La Ceja del Tambo

Empresas Públicas de La Ceja E.S.P

El Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información.

2025

SC-CER731026 SA-CER731029 OS-CER731023

Calle 20 #22-05, La Ceja (Ant)
NIT 811.009.329-0
553 77 88
www.eeppdelaceja.gov.co
esplaceja@eeppdelaceja.gov.co

1. Introducción

El Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información tiene como objetivo identificar, evaluar y mitigar los riesgos que puedan afectar la confidencialidad, integridad y disponibilidad de la información gestionada por Empresas de Servicios Públicos de La Ceja E.S.P., en cumplimiento con la normativa vigente, como la Ley 1581 de 2012 (Protección de Datos Personales), la Ley 1266 de 2008 (Tratamiento de la Información Financiera) y las disposiciones establecidas por el MINTIC.

Objetivo

El **Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información** de Empresas Públicas de La Ceja tiene como objetivo identificar, evaluar, gestionar y mitigar los riesgos asociados con la seguridad y privacidad de la información que maneja la empresa. Este plan busca proteger la integridad, disponibilidad y confidencialidad de los datos de la organización y de sus usuarios, garantizando el cumplimiento de las normativas vigentes en materia de protección de datos personales (como la Ley 1581 de 2012 y demás regulaciones locales e internacionales aplicables).

El plan debe establecer un marco de acciones preventivas y correctivas para minimizar los riesgos inherentes a las actividades diarias de la organización, mediante la implementación de controles adecuados, estrategias de mitigación, y la formación continua de los empleados. De esta manera, se busca salvaguardar la confianza de los ciudadanos, garantizar la continuidad operativa y cumplir con las expectativas de seguridad y privacidad requeridas por los stakeholders y las autoridades competentes.

Alcance

El alcance del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información de Empresas Públicas de La Ceja cubre todos los aspectos relacionados con la protección de la información y los sistemas de tecnología utilizados por la organización en el desarrollo de sus actividades. Este plan abarca los siguientes elementos clave:

1. **Ámbito Geográfico**: El plan aplica a todas las operaciones de Empresas Públicas de La Ceja dentro de su área de influencia, incluyendo sus sedes

principales y cualquier otra instalación, oficina, o infraestructura remota asociada a sus actividades.

2. **Ámbito Operativo**: Este plan cubre todos los procesos operativos y administrativos de la organización que involucran el manejo, almacenamiento, tratamiento y transmisión de datos personales y de la empresa, ya sea en formato físico o digital.

3. **Usuarios y Personal**: Abarca a todos los empleados, contratistas, proveedores, y demás partes interesadas que tengan acceso a los sistemas de información, bases de datos, y recursos tecnológicos de Empresas Públicas de La Ceja, así como los datos personales de los clientes, usuarios y demás interesados.

4. **Tecnologías y Sistemas**: El plan cubre todos los sistemas tecnológicos utilizados para gestionar, almacenar, procesar o transmitir información dentro de la organización. Esto incluye servidores, bases de datos, sistemas de comunicación, aplicaciones y cualquier infraestructura tecnológica relacionada.

5. **Cumplimiento Normativo**: El alcance incluye el cumplimiento de las leyes y normativas nacionales e internacionales en materia de seguridad y privacidad de la información, tales como la Ley 1581 de 2012, la Ley 1266 de 2008, y las disposiciones del MINTIC, así como cualquier otra regulación relevante que afecte la gestión de la seguridad y privacidad de la información.

6. **Gestión de Riesgos**: El plan abarca todas las actividades necesarias para la identificación, evaluación, tratamiento, monitoreo y revisión de los riesgos de seguridad y privacidad que puedan afectar a la información manejada por la empresa, incluyendo el análisis de vulnerabilidades, amenazas y consecuencias potenciales de los riesgos.

7. **Formación y Concienciación**: Incluye la capacitación y sensibilización continua de todos los empleados y colaboradores en materia de seguridad de la información y protección de datos personales, asegurando que todos estén alineados con las políticas y buenas prácticas de la organización.

8. **Planes de Respuesta ante Incidentes**: El alcance del plan también cubre las acciones a seguir en caso de incidentes de seguridad que afecten la información de la empresa o de los clientes, incluyendo la identificación, contención, recuperación y notificación de incidentes.

2. Identificación de Riesgos

Esta sección debe contemplar los riesgos potenciales relacionados con la seguridad de la información y la privacidad de los datos personales, alineados con los lineamientos del MINTIC y las normativas locales.

