PLAN DE TRATAMIENTO RIESGO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN Y PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

CONTRALORIA DISTRITAL DE CARTAGENA DE INDIAS

ALCIBALDO ENRIQUE SEGUNDO CRUZ LEON

CONTRALOR DISTRITAL DE CARTAGENA DE INDIAS DESIGNADO

URIEL ANGEL PEREZ MARQUEZ

SECRETARIO GENERAL

MANUEL CASSIANI CAÑATE

JAY MONTESINO UPARELA

PROCESO DE TECNOLOGIAS DE LA INFORMACION Y LAS COMUNICACIONES

Contraloría
Distrital de Cartagena de Indias

CONTENIDO

INTRODUCCIÓN

Objetivo General: Proporcionar una descripción completa del propósito, el alcance y la estructura del plan de seguridad, riesgo y privacidad de la información, estableciendo su relevancia para la Contraloría Distrital de Cartagena de Indias en su rol como entidad pública responsable de la vigilancia y control fiscal del distrito de Cartagena de Indias.

Contexto Institucional y Necesidad del Plan

La Contraloría Distrital de Cartagena de Indias tiene el mandato de ejercer control y vigilancia sobre el manejo de los recursos públicos y bienes del distrito, verificando que su uso esté orientado al beneficio de la ciudadanía y que cumpla con los principios de legalidad, transparencia y eficiencia. En un entorno donde la tecnología y la digitalización son fundamentales para la gestión pública, la seguridad de la información se convierte en un aspecto crucial para mantener la integridad y la confianza en las operaciones de la Contraloría Distrital de Cartagena de Indias.

A medida que la entidad maneja y almacena datos sensibles, tanto de funcionarios como de ciudadanos y de otros actores vinculados a la gestión fiscal, surgen riesgos asociados con el tratamiento y la protección de dicha información. Estos riesgos incluyen posibles amenazas cibernéticas, accesos no autorizados, pérdida de datos y violaciones de la privacidad, situaciones que podrían comprometer tanto la seguridad como la misión de la Contraloría Distrital de Cartagena de Indias.

Justificación del Plan

Para enfrentar estos desafíos, el plan de seguridad, riesgo y privacidad de la información busca dotar a la Contraloría de una estructura formal y coherente para la gestión de los riesgos de seguridad, protección de datos personales y cumplimiento normativo. Esto asegura que cada proceso y sistema de la entidad tenga mecanismos de protección que garanticen:

- La confidencialidad de la información, permitiendo que solo personal autorizado acceda a los datos sensibles.
- La integridad de los datos, para que la información no sea alterada de forma no autorizada.
- La disponibilidad de los sistemas y la información, asegurando que los servicios de la Contraloría puedan continuar operando y sean accesibles en todo momento.

Objetivos Específicos del Plan

El plan se centra en cumplir con una serie de objetivos específicos que contribuyen directamente a la misión de la Contraloría y a la protección de sus activos de información:

1. Proteger la información institucional y los datos personales: Implementar controles técnicos y administrativos que garanticen la seguridad de la información en todas sus formas, protegiendo los datos de la Contraloría contra amenazas internas y externas.
2. Evaluar y gestionar los riesgos de seguridad: Establecer un sistema de gestión de riesgos que permita identificar, evaluar y mitigar los riesgos asociados con la infraestructura tecnológica y los procesos de la Contraloría Distrital de Cartagena de Indias.

3. Cumplir con las normativas y estándares nacionales e internacionales: Asegurar que todos los procesos de gestión de la información de la Contraloría Distrital de Cartagena de Indias cumplan con las normativas aplicables en Colombia, especialmente en protección de datos personales, ciberseguridad y transparencia.
4. Promover una cultura de seguridad y conciencia en todo el personal: Fortalecer el conocimiento y la concienciación del personal en prácticas de seguridad de la información, asegurando que cada funcionario conozca su rol y responsabilidades en la protección de los activos de información.
5. Implementar medidas para la continuidad operativa y recuperación ante desastres: Desarrollar planes de continuidad y recuperación que permitan a la Contraloría Distrital de Cartagena de Indias responder rápidamente ante eventos críticos o emergencias, garantizando la resiliencia de los sistemas y la rápida restauración de las operaciones.

Alcance del Plan

El alcance del plan abarca todos los componentes necesarios para asegurar la protección de la información y la infraestructura de la Contraloría, incluyendo:

- Activos de Información y Sistemas de la Entidad: La seguridad cubre todos los activos de información gestionados en la Contraloría, como sistemas de información de control fiscal, plataformas de comunicación interna, bases de datos, y cualquier recurso de TI utilizado para el desempeño de sus funciones.
- Todo el Personal y Colaboradores de la Contraloría: Involucra a todos los funcionarios, contratistas, consultores y cualquier personal en misión que tenga acceso a los activos de información de la Contraloría. Incluye la implementación de controles de acceso, políticas de uso adecuado y sensibilización en buenas prácticas de seguridad.
- Infraestructura Tecnológica y Redes de Comunicación: Protege todos los sistemas de TI, equipos de red, servidores, estaciones de trabajo y dispositivos móviles utilizados para el manejo y procesamiento de la información de la Contraloría. También se incluye la protección de las redes internas y externas de comunicación.
- Proveedores y Terceros con Acceso a Información de la Contraloría: Incluye a todos los proveedores de servicios tecnológicos y terceros que, de manera directa o indirecta, tengan acceso a la infraestructura o a la información de la entidad. Esto implica establecer acuerdos de confidencialidad, controles de acceso y evaluaciones de seguridad.

Principios Rectores del Plan

Los principios rectores establecen la base ética y normativa sobre la cual se implementa el plan de seguridad, riesgo y privacidad de la información:

1. Legalidad y Transparencia: Cumplimiento estricto de las leyes y regulaciones de Colombia en materia de protección de datos y seguridad de la información, asegurando que todas las prácticas de seguridad sean transparentes y estén debidamente documentadas.

2. Confidencialidad: Compromiso de asegurar que la información sensible esté protegida contra accesos no autorizados,
   garantizando que solo las personas autorizadas puedan acceder a dicha información.
3. Responsabilidad y Rendición de Cuentas: Cada funcionario y contratista de la Contraloría es responsable de la seguridad de la información que maneja y debe cumplir con las políticas establecidas en el plan.
4. Minimización y Uso Responsable de la Información: Recolección y tratamiento de la mínima cantidad de información necesaria para el cumplimiento de las funciones de la Contraloría, limitando su uso a los fines definidos y autorizados.
5. Prevención y Proactividad: Fomentar un enfoque preventivo en el manejo de riesgos de seguridad y privacidad, implementando controles y políticas que reduzcan la probabilidad de incidentes y permitan una respuesta ágil y oportuna en caso de que ocurran.

Estructura del Plan

El plan está estructurado en diversas unidades temáticas, cada una enfocada en un aspecto fundamental de la seguridad de la información y la privacidad, permitiendo una gestión integral y enfocada en áreas críticas de protección. A continuación, se describe brevemente la estructura del plan:

1. Marco Normativo y de Cumplimiento
   Define las leyes, normativas y estándares nacionales e internacionales que rigen la seguridad de la información y la protección de datos en la Contraloría.
2. Gestión de Activos de Información
   Identifica y clasifica los activos de información, asegurando su protección en función de su criticidad y sensibilidad.
3. Evaluación y Gestión de Riesgos
   Establece un sistema de evaluación de riesgos para identificar amenazas y mitigar el impacto potencial en los activos de información.
4. Protección de la Confidencialidad, Integridad y Disponibilidad
   Describe los controles de seguridad implementados para garantizar la confidencialidad, integridad y disponibilidad de los datos y sistemas críticos.
5. Gestión de Incidentes de Seguridad
   Establece un proceso para la detección, respuesta y registro de incidentes de seguridad, minimizando su impacto en las operaciones.
6. Capacitación y Conciencia en Seguridad
   Promueve la capacitación y sensibilización continua del personal sobre las políticas y prácticas de seguridad.
7. Protección de Datos Personales y Privacidad
   Define los procedimientos para el tratamiento adecuado y seguro de los datos personales, en cumplimiento con la Ley 1581 de 2012.
8. Cumplimiento Normativo y Auditoría
   Establece auditorías internas y externas para verificar el cumplimiento con los controles de seguridad y las políticas internas.

9. Gestión de Incumplimientos y Acciones Correctivas
   Incluye procedimientos para identificar y corregir incumplimientos
   de seguridad y para tomar acciones disciplinarias en caso de violaciones de las políticas.
10. Continuidad Operativa y Recuperación ante Desastres
    Describe los planes y medidas necesarias para mantener la operatividad de la Contraloría en situaciones de crisis o desastres.
11. Evaluación y Mejora Continua de la Seguridad de la Información
    Detalla los procesos de evaluación y mejora continua de la seguridad de la información, adaptándose a los cambios en el entorno de amenazas y requisitos normativos.

Beneficios del Plan para la Contraloría Distrital

La implementación de este plan trae múltiples beneficios para la Contraloría, fortaleciendo su capacidad de operar de manera segura y en cumplimiento con sus responsabilidades:

- Mayor Resiliencia ante Amenazas: La Contraloría puede responder rápidamente a incidentes y minimizar los efectos adversos sobre sus sistemas y datos.
- Protección de la Privacidad y Cumplimiento Normativo: El plan garantiza que la entidad cumpla con las normativas de protección de datos y transparencia, evitando sanciones y fortaleciendo la confianza ciudadana.
- Optimización de Recursos y Reducción de Costos por Incidentes: Al prevenir riesgos, se optimizan los recursos y se reducen los costos asociados con la respuesta y recuperación de incidentes.
- Cultura de Seguridad y Responsabilidad en el Personal: La capacitación y concienciación constante del personal promueve una cultura de responsabilidad, donde cada empleado asume un rol activo en la protección de la información de la entidad.

MARCO NORMATIVO Y DE CUMPLIMIENTO EN SEGURIDAD Y PRIVACIDAD

Objetivo General: Establecer los lineamientos legales y normativos que guían la seguridad de la información y la protección de datos personales en la Contraloría Distrital de Cartagena de Indias, asegurando el cumplimiento con las regulaciones nacionales y los estándares internacionales pertinentes para fortalecer la confianza pública y la transparencia en la gestión de la información.

Importancia del Cumplimiento Normativo

Como entidad pública responsable de la vigilancia y control fiscal en el Distrito de Cartagena de Indias, la Contraloría tiene la obligación de cumplir con un marco normativo riguroso que asegura la transparencia y la protección de la información. La información gestionada por la Contraloría, que incluye datos de ciudadanos, entidades públicas y otros actores vinculados a la gestión de recursos públicos, requiere altos estándares de protección para evitar su mal uso, pérdida o vulneración.

El cumplimiento normativo garantiza que la Contraloría no solo actúe dentro del marco legal colombiano, sino que también fortalezca la confianza ciudadana y minimice los riesgos de sanciones, reputacionales y de seguridad que podrían afectar su funcionamiento. Este marco regula cómo se recopila, almacena, usa y elimina la información, lo cual es clave para asegurar que las prácticas de la entidad estén alineadas con los derechos de los titulares de los datos y con la misión de la Contraloría.

Normativa Nacional en Seguridad de la Información y Protección de Datos Personales
En el contexto colombiano, varias leyes y decretos regulan el manejo seguro y la protección de datos personales y de información sensible en el sector público. La Contraloría Distrital de Cartagena de Indias debe cumplir con las siguientes normativas:

1. Ley 1581 de 2012 (Ley de Protección de Datos Personales):
    - La Ley 1581 establece los principios y derechos fundamentales para la protección de datos personales en Colombia. Esta ley asegura que cualquier tratamiento de datos personales cuente con la autorización explícita del titular y que se respeten los derechos de acceso, rectificación, cancelación y oposición (derechos ARCO).
    - Obligaciones de la Contraloría: Implementar políticas claras para el tratamiento de datos, obtener el consentimiento informado de los titulares, aplicar medidas de seguridad para proteger la integridad y confidencialidad de los datos, y establecer procedimientos para el ejercicio de los derechos ARCO.
2. Decreto 1377 de 2013 (Reglamentación de la Ley 1581):
    - Este decreto complementa la Ley 1581 y establece requisitos específicos, como la necesidad de políticas de privacidad claras, la definición de los encargados y responsables del tratamiento de datos y el mantenimiento de registros de datos personales.
    - Obligaciones de la Contraloría: Contar con una política de tratamiento de datos personales, designar un responsable del tratamiento de datos y asegurar que los encargados externos, como proveedores de servicios, también cumplan con estas disposiciones.
3. Ley 1712 de 2014 (Ley de Transparencia y Acceso a la Información Pública):
    - Esta ley promueve la transparencia en la administración pública y el derecho de los ciudadanos a acceder a la información en poder de las entidades públicas. Además, establece obligaciones de publicación de información relevante y el derecho de acceso a la información pública sin necesidad de justificación.
    - Obligaciones de la Contraloría: Publicar y poner a disposición de los ciudadanos información relevante de manera proactiva y accesible, asegurando que la divulgación no comprometa la confidencialidad de datos personales o información sensible.
4. Decreto 1081 de 2015 (Decreto Único Reglamentario del Sector Presidencia de la República):

- Este decreto unifica la normativa en cuanto a transparencia y acceso a la información pública, reforzando
  la obligación de las entidades públicas de ser accesibles y transparentes con la información de carácter público, respetando los límites establecidos para proteger los datos personales y la seguridad de la información.
- Obligaciones de la Contraloría: Mantener un portal de transparencia, establecer un procedimiento de solicitud de acceso a la información y realizar una clasificación adecuada para proteger los datos confidenciales.

