotas hacia la plataforma tecnológica de la Corporación.
- ✓ El Profesional universitario Oficina TIC deben restringir las conexiones remotas a los recursos de la plataforma tecnológica; únicamente se deben permitir estos accesos a personal autorizado, de acuerdo con las labores desempeñadas.
- ✓ El Profesional universitario Oficina TIC deben verificar la efectividad de los controles aplicados sobre las conexiones remotas a los recursos de la plataforma tecnológica de la Corporación.
- ✓ Se debe contar con llave privada para la conexión a cualquiera de los servidores de la corporación

Normas dirigidas a: Todos los usuarios.

- ✓ Los usuarios que realizan conexión remota deben acatar las condiciones de uso establecidas para dichas conexiones.

Requerimientos:

- ✓ Conexión a internet.
- ✓ Nombre del servidor de acceso remoto o dirección Ip del mismo.
- ✓ Nombre del usuario de acceso remoto, su contraseña correspondiente y el nombre del dominio al que se realizara la conexión.

Condiciones de uso:

- ✓ Solo los usuarios previamente configurados en el dispositivo destinado para dichas conexiones podrán realizar la conexión.
- ✓ La persona autorizada para realizar este tipo de conexión contara con un usuario y contraseña únicos suministrados por El Profesional universitario Oficina TIC.
- ✓ La cuenta de acceso es personal e intransferible, no pudiéndose ceder a terceros, tengan o no relación con la corporación.
- ✓ El usuario es responsable de todas las actividades realizadas con su cuenta de acceso proporcionada por la Corporación.
- ✓ El procedimiento para la configuración y conexión a la VPN se describe en el documento “Instructivo para configuración y conexión a VPN.pdf”, que es enviado al correo de la persona que es autorizada para realizar la conexión VPN.
- ✓ No está permitido la difusión deliberada de virus, gusanos o cualquier intento de atentar a la seguridad de otros equipos o usuarios de la red.
- ✓ Utilizar la conexión VPN de la Corporación para el manejo de contenidos inapropiados.
- ✓ Realizar acciones con objeto de dificultar el acceso a la red o el uso de cualquier servicio proporcionado por la Corporación

8.4. Política de tratamiento de información

La Corporación Gilberto Echeverri Mejía, ha creado la política de tratamiento de datos, con el objetivo de garantizar el cumplimiento de las disposiciones plasmadas en los artículos 15 y 20 de la Constitución. La política se encuentra descrita en el "Anexo 4. MANUAL-POLITICA-TRATAMIENTO-DE-DATOS-2021 V3"

9. Políticas de gestión de activos de información

9.1. Política de responsabilidad por los activos

La Corporación Gilberto Echeverri Mejía como propietario de la información física, así como de la información generada, procesada, almacenada y transmitida con su plataforma tecnológica, otorgará responsabilidad a las áreas sobre sus activos de información, asegurando el cumplimiento de las directrices que regulen el uso adecuado de la misma.

La información, archivos físicos, los sistemas, los servicios y los equipos (ej. estaciones de trabajo, equipos portátiles, impresoras, redes, Internet, correo electrónico, herramientas de acceso remoto, aplicaciones y teléfonos, entre otros) propiedad de la Corporación, son activos de la Entidad y se proporcionan a los vinculados y terceros autorizados.

Toda la información sensible de la Entidad, así como los activos donde ésta se almacena y se procesa deben ser asignados a un responsable, inventariados y posteriormente clasificados, de acuerdo con los requerimientos y los criterios que dicten El Profesional universitario Oficina TIC. Los propietarios de los activos de información deben llevar a cabo el levantamiento y la actualización permanente del inventario de activos de información al interior de sus procesos o áreas.

9.1.1. Normas de responsabilidad por los activos

Normas dirigidas a: Profesional universitario Oficina TIC.

- ✓ El Profesional universitario Oficina TIC son los responsables de los activos de información correspondientes a la plataforma tecnológica de la Corporación y, en consecuencia, deben asegurar su apropiada operación y administración.
- ✓ El Profesional universitario Oficina TIC son quienes deben autorizar la instalación, cambio o eliminación de componentes de la plataforma tecnológica de la Corporación.
- ✓ El Profesional universitario Oficina TIC deben establecer una configuración adecuada para los recursos tecnológicos, con el fin de preservar la seguridad de la información y hacer un uso adecuado de ellos.
- ✓ El Profesional universitario Oficina TIC es responsable de preparar las estaciones de trabajo fijas y/o portátiles de los vinculados y de hacer entrega de las mismas.
- ✓ El Profesional universitario Oficina TIC son responsables de recibir los equipos de trabajo fijo y/o portátil para su reasignación o disposición final, y generar copias de seguridad de la información de los empleados que se retiran o cambian de labores, cuando les es formalmente solicitado.
- ✓ El Profesional universitario Oficina TIC deben definir las condiciones de uso y protección de los activos de información, tanto los tecnológicos como aquellos que no lo son.

- ✓ El Profesional universitario Oficina TIC deben realizar revisiones periódicas de los recursos de la plataforma tecnológica y los sistemas de información de la Corporación.

Normas dirigidas a: Todos los usuarios.

- ✓ Los recursos tecnológicos de la Corporación deben ser utilizados de forma ética y responsable, con el fin de evitar daños o pérdidas sobre la operación o la imagen de la Corporación.
- ✓ Los recursos tecnológicos de la Corporación provistos a los vinculados, contratistas o terceras personas, son proporcionados con el único fin de llevar a cabo las labores de la Entidad; por consiguiente, no deben ser utilizados para fines personales o ajenos a este.
- ✓ Los vinculados no deben utilizar sus equipos de cómputo y dispositivos móviles personales para desempeñar las actividades laborales.
- ✓ Los vinculados no deben utilizar software no autorizado o de su propiedad en la plataforma tecnológica de la Corporación.

9.2. Política de clasificación y manejo de la información

La Corporación Gilberto Echeverri Mejía definirá los niveles más adecuados para clasificar su información de acuerdo con su sensibilidad

Toda la información de la Corporación debe ser identificada, clasificada y documentada de acuerdo con las guías de clasificación de la información aprobadas por la dirección.

Una vez clasificada la información, la Entidad proporcionará los recursos necesarios para la aplicación de controles en busca de preservar la confidencialidad, integridad y disponibilidad de esta, con el fin de promover el uso adecuado por parte de los vinculados, contratistas y terceras personas.

9.2.1. Normas para la clasificación y manejo de la información

- ✓ Se definieron los niveles de clasificación de la información para La Corporación Gilberto Echeverri Mejía
- ✓ Se debe socializar y divulgar la guía de clasificación de la Información de la Corporación a los vinculados, contratistas y terceras personas.
- ✓ Se debe monitorear con una periodicidad establecida por un comité interdisciplinario, la aplicación de la guía de clasificación de la Información.

Normas dirigidas a: Profesional universitario Oficina TIC.

- ✓ El Profesional universitario Oficina TIC deben efectuar la eliminación segura de la información, a través de los mecanismos necesarios en la plataforma tecnológica, ya sea cuando son dados de baja o cambian de usuario.

Normas dirigidas a: Gestión documental.

- ✓ Gestión documental está facultada para destruir o desechar correctamente la documentación física cuando se ha cumplido el ciclo de almacenamiento, basándose a partir del documento de tablas de retención documental

Normas dirigidas a: Todos los usuarios.

- ✓ Los usuarios deben acatar los lineamientos guía de clasificación de la Información para el acceso, divulgación, almacenamiento, copia, transmisión, etiquetado y eliminación de la información contenida en los recursos tecnológicos, así como de la información física de la Corporación.
- ✓ La información física y digital de la Corporación debe tener un periodo de almacenamiento que puede ser dictaminado por requerimientos legales o misionales; este período debe ser indicado en las tablas de retención documental y cuando se cumpla el periodo de expiración, toda la información debe ser eliminada adecuadamente.
- ✓ Los usuarios deben tener en cuenta las siguientes consideraciones cuando impriman, escaneen, saquen copias y envíes faxes: verificar las áreas adyacentes a impresoras, escáneres, fotocopiadoras y máquinas de fax para asegurarse que no quedaron documentos relacionados o adicionales; asimismo, recoger de las impresoras, escáneres, fotocopiadoras y máquinas de fax los documentos para evitar su divulgación no autorizada.
- ✓ Tanto los vinculados deben asegurarse de que, en el momento de ausentarse de su puesto de trabajo, sus escritorios se encuentren libres de documentos y medios de almacenamiento, utilizados para el desempeño de sus labores.
- ✓ La información que se encuentra en documentos físicos debe ser protegida, a través de controles de acceso físico y las condiciones adecuadas de almacenamiento y resguardo.