Componentes a considerar:

- **Riesgos de seguridad informática:** Ataques cibernéticos (phishing, ransomware, malware, etc.), accesos no autorizados a sistemas.
- **Riesgos físicos:** Robo de equipos, daño físico a servidores, accesos no controlados a instalaciones.
- **Riesgos organizacionales:** Falta de capacitación, errores humanos, políticas deficientes.
- **Riesgos relacionados con la privacidad:** Uso indebido de datos personales, divulgación no autorizada de información, falta de políticas de consentimientos claros.

Ejemplo de Identificación de Riesgos:

- Accesos no autorizados a información confidencial almacenada en bases de datos de clientes.
- Exposición de datos personales sensibles debido a brechas de seguridad en plataformas de servicios públicos.
- Errores humanos en el manejo de datos o configuraciones de seguridad incorrectas.
- Inadecuado manejo de contraseñas y otros mecanismos de autenticación.

3. Evaluación de Riesgos

El objetivo de esta sección es identificar, analizar y evaluar los riesgos asociados con la seguridad y privacidad de la información en la organización. Se deben considerar tanto la probabilidad de ocurrencia de los riesgos como su impacto potencial sobre las operaciones, la reputación y los activos de la empresa, con el fin de priorizar los esfuerzos de mitigación y establecer planes de respuesta adecuados.

3.1 Metodología para la Evaluación de Riesgos

La evaluación de riesgos debe basarse en una metodología clara que permita clasificar los riesgos en función de dos factores principales: **probabilidad de**

ocurrencia e **impacto potencial**. De esta manera, se puede asignar una prioridad a cada riesgo y determinar las acciones a seguir.

1. **Probabilidad de Ocurrencia**:
    - **Baja**: El riesgo tiene pocas posibilidades de materializarse. Ocurre rara vez.
    - **Media**: El riesgo tiene una probabilidad moderada de ocurrir, basado en antecedentes o en la exposición actual.
    - **Alta**: El riesgo tiene alta probabilidad de materializarse, ya sea debido a la frecuencia de amenazas conocidas o a vulnerabilidades específicas.
2. **Impacto Potencial**:
    - **Bajo**: El impacto en las operaciones o la seguridad de la información sería limitado. Los efectos no son críticos y pueden resolverse rápidamente.
    - **Medio**: El impacto afectaría las operaciones o la seguridad de la información de manera significativa, pero sería manejable con procedimientos estándar.
    - **Alto**: El impacto tendría consecuencias graves sobre las operaciones, la reputación, o la seguridad de la información. Puede generar pérdidas económicas, daños legales o afectar la continuidad del negocio.

3.2 Proceso de Evaluación de Riesgos

1. **Identificación de Riesgos**:
    - El primer paso es realizar un inventario de todos los activos de información críticos, sistemas y procesos de negocio, y luego identificar los riesgos potenciales que podrían afectar estos activos.
    - **Ejemplos de riesgos comunes**:
        - Riesgo de acceso no autorizado a la información sensible.
        - Riesgo de pérdida de datos debido a fallos en el sistema.
        - Riesgo de ciberataques o malware.

- Riesgo de incumplimiento de normativas de privacidad (como la Ley 1581 de 2012).

2. **Análisis de Riesgos**:
   - Para cada riesgo identificado, se debe determinar su probabilidad de ocurrencia y su impacto potencial en la organización. Esta evaluación se debe hacer de manera cualitativa o cuantitativa, dependiendo de la complejidad y los recursos disponibles.
   - **Ejemplo de análisis**:
     - **Riesgo de acceso no autorizado a la base de datos de clientes**:
       - **Probabilidad**: Media
       - **Impacto**: Alto
       - **Descripción**: Si un atacante obtiene acceso no autorizado a la base de datos, podría comprometer la información sensible de los clientes, lo que generaría consecuencias legales y reputacionales graves.
3. **Valoración del Riesgo**:
   - Para cada riesgo, se asignará una puntuación que combine la probabilidad de ocurrencia y el impacto potencial, lo que permite clasificar los riesgos en categorías de prioridad.
   - **Ejemplo de valoración**:
     - Riesgo de acceso no autorizado: **Probabilidad (Media)** + **Impacto (Alto)** = **Puntaje de riesgo: Alto**
     - Riesgo de pérdida de datos debido a fallos en el sistema: **Probabilidad (Baja)** + **Impacto (Alto)** = **Puntaje de riesgo: Medio**
4. **Clasificación de Riesgos**:
   - Con base en la evaluación de probabilidad e impacto, los riesgos pueden clasificarse en diferentes categorías de prioridad:
     - **Alto (Crítico)**: Requiere acciones inmediatas y planes de mitigación urgentes.

- **Medio (Moderado)**: Requiere seguimiento regular y acciones de mitigación a mediano plazo.
- **Bajo (Aceptable)**: Riesgos que son aceptables y no requieren medidas inmediatas, pero deben ser monitoreados.