5. Ley 1266 de 2008 (Ley de Habeas Data Financiero):
   - Esta ley regula el manejo de datos personales en los sistemas de información de crédito. Aunque se enfoca principalmente en el sector financiero, establece pautas sobre la administración de datos sensibles y la protección de los derechos de los titulares.
   - Obligaciones de la Contraloría: Asegurar que cualquier dato financiero o sensible manejado por la entidad cumpla con los principios de confidencialidad, exactitud y actualización permanente de la información.

Estándares Internacionales y Buenas Prácticas en Seguridad de la Información
Además de las normativas nacionales, la Contraloría Distrital de Cartagena de Indias se adhiere a estándares internacionales para fortalecer su gestión de seguridad de la información y alinearse con prácticas globales de protección de datos:

1. ISO/IEC 27001:2022 (Sistema de Gestión de Seguridad de la Información):
   a. La ISO 27001 es un estándar reconocido globalmente que establece un marco para implementar, mantener y mejorar un sistema de gestión de seguridad de la información (SGSI). Este estándar ayuda a identificar y mitigar riesgos de seguridad, asegurando un enfoque sistemático para la protección de la información.
   b. Aplicación en la Contraloría: Implementar controles y políticas basados en el estándar ISO 27001 para gestionar los riesgos de seguridad y proteger los datos de la entidad y de los ciudadanos. Esta norma permite a la Contraloría seguir una metodología de mejora continua en la gestión de seguridad.
2. ISO/IEC 27701:2019 (Gestión de la Privacidad de la Información):
   a. Este estándar complementa la ISO 27001 al ofrecer un marco específico para la gestión de la privacidad de la información, ayudando a las organizaciones a cumplir con los requisitos de privacidad y protección de datos.
   b. Aplicación en la Contraloría: Alinear las políticas de privacidad de datos con los requisitos del estándar ISO 27701, garantizando que la gestión de datos personales se realice con una protección adecuada y que se respeten los derechos de los titulares.
3. ISO/IEC 27018 (Protección de Datos en la Nube):

   a. ISO 27018 es una extensión de la ISO 27001 enfocada en la protección de datos personales en entornos de computación en la nube, asegurando que las organizaciones que utilizan servicios en la nube mantengan altos niveles de seguridad y privacidad.
   b. Aplicación en la Contraloría: Adoptar políticas y controles para proteger la información en la nube, especialmente si la entidad almacena o procesa datos personales de manera remota, aplicando medidas de cifrado y autenticación estrictas.
4. NIST Framework for Improving Critical Infrastructure Cybersecurity:
   a. Este marco, desarrollado por el Instituto Nacional de Estándares y Tecnología de los EE.UU. (NIST), proporciona un enfoque para gestionar y reducir riesgos cibernéticos en infraestructura crítica.
   b. Aplicación en la Contraloría: Usar este marco como referencia para fortalecer la infraestructura de seguridad de la información, especialmente en los sistemas que soportan funciones críticas y requieren una protección elevada contra ciberamenazas.

Directrices de Entidades Regulatorias y Órganos de Control en Colombia

Para una adecuada implementación de las normativas de seguridad y protección de datos, la Contraloría también debe seguir las directrices de las siguientes entidades reguladoras y de control:

1. Superintendencia de Industria y Comercio (SIC):
   a. La SIC es la entidad encargada de supervisar el cumplimiento de la Ley 1581 de 2012 y su decreto reglamentario, con la autoridad para imponer sanciones en casos de incumplimiento y orientar sobre el tratamiento adecuado de los datos personales.
   b. Aplicación en la Contraloría: Alinear todas las políticas de protección de datos personales con las directrices de la SIC y someterse a auditorías de cumplimiento cuando sean requeridas. La Contraloría debe también notificar a la SIC en caso de incidentes de seguridad que comprometan datos personales.
2. Agencia Nacional de Ciberseguridad y Ciberdefensa (ANCC):
   a. La ANCC establece protocolos y directrices para fortalecer la ciberseguridad en las entidades públicas, brindando apoyo en la prevención y respuesta ante incidentes cibernéticos.
   b. Aplicación en la Contraloría: Implementar las directrices de ciberseguridad recomendadas por la ANCC y participar en capacitaciones y ejercicios de simulación para fortalecer la capacidad de respuesta a incidentes cibernéticos.
3. Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC):
   a. El MinTIC provee políticas de ciberseguridad y directrices específicas para el sector público, incluyendo lineamientos para proteger la información y mejorar las capacidades de seguridad digital en las entidades del Estado.

b. Aplicación en la Contraloría: Adoptar los lineamientos del MinTIC en su estrategia de seguridad, integrando sus políticas en los sistemas de información de la entidad para asegurar la alineación con las prácticas de seguridad recomendadas.

Políticas Internas y Directrices de Cumplimiento en la Contraloría
Además de los marcos legales y normativos externos, la Contraloría debe contar con un conjunto de políticas internas que traduzcan estos principios en prácticas específicas para su funcionamiento diario.

1. Política de Seguridad de la Información:
   a. Define los principios y directrices que rigen la protección de la información en la Contraloría, estableciendo compromisos específicos de la entidad para asegurar la seguridad de sus activos de información.
   b. Aplicación: La política de seguridad debe ser revisada y aprobada por la alta dirección y debe comunicarse a todos los empleados y contratistas, asegurando su cumplimiento mediante capacitaciones y auditorías regulares.
2. Política de Protección de Datos Personales:
   a. Establece las directrices para el tratamiento adecuado de datos personales en la Contraloría, incluyendo la recolección, almacenamiento, tratamiento y eliminación de dichos datos.
   b. Aplicación: Asegurar que la política de protección de datos cumpla con la Ley 1581 de 2012 y esté alineada con las mejores prácticas internacionales, permitiendo la protección de los derechos de los titulares de datos.
3. Política de Continuidad Operativa y Recuperación ante Desastres:
   a. Esta política define los lineamientos para asegurar la continuidad de las operaciones críticas y la recuperación rápida de los sistemas ante incidentes o desastres que afecten la infraestructura de TI.
   b. Aplicación: Desarrollar y probar regularmente planes de continuidad y recuperación, asegurando que los sistemas y servicios críticos puedan ser restaurados en caso de interrupciones o ataques.
4. Política de Gestión de Incidentes de Seguridad:
   a. Proporciona un marco para la identificación, análisis, respuesta y documentación de incidentes de seguridad que puedan afectar a la Contraloría.
   b. Aplicación: Asegurar que la Contraloría cuente con procedimientos para responder de manera rápida y eficaz ante incidentes de seguridad, con un enfoque en minimizar el impacto y fortalecer los controles.

GESTIÓN DE ACTIVOS DE INFORMACIÓN
Objetivo: Establecer un proceso integral y sistemático para la identificación, clasificación, protección y gestión de todos los activos de información en la Contraloría Distrital de Cartagena

de Indias. Este proceso busca garantizar que cada activo tenga una protección adecuada según su criticidad y que se mantenga una actualización constante del inventario de activos.

Identificación y Registro de Activos
Este primer paso permite catalogar todos los activos de información de la entidad y sus atributos, facilitando su gestión y seguridad en los procesos internos.

1. Inventario Detallado de Activos:
    a. Definición de Activos: Considerar como activos toda la información digital y física, sistemas de software, dispositivos (computadoras, móviles, servidores), documentos físicos importantes y bases de datos.
    b. Registro Centralizado: Crear un sistema centralizado de registro que contenga toda la información relevante de cada activo (nombre, ubicación, tipo, usuario propietario, fecha de incorporación, y clasificación de seguridad).
    c. Categorías de Activos:
        i. Digitales: Incluyen bases de datos, aplicaciones, archivos digitales y servidores.
        ii. Físicos: Documentación impresa, dispositivos de almacenamiento (USB, discos duros) y dispositivos de red.
        iii. Humanos: Empleados y contratistas que manipulan o acceden a información crítica.
2. Asignación de Propietarios y Custodios de Activos:
    a. Propietario del Activo: Cada activo debe tener un propietario designado, normalmente el responsable del área o función que depende de ese activo. El propietario es responsable de definir permisos de acceso, supervisar el uso y la clasificación del activo.
    b. Custodio del Activo: En algunos casos, el custodio será la persona responsable de implementar y mantener los controles de seguridad para el activo. Ejemplos incluyen el equipo de TI para sistemas digitales o el personal de archivo para documentos físicos.
3. Procedimientos de Actualización y Mantenimiento del Inventario:
    a. Revisión Periódica: Actualizar el inventario cada seis meses, verificando si existen nuevos activos, si se han realizado bajas, o si ha cambiado el estatus de algún activo.
    b. Registro de Cambios: Mantener un historial de cambios en el inventario, incluyendo detalles de cualquier modificación, eliminación o incorporación de activos, y la fecha en que se realizó el cambio.
    c. Acceso Controlado: Asegurar que solo el personal autorizado pueda acceder y modificar el inventario de activos, garantizando la precisión de la información y la confidencialidad.

Clasificación de Activos

La clasificación de los activos es crucial para priorizar los esfuerzos de seguridad y aplicar controles adecuados según el nivel de criticidad.

1. Criterios de Clasificación:
    a. Confidencialidad: Determinar si el acceso a la información debe restringirse solo a personas específicas. Información clasificada como "Confidencial" debe tener controles estrictos.
    b. Integridad: Evaluar si la precisión y consistencia de los datos son críticas para las operaciones de la Contraloría.
    c. Disponibilidad: Valorar la importancia de que el activo esté accesible en todo momento para no afectar la continuidad operativa.
2. Niveles de Clasificación:
    a. Alta (Crítica): Activos esenciales cuya pérdida, corrupción o indisponibilidad podrían interrumpir las operaciones de la entidad (ej. registros fiscales, bases de datos de auditorías).
    b. Media (Sensitiva): Activos de importancia moderada que pueden causar un impacto en los procesos internos o en la reputación de la entidad.
    c. Baja (General): Activos que, si se ven comprometidos, no causan un impacto significativo en las operaciones o seguridad.
3. Procedimientos de Clasificación:
    a. Clasificación Inicial: Clasificar cada nuevo activo en el momento de su registro en el inventario, asignando el nivel adecuado de seguridad.
    b. Revisión de Clasificación: Revisar la clasificación de cada activo en intervalos definidos (al menos anualmente) y en caso de cambios en su criticidad o función.
    c. Documentación y Etiquetado: Asegurar que cada activo tenga un etiquetado físico o digital que indique su clasificación y nivel de sensibilidad, con acceso restringido según su nivel de confidencialidad.

Medidas de Seguridad para Activos

Las medidas de seguridad deben aplicarse con base en la clasificación de cada activo, protegiendo así su confidencialidad, integridad y disponibilidad.

1. Seguridad Física:
    a. Control de Acceso: Implementar controles de acceso físico en áreas donde se encuentren activos críticos o sensitivos, como áreas de servidores o archivos de documentación sensible.
    b. Protección de Documentos Físicos: Usar archivadores cerrados y con acceso restringido para documentos físicos clasificados.
    c. Almacenamiento Seguro de Dispositivos: Los dispositivos de almacenamiento externo deben ser protegidos en áreas seguras y, de ser posible, almacenados en dispositivos cifrados.
2. Seguridad Lógica:

a. Acceso Basado en Roles: Configurar accesos a los activos digitales de acuerdo con el rol de cada usuario, limitando el acceso únicamente a los que necesitan utilizar ese recurso.
b. Autenticación Multifactor: Implementar autenticación multifactor (MFA) en todos los sistemas críticos para añadir una capa extra de seguridad.
c. Cifrado de Información Sensible: Aplicar cifrado en datos sensibles, tanto en tránsito como en reposo, utilizando estándares de cifrado seguros.

3. Seguridad de Redes:
   a. Segmentación de Redes: Segmentar las redes para minimizar el acceso entre redes internas y externas, evitando que la información confidencial esté expuesta.
   b. Monitoreo Continuo: Utilizar herramientas de monitoreo y detección de intrusiones para identificar accesos no autorizados y actividades sospechosas en tiempo real.
4. Respaldo y Recuperación:
   a. Frecuencia de Respaldo: Programar respaldos diarios para la información clasificada como crítica, y respaldos semanales para información sensible.
   b. Almacenamiento en Ubicaciones Seguras: Guardar las copias de respaldo en ubicaciones seguras, preferiblemente en un sitio alternativo o en la nube con cifrado.
   c. Pruebas de Recuperación: Realizar pruebas de restauración trimestrales para verificar la integridad de las copias y asegurar la recuperación de la información en caso de un incidente.