9.3. Política para uso de tokens de seguridad

La Corporación Gilberto Echeverri Mejía proveerá las condiciones de manejo de los tokens de seguridad para los procesos que los utilizan y velará porque se haga un uso responsable de estos.

9.3.1. Normas para uso de tokens de seguridad

Normas dirigidas a: Usuarios de tokens de seguridad.

- ✓ Los usuarios que requieren utilizar los tokens de seguridad deben contar con una cuenta de usuario en los portales o sitios de uso de estos; dichos tokens harán parte del inventario físico de cada usuario a quien se haya asignado.
- ✓ Cada usuario de los portales o sitios de uso de los tokens debe tener su propio dispositivo, el cual es exclusivo, personal e intransferible, al igual que la cuenta de usuario y la contraseña de acceso.
- ✓ El almacenamiento de los tokens debe efectuarse bajo estrictas medidas de seguridad, en la tula o sobre asignado para cada token, dentro de caja fuerte o escritorios con llave al interior de las áreas usuarias, de tal forma que se mantengan fuera del alcance de terceros no autorizados.
- ✓ Los usuarios deben notificar a las entidades emisoras de dichos tokens en caso de robo, pérdida, mal funcionamiento o caducidad.

- ✓ Los usuarios no deben permitir que terceras personas observen la clave que genera el token, así como no deben aceptar ayuda de terceros para la utilización del token.
- ✓ Los usuarios deben responder por las transacciones electrónicas que se efectúen con la cuenta de usuario, clave y el token asignado, en el desarrollo de sus actividades. En caso de que suceda algún evento irregular con los tokens los usuarios deben asumir la responsabilidad administrativa, disciplinaria y económica.
- ✓ Los usuarios deben mantener los tokens asignados en un lugar seco y no introducirlos en agua u otros líquidos.
- ✓ Los usuarios deben evitar exponer los tokens a campos magnéticos y a temperaturas extremas.
- ✓ Los usuarios deben evitar que los tokens sean golpeados o sometidos a esfuerzo físico.
- ✓ Los usuarios no deben abrir los tokens, retirar la batería o placa de circuitos, ya que ocasionará su mal funcionamiento.
- ✓ Los usuarios no deben usar los tokens fuera de las instalaciones de la Corporación para evitar pérdida o robo de estos.

9.4. Política para uso de multifactor

La Corporación Gilberto Echeverri Mejía proveerá las condiciones de manejo procesos de autenticación MFA donde sea necesario.

9.4.1. Normas para uso de tokens de MFA

Normas dirigidas a: Usuarios con **MFA**.

- ✓ Cada usuario será responsable por el uso del código **MFA**.
- ✓ Cada usuario de los portales o sitios de uso de los tokens debe tener su propio dispositivo, el cual es exclusivo, personal e intransferible, al igual que la cuenta de usuario y la contraseña de acceso.
- ✓ Los usuarios deben notificar a la corporación la pérdida del dispositivo donde se tiene configurada el **MFA.**
- ✓ Los usuarios no deben permitir que terceras personas observen la clave que genera el **MFA.**

9.5. Política de uso de periféricos y medios de almacenamiento

El uso de periféricos y medios de almacenamiento en los recursos de la plataforma tecnológica de la Corporación será reglamentado por El Profesional universitario Oficina TIC considerando las labores realizadas por los vinculados y su necesidad de uso.

9.5.1. Normas uso de periféricos y medios de almacenamiento

Normas dirigidas a: Profesional universitario Oficina TIC.

- ✓ El Profesional universitario Oficina TIC deben establecer las condiciones de uso de periféricos y medios de almacenamiento en la plataforma tecnológica de la Corporación.
- ✓ El Profesional universitario Oficina TIC deben implantar los controles que regulen el uso de periféricos y medios de almacenamiento en la plataforma tecnológica de la Corporación.
- ✓ El Profesional universitario Oficina TIC deben generar y aplicar lineamientos para la disposición segura de los medios de almacenamiento del instituto, ya sea cuando son dados de baja o reasignados a un nuevo usuario.

Normas dirigidas a: Todos los usuarios.

- ✓ Los vinculados, contratistas y terceras personas deben acoger las condiciones de uso de los periféricos y medios de almacenamiento establecidos por El Profesional universitario Oficina TIC.
- ✓ Los vinculados, contratistas y terceras personas son responsables por la custodia de los medios de almacenamiento institucionales asignados.

10. Políticas de control de acceso

10.1. Política de acceso a redes y recursos de red

El Profesional universitario Oficina TIC de la Corporación, como responsables de las redes de datos y los recursos de red, deben propender porque dichas redes sean debidamente protegidas contra accesos no autorizados a través de mecanismos de control de acceso lógico.

10.1.1. Normas de acceso a redes y recursos de red

Normas dirigidas a: Profesional universitario Oficina TIC.

- ✓ El Profesional universitario Oficina TIC deben establecer un procedimiento de autorización y controles para proteger el acceso a las redes de datos y los recursos de red de la Corporación.
- ✓ El Profesional universitario Oficina TIC deben asegurar que las redes inalámbricas de la corporación cuenten con métodos de autenticación que evite accesos no autorizados.
- ✓ El Profesional universitario Oficina TIC deben establecer controles para la identificación y autenticación de los usuarios provistos por terceros en las redes o recursos de red de la Corporación, así como velar por la aceptación de las responsabilidades de estos y formalizar su aceptación de las Políticas de Seguridad de la Información.
- ✓ El Profesional universitario Oficina TIC deben verificar periódicamente los controles de acceso para los usuarios provistos para terceros, 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.

Normas dirigidas a: Todos los usuarios.

- ✓ Los equipos de cómputo de usuario final que se conecten o deseen conectarse a las redes de datos de la Corporación deben cumplir con todos los requisitos o controles para autenticarse en ellas y únicamente podrán realizar las tareas para las que fueron autorizados.

10.2. Política de control de acceso a sistemas y aplicativos

El Profesional universitario Oficina TIC como responsables de la administración de los sistemas de información y aplicativos, propenderá para que estos sean debidamente protegidos contra accesos no autorizados a través de mecanismos de control de acceso lógico. Así mismo, velará porque los desarrolladores, tanto internos como externos, acojan buenas prácticas de desarrollo en los productos generados para controlar el acceso lógico y evitar accesos no autorizados a los sistemas administrados.

10.2.1. Normas de control de acceso a sistemas y aplicativos

Normas dirigidas a: Profesional universitario Oficina TIC.

- ✓ El Profesional universitario Oficina TIC deben establecer un procedimiento para la asignación de accesos a los sistemas y aplicativos de la Corporación.
- ✓ El Profesional universitario Oficina TIC deben asegurar, mediante los controles necesarios, que los usuarios utilicen diferentes perfiles para los ambientes de desarrollo, pruebas y producción, y así mismo que los menús muestren los mensajes de identificación apropiados para reducir los riesgos de error.
- ✓ El Profesional universitario Oficina TIC deben establecer el procedimiento y los controles de acceso a los ambientes de producción de los sistemas de información; así mismo, debe asegurarse que los desarrolladores internos o externos, posean acceso limitado y controlado a los datos y archivos que se encuentren en los ambientes de producción.
- ✓ El Profesional universitario Oficina TIC deben proporcionar repositorios de archivos fuente de los sistemas de información; estos deben contar con acceso controlado y restricción de privilegios, además de un registro de acceso a dichos archivos.