3.3 Ejemplos de Evaluación de Riesgos

Aquí se incluyen ejemplos para ilustrar cómo se deben documentar los riesgos y cómo se debe realizar la evaluación en función de la probabilidad y el impacto.

1. **Riesgo: Acceso no autorizado a la base de datos de clientes**
   - **Probabilidad**: Media
   - **Impacto**: Alto
   - **Descripción**: Si un atacante obtiene acceso no autorizado a la base de datos de clientes, se podría comprometer la información personal sensible, lo que generaría consecuencias legales y reputacionales graves. Además, podría acarrear multas por incumplimiento de regulaciones como la Ley 1581 de 2012.
   - **Clasificación del riesgo**: **Alto (Crítico)**
   - **Acciones de mitigación**:
     - Implementar autenticación multifactor para el acceso a la base de datos.
     - Realizar auditorías periódicas de acceso.
     - Establecer políticas de control de acceso rigurosas.
2. **Riesgo: Pérdida de datos por fallo en el servidor**
   - **Probabilidad**: Baja
   - **Impacto**: Alto
   - **Descripción**: Un fallo técnico grave en los servidores que almacenen datos críticos podría resultar en la pérdida de información vital para las operaciones del negocio. La recuperación de los datos podría ser costosa y podría interrumpir las operaciones durante un periodo considerable.
   - **Clasificación del riesgo**: **Medio (Moderado)**

- **Acciones de mitigación**:
  - Implementar soluciones de respaldo automático y redundante.
  - Realizar pruebas de recuperación de datos de forma periódica.

3. **Riesgo: Ciberataques (ransomware)**
   - **Probabilidad**: Alta
   - **Impacto**: Alto
   - **Descripción**: La organización podría ser víctima de un ciberataque mediante ransomware, lo que podría cifrar datos críticos y exigir un rescate. Este tipo de ataque podría paralizar las operaciones y generar una pérdida de confianza por parte de los clientes y stakeholders.
   - **Clasificación del riesgo**: **Alto (Crítico)**
   - **Acciones de mitigación**:
     - Implementar herramientas de detección y prevención de intrusiones (IDS/IPS).
     - Realizar entrenamientos regulares de concienciación sobre ciberseguridad para los empleados.
     - Mantener actualizados los sistemas y aplicar parches de seguridad de manera oportuna.

3.4 Priorización de Riesgos

Con base en la evaluación, los riesgos identificados deben ser priorizados para determinar cuáles requieren atención inmediata y cuáles pueden ser tratados a largo plazo. Esta priorización debe basarse en el **puntaje global** que combina la probabilidad y el impacto, lo que facilitará la asignación de recursos para mitigar los riesgos más críticos.

1. **Alto (Crítico)**: Requiere mitigación inmediata y vigilancia continua. Los riesgos críticos deben abordarse de inmediato para minimizar su impacto.
2. **Medio (Moderado)**: Requiere medidas preventivas en el corto a mediano plazo. Estos riesgos deben ser monitoreados y gestionados de manera regular.

3. **Bajo (Aceptable)**: Aceptable, pero debe ser monitoreado. Se necesita vigilancia periódica para asegurar que no se materialicen en amenazas mayores.

3.5 Plan de Acción y Mitigación de Riesgos

Por último, para cada riesgo identificado y evaluado, deben establecerse **planes de acción específicos** que incluyan medidas de mitigación. Estos planes deben tener en cuenta la naturaleza del riesgo, su prioridad y los recursos disponibles. Además, es importante asignar responsables y establecer plazos para implementar las acciones correctivas.

4. Tratamiento de Riesgos

El objetivo de esta sección es describir las acciones concretas que se implementarán para tratar los riesgos identificados en la evaluación de riesgos. Esto incluye medidas para mitigar los riesgos, transferirlos a terceros, aceptar los riesgos cuando sea apropiado o eliminarlos por completo. Cada riesgo debe tener una acción asignada, un responsable claro y un plazo definido para su implementación.

4.1 Componentes del Tratamiento de Riesgos

1. **Mitigación**
    - **Descripción:** La mitigación se refiere a la implementación de controles que buscan reducir la probabilidad de que un riesgo ocurra o disminuir el impacto que tendría en la organización si se materializa. Las medidas de mitigación pueden incluir controles técnicos, organizacionales y procedimentales.
    - **Ejemplos de medidas de mitigación:**
        - **Firewalls y sistemas de detección de intrusiones:** Para prevenir accesos no autorizados a la red.
        - **Autenticación multifactor:** Para fortalecer la seguridad en el acceso a sistemas y aplicaciones críticas.
        - **Cifrado de datos:** Para proteger la confidencialidad de los datos almacenados y en tránsito.
        - **Actualización y parches de seguridad**: Para reducir las vulnerabilidades conocidas en los sistemas.