Capacitación en Gestión de Activos

La capacitación es esencial para que el personal entienda la importancia de una adecuada gestión de activos y aplique los controles de seguridad correspondientes.

1. Formación Inicial:
   a. Sensibilización sobre la Clasificación de Activos: Proporcionar capacitación a los empleados nuevos sobre los procedimientos de clasificación y los niveles de sensibilidad de los activos de información.
   b. Roles y Responsabilidades: Capacitar a los propietarios y custodios de activos para que comprendan sus responsabilidades específicas en cuanto a la gestión y protección de los activos asignados.
2. Capacitación Continua:
   a. Actualización en Procedimientos de Seguridad: Realizar talleres de actualización cada seis meses para reforzar los procedimientos de seguridad aplicables a la gestión de activos.
   b. Buenas Prácticas de Gestión de Activos: Incluir temas de buenas prácticas como el uso seguro de dispositivos de almacenamiento, manejo de contraseñas, y el reporte de cualquier anomalía en los activos.

c. Evaluación de Conocimientos: Realizar exámenes periódicos para evaluar el conocimiento del personal en gestión de activos y seguridad de la información.

Resumen de Responsabilidades

Para garantizar el éxito en la gestión de activos de información, la Contraloría Distrital de Cartagena de Indias asignará las siguientes responsabilidades:

1. Propietarios de Activos:
   a. Clasificación y actualización de permisos de acceso.
   b. Supervisión de los niveles de seguridad aplicables a los activos.
2. Custodios de Activos:
   Implementación de controles de seguridad para proteger la integridad, confidencialidad y disponibilidad de los activos.
3. Proceso de Tecnologías de Información y las Comunicaciones:
   a. Mantenimiento del inventario de activos.
   b. Realización de auditorías y verificaciones de seguridad para asegurar la conformidad con las políticas de gestión de activos.

EVALUACIÓN Y GESTIÓN DE RIESGOS

La gestión de riesgos es fundamental para proteger los activos de información de la Contraloría Distrital de Cartagena de Indias y garantizar la continuidad de las operaciones. Esta unidad tiene como propósito identificar, evaluar, clasificar y mitigar los riesgos relacionados con la seguridad de la información y los activos de la entidad, priorizando aquellos que pueden afectar la confidencialidad, integridad y disponibilidad de los datos.

Objetivo: Establecer un proceso sistemático de identificación y tratamiento de riesgos, basado en metodologías internacionales y en las normativas vigentes en seguridad de la información.

Identificación de Riesgos

La identificación de riesgos consiste en reconocer todas las amenazas y vulnerabilidades que podrían comprometer los activos de información de la Contraloría Distrital de Cartagena de Indias.

1. Análisis de Amenazas:
   a. Fuentes Internas y Externas: Identificar amenazas tanto internas (fallos de personal, errores en los sistemas) como externas (ciberataques, desastres naturales, cortes de energía).
   b. Tipos de Amenazas:
      i. Humanas: Errores humanos, actos maliciosos de empleados o contratistas, fallos de capacitación.
      ii. Tecnológicas: Vulnerabilidades en software, configuraciones incorrectas, accesos no autorizados.

iii. Ambientales: Amenazas externas como desastres naturales, incendios o inundaciones.

2. Detección de Vulnerabilidades:
    a. Evaluación Técnica: Realizar evaluaciones periódicas de seguridad en los sistemas de información, identificando debilidades en software, hardware y configuraciones.
    b. Revisión de Procedimientos: Revisar los procedimientos de seguridad para identificar lagunas o áreas donde podrían existir vulnerabilidades (ej. accesos no monitorizados o falta de autenticación multifactor).
    c. Auditorías de Configuración: Realizar auditorías de configuración en todos los dispositivos de red y servidores para detectar configuraciones inseguras o sin las actualizaciones necesarias.
3. Registro de Riesgos:
    a. Creación de un Registro de Riesgos: Documentar cada riesgo identificado en un registro central, detallando su tipo, activos afectados, descripción y posibles causas.
    b. Actualización Continua: Actualizar el registro cada vez que se identifique un nuevo riesgo o se modifiquen los activos de información, asegurando una lista vigente y precisa.

Evaluación y Priorización de Riesgos

La evaluación de riesgos permite clasificar y priorizar los riesgos con base en su impacto y probabilidad de ocurrencia, facilitando la asignación de recursos para su mitigación.

1. Matriz de Riesgos:
    a. Impacto: Evaluar el impacto de cada riesgo en la confidencialidad, integridad y disponibilidad de los activos afectados. Clasificar los impactos en niveles (alto, medio, bajo) según el daño potencial.
    b. Probabilidad: Estimar la probabilidad de ocurrencia de cada riesgo, con base en datos históricos, auditorías previas y el contexto actual de amenazas.
    c. Asignación de Nivel de Riesgo: Combinar impacto y probabilidad en una matriz de riesgos para clasificar cada riesgo como crítico, alto, medio o bajo, permitiendo una priorización clara.
2. Escenarios de Riesgo:
    a. Simulaciones de Impacto: Realizar simulaciones o ejercicios de análisis de impacto en los activos críticos, para evaluar el efecto que tendría la materialización del riesgo.
    b. Evaluación de Dependencias: Determinar cómo los riesgos en un activo pueden afectar a otros activos o áreas de la entidad. Esto es importante para activos interconectados o dependientes de servicios de red y telecomunicaciones.
3. Informe de Evaluación de Riesgos:

a. Documentación: Elaborar un informe detallado con los riesgos priorizados, incluyendo la descripción del riesgo, activos afectados, nivel de criticidad y controles existentes.
b. Presentación a la Alta Dirección: Presentar los resultados de la evaluación de riesgos a la alta dirección para aprobación y toma de decisiones sobre la asignación de recursos.

Plan de Mitigación de Riesgos

Una vez priorizados, es necesario definir y aplicar controles que mitiguen los riesgos más críticos y minimizar las vulnerabilidades detectadas.

1. Desarrollo de Controles de Seguridad:
   a. Controles Preventivos: Diseñar e implementar controles preventivos, como actualizaciones de seguridad, autenticación multifactor y políticas de acceso basado en roles.
   b. Controles de Detección: Implementar sistemas de detección de intrusos (IDS) y monitoreo de redes que permitan identificar accesos no autorizados o actividades inusuales en tiempo real.
   c. Controles Correctivos: Establecer mecanismos de respuesta y recuperación ante incidentes, tales como copias de seguridad y planes de recuperación ante desastres.
2. Asignación de Recursos para Mitigación:
   a. Recursos Humanos y Tecnológicos: Asegurar que se asignen los recursos humanos y tecnológicos necesarios para implementar los controles. Esto incluye tanto capacitación como adquisición de herramientas tecnológicas.
   b. Implementación de Controles según la Criticidad: Priorizar la implementación de controles en función de la clasificación de los riesgos. Por ejemplo, para los riesgos críticos se pueden adoptar controles de alta seguridad y frecuencias de monitoreo intensivas.
3. Revisión de Controles y Procedimientos:
   a. Validación de la Eficacia: Realizar auditorías y pruebas para validar la eficacia de los controles de seguridad implementados. Esto puede incluir pruebas de penetración y auditorías de conformidad con estándares de seguridad.
   b. Reajuste de Controles: Adaptar los controles cuando se detecten nuevas amenazas o cambien las condiciones del entorno de seguridad. Estos reajustes son críticos para mantener una respuesta efectiva y actualizada a los riesgos.

Revisión y Actualización Continua

El entorno de seguridad está en constante cambio; por tanto, la gestión de riesgos debe ser un proceso continuo que se revise y actualice regularmente.

1. Reevaluación Periódica:
   a. Frecuencia de Revisión: Realizar revisiones semestrales del plan de gestión de riesgos para asegurar su vigencia.

b. Actualización por Cambios en el Entorno: Reevaluar el riesgo cada vez que haya cambios significativos en el
entorno (nuevas amenazas, cambios en los activos de información, actualizaciones de software).

2. Análisis Post-Incidente:
   a. Revisión de Incidentes: Tras cada incidente de seguridad, realizar un análisis de causa raíz para identificar fallas en los controles de riesgo y documentar las lecciones aprendidas.
   b. Mejora Continua: Incorporar las lecciones aprendidas y ajustar los procedimientos y controles para evitar la recurrencia del riesgo.
3. Auditoría del Proceso de Gestión de Riesgos:
   a. Auditorías Internas y Externas: Realizar auditorías regulares para evaluar la eficacia del proceso de gestión de riesgos y el cumplimiento de las normativas de seguridad.
   b. Cumplimiento Normativo: Asegurarse de que la gestión de riesgos cumpla con las leyes y normativas locales (como la Ley 1581 de 2012 y la Ley 1712 de 2014) y estándares internacionales de seguridad, como ISO/IEC 27001.

Resumen de Responsabilidades
Para el adecuado funcionamiento de esta unidad, se asignarán responsabilidades específicas:

- Propietario del Proceso de Gestión de Riesgos:
  - Supervisar la identificación, evaluación y tratamiento de los riesgos.
  - Informar a la alta dirección sobre el estado y las necesidades de gestión de riesgos.
- Proceso de Tecnologías de Información y las Comunicaciones:
  Realizar auditorías técnicas, aplicar controles de seguridad y monitorear la eficacia de las medidas implementadas.
- Alta Dirección:
  Tomar decisiones sobre la asignación de recursos y aprobar el plan de mitigación de riesgos, asegurando su alineación con los objetivos estratégicos de la entidad.

PROTECCIÓN DE LA CONFIDENCIALIDAD, INTEGRIDAD Y DISPONIBILIDAD (CID)
Esta unidad se enfoca en aplicar controles específicos que aseguren la confidencialidad, integridad y disponibilidad de los activos de información de la Contraloría Distrital de Cartagena de Indias. Este marco de protección es fundamental para prevenir accesos no autorizados, asegurar la exactitud de los datos y mantener la disponibilidad de la información crítica en todo momento.

Objetivo: Implementar medidas de seguridad que protejan los activos de información y mantengan los tres pilares de la seguridad de la información: confidencialidad, integridad y disponibilidad, según los lineamientos de la política de seguridad.

Confidencialidad

La confidencialidad tiene como propósito restringir el acceso a la información para protegerla de accesos no autorizados o divulgaciones indebidas. Las actividades en esta sección están orientadas a limitar el acceso y proteger la información sensible de la entidad.

1. Control de Acceso Basado en Roles (RBAC):
    a. Asignación de Roles: Definir roles y permisos de acceso que limiten el uso de cada activo según la función del usuario. Ejemplo: solo el personal de contabilidad tendrá acceso a información financiera sensible.
    b. Principio de Mínimo Privilegio: Asegurar que cada usuario solo tenga acceso a la información y los recursos necesarios para realizar su trabajo.
    c. Revisión Periódica de Accesos: Revisar y actualizar los permisos de acceso cada seis meses para retirar permisos innecesarios y prevenir posibles accesos indebidos.
2. Autenticación Multifactor (MFA):
    a. MFA para Información Crítica: Implementar autenticación multifactor en los sistemas de información críticos y en los dispositivos que manejen datos clasificados como sensibles.
    b. Reforzamiento de Seguridad en Contraseñas: Requerir que las contraseñas se actualicen periódicamente y cumplan con políticas de complejidad, para reducir la posibilidad de ataques de fuerza bruta.
3. Acuerdos de Confidencialidad:
    a. Firma de Acuerdos: Todo el personal, contratistas y terceros que accedan a información confidencial deben firmar acuerdos de confidencialidad, comprometiéndose a no divulgar información sensible ni durante ni después de su relación con la entidad.
    b. Sensibilización Continua: Realizar capacitaciones y recordatorios sobre la importancia de la confidencialidad de los datos, especialmente en escenarios de teletrabajo o acceso remoto.
4. Cifrado de Información Sensible:
    a. Cifrado de Datos en Tránsito y en Reposo: Asegurar que toda la información sensible se cifre tanto en tránsito como en reposo, utilizando protocolos seguros (ej. HTTPS, VPN, TLS).
    b. Gestión de Claves de Cifrado: Implementar un sistema de gestión seguro para las claves de cifrado, con acceso controlado y procedimientos para la rotación y renovación de claves.

Integridad

La integridad asegura que los datos se mantengan precisos y completos a lo largo de su ciclo de vida, evitando modificaciones no autorizadas que comprometan su veracidad.