Normas dirigidas a: Desarrolladores (internos y externos)

- ✓ Los desarrolladores deben asegurar que los sistemas de información construidos requieran autenticación para todos los recursos y páginas, excepto aquellas específicamente clasificadas como públicas.
- ✓ Los desarrolladores deben certificar la confiabilidad de los controles de autenticación, utilizando implementaciones centralizadas para dichos controles.
- ✓ Los desarrolladores deben certificar que no se almacenen contraseñas, cadenas de conexión u otra información sensible en texto claro y que se implementen controles de integridad de dichas contraseñas.
- ✓ Los desarrolladores deben establecer los controles de autenticación de tal manera que cuando fallen, lo hagan de una forma segura, evitando indicar específicamente cual fue la falla durante el proceso de autenticación y, en su lugar, generando mensajes generales de falla.
- ✓ Los desarrolladores deben asegurar que no se despliegan en la pantalla las contraseñas ingresadas, así como deben deshabilitar la funcionalidad de recordar campos de contraseñas.
- ✓ Los desarrolladores deben certificar que se inhabilitan las cuentas luego de tres (3) intentos fallidos de ingreso a los sistemas desarrollados.
- ✓ Los desarrolladores deben asegurar que, si se utiliza la reasignación de contraseñas, únicamente se envíe un enlace o contraseñas temporales a cuentas de correo electrónico previamente registradas en los aplicativos, los cuales deben tener un periodo de validez establecido; se debe forzar el cambio de las contraseñas temporales después de su utilización.
- ✓ Los desarrolladores deben certificar que el último acceso (fallido o exitoso) sea reportado al usuario en su siguiente acceso exitoso a los sistemas de información.
- ✓ Los desarrolladores deben asegurar la re-autenticación de los usuarios antes de la realización de operaciones críticas en los aplicativos.

- ✓ Los desarrolladores deben, a nivel de los aplicativos, restringir acceso a archivos u otros recursos, a direcciones URL protegidas, a funciones protegidas, a servicios, a información de las aplicaciones, a atributos y políticas utilizadas por los controles de acceso y a la información relevante de la configuración, solamente a usuarios autorizados.
- ✓ Los desarrolladores deben establecer que periódicamente se revalide la autorización de los usuarios en los aplicativos y se asegure que sus privilegios no han sido modificados.

11. Políticas de seguridad física

11.1. Política de áreas seguras

La Corporación proveerá la implantación y velará por la efectividad de los mecanismos de seguridad física y control de acceso que aseguren el perímetro de sus instalaciones. Así mismo, controlará las amenazas físicas externas e internas y las condiciones medioambientales de sus oficinas.

Todas las áreas destinadas al procesamiento o almacenamiento de información sensible, así como aquellas en las que se encuentren los equipos y demás infraestructura de soporte a los sistemas de información y comunicaciones, se consideran áreas de acceso restringido.

11.1.1. Normas de áreas seguras

Normas dirigidas a: Profesional universitario Oficina TIC.

- ✓ Las solicitudes de acceso al centro de cómputo o a los centros de cableado deben ser aprobadas por El Profesional universitario Oficina TIC; no obstante, los visitantes siempre deberán estar acompañados por uno de El Profesional universitario Oficina TIC durante su visita al centro de cómputo o los centros de cableado.
- ✓ El Profesional universitario Oficina TIC deben registrar el ingreso de los visitantes al centro de cómputo y a los centros de cableado que están bajo su custodia en una bitácora.
- ✓ El Profesional universitario Oficina TIC deben proveer las condiciones físicas y medioambientales necesarias para certificar la protección y correcta operación de los recursos de la plataforma tecnológica ubicados en el centro de cómputo; deben existir sistemas de control ambiental de temperatura y humedad, sistemas de detección y extinción de incendios, sistemas de descarga eléctrica, sistemas de vigilancia y monitoreo y alarmas en caso de detectarse condiciones ambientales inapropiadas. Estos sistemas se deben monitorear de manera permanente.
- ✓ El Profesional universitario Oficina TIC deben velar porque los recursos de la plataforma tecnológica de la Corporación ubicados en el centro de cómputo se encuentran protegidos contra fallas o interrupciones eléctricas.
- ✓ El Profesional universitario Oficina TIC deben certificar que el centro de cómputo y los centros de cableado que están bajo su custodia, se encuentren separados de áreas que tengan líquidos inflamables o que corran riesgo de inundaciones e incendios.
- ✓ El Profesional universitario Oficina TIC deben asegurar que las labores de mantenimiento de redes eléctricas y de datos, sean realizadas por personal idóneo y apropiadamente autorizado e identificado; así mismo, se debe llevar control de la programación de los mantenimientos preventivos.

Normas dirigidas a: Todos los usuarios.

- ✓ Los vinculados y contratistas deberán portar el carné que los identifica como tales en un lugar visible mientras se encuentren en las instalaciones de la Corporación; en caso de pérdida del carné, deben reportarlo a la mayor brevedad posible.
- ✓ Aquellos vinculados, contratistas o terceras personas para los que aplique, en razón del servicio prestado, deben utilizar prendas distintivas que faciliten su identificación.
- ✓ Los vinculados, contratistas o terceras personas no deben intentar ingresar a áreas a las cuales no tengan autorización.

11.2. Política de seguridad para los equipos institucionales

La Corporación para evitar la pérdida, robo o exposición al peligro de los recursos de la plataforma tecnológica del instituto que se encuentren dentro o fuera de sus instalaciones, proveerá los recursos que garanticen la mitigación de riesgos sobre dicha plataforma tecnológica.

11.2.1. Normas de seguridad para los equipos institucionales

- ✓ Se debe revisar los accesos físicos en horas no hábiles a las áreas donde se procesa información.
- ✓ Se debe restringir el acceso físico a los equipos de cómputo de áreas donde se procesa información sensible.
- ✓ El cableado de red se instalará físicamente separado de cualquier otro tipo de cables, llámese a estos de corriente o energía eléctrica, para evitar interferencias.
- ✓ Toda oficina o área de trabajo debe poseer entre sus inventarios, herramientas auxiliares (extintores, alarmas contra incendios, lámpara de emergencia), necesarias para salvaguardar los recursos tecnológicos y la información.
- ✓ Las instalaciones de las áreas de trabajo deben contar con una adecuada instalación eléctrica, y proveer del suministro de energía mediante una estación de alimentación ininterrumpida o UPS para poder proteger la información.
- ✓ Se deberá considerar los estándares vigentes de cableado estructurado durante el diseño de nuevas áreas o en el crecimiento de las áreas existentes.

Normas dirigidas a: Profesional universitario Oficina TIC.

- ✓ El Profesional universitario Oficina TIC deben proveer los mecanismos y estrategias necesarios para proteger la confidencialidad, integridad y disponibilidad de los recursos tecnológicos, dentro y fuera de las instalaciones de la Corporación.
- ✓ El Profesional universitario Oficina TIC deben realizar mantenimientos preventivos y correctivos de los recursos de la plataforma tecnológica de la Entidad.
- ✓ El Profesional universitario Oficina TIC deben generar estándares de configuración segura para los equipos de cómputo de la Corporación y configurar dichos equipos acogiendo los estándares generados.
- ✓ El Profesional universitario Oficina TIC deben establecer las condiciones que deben cumplir los equipos de cómputo de los terceros externos, que requieran conectarse a la red de datos de la

Corporación y verificar el cumplimiento de dichas condiciones antes de conceder a estos equipos acceso a los servicios de red.

- ✓ El Profesional universitario Oficina TIC deben generar y aplicar lineamientos para la disposición segura de los equipos de cómputo de la Corporación, ya sea cuando son dados de baja o cambian de usuario.
- ✓ El Profesional universitario Oficina TIC entregaran los equipos a los usuarios y/o jefes de área, los cuales determinaran cual será el lugar de trabajo para los equipos de computo

Normas dirigidas a: Todos los usuarios.