- **Acción a seguir:** Implementar controles preventivos y de detección para mitigar los riesgos identificados.

2. **Transferencia**

   - **Descripción:** La transferencia implica trasladar el riesgo a otra entidad, ya sea mediante contratos de seguro, externalización de ciertos procesos o el uso de proveedores especializados en la gestión de riesgos. La transferencia no elimina el riesgo, pero lo minimiza al ponerlo bajo la responsabilidad de un tercero.
   - **Ejemplos de transferencia de riesgos:**
     - **Contratar seguros:** Para cubrir posibles pérdidas derivadas de un ciberataque o un desastre natural.
     - **Externalización de servicios de seguridad:** Como la gestión de la infraestructura de TI o la auditoría de seguridad, delegando estos riesgos en un proveedor especializado.
     - **Acuerdos con proveedores:** Establecer acuerdos de nivel de servicio (SLAs) con proveedores clave para garantizar la continuidad y la seguridad.
   - **Acción a seguir**: Establecer contratos o acuerdos con terceros que asuman parte del riesgo.

3. **Aceptación**

   - **Descripción:** La aceptación de un riesgo ocurre cuando el costo de mitigación es más alto que el impacto potencial del riesgo. En estos casos, la organización decide no invertir recursos adicionales en la mitigación, pero sigue monitoreando el riesgo de manera continua.
   - **Ejemplos de aceptación de riesgos:**
     - **Riesgos de baja probabilidad e impacto:** Riesgos menores, como el acceso no autorizado ocasional a sistemas poco críticos, que se consideran aceptables por el costo de mitigación.
     - **Riesgos de bajo impacto económico:** Como el costo mínimo que se incurre si ocurre un pequeño incidente de seguridad.

- **Acción a seguir:** Realizar un análisis costo-beneficio para determinar si el riesgo debe ser aceptado**.**

4. **Eliminación**

- **Descripción:** La eliminación de un riesgo implica modificar procesos, prácticas o sistemas para evitar que el riesgo se materialice. Esto es lo más efectivo, pero no siempre es posible. En este caso, la organización toma medidas drásticas para eliminar la causa del riesgo.
- **Ejemplos de eliminación de riesgos:**
  - **Eliminar un proceso inseguro:** Si un proceso es identificado como una fuente de riesgo, se puede cambiar o eliminar el proceso para reducir el riesgo.
  - **Descontinuar el uso de tecnologías obsoletas:** Reemplazar software o hardware antiguo con soluciones más seguras.
- **Acción a seguir:** Modificar procesos o sistemas para eliminar la fuente del riesgo.

4.2 Plan de Tratamiento de Riesgos

Evaluación de riesgos:

Riesgo Identificado	Acción a Seguir	Responsable	Plazo
Riesgo: Acceso no autorizado a la base de datos de clientes	Implementar autenticación multifactor y cifrado de datos	Jefe de Seguridad Informática	3 meses
Riesgo: Pérdida de datos debido a fallo en el servidor	Implementar un sistema de respaldo automático y redundancia	Administrador de Sistemas	2 meses
Riesgo: Ciberataque **(ransomware)**	Instalar software antivirus y realizar capacitación de ciberseguridad a los empleados	Jefe de TI	1 mes
Riesgo: Incumplimiento de la Ley 1581 de 2012	Realizar auditoría de cumplimiento con la Ley 1581	Responsable de Cumplimiento	4 meses

Riesgo Identificado	Acción a Seguir	Responsable	Plazo
	de 2012 y actualizar políticas de privacidad		
Riesgo: Vulnerabilidad en software desactualizado	Establecer un proceso de actualización regular de software y parches de seguridad	Jefe de Tecnología	1 mes
Riesgo: Ataques de phishing dirigidos a empleados	Implementar filtros de correo electrónico y realizar simulaciones de ataques de phishing	Responsable de Seguridad	2 meses

4.3 Procedimiento para el Tratamiento de Riesgos

1. **Identificación de la Acción de Tratamiento**: Para cada riesgo, el equipo de seguridad debe definir qué tipo de tratamiento se aplicará: mitigación, transferencia, aceptación o eliminación.
2. **Asignación de Responsabilidades:** Se debe designar a un responsable para cada acción de tratamiento, quien será el encargado de implementar las medidas y realizar un seguimiento.
3. **Establecimiento de Plazos:** Cada acción debe tener un plazo claro para su implementación. Esto asegurará que los riesgos sean tratados dentro de un marco temporal adecuado.
4. **Monitoreo y Seguimiento:** Una vez que se implementen las acciones de tratamiento, debe realizarse un monitoreo continuo para asegurarse de que los controles sean efectivos y que los riesgos se mantengan dentro de niveles aceptables.
5. **Revisión Periódica:** Se deben revisar las acciones de tratamiento de forma periódica para asegurarse de que siguen siendo relevantes y eficaces ante los cambios en el entorno de riesgos.