1. Registros de Actividad (Logs):

   a. Generación de Logs: Habilitar registros de actividad en todos los sistemas críticos, que incluyan detalles sobre accesos, modificaciones y eliminaciones de datos.
   b. Protección de Logs: Asegurar que los logs sean inmutables y estén protegidos contra modificaciones, ya sea mediante cifrado o almacenamiento en un sistema seguro.
2. Controles de Versiones:
   a. Control de Versiones de Documentos Críticos: Utilizar herramientas de control de versiones para documentos y archivos sensibles, permitiendo rastrear cualquier cambio y facilitar la restauración de versiones previas si es necesario.
   b. Auditoría de Cambios: Llevar un registro claro y detallado de cualquier cambio realizado en la información crítica, con datos sobre quién realizó la modificación y cuándo.
3. Integridad de los Datos en Sistemas de Transferencia:
   a. Protocolos de Transferencia Segura: Asegurar que toda transferencia de datos entre sistemas utilice protocolos seguros (como SFTP o HTTPS) para evitar la corrupción de datos durante su transmisión.
   b. Verificación de Integridad: Implementar métodos de verificación de integridad, como sumas de verificación (hashing) o controles de redundancia cíclica (CRC), para confirmar que los datos no han sido alterados durante su transferencia.
4. Evaluaciones de Integridad:
   a. Pruebas Periódicas: Realizar auditorías y pruebas de integridad en bases de datos y sistemas de información críticos para asegurar que los datos sean precisos y completos.
   b. Validación de Procesos: Verificar que todos los sistemas y procesos de la entidad garanticen la consistencia y exactitud de la información en su ciclo de vida.

Disponibilidad

La disponibilidad se enfoca en asegurar que los datos y sistemas estén accesibles y operativos cuando los usuarios autorizados los necesiten. Esto es vital para la continuidad de las operaciones de la Contraloría Distrital de Cartagena de Indias.

1. Planes de Respaldo y Recuperación:
   a. Frecuencia de Respaldos: Realizar respaldos diarios para la información de alta criticidad y semanalmente para la información de menor criticidad.
   b. Almacenamiento Seguro de Respaldos: Almacenar las copias de respaldo en ubicaciones seguras y separadas físicamente de los sistemas principales, utilizando servicios de almacenamiento en la nube cifrado o centros de datos externos.
   c. Pruebas de Restauración: Realizar pruebas de restauración trimestrales para verificar la eficacia de los respaldos y la integridad de la información almacenada en ellos.
2. Plan de Continuidad de Operaciones y Recuperación ante Desastres:

a. Análisis de Impacto: Identificar sistemas y datos críticos, evaluando el impacto de su posible indisponibilidad en las operaciones de la Contraloría Distrital de Cartagena de Indias.
b. Plan de Recuperación ante Desastres: Desarrollar un plan detallado de recuperación ante desastres (DRP), que incluya procedimientos específicos para restaurar los sistemas en caso de eventos catastróficos, como desastres naturales o ciberataques.
c. Simulacros de Continuidad: Realizar simulacros y pruebas del plan de continuidad al menos una vez al año, verificando la capacidad de respuesta ante situaciones de emergencia.

3. Mantenimiento Preventivo de Infraestructura:
   a. Calendario de Mantenimiento: Establecer un cronograma de mantenimiento preventivo para todos los sistemas de hardware, servidores y equipos de red, minimizando el riesgo de fallos no planificados.
   b. Monitoreo de Estado de Sistemas: Implementar sistemas de monitoreo en tiempo real para detectar problemas potenciales en la infraestructura y tomar medidas preventivas antes de que se presenten fallos críticos.
4. Redundancia de Infraestructura y Recursos Críticos:
   a. Implementación de Redundancia: Configurar redundancia en los servidores y sistemas críticos para asegurar que, en caso de fallo de un componente, otro pueda continuar con la operación.
   b. Uso de Infraestructura en la Nube: Utilizar soluciones en la nube para garantizar alta disponibilidad de los sistemas en caso de interrupciones en el centro de datos local.
   c. Balanceo de Carga: Implementar balanceo de carga para distribuir eficientemente el tráfico entre diferentes servidores, evitando la sobrecarga y asegurando la disponibilidad constante del servicio.

Resumen de Responsabilidades

Para asegurar que los controles de confidencialidad, integridad y disponibilidad se implementen y mantengan de forma adecuada, se asignarán responsabilidades específicas:

1. Propietarios de Información:
   a. Supervisar y mantener la confidencialidad, integridad y disponibilidad de los datos y sistemas bajo su control.
   b. Coordinar con el equipo de TI para implementar medidas de seguridad específicas.
2. Proceso de Tecnologías de la Información y las Comunicaciones:
   a. Implementar y monitorear los controles de seguridad, como autenticación multifactor, cifrado, y mecanismos de control de acceso.
   b. Realizar pruebas periódicas de integridad y disponibilidad de los sistemas críticos.
3. Alta Dirección:

a. Aprobar los planes de respaldo, continuidad y recuperación ante desastres, asegurando que estén alineados con los objetivos de la entidad.
b. Revisar periódicamente los informes de cumplimiento y el estado de los controles de CID.

GESTIÓN DE INCIDENTES DE SEGURIDAD

Esta unidad establece un enfoque formal para la identificación, respuesta, y registro de incidentes de seguridad de la información. La gestión eficaz de incidentes permite responder rápida y adecuadamente a eventos que comprometan la seguridad de los activos de información, minimizando el impacto y reduciendo los riesgos de futuros incidentes.

Objetivo: Crear un proceso de gestión de incidentes que garantice la identificación, reporte, respuesta y documentación de todos los incidentes de seguridad de la información, de manera que se pueda mitigar rápidamente cualquier riesgo y mejorar la respuesta ante futuras amenazas.

Detección y Reporte de Incidentes

Este primer paso se centra en identificar incidentes de seguridad tan pronto ocurran, garantizando un reporte rápido y claro que permita una respuesta oportuna.

1. Definición de Incidente de Seguridad:
   a. Concepto de Incidente: Cualquier evento que comprometa la confidencialidad, integridad o disponibilidad de la información. Ejemplos incluyen accesos no autorizados, malware, violaciones de políticas de acceso y pérdida o robo de dispositivos.
   b. Clasificación de Incidentes: Clasificar los incidentes según su criticidad en categorías tales como bajo, medio, alto y crítico, de acuerdo con el impacto potencial en la organización y en sus operaciones.
2. Canales de Reporte de Incidentes:
   a. Establecimiento de un Canal Formal: Implementar un canal oficial (correo electrónico, sistema de tickets o plataforma de incidentes) para que el personal pueda reportar incidentes de seguridad.
   b. Comunicación Inmediata: Asegurar que todos los empleados y contratistas conozcan el canal de reporte y comprendan la importancia de notificar de inmediato cualquier evento sospechoso.
   c. Registro de Reportes: Documentar cada incidente reportado, registrando detalles como la fecha y hora de detección, tipo de incidente, activos afectados y usuario que realizó el reporte.
3. Detección Automática de Incidentes:
   a. Monitoreo de Redes y Sistemas: Utilizar herramientas de monitoreo que detecten automáticamente accesos no autorizados, movimientos inusuales de datos y otras actividades sospechosas.

b. Sistemas de Detección de Intrusos (IDS): Implementar IDS para detectar accesos inusuales y potenciales ataques en
tiempo real, y alertar al equipo de seguridad para una intervención rápida.

Respuesta a Incidentes

El proceso de respuesta a incidentes define las acciones que deben tomarse para contener, erradicar y recuperar los sistemas comprometidos, limitando el impacto de cualquier amenaza.

1. Equipo de Respuesta a Incidentes (CSIRT):
   a. Definición de Responsabilidades: Designar un equipo de respuesta a incidentes que incluya personal con conocimientos de seguridad de la información, TI, y representantes de cada área crítica.
   b. Capacitación Continua: Capacitar al equipo en procedimientos de respuesta ante incidentes, simulacros y ejercicios para asegurar que puedan actuar de manera rápida y eficaz en un escenario real.
2. Proceso de Respuesta:
   a. Identificación del Incidente: Confirmar la naturaleza del incidente y determinar su alcance, analizando el tipo de ataque y los activos afectados.
   b. Contención Inmediata: Tomar medidas para contener el incidente y prevenir su propagación, como desconectar sistemas afectados, bloquear usuarios comprometidos o deshabilitar funciones específicas.
   c. Erradicación de la Amenaza: Identificar y eliminar la causa raíz del incidente (como malware, usuarios comprometidos o configuraciones inseguras).
3. Recuperación y Restauración:
   a. Recuperación de Sistemas: Restaurar los sistemas y datos afectados, asegurando que se encuentren en condiciones seguras antes de reactivarlos. Si es necesario, utilizar copias de respaldo verificadas.
   b. Validación de la Recuperación: Probar los sistemas restaurados para confirmar que el incidente ha sido completamente resuelto y que los sistemas funcionan adecuadamente.

Registro y Seguimiento de Incidentes

Registrar y analizar los incidentes de seguridad permite entender sus causas, mejorar los controles de seguridad y prevenir futuros eventos similares.

1. Registro Detallado de Incidentes:
   a. Documentación de Detalles: Registrar toda la información relevante del incidente, incluyendo la descripción del evento, activos afectados, impacto, y las acciones de respuesta implementadas.
   b. Archivo Centralizado de Incidentes: Mantener un registro centralizado y seguro de todos los incidentes documentados para facilitar auditorías y análisis.
2. Análisis Post-Incidente (Lecciones Aprendidas):

a. Análisis de Causa Raíz: Realizar un análisis detallado para identificar las causas profundas del incidente, evaluando
las debilidades o vulnerabilidades que permitieron que ocurriera.
b. Evaluación de la Respuesta: Analizar el tiempo de respuesta, las acciones implementadas y el impacto del incidente, identificando cualquier mejora posible en el proceso de gestión de incidentes.
c. Informe de Lecciones Aprendidas: Crear un informe con las lecciones aprendidas y recomendaciones de mejora, distribuyéndolo al equipo de seguridad y otras áreas relevantes.

3. Ajuste de Controles:
   a. Revisión de Políticas y Procedimientos: Revisar y ajustar los procedimientos de seguridad de la información y los controles de riesgo, incorporando las lecciones aprendidas para prevenir incidentes similares.
   b. Actualización de la Documentación: Modificar políticas, guías de respuesta a incidentes y protocolos según las conclusiones del análisis post-incidente, reforzando la protección.

Prevención y Mejora Continua
La prevención se centra en reducir la probabilidad de futuros incidentes a través de controles proactivos y prácticas de seguridad robustas.

1. Auditorías y Simulacros:
   a. Auditorías de Seguridad Periódicas: Realizar auditorías de seguridad internas y externas para identificar posibles debilidades en los sistemas y procedimientos actuales.
   b. Simulacros de Incidentes: Organizar simulacros de respuesta ante incidentes, especialmente para los escenarios de alto impacto, evaluando la capacidad de respuesta del equipo y las áreas de mejora.
2. Monitoreo Proactivo de Vulnerabilidades:
   a. Gestión de Parches y Actualizaciones: Mantener actualizado todo el software, aplicando parches de seguridad tan pronto como se publiquen.
   b. Escaneos de Vulnerabilidades: Realizar escaneos de vulnerabilidades de manera periódica en sistemas críticos y redes, con un seguimiento de corrección inmediata.
3. Sensibilización y Capacitación Continua:
   a. Entrenamiento Regular: Capacitar al personal regularmente en prácticas seguras y en la detección de posibles amenazas, como phishing y accesos no autorizados.
   b. Promoción de Cultura de Reporte: Fomentar una cultura donde el personal se sienta cómodo y motivado para reportar cualquier actividad sospechosa, minimizando el tiempo de respuesta ante incidentes.

Resumen de Responsabilidades
Para asegurar la implementación y eficacia de la gestión de incidentes, se asignarán responsabilidades específicas:

1. Equipo de Respuesta a Incidentes (CSIRT):
    a. Gestionar todos los aspectos de respuesta ante incidentes, desde la detección hasta la recuperación.
    b. Mantener la comunicación con la alta dirección y otras áreas afectadas durante el incidente.
2. Proceso de Tecnologías de la Información y las Comunicaciones:
    a. Monitorear continuamente la infraestructura para detectar posibles amenazas.
    b. Implementar medidas de prevención y realizar simulacros de incidentes.
3. Alta Dirección:
    a. Aprobar los protocolos de respuesta y los recursos necesarios para la gestión de incidentes.
    b. Revisar los informes de lecciones aprendidas y apoyar la implementación de mejoras.

CAPACITACIÓN Y CONCIENCIA EN SEGURIDAD DE LA INFORMACIÓN

Esta unidad está diseñada para fortalecer la cultura de seguridad de la información dentro de la Contraloría Distrital de Cartagena de Indias. Una fuerza laboral informada y consciente de las buenas prácticas de seguridad es esencial para reducir el riesgo de incidentes de seguridad y garantizar la protección continua de los activos de información.

Objetivo: Fomentar una cultura de seguridad mediante la capacitación continua y la sensibilización de todos los empleados y contratistas en prácticas de seguridad de la información. Esto permitirá reducir errores humanos y aumentar la capacidad de respuesta ante amenazas.

Capacitación Inicial en Seguridad de la Información

El objetivo de esta etapa es asegurar que todo el personal nuevo comprenda las políticas de seguridad de la información y sus responsabilidades desde su primer día en la entidad.