- ✓ El Profesional universitario Oficina TIC son las únicas personas autorizadas para realizar movimientos y asignaciones de recursos tecnológicos; por consiguiente, se encuentra prohibida la disposición que pueda hacer cualquier persona diferente de los recursos tecnológicos de la Corporación.
- ✓ Las estaciones de trabajo, dispositivos móviles y demás recursos tecnológicos asignados a los vinculados deben acoger las instrucciones técnicas que proporcionen El Profesional universitario Oficina TIC.
- ✓ Cuando se presente una falla o problema de hardware o software en una estación de trabajo u otro recurso tecnológico propiedad de la Corporación el usuario responsable debe informar a la Mesa de Ayuda en donde se atenderá el caso con el fin de realizar una asistencia adecuada. El usuario no debe intentar solucionar el problema.
- ✓ La instalación, reparación o retiro de cualquier componente de hardware o software de las estaciones de trabajo, dispositivos móviles y demás recursos tecnológicos de la Corporación, solo puede ser realizado por El Profesional universitario Oficina TIC, o personas autorizadas por los profesionales.
- ✓ Los vinculados, contratistas o terceras personas deben bloquear sus estaciones de trabajo o actividad en el momento de abandonar el lugar asignado.
- ✓ Los vinculados, contratistas o terceras personas no deben dejar encendidas las estaciones de trabajo o actividad u otros recursos tecnológicos en horas no laborables.
- ✓ Los equipos de cómputo, en ninguna circunstancia, deben ser dejados desatendidos en lugares públicos o a la vista, en el caso de que estén siendo transportados.
- ✓ Los equipos de cómputo deben ser transportados con las medidas de seguridad apropiadas, que garanticen su integridad física.
- ✓ Los equipos portátiles siempre deben ser llevados como equipaje de mano y se debe tener especial cuidado de no exponerlos a fuertes campos electromagnéticos.
- ✓ En caso de pérdida o robo de un equipo de cómputo de la Corporación, se debe informar de forma inmediata al líder del proceso para que se inicie el trámite interno y se debe poner la denuncia ante la autoridad competente.
- ✓ Es responsabilidad de los usuarios almacenar su información únicamente en OneDrive o SharePoint corporativo, ya que no está permitido almacenar información importante de forma local en los computadores
- ✓ Mientras se opera el equipo de cómputo, no se deberán consumir alimentos o ingerir líquidos.

12. Políticas de seguridad en las operaciones

12.1. Política de asignación de responsabilidades operativas

El Profesional universitario Oficina TIC, encargados de la operación y administración de los recursos tecnológicos que apoyan los procesos de la Corporación, tienen asignado funciones específicas de efectuar la operación y administración de dichos recursos tecnológicos, manteniendo y actualizando la documentación de los procesos operativos para la ejecución de las actividades. Así mismo, velarán por la eficiencia de los controles implantados en los procesos operativos asociados a los recursos tecnológicos con el objeto de proteger la confidencialidad, la integridad y la disponibilidad de la información manejada y asegurarán que los cambios efectuados sobre los recursos tecnológicos serán adecuadamente controlados y debidamente autorizados.

El Profesional universitario Oficina TIC proveerán la capacidad de procesamiento requerida en los recursos tecnológicos y sistemas de información de la Corporación, efectuando proyecciones de crecimiento y provisiones en la plataforma tecnológica con una periodicidad definida.

12.1.1. Normas de asignación de responsabilidades operativas

Normas dirigidas a: Profesional universitario Oficina TIC.

- ✓ El Profesional universitario Oficina TIC deben efectuar la documentación y actualización de los procedimientos relacionados con la operación y administración de la plataforma tecnológica de la Corporación.
- ✓ El Profesional universitario Oficina TIC deben contar con manuales de configuración y operación de los sistemas operativos, firmware, servicios de red, bases de datos y sistemas de información que conforman la plataforma tecnológica de la Corporación.
- ✓ El Profesional universitario Oficina TIC deben proveer los recursos necesarios para la implantación de controles que permitan la separación de ambientes de desarrollo, pruebas y producción, teniendo en cuenta consideraciones como: controles para el intercambio de información entre los ambientes de desarrollo y producción, la inexistencia de compiladores, editores o fuentes en los ambientes de producción y un acceso diferente para cada uno de los ambientes.
- ✓ El Profesional universitario Oficina TIC deben realizar estudios sobre la demanda y proyecciones de crecimiento de los recursos administrados (capacity planning) de manera periódica, con el fin de asegurar el desempeño y capacidad de la plataforma tecnológica. Estos estudios y proyecciones deben considerar aspectos de consumo de recursos de procesadores, memorias, discos, servicios de impresión, anchos de banda, internet y tráfico de las redes de datos, entre otros.

12.2. Política de protección frente a software malicioso

La Corporación Gilberto Echeverri Mejía proporcionará los mecanismos necesarios que garanticen la protección de la información y los recursos de la plataforma tecnológica en donde se procesa y almacena, adoptando los controles necesarios para evitar la divulgación, modificación o daño permanente ocasionados por el contagio de software malicioso. Además, proporcionará los mecanismos para generar cultura de seguridad frente a los ataques de software malicioso.

12.2.1. Normas de protección frente a software malicioso

Normas dirigidas a: El Profesional universitario Oficina TIC.

- ✓ El Profesional universitario Oficina TIC deben proveer herramientas tales como antivirus, antimalware, antispam, antispyware, entre otras, que reduzcan el riesgo de contagio de software malicioso y respalden la seguridad de la información contenida y administrada en la plataforma tecnológica de la Corporación y los servicios que se ejecutan en la misma.
- ✓ El Profesional universitario Oficina TIC deben asegurar que el software de antivirus, antimalware, antispam y antispyware cuente con las licencias de uso requeridas, certificando así su autenticidad y la posibilidad de actualización periódica de las últimas bases de datos de firmas del proveedor del servicio.
- ✓ El Profesional universitario Oficina TIC deben certificar que la información almacenada en la plataforma tecnológica sea escaneada por el software de antivirus, incluyendo la información que se encuentra contenida y es transmitida por el servicio de correo electrónico.
- ✓ El Profesional universitario Oficina TIC deben asegurarse de que los usuarios no puedan realizar cambios en la configuración del software de antivirus, antispyware, antispam, antimalware.
- ✓ El Profesional universitario Oficina TIC deben certificar que el software de antivirus, antispyware, antispam, antimalware, posea las últimas actualizaciones y parches de seguridad, para mitigar las vulnerabilidades de la plataforma tecnológica.

Normas dirigidas a: Todos los usuarios.

- ✓ Los usuarios de recursos tecnológicos deben ejecutar el software de antivirus, antispyware, antispam, antimalware sobre los archivos y/o documentos que son abiertos o ejecutados por primera vez, especialmente los que se encuentran en medios de almacenamiento externos o que provienen del correo electrónico.
- ✓ Los usuarios que sospechen o detecten alguna infección por software malicioso deben notificar por medio de la mesa de ayuda, para que, a través de ella, se tomen las medidas de control correspondientes.

12.3. Política de copias de respaldo de la información

La Corporación Gilberto Echeverri Mejía certificará la generación de copias de respaldo y almacenamiento de su información crítica, proporcionando los recursos necesarios y estableciendo los procedimientos y mecanismos para la realización de estas actividades. Las áreas propietarias de la información, con el apoyo de El Profesional universitario Oficina TIC, encargados de la generación de copias de respaldo, definirán la estrategia a seguir y los periodos de retención para el respaldo y almacenamiento de la información.

12.3.1. Normas de copias de respaldo de la información

Normas dirigidas a: Profesional universitario Oficina TIC.

- ✓ El Profesional universitario Oficina TIC deben disponer de los recursos necesarios para permitir la identificación de los medios de almacenamiento, la información contenida en ellos y la ubicación

física de los mismos para permitir un rápido y eficiente acceso a los medios que contienen la información resguardada.

- ✓ El Profesional universitario Oficina TIC deben llevar a cabo las pruebas de recuperación a las copias de respaldo, para así comprobar su integridad y posibilidad de uso en caso de ser necesario.

Normas dirigidas a: Todos los usuarios.