4.4 Informe de Tratamiento de Riesgos

El proceso de tratamiento debe ser documentado en un informe detallado que incluya:

- **Descripción del riesgo:** Un resumen de cada riesgo identificado.
- **Tipo de tratamiento:** Detalles sobre si el riesgo será mitigado, transferido, aceptado o eliminado.
- **Acciones a implementar:** Una descripción clara de las medidas que se tomarán.
- **Responsables y plazos:** Asignación de responsabilidades y plazos para la implementación de cada acción.
- **Monitoreo y seguimiento:** Estrategias para asegurar que las medidas sean efectivas a largo plazo.

5. Plan de Continuidad y Recuperación ante Desastres

El objetivo de este componente es asegurar que la organización pueda continuar sus operaciones críticas y recuperar la seguridad y la integridad de la información en caso de un incidente que afecte la infraestructura tecnológica o los sistemas de información. Este plan debe incluir acciones detalladas para garantizar la protección de datos, la recuperación de servicios y la mínima interrupción de la actividad empresarial.

5.1 Componentes Principales del Plan de Continuidad y Recuperación

1. **Respaldo de Información Crítica**
    - **Objetivo**: Asegurar que la información crítica de la organización se respalde de forma periódica y que esté disponible para su recuperación inmediata en caso de fallo del sistema o pérdida de datos.
    - **Acciones clave**:
        - **Respaldo de datos periódicos**: Implementar un sistema de respaldo automático y manual para las bases de datos y otros archivos críticos.
        - **Redundancia de datos**: Implementar sistemas de redundancia para garantizar que, en caso de fallo de un sistema, los datos no se pierdan. Esto incluye configuraciones como el uso de almacenamiento en la nube o servidores de respaldo.
        - **Replicación en tiempo real**: Asegurar que los sistemas de servidores replicados en tiempo real puedan tomar el control

de la operación sin perder la información o interrumpir el servicio.

- **Monitoreo de respaldos**: Establecer procedimientos de monitoreo para verificar regularmente que los respaldos se estén realizando correctamente y que los datos sean recuperables.

2. **Planes de Contingencia**

Establecer protocolos claros y procedimientos detallados para la recuperación de sistemas, aplicaciones y datos ante incidentes o desastres, minimizando el tiempo de inactividad y la pérdida de datos.

- **Acciones clave**:
  - **Planes de recuperación ante desastres (DRP)**: Desarrollar un Plan de Recuperación ante Desastres que detalle los pasos a seguir para restaurar los sistemas y servicios esenciales.
  - **Recuperación de servicios críticos**: Definir cuáles son los servicios críticos de la organización y establecer procedimientos para su rápida restauración en caso de fallo.
  - **Establecimiento de prioridades**: Identificar los sistemas y aplicaciones más críticos para la operación de la empresa y establecer las prioridades para su recuperación.
  - **Simulacros y pruebas**: Realizar pruebas periódicas de los procedimientos de recuperación para verificar su eficacia y asegurarse de que el personal esté preparado ante posibles incidentes.

3. **Plan de Comunicación en Caso de Desastre**

- **Objetivo**: Garantizar que haya una comunicación efectiva durante y después de un desastre o incidente, tanto interna como externamente.
- **Acciones clave**:
  - **Protocolos de comunicación**: Definir cómo se comunicará la información sobre el incidente a los empleados, clientes, proveedores y otras partes interesadas.

- **Asignación de roles y responsabilidades**: Establecer roles claros para quienes serán responsables de la comunicación durante un incidente, incluyendo contactos de emergencia y portavoces autorizados.
- **Uso de múltiples canales**: Asegurar que se utilicen múltiples canales de comunicación (correo electrónico, mensajes de texto, llamadas telefónicas) para asegurar que la información llegue a todos los interesados de manera oportuna.