1. Programa de Inducción en Seguridad:
    a. Contenido del Programa: Introducir los conceptos básicos de seguridad de la información, como la confidencialidad, integridad y disponibilidad de los datos, y las principales políticas de la Contraloría.
    b. Políticas de Seguridad: Explicar las políticas clave de seguridad y su importancia en la protección de los activos de información, incluidas las políticas de acceso, control de dispositivos, protección de datos y uso de correo electrónico institucional.
2. Responsabilidades en Seguridad de la Información:

a. Tareas Específicas: Definir las responsabilidades de cada rol en cuanto a la seguridad de la información, según su nivel de acceso y funciones específicas dentro de la entidad.
b. Acuerdos de Confidencialidad: Requerir la firma de acuerdos de confidencialidad y compromisos de uso adecuado de la información para todos los nuevos empleados y contratistas.

3. Evaluación de Comprensión:
   a. Examen Inicial: Realizar un examen de comprensión al final de la inducción para asegurar que el personal haya entendido los conceptos y políticas de seguridad fundamentales.
   b. Seguimiento de Resultados: Llevar un registro de los resultados de las evaluaciones y proporcionar sesiones de refuerzo a quienes necesiten más claridad en los temas tratados.

Sensibilización Continua en Seguridad de la Información

La sensibilización continua es crucial para mantener el conocimiento de seguridad actualizado y recordar al personal las mejores prácticas y protocolos a seguir.

1. Campañas de Conciencia de Seguridad:
   a. Boletines de Seguridad: Enviar boletines mensuales que incluyan temas de seguridad, nuevos riesgos, y mejores prácticas, especialmente sobre phishing, ingeniería social y amenazas emergentes.
   b. Pósters y Recordatorios Visuales: Colocar pósters y recordatorios en las áreas de trabajo y espacios comunes sobre temas de seguridad, como protección de contraseñas y precauciones en el uso de dispositivos externos.
2. Charlas y Seminarios de Actualización:
   a. Charlas Trimestrales: Organizar charlas trimestrales en las que se traten temas específicos como la detección de amenazas, manejo seguro de datos y uso de aplicaciones seguras.
   b. Invitación de Expertos Externos: Invitar a expertos en ciberseguridad para que proporcionen sesiones de actualización y compartan experiencias y buenas prácticas.
3. Simulaciones de Incidentes de Seguridad:
   a. Simulaciones de Phishing: Realizar campañas de simulación de ataques de phishing para evaluar la capacidad del personal para detectar correos falsos y educarlos en la identificación de este tipo de amenazas.
   b. Evaluación de Respuesta: Analizar los resultados de las simulaciones y proporcionar retroalimentación inmediata, además de reforzar el aprendizaje con ejemplos prácticos.

Evaluación de Conocimientos y Cultura de Seguridad

Realizar evaluaciones periódicas es esencial para medir el conocimiento y la conciencia en seguridad de los empleados, identificando áreas de mejora y adaptando los programas de capacitación en consecuencia.

1. Evaluaciones Regulares:
    a. Exámenes Semestrales: Administrar exámenes de conocimiento cada seis meses para verificar el nivel de comprensión sobre las políticas y buenas prácticas de seguridad.
    b. Evaluaciones Temáticas: Realizar evaluaciones específicas para temas críticos, como manejo de datos personales, uso de dispositivos y reconocimiento de incidentes de seguridad.
2. Simulaciones de Incidentes Reales:
    a. Escenarios Prácticos: Implementar simulacros de respuesta a incidentes (como pérdida de dispositivos o ciberataques) en los que se evalúe la capacidad del personal para actuar según los procedimientos de respuesta establecidos.
    b. Revisión de Resultados: Analizar los resultados de estos simulacros y crear planes de mejora en caso de identificar debilidades en la respuesta del personal.
3. Evaluación de Cultura Organizacional de Seguridad:
    a. Encuestas de Cultura de Seguridad: Realizar encuestas para medir la percepción y compromiso del personal con la seguridad de la información, identificando actitudes o comportamientos de riesgo.
    b. Análisis de Resultados: Evaluar los resultados y hacer ajustes en las campañas de concienciación según las áreas de oportunidad detectadas, mejorando así el enfoque de los programas de sensibilización.

Refuerzo y Sanciones por Incumplimiento
Es importante establecer un sistema de refuerzo positivo y sanciones en caso de incumplimiento de las políticas de seguridad, para asegurar el compromiso del personal con la protección de la información.

1. Refuerzo Positivo:
    a. Reconocimiento a Buenas Prácticas: Crear un sistema de reconocimiento para empleados que demuestren un compromiso ejemplar con la seguridad de la información, como reportar incidentes o seguir procedimientos de seguridad.
    b. Incentivos por Participación en Simulacros: Ofrecer incentivos para aquellos que participen activamente en simulacros y actividades de capacitación, motivando la participación continua en temas de seguridad.
2. Sanciones por Incumplimiento:
    a. Política de Sanciones Graduales: Implementar una política de sanciones que varíe según la gravedad del incumplimiento. Ejemplos: advertencias, suspensión de acceso.
    b. Registro de Incumplimientos: Mantener un registro de incidentes relacionados con incumplimientos de las políticas de seguridad y las medidas correctivas tomadas para cada caso.
3. Sesiones de Refuerzo para Incumplimientos Menores:

a. Capacitación Correctiva: Ofrecer sesiones de capacitación correctiva para aquellos empleados que hayan cometido
errores de menor gravedad, como no seguir un procedimiento de seguridad o exponer datos accidentalmente.
b. Reevaluación de Comprensión: Requerir que el personal participe en evaluaciones de comprensión luego de recibir la capacitación correctiva, para asegurar que entiendan las políticas y procedimientos de seguridad.

Resumen de Responsabilidades
Para garantizar la efectividad de esta unidad, se asignarán las siguientes responsabilidades:

1. Equipo de Recursos Humanos:
   a. Coordinar el programa de inducción y las evaluaciones iniciales de seguridad para los nuevos empleados.
   b. Colaborar en la implementación de sanciones y refuerzos positivos en caso de incumplimiento o compromiso ejemplar.
2. Proceso de Tecnologías de Información y las Comunicaciones:
   a. Diseñar y liderar las campañas de concienciación, simulaciones de phishing y charlas de actualización.
   b. Evaluar los resultados de las evaluaciones de conocimiento y cultura de seguridad, adaptando los programas de capacitación según sea necesario.
3. Alta Dirección:
   a. Aprobar el plan de capacitación en seguridad y revisar los informes de cultura organizacional para evaluar su alineación con los objetivos estratégicos de la entidad.
   b. Apoyar la implementación de incentivos y sanciones para promover el cumplimiento de las políticas de seguridad.

PROTECCIÓN DE DATOS PERSONALES Y PRIVACIDAD
Esta unidad se enfoca en asegurar que la Contraloría Distrital de Cartagena de Indias cumpla con las normativas vigentes de protección de datos personales, especialmente la Ley 1581 de 2012 (Ley de Protección de Datos Personales) de Colombia. La protección de datos personales es fundamental para respetar los derechos de privacidad de los titulares y para evitar sanciones por incumplimiento normativo.

Objetivo: Establecer procedimientos que garanticen el tratamiento adecuado y seguro de los datos personales, promoviendo la privacidad y el cumplimiento de los derechos de los titulares de la información de acuerdo con la legislación vigente.

Recolección y Consentimiento Informado de los Titulares
La recolección de datos personales debe realizarse de manera responsable, asegurando que los titulares conozcan el propósito del tratamiento y otorguen su consentimiento de forma libre e informada.

1. Consentimiento Explícito del Titular:
    a. Requerimiento de Autorización: Asegurar que los datos personales solo se recolecten cuando el titular haya dado su consentimiento explícito mediante un formulario o declaración de privacidad.
    b. Excepciones al Consentimiento: Identificar y respetar las excepciones de la ley en las que no se requiere consentimiento, como en casos de seguridad nacional, investigaciones judiciales o cuando los datos sean de acceso público.
2. Información al Titular sobre sus Derechos:
    a. Derecho a la Información: Informar al titular sobre los derechos que tiene en relación con sus datos personales, como los derechos de acceso, rectificación, actualización y eliminación de sus datos.
    b. Finalidad del Tratamiento: Informar claramente al titular sobre los propósitos específicos para los cuales se recolectan sus datos, y garantizar que dichos datos no se usen para fines distintos sin consentimiento.
3. Documentación de Consentimiento:
    a. Almacenamiento de Autorizaciones: Mantener un registro de todos los consentimientos obtenidos, asegurando que estén organizados y disponibles en caso de requerimientos legales o auditorías.
    b. Recolección en Múltiples Canales: Documentar los procedimientos de recolección de datos a través de diversos canales, como formularios físicos, páginas web o aplicaciones, asegurando que se ofrezca información clara y transparente.

Confidencialidad y Seguridad de Datos Personales

Implementar controles que garanticen la confidencialidad y seguridad de los datos personales en cada etapa de su ciclo de vida, desde la recolección hasta su eliminación.

1. Cifrado y Protección de Datos Sensibles:
    a. Cifrado en Tránsito y en Reposo: Utilizar cifrado para proteger datos personales tanto en tránsito como en reposo, garantizando que solo los usuarios autorizados puedan acceder a ellos.
    b. Protección de Accesos: Limitar el acceso a los datos personales mediante autenticación multifactor y controles basados en roles para minimizar el riesgo de accesos no autorizados.
2. Seguridad en Dispositivos y Medios de Almacenamiento:
    a. Restricción de Dispositivos: Prohibir el almacenamiento de datos personales en dispositivos no autorizados o inseguros, como USB sin cifrado o dispositivos móviles personales.
    b. Control de Acceso a Medios Físicos: Mantener los documentos físicos que contengan datos personales en archivadores seguros y con acceso controlado, evitando que personas no autorizadas puedan acceder a ellos.
3. Capacitación en Protección de Datos Personales:

a. Sensibilización del Personal: Capacitar al personal en prácticas seguras para el tratamiento de datos personales y
en el cumplimiento de los derechos de privacidad de los titulares.
b. Actualización en Normativas: Actualizar regularmente al personal sobre cambios en la legislación de protección de datos y en las políticas de privacidad de la entidad.

Retención y Eliminación de Datos Personales
Definir políticas de retención que limiten el tiempo que los datos personales se almacenan y garanticen su eliminación segura una vez que ya no sean necesarios.

1. Política de Retención de Datos:
   a. Criterios de Retención: Establecer criterios específicos para la retención de datos según el tipo de información y la finalidad de su tratamiento. Por ejemplo, conservar datos de empleados mientras dure la relación contractual y por un período adicional estipulado en la ley.
   b. Revisión Periódica de Retención: Revisar y actualizar la política de retención periódicamente, asegurando que cumpla con los requisitos legales y operativos.
2. Eliminación Segura de Datos:
   a. Procedimiento de Eliminación Física y Digital: Implementar procedimientos para la destrucción segura de documentos físicos (como triturado) y digitales (como borrado seguro), evitando la posibilidad de recuperar los datos.
   b. Documentación de la Eliminación: Llevar un registro de todos los procesos de eliminación de datos personales, incluyendo la fecha, los datos eliminados y el método utilizado.
3. Almacenamiento Seguro de Datos de Retención Prolongada:
   a. Datos de Archivo: Identificar aquellos datos personales que deban ser retenidos por periodos extendidos (por requisitos legales o auditorías) y almacenarlos en sistemas de alta seguridad.
   b. Revisión de Cumplimiento: Realizar auditorías para asegurar que los datos retenidos cumplan con las normativas vigentes y que se mantengan solo por el tiempo necesario.

Respuesta a Solicitudes de los Titulares de Datos
Atender de manera oportuna las solicitudes de los titulares de datos en relación con sus derechos, garantizando un proceso de respuesta ágil y conforme a la ley.

1. Canales para Solicitudes de Derechos:
   a. Portal de Solicitudes: Crear un portal o sistema específico para la recepción de solicitudes de derechos de los titulares, como acceso, rectificación, actualización o eliminación de sus datos.
   b. Puntos de Contacto Designados: Asignar un punto de contacto en la entidad para atender las solicitudes de los titulares y garantizar que las respuestas se realicen dentro de los tiempos estipulados por la ley.

2. Procedimientos de Respuesta y Verificación:
    a. Verificación de Identidad: Implementar un proceso de verificación de identidad para asegurar que solo el titular o una persona autorizada pueda solicitar la modificación o eliminación de sus datos.
    b. Tiempos de Respuesta: Asegurar que las solicitudes se respondan en los plazos establecidos por la ley, ofreciendo al titular una respuesta clara y completa sobre el estado de su solicitud.
3. Documentación de Solicitudes y Respuestas:
    a. Registro de Solicitudes: Mantener un registro de todas las solicitudes recibidas, incluyendo detalles del tipo de solicitud, fecha, titular y la respuesta dada.
    b. Análisis de Solicitudes Frecuentes: Analizar periódicamente las solicitudes para identificar patrones o áreas de mejora en la gestión de datos personales.