- ✓ Es responsabilidad de los usuarios de la plataforma tecnológica de la Corporación identificar la información crítica que debe ser respaldada y almacenarla de acuerdo con su nivel de clasificación en la partición de disco denominada “Datos”.

12.4. Política de control al software operativo

La Corporación Gilberto Echeverri Mejía, a través de El Profesional universitario Oficina TIC, establecerá procedimientos para controlar la instalación de software operativo, se cerciorará de contar con el soporte de los proveedores de dicho software y asegurará la funcionalidad de los sistemas de información que operan sobre la plataforma tecnológica cuando el software operativo es actualizado. **Normas de control al software operativo**

Normas dirigidas a: Profesional universitario Oficina TIC.

- ✓ El Profesional universitario Oficina TIC deben establecer responsabilidades y procedimientos para controlar la instalación del software operativo, que interactúen con el procedimiento de control de cambios existente en la Corporación.
- ✓ El Profesional universitario Oficina TIC deben asegurarse de que el software operativo instalado en la plataforma tecnológica de la Corporación cuenta con soporte de los proveedores.
- ✓ El Profesional universitario Oficina TIC deben conceder accesos temporales y controlados a los proveedores para realizar las actualizaciones sobre el software operativo, así como monitorear dichas actualizaciones.
- ✓ El Profesional universitario Oficina TIC deben validar los riesgos que genera la migración hacia nuevas versiones del software operativo. Se debe asegurar el correcto funcionamiento de sistemas de información y herramientas de software que se ejecutan sobre la plataforma tecnológica cuando el software operativo es actualizado.
- ✓ El Profesional universitario Oficina TIC deben establecer las restricciones y limitaciones para la instalación de software operativo en los equipos de cómputo de la Corporación.

Seguridad perimetral

La seguridad perimetral es uno de los métodos posibles de protección de la Red, basado en el establecimiento de recursos de seguridad en el perímetro externo de la red y a diferentes niveles. Esto permite definir niveles de confianza, permitiendo el acceso de determinados usuarios internos o externos a determinados servicios, y denegando cualquier tipo de acceso a otros.

Implementar soluciones lógicas y físicas que garanticen la protección de la información de la Corporación de posibles ataques internos o externos.

- ✓ Rechazar conexiones a servicios comprometidos
- ✓ Permitir sólo ciertos tipos de tráfico (p. ej. correo electrónico, http, https).
- ✓ Proporcionar un único punto de interconexión con el exterior.
- ✓ Redirigir el tráfico entrante a los sistemas adecuados dentro de la intranet (Red Interna).
- ✓ Ocultar sistemas o servicios vulnerables que no son fáciles de proteger desde Internet.
- ✓ Auditar el tráfico entre el exterior y el interior.
- ✓ La solución de seguridad perimetral debe ser controlada con un Firewall por Hardware (físico) que se encarga de controlar puertos y conexiones, es decir, de permitir el paso y el flujo de datos entre los puertos, ya sean clientes o servidores.
- ✓ El Profesional universitario Oficina TIC establecerán las reglas en el Firewall necesarias para bloquear, permitir o ignorar el flujo de datos entrante y saliente de la Red.
- ✓ El firewall debe bloquear las "conexiones extrañas" y no dejarlas pasar para que no causen problemas.
- ✓ El firewall debe controlar los ataques de "Denegación de Servicio" y controlar también el número de conexiones que se están produciendo, y en cuanto detectan que se establecen más de las normales desde un mismo punto bloquearlas y mantener el servicio a salvo.
- ✓ Controlar las aplicaciones que acceden a Internet para impedir que programas a los que no hemos permitido explícitamente acceso a Internet, puedan enviar información interna al exterior (tipo troyanos).
- ✓ La publicación de las aplicaciones diseñadas para llevar a cabo los procesos de La Corporación Gilberto Echeverri Mejía será llevada a cabo solo por El Profesional universitario Oficina TIC, previo análisis de seguridad y configuraciones necesarias.
- ✓ La habilitación de puertos de comunicación externos a la Corporación deberá pasar por previo análisis por parte de El Profesional universitario Oficina TIC, para así determinar los riesgos de seguridad, posibles ataques informáticos y soluciones.
- ✓ Se revisará diariamente el log de conexiones por medio de VPN.
- ✓ La configuración de los grupos de navegación solo será realizada por El Profesional universitario Oficina TIC.
- ✓ La decisión de incluir a un usuario a estos grupos de navegación será tomada por la dirección ejecutiva.

13. Políticas de seguridad en las comunicaciones

13.1. Política de gestión y aseguramiento de las redes de datos

La Corporación Gilberto Echeverri Mejía establecerá, a través de El Profesional universitario Oficina TIC, los mecanismos de control necesarios para proveer la disponibilidad de las redes de datos y de los servicios que dependen de ellas; así mismo, velará por que se cuente con los mecanismos de seguridad que protejan la integridad y la confidencialidad de la información que se transporta a través de dichas redes de datos.

De igual manera, propenderá por el aseguramiento de las redes de datos, el control del tráfico en dichas redes y la protección de la información reservada y restringida de la corporación.

13.1.1. Normas de gestión y aseguramiento de las redes de datos

Normas dirigidas a: Profesional universitario Oficina TIC.

- ✓ El Profesional universitario Oficina TIC deben adoptar medidas para asegurar la disponibilidad de los recursos y servicios de red de la Corporación.
- ✓ El Profesional universitario Oficina TIC deben implantar controles para minimizar los riesgos de seguridad de la información transportada por medio de las redes de datos.
- ✓ El Profesional universitario Oficina TIC deben mantener las redes de datos segmentadas por dominios, grupos de servicios, grupos de usuarios, ubicación geográfica o cualquier otra tipificación que se considere conveniente para la corporación.
- ✓ El Profesional universitario Oficina TIC deben establecer los estándares técnicos de configuración de los dispositivos de seguridad y de red de la plataforma tecnológica del instituto, acogiendo buenas prácticas de configuración segura.
- ✓ El Profesional universitario Oficina TIC deben identificar, justificar y documentar los servicios, protocolos y puertos permitidos por el instituto en sus redes de datos e inhabilitar o eliminar el resto de los servicios, protocolos y puertos.
- ✓ El Profesional universitario Oficina TIC deben velar por la confidencialidad de la información del direccionamiento y el enrutamiento de las redes de datos de la Corporación.

13.2. Política de uso del correo electrónico

La Corporación Gilberto Echeverri Mejía, entendiendo la importancia del correo electrónico como herramienta para facilitar la comunicación entre los vinculados, contratistas o terceras personas, proporcionará un servicio idóneo y seguro para la ejecución de las actividades que requieran el uso del correo electrónico, respetando siempre los principios de confidencialidad, integridad, disponibilidad y autenticidad de quienes realizan las comunicaciones a través de este medio.

13.2.1. Normas de uso del correo electrónico

Normas dirigidas a: Profesional universitario Oficina TIC.

- ✓ El Profesional universitario Oficina TIC deben generar y divulgar un procedimiento para la administración de cuentas de correo electrónico.
- ✓ El Profesional universitario Oficina TIC deben diseñar y divulgar las directrices técnicas para el uso de los servicios de correo electrónico.
- ✓ El Profesional universitario Oficina TIC deben proveer un ambiente seguro y controlado para el funcionamiento de la plataforma de correo electrónico.
- ✓ El Profesional universitario Oficina TIC deben establecer procedimientos e implantar controles que permitan detectar y proteger la plataforma de correo electrónico contra código malicioso que pudiera ser transmitido a través de los mensajes.
- ✓ El Profesional universitario Oficina TIC deben generar campañas para concientizar tanto los vinculados y contratistas, como a los terceros, respecto a las precauciones que deben adoptar en el intercambio de información sensible por medio del correo electrónico.

Normas dirigidas a: Todos los usuarios.