4. **Capacitación y Concienciación sobre Continuidad**
   - **Objetivo**: Asegurar que todo el personal esté capacitado en el Plan de Continuidad y Recuperación ante Desastres, y que conozcan sus roles y responsabilidades en caso de un incidente.
   - **Acciones clave**:
     - **Entrenamiento regular**: Realizar programas de capacitación anuales para que el personal esté familiarizado con los procedimientos de emergencia, incluidos los pasos a seguir en caso de incidentes que afecten la seguridad de la información.
     - **Simulacros de recuperación**: Organizar simulacros de desastre para poner a prueba la efectividad del plan, los tiempos de recuperación y la capacidad de los empleados para actuar bajo presión.
     - **Documentación clara**: Proporcionar documentación clara y accesible sobre los procedimientos a seguir en caso de desastre, para que los empleados puedan consultar rápidamente las acciones necesarias.
5. **Evaluación y Mejora Continua del Plan**
   - **Objetivo**: Asegurar que el Plan de Continuidad y Recuperación ante Desastres se mantenga actualizado, eficiente y alineado con los cambios organizacionales, tecnológicos y las nuevas amenazas.
   - **Acciones clave**:
     - **Revisión periódica**: El plan debe ser revisado anualmente o cuando se presenten cambios importantes en la infraestructura tecnológica o en los procesos de negocio. Esto

incluye evaluar si el plan sigue siendo adecuado para los riesgos actuales.

- **Lecciones aprendidas de incidentes anteriores**: Después de un incidente o simulacro, realizar una evaluación para identificar áreas de mejora en los procedimientos y en la implementación del plan.
- **Actualización de protocolos**: Basado en los resultados de las revisiones y las lecciones aprendidas, actualizar los protocolos, procesos y herramientas utilizados en el plan de continuidad.

5.2 Estrategias de Recuperación

1. **Recuperación a Nivel de Sistema**
   - **Objetivo**: Recuperar los sistemas operativos y aplicaciones de misión crítica en el menor tiempo posible.
   - **Acciones clave**:
     - **Imágenes de disco y sistemas de virtualización**: Crear imágenes de disco completas de los sistemas operativos y aplicaciones más importantes para facilitar su recuperación rápida.
     - **Instalación de servidores de contingencia**: Tener servidores de contingencia disponibles para asumir la carga en caso de que los sistemas principales fallen.
2. **Recuperación a Nivel de Base de Datos**
   - **Objetivo**: Asegurar la integridad y disponibilidad de las bases de datos críticas para las operaciones del negocio.
   - **Acciones clave**:
     - **Respaldo de bases de datos**: Implementar respaldos frecuentes y replicación en tiempo real de las bases de datos.
     - **Restauración rápida**: Contar con procedimientos para restaurar bases de datos desde respaldos de forma eficiente.

3. **Recuperación a Nivel de Red**
    - **Objetivo**: Restaurar las redes de comunicación de la organización rápidamente para minimizar el tiempo de inactividad.
    - **Acciones clave**:
        - **Redundancia de red**: Implementar redes redundantes y tecnologías de balanceo de carga para asegurar que las comunicaciones y el tráfico de datos no se interrumpan.
        - **Procedimientos para recuperación de conectividad**: Establecer procedimientos para restablecer la conectividad en caso de fallos de red, incluyendo el uso de enlaces alternativos o provisionales.

5.3 responsables del Plan de Continuidad y Recuperación

El Plan de Continuidad y Recuperación debe contar con una estructura de responsables claramente definida para asegurar su ejecución efectiva.

1. **Responsable de Continuidad y Recuperación**:
    - **Rol**: Dirigir la implementación, actualización y gestión del plan.
    - **Responsabilidad**: Asegurarse de que el plan esté actualizado, que los sistemas de respaldo funcionen correctamente y que los empleados estén capacitados.
2. **Equipo de Respuesta ante Incidentes**:
    - **Rol**: Encargados de llevar a cabo las acciones inmediatas de recuperación tras un incidente.
    - **Responsabilidad**: Implementar los procedimientos de recuperación y coordinar la restauración de los sistemas y datos críticos.
3. **Equipo de Comunicación**:
    - **Rol**: Responsable de gestionar las comunicaciones internas y externas durante y después de un incidente.
    - **Responsabilidad**: Garantizar que toda la información relevante sea comunicada de manera clara y eficiente.

6. Capacitación y Concienciación en Seguridad y Privacidad de la Información

Objetivo

El objetivo principal de este componente es asegurar que todos los empleados de Empresas de Servicios Públicos de La Ceja E.S.P. estén debidamente capacitados y concienciados sobre la importancia de la seguridad y privacidad de la información, promoviendo una cultura organizacional basada en buenas prácticas de protección de datos y manejo seguro de la información.

6.1 Plan de Capacitación

El plan debe definir las actividades, métodos, frecuencia y responsables de la capacitación y concienciación.