Cumplimiento Normativo y Auditoría de Privacidad

La protección de datos personales debe alinearse con las normativas legales y estándares internacionales, lo cual requiere una supervisión constante a través de auditorías y procesos de cumplimiento.

1. Revisión de Cumplimiento Normativo:
    a. Conformidad con la Ley 1581 de 2012: Asegurar que todas las prácticas de tratamiento de datos personales se alineen con la Ley 1581 y sus decretos reglamentarios, además de la Ley 1712 de 2014 (Ley de Transparencia).
    b. Adaptación a Normas Internacionales: Considerar el cumplimiento de normas internacionales como ISO/IEC 27701 (Gestión de la Privacidad de la Información) para fortalecer la gestión de privacidad y demostrar compromiso con estándares globales.
2. Auditorías Internas y Externas:
    a. Auditorías de Cumplimiento: Realizar auditorías internas periódicas para evaluar el cumplimiento de las políticas de protección de datos, y contratar auditorías externas anuales para asegurar la objetividad y precisión en la evaluación.
    b. Revisión de Controles de Privacidad: Analizar y ajustar los controles de privacidad en función de los hallazgos de las auditorías, asegurando que se apliquen recomendaciones y medidas correctivas.
3. Informes y Responsabilidad ante la Alta Dirección:
    a. Informe Anual de Privacidad: Preparar un informe anual para la alta dirección con los resultados de las auditorías y una evaluación de los controles de privacidad implementados.
    b. Plan de Mejora Continua: Proponer un plan de mejora basado en los resultados del informe, priorizando las recomendaciones para reducir riesgos y fortalecer la protección de datos.

Resumen de Responsabilidades

Para asegurar la implementación y eficacia de la gestión de datos personales y privacidad,

se asignarán responsabilidades específicas:

1. Responsable de Protección de Datos (DPO):
    a. Coordinar el cumplimiento de la Ley 1581 de 2012 y otras normativas aplicables.
    b. Atender las solicitudes de los titulares de datos y realizar auditorías de cumplimiento de protección de datos personales.
2. Proceso de Tecnologías de Información y las Comunicaciones:
    a. Implementar controles de cifrado, protección de accesos y eliminación segura para los datos personales.
    b. Asegurar que todos los sistemas que almacenen datos personales cumplan con los requisitos de seguridad.
3. Alta Dirección:
    a. Aprobar políticas de protección de datos y revisar informes de cumplimiento y auditoría.
    b. Apoyar y promover la cultura de privacidad dentro de la Contraloría.

CUMPLIMIENTO NORMATIVO Y AUDITORÍA

Esta unidad se centra en garantizar que todas las prácticas de seguridad de la información y protección de datos de la Contraloría Distrital de Cartagena de Indias cumplan con las normativas legales y estándares nacionales e internacionales. Las auditorías periódicas permiten evaluar la efectividad de los controles de seguridad, identificar áreas de mejora y asegurar que se sigan las mejores prácticas de la industria.

Objetivo: Asegurar el cumplimiento continuo con las normativas nacionales e internacionales aplicables a la seguridad de la información y privacidad, y mantener un proceso de auditoría que permita evaluar, mejorar y supervisar la implementación de políticas y controles en la Contraloría.

Cumplimiento de Normativas Nacionales e Internacionales

El cumplimiento normativo implica alinearse con las leyes y regulaciones que rigen la seguridad de la información y la protección de datos personales.

1. Marco Legal Nacional:
    a. Ley 1581 de 2012 (Protección de Datos Personales): Cumplir con todos los principios, derechos y procedimientos establecidos por la ley de protección de datos, incluyendo la recolección, almacenamiento, tratamiento y eliminación de datos personales.
    b. Ley 1712 de 2014 (Transparencia y Acceso a la Información Pública): Asegurar el acceso a la información pública mientras se protegen los datos clasificados y sensibles de acuerdo con las restricciones legales.
    c. Decreto 1377 de 2013: Adaptar los procedimientos de consentimiento y manejo de datos a los lineamientos específicos establecidos en el decreto.
2. Adopción de Normas Internacionales:

a. ISO/IEC 27001:2022 (Gestión de Seguridad de la Información): Alinear los procesos de gestión de seguridad
con el estándar internacional, implementando un Sistema de Gestión de Seguridad de la Información (SGSI) para minimizar los riesgos.
b. ISO/IEC 27701:2019 (Gestión de la Privacidad de la Información): Incorporar los requisitos de gestión de la privacidad de la información, garantizando la protección de datos personales y la privacidad en los sistemas de información.
c. ISO/IEC 27018 (Protección de Datos en la Nube): En caso de usar servicios en la nube, verificar que los proveedores cumplan con los requisitos de protección de datos personales, como cifrado y controles de acceso.

3. Cumplimiento de Regulaciones Específicas de Ciberseguridad:
   a. Guías del Ministerio TIC y la Superintendencia de Industria y Comercio: Alinear las políticas de la Contraloría con las guías y mejores prácticas emitidas por autoridades regulatorias para cumplir con estándares nacionales de ciberseguridad.
   b. Normativas de Acceso Seguro: Implementar controles que cumplan con los requisitos de autenticación segura, como la autenticación multifactor, para acceder a información crítica o confidencial.

Auditorías Internas y Externas
Las auditorías son fundamentales para revisar y mejorar los controles de seguridad de la información y protección de datos.

1. Auditorías Internas:
   a. Revisión de Procedimientos de Seguridad: Realizar auditorías internas periódicas para asegurar que los procedimientos de seguridad y privacidad se implementen correctamente y estén alineados con las políticas de la entidad.
   b. Análisis de Incidentes y No Conformidades: Revisar los incidentes de seguridad y los hallazgos de auditorías anteriores para identificar áreas de mejora y asegurar que las no conformidades se resuelvan adecuadamente.
   c. Auditoría de Cumplimiento Normativo: Verificar el cumplimiento con las regulaciones nacionales y normativas internas, generando un informe detallado de cualquier incumplimiento o mejora recomendada.
2. Auditorías Externas:
   a. Evaluación Objetiva de Cumplimiento: Recibir auditorías externas anuales para obtener una evaluación objetiva de los controles de seguridad y su alineación con los estándares internacionales.
   b. Informe de Auditoría y Recomendaciones: Recibir un informe completo de la auditoría externa que incluya una lista de recomendaciones para fortalecer la seguridad y el cumplimiento normativo.
   c. Certificaciones Internacionales: En caso de ser requerido, obtener certificaciones ISO o de cumplimiento con normativas nacionales para demostrar el

compromiso de la Contraloría Distrital de Cartagena de Indias con la seguridad y privacidad de la información.

3. Revisión de Auditorías y Toma de Decisiones:
    a. Revisión de Informes de Auditoría por la Alta Dirección: La alta dirección debe revisar y aprobar los informes de auditoría, priorizando la implementación de mejoras y asignando los recursos necesarios para cerrar las brechas de seguridad.
    b. Actualización de Políticas Basadas en Hallazgos de Auditoría: Revisar y actualizar las políticas de seguridad y procedimientos internos según las recomendaciones de las auditorías para garantizar una mejora continua.

Monitoreo y Evaluación Continua

El monitoreo continuo de los sistemas y procesos es esencial para asegurar el cumplimiento constante y la pronta identificación de problemas de seguridad.

1. Monitoreo de Sistemas y Redes:
    a. Herramientas de Monitoreo en Tiempo Real: Utilizar herramientas de monitoreo de seguridad en tiempo real para identificar cualquier actividad inusual o potenciales vulnerabilidades en los sistemas de la Contraloría.
    b. Análisis de Logs y Registros de Actividad: Revisar los logs de actividad de forma periódica para detectar accesos no autorizados, modificaciones sospechosas o posibles violaciones de seguridad.
2. Evaluaciones de Conformidad Normativa:
    a. Evaluación Semestral de Conformidad: Realizar revisiones trimestrales de conformidad para verificar que todos los sistemas y prácticas estén alineados con las políticas y normativas aplicables.
    b. Seguimiento de Cambios Regulatorios: Mantenerse actualizado con cualquier cambio en la legislación o normativa, adaptando los procedimientos y políticas para asegurar el cumplimiento continuo.
3. Revisión de Controles de Seguridad:
    a. Evaluación de Eficacia de los Controles: Verificar periódicamente que los controles de seguridad implementados, como el cifrado, autenticación y segmentación de redes, estén funcionando de manera efectiva y se mantengan actualizados.
    b. Pruebas de Vulnerabilidad y Penetración: Realizar pruebas de penetración y análisis de vulnerabilidades en los sistemas críticos para identificar y corregir posibles brechas de seguridad.

Informes de Cumplimiento y Mejora Continua

La documentación y reporte son claves para el proceso de mejora continua, asegurando que todas las áreas de la Contraloría Distrital de Cartagena de Indias participen en el fortalecimiento de la seguridad de la información.

1. Informes Periódicos de Cumplimiento:

a. Reporte Semestral de Cumplimiento: Preparar un informe semestral sobre el estado de cumplimiento normativo,
identificando cualquier área de incumplimiento y las acciones tomadas para corregirlo.
b. Informe de Auditoría Anual para la Alta Dirección: Presentar un resumen anual a la alta dirección con los hallazgos de auditorías, el estado de los controles de seguridad y las recomendaciones de mejora.

2. Plan de Mejora Continua:
   a. Planificación de Acciones Correctivas: Crear un plan detallado de acciones correctivas y preventivas para abordar las áreas de mejora detectadas en las auditorías o revisiones internas.
   b. Evaluación de la Eficacia de las Acciones Correctivas: Revisar periódicamente la eficacia de las acciones implementadas, asegurándose de que las brechas de seguridad y no conformidades se hayan resuelto completamente.
3. Capacitación en Cumplimiento Normativo:
   a. Entrenamiento Regular: Proporcionar formación continua a los empleados sobre las regulaciones nacionales y estándares internacionales relevantes para su rol.
   b. Concienciación en el Cumplimiento Normativo: Realizar campañas de sensibilización para asegurar que todos los empleados comprendan la importancia del cumplimiento normativo y cómo aplicar las políticas en su trabajo diario.

Resumen de Responsabilidades
Para garantizar la implementación y éxito de esta unidad, se asignarán las siguientes responsabilidades:

1. Responsable de Cumplimiento Normativo:
   a. Supervisar el cumplimiento de las normativas nacionales e internacionales aplicables, y coordinar auditorías de seguridad de la información.
   b. Realizar informes periódicos sobre el estado de cumplimiento y la implementación de las recomendaciones de mejora.
2. Equipo de Control Interno:
   a. Llevar a cabo auditorías internas para evaluar el cumplimiento de las políticas de seguridad y los controles de privacidad.
   b. Colaborar con auditores externos y asegurar que las auditorías cumplan con los estándares y objetivos de la Contraloría.
3. Alta Dirección:
   a. Revisar y aprobar los informes de cumplimiento y auditoría, y priorizar los recursos necesarios para implementar mejoras en seguridad y privacidad.
   b. Promover una cultura de cumplimiento y transparencia en toda la organización.

GESTIÓN DE INCUMPLIMIENTOS Y ACCIONES CORRECTIVAS

La presente unidad se enfoca en la detección, gestión y resolución de incumplimientos en los controles de seguridad de la información, así como en la implementación de acciones correctivas para prevenir la recurrencia de problemas. La identificación y manejo adecuado de los incumplimientos es clave para mantener la integridad de los sistemas y evitar sanciones regulatorias.

Objetivo: Establecer un proceso sistemático para detectar y gestionar los incumplimientos de las políticas de seguridad y protección de datos de la Contraloría Distrital de Cartagena de Indias, tomando medidas correctivas y preventivas que aseguren una mejora continua en el sistema de gestión de seguridad de la información.

Detección y Notificación de Incumplimientos

Este proceso se centra en la detección temprana de cualquier incumplimiento de las políticas de seguridad y en la notificación inmediata a los responsables correspondientes.

1. Monitoreo y Detección de Incumplimientos:
    a. Sistemas de Monitoreo: Implementar herramientas de monitoreo para detectar posibles incumplimientos de políticas, como accesos no autorizados, fallas en la autenticación y violaciones de los procedimientos de protección de datos.
    b. Revisión de Logs: Realizar análisis regulares de los registros de actividad (logs) para identificar patrones inusuales, accesos indebidos o errores de configuración que puedan indicar un incumplimiento.
2. Notificación de Incumplimientos:
    a. Procedimientos de Notificación: Establecer procedimientos claros para que el personal pueda notificar cualquier incumplimiento o sospecha de infracción a través de un sistema de tickets o un canal designado.
    b. Reporte Inmediato a Responsables: Asegurar que los informes de incumplimiento lleguen de manera oportuna al equipo de seguridad y al responsable de cumplimiento normativo para iniciar las acciones correctivas.
3. Fomento de una Cultura de Reporte:
    a. Promoción de la Transparencia: Incentivar a los empleados y contratistas a reportar cualquier actividad sospechosa sin temor a represalias, promoviendo una cultura de transparencia.
    b. Protección del Informante: Asegurar que quienes reporten incidentes o incumplimientos sean protegidos y reconocidos por su contribución a la seguridad de la información.