- ✓ La cuenta de correo electrónico asignada es de carácter individual; por consiguiente, ningún funcionario de la corporación o provisto por un tercero, bajo ninguna circunstancia debe utilizar una cuenta de correo que no sea la suya.
- ✓ Los mensajes y la información contenida en los correos electrónicos deben ser relacionados con el desarrollo de las labores y funciones de cada usuario en apoyo al objetivo misional de la Corporación. El correo institucional no debe ser utilizado para actividades personales.
- ✓ Los mensajes y la información contenida en los buzones de correo son propiedad de la Corporación y cada usuario, como responsable de su buzón, debe mantener solamente los mensajes relacionados con el desarrollo de sus funciones.
- ✓ Los usuarios de correo electrónico institucional tienen prohibido él envió de cadenas de mensajes de cualquier tipo, ya sea comercial, político, religioso, material audiovisual, contenido discriminatorio, pornografía y demás condiciones que degraden la condición humana y resulten ofensivas para los vinculados, contratistas o terceras personas.
- ✓ Todos los mensajes enviados deben respetar el estándar de formato e imagen corporativa definidos por la Corporación y deben conservar en todos los casos el mensaje legal corporativo de confidencialidad.
- ✓ Ningún usuario externo a la Corporación puede usar los servicios de correo electrónico proporcionado por la red institucional.

13.3. Política de uso adecuado de internet

La Corporación Gilberto Echeverri Mejía consciente de la importancia de Internet como una herramienta para el desempeño de labores, proporcionará los recursos necesarios para asegurar su disponibilidad a los usuarios que así lo requieran para el desarrollo de sus actividades diarias.

13.3.1. Normas de uso adecuado de internet

- ✓ Se debe generar campañas para concientizar tanto a los tanto a los vinculados, contratistas, como a terceros, respecto a las precauciones que deben tener en cuenta cuando utilicen el servicio de Internet.
- ✓ Todos los accesos a Internet tienen que ser realizados a través de los canales de acceso provistos por la Corporación.

Normas dirigidas a: Profesional universitario Oficina TIC.

- ✓ El Profesional universitario Oficina TIC deben proporcionar los recursos necesarios para la implementación, administración y mantenimiento requeridos para la prestación segura del servicio de Internet, bajo las restricciones de los perfiles de acceso establecidos.
- ✓ El Profesional universitario Oficina TIC deben diseñar e implementar mecanismos que permitan la continuidad o restablecimiento del servicio de Internet en caso de contingencia interna.
- ✓ El Profesional universitario Oficina TIC deben monitorear continuamente el canal o canales del servicio de Internet.

- ✓ El Profesional universitario Oficina TIC deben establecer procedimientos e implementar controles para evitar la descarga de software no autorizado, evitar código malicioso proveniente de Internet y evitar el acceso a sitios catalogados como restringidos.
- ✓ El Profesional universitario Oficina TIC deben generar registros de la navegación y los accesos de los usuarios a Internet, así como establecer e implantar procedimientos de monitoreo sobre la utilización del servicio de Internet.

Normas dirigidas a: Todos los usuarios.

- ✓ Los usuarios del servicio de Internet de la Corporación deben hacer uso del mismo en relación con las actividades laborales que así lo requieran.
- ✓ No está permitido el acceso a páginas relacionadas con pornografía, drogas, alcohol, webproxys, hacking y/o cualquier otra página que vaya en contra de la ética moral, las leyes vigentes o políticas establecidas en este documento.
- ✓ No está permitido la descarga, uso, intercambio y/o instalación de juegos, música, películas, protectores y fondos de pantalla, software de libre distribución, información y/o productos que de alguna forma atenten contra la propiedad intelectual de sus autores, o que contengan archivos ejecutables y/o herramientas que atenten contra la integridad, disponibilidad y/o confidencialidad de la infraestructura tecnológica (hacking), entre otros. La descarga, uso, intercambio y/o instalación de información audiovisual (videos e imágenes) utilizando sitios públicos en Internet debe ser autorizada por el jefe respectivo y El Profesional universitario Oficina TIC.
- ✓ No está permitido el intercambio no autorizado de información de propiedad de la Corporación, de sus clientes y/o de sus vinculados, con terceros.

Restricciones/prohibiciones de acceso a Internet

- ✓ El uso de programas para compartir archivos (Peer to Peer).
- ✓ El acceso a páginas con cualquier tipo de contenido explícito de pornografía.
- ✓ El uso de sitios de videos en línea o en tiempo real.
- ✓ No se permite la conexión a estaciones de radio por Internet.
- ✓ Uso de JUEGOS "on line" en la red.

14. Políticas de adquisición, desarrollo y mantenimiento de sistemas de información

14.1. Política para el establecimiento de requisitos de seguridad

La Corporación Gilberto Echeverri Mejía asegurará que el software adquirido y desarrollado tanto al interior de la Entidad, como por terceros, cumpla con los requisitos de seguridad y calidad establecidos. El Profesional universitario Oficina TIC incluirán requisitos de seguridad en la definición de requerimientos y, posteriormente se asegurarán de que estos se encuentren generados a cabalidad durante las pruebas realizadas sobre los desarrollos del software construido.

14.1.1. Normas para el establecimiento de requisitos de seguridad

Normas dirigidas a: Profesional universitario Oficina TIC y usuarios finales.

- ✓ El Profesional universitario Oficina TIC deben establecer metodologías para el desarrollo de software, que incluyan la definición de requerimientos de seguridad y las buenas prácticas de desarrollo seguro, con el fin de proporcionar a los desarrolladores una visión clara de lo que se espera.
- ✓ Los usuarios finales, en acompañamiento con El Profesional universitario Oficina TIC, deben establecer las especificaciones de adquisición o desarrollo de sistemas de información, considerando requerimientos de seguridad de la información.
- ✓ Los usuarios finales deben definir qué información sensible puede ser eliminada de sus sistemas y solicitar que estos soporten la eliminación de dicha información, como es el caso de los datos personales o financieros, cuando estos ya no son requeridos.
- ✓ El Profesional universitario Oficina TIC deben liderar la definición de requerimientos de seguridad de los sistemas de información, teniendo en cuenta aspectos como la estandarización de herramientas de desarrollo, controles de autenticación, controles de acceso y arquitectura de aplicaciones.

Normas dirigidas a: Desarrolladores (internos o externos).

- ✓ Los desarrolladores deben documentar los requerimientos establecidos y definir la arquitectura de software más conveniente para cada sistema de información que se quiera desarrollar, de acuerdo con los requerimientos de seguridad y los controles deseados.
- ✓ Los desarrolladores deben certificar que todo sistema de información adquirido o desarrollado utilice herramientas de desarrollo licenciadas y reconocidas en el mercado.
- ✓ Los desarrolladores deben deshabilitar las funcionalidades de completar automáticamente en formularios de solicitud de datos que requieran información sensible.
- ✓ Los desarrolladores deben establecer el tiempo de duración de las sesiones activas de las aplicaciones, terminándolas una vez se cumpla este tiempo.
- ✓ Los desarrolladores deben asegurar que no se permitan conexiones recurrentes a los sistemas de información construidos con el mismo usuario.
- ✓ Los desarrolladores deben utilizar los protocolos sugeridos por El Profesional universitario Oficina TIC en los aplicativos desarrollados.
- ✓ Los desarrolladores deben certificar la transmisión de información relacionada con pagos o transacciones en línea a los operadores encargados, por medio de canales seguros.

14.2. Política de desarrollo seguro, realización de pruebas y soporte de los sistemas

La Corporación Gilberto Echeverri Mejía velará porque el desarrollo interno o externo de los sistemas de información cumpla con los requerimientos de seguridad esperados, con las buenas prácticas para desarrollo seguro de aplicativos, así como con metodologías para la realización de pruebas de aceptación y seguridad al software desarrollado. Además, se asegurará que todo software desarrollado o adquirido, interna o externamente cuenta con el nivel de soporte que requiere la Entidad.

14.2.1. Normas de desarrollo seguro, realización de pruebas y soporte de los sistemas

Normas dirigidas a: Usuarios finales.

- ✓ Los usuarios finales son responsables de realizar las pruebas para asegurar que cumplen con los requerimientos de seguridad establecidos antes del paso a producción de los sistemas, utilizando metodologías establecidas para este fin, documentado las pruebas realizadas y aprobando los pasos a producción. Estas pruebas deben realizarse por entrega de funcionalidades nuevas, por ajustes de funcionalidad o por cambios sobre la plataforma tecnológica en la cual funcionan los aplicativos.