Actividades principales:

1. **Talleres y seminarios**:
    - **Frecuencia**: Trimestrales o semestrales, dependiendo del nivel de riesgo o cambios normativos.
    - **Temas**:
        - Gestión de riesgos informáticos.
        - Protección de datos personales y cumplimiento con la Ley 1581 de 2012.
        - Buenas prácticas para la gestión de contraseñas.
        - Uso seguro de equipos y dispositivos (móviles, computadoras, servidores).
        - Identificación de amenazas como phishing, ransomware y otros ataques cibernéticos.
    - **Metodología**:
        - Presenciales o virtuales, según disponibilidad.
        - Incluir ejemplos prácticos, simulaciones o casos reales.
        - Presentaciones interactivas, videos educativos y cuestionarios.

2. **Capacitación inicial para nuevos empleados**:
    - **Temas**:
        - Introducción a la política de seguridad y privacidad de la información.
        - Responsabilidades legales y organizacionales en el manejo de la información.
        - Uso adecuado de herramientas y sistemas corporativos.
    - **Frecuencia**: Al momento de la contratación.
3. **Sesiones de actualización**:
    - **Frecuencia**: Anuales o cuando haya cambios normativos importantes (como actualizaciones en la Ley de Protección de Datos Personales).
    - **Temas**:
        - Nuevas amenazas y tendencias en ciberseguridad.
        - Actualización sobre normativas nacionales e internacionales.

6.2 Estrategias de Concienciación

La concienciación es un proceso continuo que busca sensibilizar a todos los miembros de la organización sobre la importancia de la seguridad de la información.

Acciones clave:

1. **Campañas de sensibilización**:
    - **Frecuencia**: Trimestrales o bimestrales.
    - **Métodos**:
        - Boletines informativos (por correo electrónico o carteleras internas).
        - Recordatorios sobre buenas prácticas de seguridad (ej. creación de contraseñas seguras).
        - Videos cortos sobre ciberseguridad y protección de datos.

- Posters o banners con mensajes clave sobre privacidad y seguridad.

- **Temas**:
  - Consecuencias de un manejo incorrecto de la información.
  - Medidas simples para proteger la información personal y corporativa.

2. **Simulaciones de ciberataques** (ej. phishing):
   - **Frecuencia**: Anual o semestral.
   - **Objetivo**: Evaluar la capacidad de los empleados para identificar amenazas comunes.
   - **Metodología**: Enviar correos simulados de phishing o realizar otras actividades para que los empleados practiquen cómo reconocer ataques.
3. **Programas de incentivos**:
   - **Objetivo**: Fomentar la participación activa en las iniciativas de seguridad.
   - **Métodos**:
     - Premios o reconocimientos a empleados que sigan las mejores prácticas de seguridad.
     - Competencias de conocimiento sobre seguridad de la información (ej. concursos de preguntas y respuestas).

6.3 Evaluación de Conocimientos

Es importante medir regularmente el nivel de conocimiento de los empleados para garantizar que las capacitaciones estén siendo efectivas y que el personal esté preparado para enfrentar riesgos asociados con la seguridad y privacidad de la información.

Métodos de evaluación:

1. **Pruebas periódicas de conocimientos**:
   - **Frecuencia**: Trimestrales o anuales.
   - **Contenido**:

- Cuestionarios sobre el manejo de información sensible.
- Evaluación de las políticas de seguridad interna.
- Preguntas sobre medidas preventivas ante amenazas de seguridad.

2. **Encuestas de satisfacción**:
    - **Objetivo**: Recoger retroalimentación sobre las capacitaciones para mejorar los programas de formación.
    - **Frecuencia**: Después de cada taller o capacitación.
    - **Contenido**: Preguntas sobre la claridad de los temas, la utilidad de los materiales, la accesibilidad de las capacitaciones, etc.
3. **Simulaciones de incidentes**:
    - **Objetivo**: Evaluar la respuesta del personal ante incidentes reales de seguridad.
    - **Frecuencia**: Anual o cuando se identifiquen nuevos riesgos.
    - **Metodología**: Simular una brecha de seguridad (como un ataque de phishing) y evaluar la respuesta del equipo.

6.4 Responsables y Recursos

Definir los responsables de la capacitación y concienciación, así como los recursos necesarios para llevar a cabo las actividades.

Responsables:

- **Equipo de Seguridad Informática**: Diseño y ejecución de programas de capacitación técnica.
- **Departamento de Recursos Humanos**: Coordinación de la logística de las capacitaciones, asegurando que todos los empleados reciban la formación necesaria.
- **Gerentes de área**: Asegurar que los equipos reciban las capacitaciones pertinentes y monitorear el cumplimiento.