Investigación y Análisis de Incumplimientos

Una vez detectado un incumplimiento, se debe realizar un análisis detallado para entender las causas y el impacto del mismo.

1. Análisis de Causa Raíz:

a. Identificación del Origen del Incumplimiento: Investigar el origen y las circunstancias que llevaron al incumplimiento, identificando si fue resultado de un error humano, fallo técnico, o vulnerabilidad de los controles.
b. Método de Análisis de Incidentes: Utilizar metodologías como el análisis de causa raíz o el análisis de fallos para profundizar en las causas subyacentes y determinar acciones correctivas efectivas.

2. Evaluación del Impacto del Incumplimiento:
   a. Impacto en Activos Críticos: Evaluar cómo el incumplimiento afectó la confidencialidad, integridad y disponibilidad de los activos críticos y si expuso a la Contraloría a riesgos legales o reputacionales.
   b. Análisis de Daños: Determinar el alcance de los daños, como pérdida de datos, compromisos de sistemas o afectación de la confianza pública, para definir las acciones correctivas necesarias.
3. Documentación de la Investigación:
   a. Informe de Incumplimiento: Elaborar un informe detallado de cada investigación, documentando los hallazgos, causas del incidente, impacto y posibles fallas en los controles.
   b. Registro de Incumplimientos: Mantener un registro de todos los incumplimientos documentados para facilitar el análisis de patrones y tendencias.

Implementación de Acciones Correctivas y Preventivas

Con base en los hallazgos de la investigación, se debe proceder a implementar acciones correctivas para abordar el incumplimiento y medidas preventivas para evitar su recurrencia.

1. Desarrollo de Acciones Correctivas:
   a. Aplicación de Cambios en Procedimientos: Modificar procedimientos y políticas según los hallazgos para evitar la repetición del incumplimiento. Esto puede incluir mejoras en los controles de acceso, ajustes en los sistemas de monitoreo o cambios en la capacitación.
   b. Soluciones Técnicas y Operativas: Implementar soluciones técnicas, como la actualización de software, implementación de parches de seguridad, o configuraciones más estrictas de control de acceso.
   c. Revisión de Roles y Responsabilidades: Ajustar los permisos y accesos de usuarios implicados, limitando el acceso a datos críticos solo a quienes lo necesiten.
2. Medidas Preventivas para Minimizar Riesgos:
   a. Refuerzo de Controles de Seguridad: Incorporar controles adicionales que refuercen la seguridad en las áreas vulnerables identificadas, como la autenticación multifactor o el cifrado de datos.

b. Actualización de Procedimientos y Documentación:
Actualizar políticas, procedimientos y manuales para que reflejen las lecciones aprendidas y nuevos estándares de seguridad.
c. Capacitación Correctiva: Organizar sesiones de capacitación dirigidas a los equipos o usuarios implicados en el incumplimiento, reforzando prácticas seguras y normativas de protección de datos.

3. Evaluación de la Eficacia de las Acciones Correctivas:
   a. Revisión Post-Acción Correctiva: Evaluar la eficacia de las acciones implementadas para confirmar que han corregido el problema y reducido la probabilidad de recurrencia.
   b. Simulaciones y Pruebas de Control: Realizar pruebas y simulacros para verificar que los controles ajustados funcionen como se espera y que el personal haya asimilado las nuevas prácticas.

Medidas Disciplinarias y Sanciones

Aplicar sanciones adecuadas para los incumplimientos que resulten de negligencia o actos malintencionados es fundamental para fomentar el cumplimiento de las políticas de seguridad.

1. Política de Sanciones Graduales:
   a. Clasificación de Incumplimientos: Establecer una clasificación de incumplimientos según su gravedad, considerando si el incidente fue resultado de un error no intencionado o de una falta grave.
   b. Medidas Escalonadas: Implementar medidas disciplinarias que van desde advertencias, sanciones temporales hasta la finalización del contrato en casos de incumplimiento severo o negligencia grave.
2. Notificación de Medidas Disciplinarias:
   a. Procedimientos de Comunicación: Asegurar que el personal esté informado sobre el procedimiento de sanciones y las consecuencias de no cumplir con las políticas de seguridad.
   b. Registro de Sanciones: Documentar todas las sanciones aplicadas, manteniendo un historial de incumplimientos y acciones disciplinarias para revisar el impacto y mejorar la efectividad de las medidas.
3. Refuerzo Positivo y Programas de Reconocimiento:
   a. Reconocimiento de Buenas Prácticas: Implementar un programa de reconocimiento para aquellos empleados que muestren un compromiso con la seguridad, como el reporte de incidentes y el cumplimiento ejemplar de políticas.
   b. Incentivos para la Prevención: Otorgar incentivos a los equipos que realicen mejoras en sus procedimientos de seguridad y mantengan un historial libre de incumplimientos.

Revisión y Mejora Continua del Proceso de Gestión de Incumplimientos

La revisión y mejora continua aseguran que el proceso de gestión de incumplimientos evolucione y se adapte a nuevos desafíos y cambios regulatorios.

1. Evaluación Periódica del Proceso:
    a. Revisión Semestral de Procedimientos: Evaluar el proceso de gestión de incumplimientos cada seis meses, revisando si las acciones correctivas han sido efectivas y si el procedimiento necesita ajustes.
    b. Adaptación a Cambios Regulatorios: Revisar el proceso y políticas de gestión de incumplimientos según los cambios en las normativas o requisitos legales.
2. Análisis de Patrones de Incumplimiento:
    a. Revisión de Incidentes Recurrentes: Analizar los incumplimientos recurrentes o similares para identificar patrones y debilidades en los sistemas de seguridad, mejorando así los controles.
    b. Evaluación de Lecciones Aprendidas: Incorporar lecciones aprendidas de cada incumplimiento en el proceso de mejora continua y en la capacitación del personal.
3. Informes de Incumplimiento a la Alta Dirección:
    a. Informe Trimestral: Preparar un informe trimestral que resuma los incumplimientos detectados, las acciones correctivas implementadas y las recomendaciones para reducir futuros incidentes.
    b. Revisión Estratégica: La alta dirección revisará los informes de incumplimiento para priorizar la asignación de recursos y realizar ajustes estratégicos en las políticas de seguridad.

Resumen de Responsabilidades

Para asegurar la efectividad de esta unidad, se asignarán las siguientes responsabilidades:

1. Responsable de Cumplimiento y Seguridad de la Información:
    a. Coordinar el proceso de detección, investigación y gestión de incumplimientos, garantizando la implementación de acciones correctivas y preventivas.
    b. Proporcionar informes periódicos a la alta dirección sobre el estado de cumplimiento y el progreso de las acciones correctivas.
2. Proceso de Tecnologías de Información y las Comunicaciones:
    a. Implementar los controles técnicos necesarios para la detección de incumplimientos y el monitoreo continuo de los sistemas de información.
    b. Colaborar en las investigaciones de incumplimientos y aplicar medidas técnicas para prevenir recurrencias.
3. Alta Dirección:
    a. Revisar y aprobar los informes de incumplimiento y asignar recursos para resolver problemas críticos y fortalecer el sistema de seguridad.
    b. Apoyar y promover una cultura de cumplimiento dentro de la

entidad, brindando respaldo a los equipos de seguridad y cumplimiento.

GESTIÓN DE CONTINUIDAD OPERATIVA Y RECUPERACIÓN ANTE DESASTRES

La presente unidad establece planes y procedimientos para asegurar que las funciones críticas de la Contraloría Distrital de Cartagena de Indias puedan continuar o ser restauradas rápidamente en caso de interrupciones, ya sea debido a desastres naturales, fallos tecnológicos, ataques cibernéticos, u otros eventos que afecten la disponibilidad de los sistemas de información.

Objetivo: Asegurar que la Contraloría Distrital de Cartagena de Indias cuente con un plan de continuidad operativa y recuperación ante desastres (PCO y PRD) que minimice el impacto de cualquier interrupción en los servicios críticos, garantizando la disponibilidad y accesibilidad de la información en situaciones de emergencia.

Análisis de Impacto Operativo (AIO)

El análisis de impacto operativo es la base para identificar los sistemas, procesos y activos esenciales que deben protegerse o recuperarse prioritariamente en caso de una interrupción.

1. Identificación de Procesos Críticos:
    a. Listado de Procesos Clave: Identificar y catalogar los procesos esenciales para la operatividad de la Contraloría, tales como sistemas de auditoría, gestión de datos y control financiero.
    b. Prioridad de Recuperación: Asignar un nivel de prioridad a cada proceso en función de su impacto en las operaciones y la posible afectación en caso de interrupción.
2. Evaluación del Impacto Operativo:
    a. Evaluación de Riesgos para Activos Críticos: Analizar cómo afectaría la indisponibilidad de activos críticos (datos, aplicaciones, infraestructura) a la continuidad de las funciones de la entidad.
    b. Determinación de RPO y RTO: Definir el Objetivo de Punto de Recuperación (RPO), es decir, la cantidad máxima de datos que puede perderse, y el Objetivo de Tiempo de Recuperación (RTO), que indica el tiempo máximo aceptable para restaurar el servicio.
3. Documentación del AIO:
    a. Informe de Impacto Operativo: Documentar el análisis de impacto en un informe que incluya los procesos críticos, prioridades de recuperación, RPO y RTO, y el impacto potencial de su interrupción.
    b. Actualización Continua: Revisar y actualizar el análisis de impacto operativo al menos una vez al año o cuando haya cambios significativos en la estructura operativa.

Plan de Continuidad Operativa (PCO)

El Plan de Continuidad Operativa describe las acciones necesarias para mantener la operatividad de la Contraloría Distrital de Cartagena de Indias durante una interrupción significativa.

1. Desarrollo del PCO:
    a. Definición de Estrategias de Continuidad: Crear estrategias para mitigar el impacto de eventos críticos, como el trabajo remoto para funciones clave o la migración de sistemas a la nube en caso de fallo de la infraestructura local.
    b. Asignación de Responsabilidades: Establecer un equipo de respuesta a emergencias, con funciones claramente definidas para cada miembro, como líder del equipo, coordinador de comunicación y responsables de áreas específicas (TI, finanzas, etc.).
2. Procedimientos de Continuidad por Función:
    a. Guías de Procedimiento para Procesos Críticos: Crear procedimientos detallados para cada proceso crítico, describiendo los pasos para mantener su operatividad, los recursos necesarios y los tiempos de respuesta.
    b. Provisión de Recursos Alternativos: Definir ubicaciones de respaldo, herramientas y sistemas alternativos que permitan la continuidad de los procesos esenciales (por ejemplo, respaldos en la nube).
3. Plan de Comunicación en Caso de Crisis:
    a. Establecimiento de Canales de Comunicación: Definir los canales de comunicación que se usarán para informar a los empleados y partes interesadas en caso de emergencia (correo electrónico, mensajería interna, teléfonos de emergencia).
    b. Designación de Voceros: Asignar un vocero oficial que comunique el estado de la emergencia y las medidas adoptadas, manteniendo informados a la alta dirección y a otras partes clave.
4. Simulacros y Pruebas de PCO:
    a. Simulaciones Periódicas: Realizar simulacros de continuidad al menos una vez al año para evaluar la efectividad del plan y la preparación del personal.
    b. Evaluación de Resultados y Mejoras: Analizar los resultados de las pruebas y actualizar el plan de continuidad en función de las lecciones aprendidas.

Plan de Recuperación ante Desastres (PRD)

El PRD detalla los pasos específicos para restaurar los sistemas críticos y la infraestructura de TI tras un evento de desastre, permitiendo una recuperación rápida y el retorno a las operaciones normales.

1. Identificación de Recursos de Recuperación:
    a. Recursos de Backup: Mantener copias de seguridad actualizadas de los datos críticos en ubicaciones seguras y fuera de la infraestructura principal.

   b. Infraestructura Alternativa: Identificar y asegurar el acceso a infraestructura alternativa, como servidores en la nube, para recuperación rápida en caso de desastre físico.

2. Procedimientos de Restauración:
   a. Proceso de Restauración de Sistemas Críticos: Documentar un procedimiento paso a paso para restaurar sistemas críticos, asegurando la integridad y disponibilidad de la información.
   b. Prioridades de Recuperación: Establecer el orden en el que se restaurarán los sistemas, comenzando por aquellos con los tiempos de recuperación más urgentes (RTO).
3. Copia de Seguridad y Pruebas de Restauración:
   a. Programación de Respaldos: Realizar copias de seguridad periódicas en función de los RPO definidos y verificar que se almacenan en ubicaciones seguras.
   b. Pruebas de Recuperación de Datos: Ejecutar pruebas de restauración de datos regularmente para asegurar la integridad y disponibilidad de las copias de respaldo.
4. Evaluación Post-Desastre y Actualización del PRD:
   a. Revisión del Proceso de Recuperación: Después de un incidente, realizar una evaluación completa del proceso de recuperación, identificando áreas de mejora.
   b. Actualización del Plan: Actualizar el PRD según los resultados de la evaluación y de las pruebas, adaptándolo a posibles cambios tecnológicos o operativos.