Normas dirigidas a: Profesional universitario Oficina TIC.

- ✓ El Profesional universitario Oficina TIC deben implantar los controles necesarios para asegurar que las migraciones entre los ambientes de desarrollo, pruebas y producción han sido aprobadas, de acuerdo con el procedimiento de control de cambios.
- ✓ El Profesional universitario Oficina TIC deben asegurase que los sistemas de información adquiridos o desarrollados por terceros cuenten con un acuerdo de licenciamiento el cual debe especificar las condiciones de uso del software y los derechos de propiedad intelectual.
- ✓ El Profesional universitario Oficina TIC deben generar metodologías para la realización de pruebas al software desarrollado, que contengan pautas para la selección de escenarios, niveles, tipos, datos de pruebas y sugerencias de documentación.
- ✓ El Profesional universitario Oficina TIC deben asegurar que la plataforma tecnológica, las herramientas de desarrollo y los componentes de cada sistema de información estén actualizados con todos los parches generados para las versiones en uso y que estén ejecutando la última versión aprobada del sistema.

Normas dirigidas a: Desarrolladores (internos o externos).

- ✓ Los desarrolladores de los sistemas de información deben considerar las buenas prácticas y lineamientos de desarrollo seguro durante el ciclo de vida de los mismos, pasando desde el diseño hasta la puesta en marcha.
- ✓ Los desarrolladores deben proporcionar un nivel adecuado de soporte para solucionar los problemas que se presenten en el software aplicativo de la Corporación; dicho soporte debe contemplar tiempos de respuesta aceptables.
- ✓ Los desarrolladores deben construir los aplicativos de tal manera que efectúen las validaciones de datos de entrada y la generación de los datos de salida de manera confiable, utilizando rutinas de validación centralizadas y estandarizadas.
- ✓ Los desarrolladores deben asegurar que los sistemas de información construidos validen la información suministrada por los usuarios antes de procesarla, teniendo en cuenta aspectos como: tipos de datos, rangos válidos, longitud, listas de caracteres aceptados, caracteres considerados peligrosos y caracteres de alteración de rutas, entre otros.
- ✓ Los desarrolladores deben suministrar opciones de desconexión o cierre de sesión de los aplicativos (logout) que permitan terminar completamente con la sesión o conexión asociada, las cuales deben encontrarse disponibles en todas las páginas protegidas por autenticación.
- ✓ Los desarrolladores deben asegurar el manejo de operaciones sensibles o críticas en los aplicativos desarrollados permitiendo el uso de dispositivos adicionales como tokens o el ingreso de parámetros adicionales de verificación.

- ✓ Los desarrolladores deben asegurar que los aplicativos proporcionen la mínima información de la sesión establecida, almacenada en cookies y complementos, entre otros.
- ✓ Los desarrolladores deben garantizar que no se divulgue información sensible en respuestas de error, incluyendo detalles del sistema, identificadores de sesión o información de las cuentas de usuarios; así mismo, deben implementar mensajes de error genéricos.
- ✓ Los desarrolladores deben remover todas las funcionalidades y archivos que no sean necesarios para los aplicativos, previo a la puesta en producción.
- ✓ Los desarrolladores deben prevenir la revelación de la estructura de directorios de los sistemas de información construidos.
- ✓ Los desarrolladores deben remover información innecesaria en los encabezados de respuesta que se refieran a los sistemas operativos y versiones del software utilizado.
- ✓ Los desarrolladores deben evitar incluir las cadenas de conexión a las bases de datos en el código de los aplicativos. Dichas cadenas de conexión deben estar en archivos de configuración independientes, los cuales se recomienda que estén cifrados.
- ✓ Los desarrolladores deben certificar el cierre de la conexión a las bases de datos desde los aplicativos tan pronto como estas no sean requeridas.
- ✓ Los desarrolladores deben desarrollar los controles necesarios para la transferencia de archivos, como exigir autenticación, vigilar los tipos de archivos a transmitir, almacenar los archivos transferidos en repositorios destinados para este fin o en bases de datos, eliminar privilegios de ejecución a los archivos transferidos y asegurar que dichos archivos solo tengan privilegios de lectura.
- ✓ Los desarrolladores deben proteger el código fuente de los aplicativos construidos, de tal forma de que no pueda ser descargado ni modificado por los usuarios.
- ✓ Los desarrolladores deben asegurar que no se permite que los aplicativos desarrollados ejecuten comandos directamente en el sistema operativo.

15. Procedimiento de notificación, gestión y respuesta ante incidencias

La Corporación Gilberto Echeverri Mejía establece un procedimiento de notificación, gestión y respuesta de incidencias con el fin de garantizar la confidencialidad, disponibilidad e integridad de la información contenida en las bases de datos que están bajo su responsabilidad.

Todos los usuarios y responsables de procedimientos, así como cualquier persona que tenga relación con el almacenamiento, tratamiento o consulta de las bases de datos recogidas en este documento, deben conocer el procedimiento para actuar en caso de incidencia.

El procedimiento de notificación, gestión y respuesta ante incidencias es el siguiente:

- ✓ Cuando una persona tenga conocimiento de una incidencia que afecte o pueda afectar la confidencialidad, disponibilidad e integridad de la información protegida de la entidad deberá comunicarlo, de manera inmediata, a los responsables de seguridad, describiendo detalladamente el tipo de incidencia producida, e indicando las personas que hayan podido tener relación con la incidencia, la fecha y hora en que se ha producido, la persona que notifica la incidencia, la persona a quién se le comunica y los efectos que ha producido.

- ✓ Una vez comunicada la incidencia ha de solicitar al responsable de seguridad correspondiente un acuse de recibo en el que conste la notificación de la incidencia con todos los requisitos enumerados anteriormente.

La Corporación Gilberto Echeverri Mejía, creará un registro de incidencias que debe contener: el tipo de incidencia, fecha y hora de la misma, persona que la notifica, persona a la que se le comunica, efectos de la incidencia y medidas correctoras cuando corresponda. Este registro es gestionado por el responsable de seguridad de la base de datos.

Asimismo, debe implementarse los procedimientos para la recuperación de los datos, indicando quien ejecuta el proceso, los datos restaurados y, en su caso, los datos que han requerido ser grabados manualmente en el proceso de recuperación.

16. Políticas de cumplimiento

Funciones y obligaciones del personal

Todas las personas que intervienen en el almacenamiento, tratamiento, consulta o cualquier otra actividad relacionada con los datos personales y sistemas de información de La Corporación Gilberto Echeverri Mejía, deben actuar de conformidad a las funciones y obligaciones recogidas en el presente documento.

La Corporación Gilberto Echeverri Mejía, debe informar a su personal de las medidas y normas de seguridad que compete al desarrollo de sus funciones, así como de las consecuencias de su incumplimiento, mediante cualquier medio de comunicación que garantice su recepción o difusión (correo electrónico, carteleras, mensajes de WhatsApp de anuncios, etc.). De igual modo, debe poner a disposición del personal la presente para que puedan conocer la normativa de seguridad de la entidad y sus obligaciones en esta materia en función del cargo que ocupan.

La Corporación Gilberto Echeverri Mejía, cumple con el deber de información con su inclusión de acuerdos de confidencialidad y deber de secreto que subscribe.

Las funciones y obligaciones del personal de La Corporación Gilberto Echeverri Mejía se definen, con carácter general, según el tipo de actividad que desarrollan dentro de la entidad y, específicamente, por el contenido de esta política. La lista de usuarios y perfiles con acceso a los recursos protegidos están recogidos en el "Anexo 2. Roles y Responsabilidades". Con carácter general, cuando un usuario trate documentos o soportes que contengan datos personales tiene el deber de custodiarlos, así como de vigilar y controlar que personas no autorizadas no puedan tener acceso a ellos.