Capacitación y Sensibilización en Continuidad y Recuperación
Capacitar al personal en los planes de continuidad y recuperación es esencial para asegurar una respuesta eficaz en caso de incidentes críticos.

1. Capacitación en Procedimientos de PCO y PRD:
   a. Entrenamiento Regular: Proporcionar formación periódica para el personal que desempeña roles en el PCO y PRD, asegurando que comprenden sus responsabilidades y cómo llevar a cabo los procedimientos.
   b. Simulacros de Emergencia: Realizar simulacros para el equipo de respuesta y el personal de áreas críticas, evaluando su preparación y capacidad de reacción ante situaciones de emergencia.
2. Sensibilización General para Todo el Personal:
   a. Difusión del PCO y PRD: Informar a todos los empleados sobre la existencia del PCO y PRD, explicando los pasos a seguir en caso de emergencia y los canales de comunicación.
   b. Pruebas de Conocimiento: Realizar evaluaciones para asegurar que los empleados entienden las acciones básicas a realizar en una interrupción y saben cómo acceder a los recursos de respaldo necesarios.
3. Revisión y Actualización de Materiales de Capacitación:

a. Adaptación a Cambios en el PCO y PRD: Asegurarse de que los materiales de capacitación reflejen cualquier
actualización del PCO y PRD, y que el personal esté informado de los cambios.
b. Evaluación de Necesidades de Capacitación: Revisar periódicamente las necesidades de capacitación en función de las pruebas y simulacros, ajustando los contenidos según las áreas de mejora detectadas.

Evaluación y Mejora Continua de los Planes de Continuidad y Recuperación
Para mantener los planes de continuidad y recuperación efectivos, es necesario un proceso de revisión y actualización periódica.

1. Revisión Anual del PCO y PRD:
   a. Evaluación de Actualización: Revisar y actualizar el PCO y PRD cada año o después de cualquier cambio significativo en las operaciones o infraestructura de TI.
   b. Inclusión de Nuevos Riesgos: Incorporar nuevos riesgos identificados y ajustar los planes según las amenazas emergentes y el contexto operativo.
2. Informe de Resultados a la Alta Dirección:
   a. Presentación de Resultados de Simulacros: Informar a la alta dirección sobre los resultados de las simulaciones y evaluaciones de los planes, destacando las áreas críticas de mejora.
   b. Asignación de Recursos para Mejoras: Proponer a la alta dirección los recursos necesarios para implementar las mejoras en el PCO y PRD basadas en los hallazgos de las evaluaciones.
3. Adaptación a Nuevas Tecnologías y Normativas:
   a. Revisión de Tecnologías Emergentes: Incorporar tecnologías y herramientas que faciliten la continuidad de las operaciones y la recuperación, como soluciones de respaldo en la nube o sistemas de monitoreo avanzados.
   b. Cumplimiento Normativo: Asegurar que el PCO y PRD cumplan con las regulaciones de continuidad operativa y recuperación ante desastres aplicables, ajustándolos según las normativas vigentes.

Resumen de Responsabilidades
Para garantizar la efectividad de esta unidad, se asignarán las siguientes responsabilidades:

1. Equipo de Continuidad Operativa:
   a. Desarrollar, implementar y mantener el PCO y PRD, así como coordinar las actividades de respuesta en situaciones de emergencia.
   b. Coordinar las pruebas y simulacros de continuidad y recuperación.
2. Proceso de Tecnologías de Información y las Comunicaciones:
   a. Asegurar la realización de respaldos periódicos y la disponibilidad de infraestructura alternativa para recuperación.
   b. Apoyar en la restauración de sistemas y datos durante la ejecución del PRD.

3. Alta Dirección:
    a. Aprobar los planes de continuidad y recuperación, asignando los recursos necesarios para su implementación y pruebas.
    b. Revisar los informes de evaluación y respaldar las actualizaciones y mejoras en los planes.

EVALUACIÓN Y MEJORA CONTINUA DE LA SEGURIDAD DE LA INFORMACIÓN

Esta unidad establece un proceso de mejora continua para evaluar regularmente los sistemas de seguridad de la información en la Contraloría Distrital de Cartagena de Indias, identificar áreas de mejora y asegurar que los controles y prácticas de seguridad evolucionen conforme a las nuevas amenazas, cambios tecnológicos y requisitos normativos. Este enfoque permite mantener la seguridad de la información robusta y adaptable frente a los desafíos emergentes.

Objetivo: Implementar un proceso de mejora continua en la seguridad de la información que permita evaluar la efectividad de los controles, realizar ajustes estratégicos y adaptarse a cambios en el entorno operativo, tecnológico y regulatorio.

Evaluación Regular de la Seguridad de la Información

Realizar evaluaciones periódicas es esencial para entender el estado actual de los sistemas de seguridad y detectar cualquier vulnerabilidad o brecha que deba abordarse.

1. Revisión de Controles de Seguridad:
    a. Evaluación de Eficacia de Controles: Analizar la eficacia de los controles implementados para verificar si cumplen con sus objetivos de protección y reducir riesgos de forma efectiva.
    b. Ajustes en los Controles: Identificar oportunidades de mejora y realizar ajustes en los controles de seguridad cuando se detecten deficiencias o cambios en el entorno.
2. Análisis de Riesgos y Vulnerabilidades:
    a. Reevaluación de Riesgos: Realizar un análisis de riesgos al menos una vez al año para identificar nuevas amenazas y vulnerabilidades que puedan haber surgido.
    b. Escaneos de Vulnerabilidades y Pruebas de Penetración: Realizar pruebas técnicas, como escaneos de vulnerabilidades y pruebas de penetración, para detectar brechas de seguridad en la infraestructura de TI y corregirlas de inmediato.
3. Auditorías de Cumplimiento:
    a. Auditorías Internas y Externas: Realizar auditorías periódicas de cumplimiento con las políticas internas y normativas aplicables, asegurando que las prácticas de seguridad se mantengan alineadas con los requisitos regulatorios.
    b. Revisión de Incumplimientos Pasados: Analizar los incumplimientos de seguridad pasados y evaluar si las acciones correctivas implementadas han sido efectivas.

Indicadores de Rendimiento en Seguridad de la Información (KPIs)
Establecer indicadores clave de rendimiento (KPIs) permite medir la eficacia de los controles y detectar áreas de mejora.

1. Definición de KPIs de Seguridad:
    a. Indicadores Clave: Definir KPIs específicos como el número de incidentes de seguridad, tiempo de respuesta a incidentes, porcentaje de cumplimiento de políticas y frecuencia de acceso no autorizado.
    b. Metas para los KPIs: Establecer metas específicas para cada KPI, asegurando que reflejen el nivel de seguridad que la Contraloría busca alcanzar.
2. Monitoreo y Análisis de KPIs:
    a. Seguimiento Periódico de KPIs: Monitorear regularmente los KPIs para analizar el desempeño en seguridad de la información y la efectividad de los controles implementados.
    b. Informes de Rendimiento a la Alta Dirección: Proporcionar informes regulares a la alta dirección con el desempeño de los KPIs, destacando logros y áreas que requieren mejora.
3. Ajustes Basados en Resultados de KPIs:
    a. Evaluación de KPIs: Revisar los resultados de los KPIs en comparación con las metas establecidas y realizar ajustes en políticas, controles o procedimientos según sea necesario.
    b. Optimización de Recursos: Alinear los recursos y esfuerzos de seguridad en función de los resultados de los KPIs, asegurando que las áreas críticas reciban la atención necesaria.

Gestión de Cambios Tecnológicos y Regulatorios
La adaptación a cambios tecnológicos y regulatorios es crucial para mantener la relevancia y eficacia de la seguridad de la información.

1. Monitoreo de Cambios Tecnológicos:
    a. Identificación de Nuevas Tecnologías: Evaluar nuevas tecnologías o soluciones de seguridad que puedan mejorar la protección de los sistemas de la Contraloría Distrital de Cartagena de Indias (ej., inteligencia artificial para detección de amenazas, herramientas de monitoreo avanzado).
    b. Evaluación de Impacto Tecnológico: Realizar una evaluación del impacto de la adopción de nuevas tecnologías en los procesos de seguridad actuales y en los riesgos asociados.
2. Cumplimiento con Normativas Actualizadas:
    a. Revisión de Cambios Normativos: Monitorear y adaptar los controles de seguridad para cumplir con cambios en las regulaciones y normativas aplicables, como la Ley 1581 de 2012 o la Ley 1712 de 2014.

b. Ajuste de Políticas Internas: Actualizar las políticas de seguridad para alinearse con los nuevos requisitos legales y estándares de la industria.

3. Gestión del Cambio para el Personal:
   a. Capacitación en Nuevas Tecnologías y Políticas: Proporcionar capacitación al personal en nuevas tecnologías, políticas y procedimientos de seguridad que se implementen.
   b. Concienciación sobre Cambios Regulatorios: Asegurar que el personal entienda y cumpla con las nuevas normativas, con sesiones informativas y capacitaciones específicas en cambios regulatorios relevantes.

Retroalimentación y Lecciones Aprendidas de Incidentes
Aprender de los incidentes de seguridad permite fortalecer los controles y evitar la recurrencia de problemas.

1. Análisis Post-Incidente:
   a. Evaluación de Incidentes Pasados: Analizar los incidentes de seguridad anteriores para identificar las debilidades en los controles de seguridad y los errores en la respuesta a incidentes.
   b. Documentación de Lecciones Aprendidas: Documentar las lecciones aprendidas de cada incidente y asegurarse de que el equipo de seguridad y el personal relevante comprendan los puntos de mejora identificados.
2. Implementación de Mejoras Derivadas de Incidentes:
   a. Ajustes en Controles y Procedimientos: Adaptar los controles y procedimientos de seguridad para corregir las debilidades descubiertas a raíz de un incidente.
   b. Actualización de Planes de Respuesta a Incidentes: Revisar y mejorar el plan de respuesta a incidentes según las lecciones aprendidas, optimizando la preparación para futuros incidentes.
3. Difusión de Lecciones Aprendidas:
   a. Sesiones de Retroalimentación con el Personal: Organizar sesiones de retroalimentación para compartir las lecciones aprendidas de los incidentes de seguridad, ayudando a que el personal entienda y evite prácticas de riesgo.
   b. Incorporación de las Lecciones en la Capacitación: Incluir las lecciones aprendidas en los programas de capacitación para que todo el personal esté informado de las mejores prácticas en seguridad.

Planificación Estratégica y Recursos para la Mejora Continua
La planificación estratégica permite asignar recursos de manera eficaz para la mejora continua de la seguridad de la información.

1. Revisión Anual del Plan de Seguridad:
   a. Evaluación de la Estrategia de Seguridad: Revisar la estrategia de seguridad de la información cada año, asegurando que esté alineada con los objetivos de la Contraloría Distrital de Cartagena de Indias y con las necesidades operativas.

b. Definición de Prioridades Anuales: Identificar las áreas de seguridad prioritarias para el año siguiente y establecer
objetivos específicos para mejorar la protección de la información.

2. Asignación de Recursos Adecuados:
   a. Presupuesto de Seguridad: Asegurar que haya un presupuesto adecuado para implementar los controles de seguridad necesarios y realizar las mejoras identificadas.
   b. Recursos Humanos y Tecnológicos: Designar recursos humanos especializados y adquirir las herramientas tecnológicas requeridas para cumplir con los objetivos de seguridad.
3. Incorporación de la Mejora Continua en la Cultura Organizacional:
   a. Sensibilización sobre la Importancia de la Seguridad: Fomentar una cultura de seguridad en la entidad, donde todos los empleados comprendan la importancia de la mejora continua y estén comprometidos con las prácticas de seguridad.
   b. Reconocimiento de Buenas Prácticas: Implementar un sistema de reconocimiento para el personal que contribuya activamente a la mejora continua en seguridad, motivando la adopción de buenas prácticas.

Resumen de Responsabilidades

Para asegurar la implementación y éxito de esta unidad, se asignarán las siguientes responsabilidades:

1. Proceso de Tecnologías de la Información y las Comunicaciones:
   a. Supervisar el proceso de mejora continua, gestionar las evaluaciones de seguridad y coordinar la implementación de mejoras basadas en incidentes y resultados de auditorías.
   b. Presentar informes periódicos a la alta dirección sobre el estado de la seguridad y las mejoras implementadas.
2. Equipo de Control Interno:
   a. Realizar auditorías periódicas para evaluar la eficacia de los controles y políticas de seguridad y coordinar la alineación con normativas y regulaciones.
   b. Colaborar con el equipo de seguridad para implementar las recomendaciones derivadas de las auditorías y otros análisis de mejora.
3. Alta Dirección:
   a. Revisar y aprobar el presupuesto de seguridad y la planificación estratégica anual de mejora continua, asignando los recursos necesarios.
   b. Promover la cultura de seguridad y el compromiso con la mejora continua en toda la entidad.