El incumplimiento de las obligaciones y medidas de seguridad establecidas en esta política por parte del personal al servicio de La Corporación Gilberto Echeverri Mejía es sancionable de acuerdo a la normativa aplicable a la relación jurídica existente entre el usuario y la entidad.

Las funciones y obligaciones de los usuarios de las bases de datos personales bajo responsabilidad de la Corporación son las siguientes:

- ✓ Deber de secreto: Aplica a todas las personas que, en el desarrollo de su profesión, actividad o trabajo, acceden a bases de datos personales y vincula tanto a usuarios como a prestadores de servicios contratados; en cumplimiento de este deber, los usuarios de la entidad no pueden comunicar o relevar a terceras personas, datos que manejen o de los que tengan conocimiento en el desempeño de sus actividades o funciones y deben velar por la confidencialidad e integridad de estos.
- ✓ Funciones de control y autorizaciones delegadas: El responsable del tratamiento puede delegar el tratamiento de datos a terceros, para que actúe como encargado del tratamiento, mediante un contrato de transmisión de datos, los cuales deberán cumplir la presente política.

Obligaciones relacionadas con las medidas de seguridad implantadas:

- ✓ Acceder a las bases de datos con la debida autorización y cuando sea necesario para el ejercicio de sus funciones o actividades.
- ✓ No revelar información a terceras personas ni a usuarios no autorizados.
- ✓ Observar las normas de seguridad y trabajar para mejorarlas.
- ✓ No realizar acciones que supongan un peligro para la seguridad de la información.
- ✓ No sacar información de las instalaciones de la organización sin la debida autorización.

Uso de recursos y materiales de trabajo: Debe estar orientado al ejercicio de las funciones o actividades asignadas. No se autoriza el uso de estos recursos y materiales para fines personales o ajenos a las tareas o actividades asignadas. Cuando, por motivos justificados de trabajo, sea necesaria la salida de dispositivos periféricos o extraíbles, deberá comunicarse al responsable de seguridad correspondiente que podrá autorizarla y, en su caso, registrarla.

Uso de impresoras, escáneres y otros dispositivos de copia: Cuando se utilicen este tipo de dispositivos debe procederse a la recogida inmediata de las copias, evitando dejar éstas en las bandejas de los mismos.

Obligación de notificar incidencias: Los usuarios tienen la obligación de notificar las incidencias de las que tenga conocimiento a los responsables de seguridad, quienes se encargarán de su gestión y resolución. Algunos ejemplos de incidencias son: la caída del sistema de seguridad informática que permita el acceso a los datos personales a personas no autorizadas, el intento no autorizado de la salida de un documento o soporte, la pérdida de datos o la destrucción total o parcial de soportes, el cambio de ubicación física de bases de datos, el conocimiento por terceras personas de contraseñas, la modificación de datos por personal no autorizado, etc.

Deber de custodia de los soportes utilizados: Obliga al usuario autorizado a vigilar y controlar que las personas no autorizadas accedan a la información contenida en los soportes. Los soportes que contienen bases de datos deben identificar el tipo de información que contienen mediante un

sistema de etiquetado y ser inventariados. Cuando la información esté clasificada con nivel de seguridad sensible el sistema de etiquetado solo debe ser comprensible para los usuarios autorizados acceder a dicha información.

Responsabilidad sobre los terminales de trabajo y portátiles: Cada usuario es responsable de su propio terminal de trabajo; cuando esté ausente de su puesto, debe bloquear dicho terminal (ej. protector de pantalla con contraseña) para impedir la visualización o el acceso a la información que contiene; y tiene el deber de apagar el terminal al finalizar la jornada. Asimismo, los ordenadores portátiles han de estar controlados en todo momento para evitar su pérdida o sustracción.

Uso limitado de Internet y correo electrónico: El envío de información por vía electrónica y el uso de Internet por parte del personal está limitado al desempeño de sus actividades en la entidad.

Salvaguarda y protección de contraseñas: Las contraseñas proporcionadas a los usuarios son personales e intransferibles, por lo que se prohíbe su divulgación o comunicación a personas no autorizadas. Cuando el usuario accede por primera vez con la contraseña asignada es necesario que la cambie. Cuando sea necesario restaurar la contraseña, el usuario debe comunicarlo al administrador del sistema.

Copias de respaldo y recuperación de datos: Debe realizarse copia de seguridad de toda la información de bases de datos personales de la entidad.

Deber de archivo y gestión de documentos y soportes: Los documentos y soportes deben de ser debidamente archivados con las medidas de seguridad establecidas en el numeral 4 de la presente política

17. Bases de datos y sistemas de información

Las bases de datos almacenadas y tratadas por La Corporación Gilberto Echeverri Mejía se recogen en el “Anexo 1. Información de Bases de datos”, en el cual se presentan las siguientes características de cada una de ellas:

- ✓ Nombre de la Base de datos
- ✓ Finalidades
- ✓ Información contenida Nivel de Seguridad Sistema de tratamiento Cantidad de Titulares
- ✓ Origen y procedencia de los datos Colectivo o categoría de Titulares Transmisión de datos Responsables de Seguridad Control de Acceso Físico
- ✓ Gestión Documental Control de Acceso Lógico
- ✓ Copias de Respaldo y Procedimiento de Recuperación Sistema de Identificación y Autenticación.
- ✓ Registro de Acceso a los Documentos

El nombramiento de los responsables de seguridad no exonera al responsable del tratamiento o encargado del tratamiento de sus obligaciones.

La Corporación Gilberto Echeverri Mejía identifica en el “Anexo 1”.

Información de Bases de datos” a los encargados del tratamiento, así como las condiciones del encargo. Los encargados del tratamiento deberán cumplir con las funciones y obligaciones relacionadas con las medidas en materia de seguridad recogidas en la presente política.

18. Política de Ambientes de la Corporación

Para cada una de las plataformas que se tienen en la corporación se definen una política de uso, en la cual se describen criterios de actualización y/o modificación, responsables, control de acceso, usuarios, roles y responsabilidades, diferentes entornos funcionamiento y criterios de auditorias

La Corporación Gilberto Echeverri Mejía identifica la política de uso de las plataformas en el “Anexo 3. Politica de ambientes”.

19. Medidas para el transporte, destrucción y reutilización de documentos y soportes

Cuando corresponda desechar cualquier documento (original, copia o reproducción) o soporte que contenga datos personales debe procederse a su destrucción o borrado, a través de la implementación de medidas orientadas a evitar el acceso o recuperación de la información contenida en dicho documento o soporte.

Cuando se lleve a cabo el traslado físico de documentos o soportes deben adoptar las medidas necesarias para impedir el acceso indebido, la manipulación, la sustracción o la pérdida de la información. El traslado de soportes que contengan datos personales se realiza cifrando la información, o utilizando cualquier otro mecanismo que garantice que no se manipule ni se acceda a la misma.

Los datos contenidos en dispositivos portátiles deben estar cifrados cuando se hallen fuera de las instalaciones que están bajo control de La Corporación Gilberto Echeverri Mejía, Cuando no sea posible el cifrado, se debe evitar el tratamiento de datos personales mediante este tipo de dispositivos; sin embargo, se podrá proceder al tratamiento cuando sea estrictamente necesario, adoptando para ello medidas de seguridad que tengan en cuenta los riesgos e incluyéndolas en la presente política.

20. Cumplimiento

Los diferentes aspectos contemplados en esta política son de obligatorio cumplimiento para todos los vinculados, contratistas o terceras personas. En caso de que se violen las políticas de seguridad ya sea de forma intencional o por negligencia, la Corporación tomará las acciones disciplinarias y legales correspondientes.

21. Disposición final

La presente política de seguridad rige a partir de la fecha de su publicación, se divulgará a través del portal institucional, y estará sujeto actualizaciones en la medida en que se modifiquen o se dicten nuevas disposiciones legales sobre la materia.

En constancia firman:

Jessika del Carmen Hinestroza
Profesional especializada
Jurídica

Juan Camilo Diaz Valderrama
Profesional universitario Oficina
TIC

RODRIGO DE JESUS ARDILA VARGAS

Director Ejecutivo.