Recursos:

- **Presupuesto** para talleres, seminarios y materiales de capacitación.

- **Plataformas de capacitación virtual** (si se aplica) para alcanzar a los empleados de manera eficiente.

6.5 Plan de Mejora Continua

El proceso de capacitación y concienciación debe ser flexible y adaptarse a los cambios tecnológicos, nuevos riesgos y normativas. Es fundamental tener un plan de mejora continua para asegurar la efectividad a largo plazo.

Acciones:

- Revisión anual del plan de capacitación.
- Análisis de la evolución de los riesgos y amenazas.
- Actualización de los materiales de capacitación según las nuevas normativas o tecnologías.

Ejemplo:

- Realización de talleres trimestrales sobre gestión de riesgos, manejo de contraseñas y protección de datos personales.
- Evaluación periódica de conocimientos de seguridad a través de pruebas internas.

7. Monitoreo y Auditoría de Seguridad de la Información

El objetivo de este componente es establecer un proceso continuo y efectivo para monitorear, evaluar y auditar las medidas de seguridad implementadas en la organización, detectar vulnerabilidades a tiempo, garantizar el cumplimiento de las políticas de seguridad y privacidad de la información, y asegurar que las actividades de tratamiento de datos sean seguras y conforme a la normativa vigente.

7.1 Actividades de Monitoreo

El monitoreo continuo es fundamental para identificar posibles amenazas y detectar actividades anómalas a tiempo.

Actividades clave:

1. **Monitoreo de accesos a sistemas y redes:**
    - **Descripción:** Controlar y registrar todos los accesos a sistemas críticos, bases de datos, aplicaciones y servidores para detectar accesos no autorizados o actividades sospechosas.

- **Herramientas:** Implementación de sistemas de gestión de eventos e información de seguridad (SIEM) que permitan detectar patrones irregulares en los accesos.
- **Frecuencia:** Continuo, con revisión periódica de los registros.
- **Ejemplo:** Monitoreo de intentos de acceso a la base de datos de clientes y sistemas de gestión de servicios públicos.

2. **Detección de actividades sospechosas:**
   - **Descripción:** Identificación de comportamientos inusuales en la red, como intentos de intrusión, malware o transmisión de datos sensibles a ubicaciones no autorizadas.
   - **Herramientas:** Sistemas de detección de intrusos (IDS) y software de análisis de tráfico de red.
   - **Frecuencia**: Continuo, con alertas en tiempo real.
3. **Monitoreo de dispositivos móviles y endpoints:**
   - **Descripción:** Asegurar que todos los dispositivos móviles y equipos finales (como laptops, computadoras de escritorio) estén protegidos y sean monitorizados para evitar riesgos de seguridad.
   - **Herramientas:** Soluciones de gestión de dispositivos móviles (MDM) y software de seguridad en endpoints.
   - **Frecuencia:** Continuo, con alertas periódicas sobre vulnerabilidades.

7.2 Actividades de Auditoría

Las auditorías periódicas permiten revisar el cumplimiento de las políticas de seguridad y garantizar que las medidas implementadas sean efectivas.

Actividades clave:

1. **Auditorías de seguridad periódicas:**
   - **Descripción:** Realizar auditorías de seguridad semestrales o anuales para evaluar el cumplimiento de las políticas de seguridad de la información, identificar vulnerabilidades y proponer medidas correctivas.
   - **Frecuencia:** Semestral o anual.

- **Áreas a auditar:**
  - Control de acceso a sistemas y datos.
  - Uso adecuado de contraseñas y autenticación.
  - Configuración de sistemas de seguridad (firewalls, antivirus, etc.).
  - Evaluación de los registros de actividad.
- **Responsables**: Auditores internos de seguridad, o consultores externos especializados.

2. **Revisión de políticas y procedimientos de seguridad:**
   - **Descripción:** Auditar las políticas y procedimientos establecidos para garantizar que estén alineados con la normativa vigente y con las mejores prácticas de seguridad.
   - **Frecuencia:** Anual.
   - **Áreas a revisar:**
     - Política de protección de datos personales.
     - Procedimientos de gestión de incidentes de seguridad.
     - Protocolos de encriptación de datos sensibles.
   - **Responsables:** Equipo de seguridad informática y equipo legal.
3. **Evaluación de la efectividad de las medidas de seguridad:**
   - **Descripción:** Realizar pruebas de penetración o simulaciones de ataques (ethical hacking) para evaluar la robustez de las defensas de la infraestructura tecnológica.
   - **Frecuencia**: Anual o cuando se implementen nuevos sistemas o infraestructuras críticas.
   - **Responsables:** Consultores externos o equipo interno de seguridad cibernética.
   - **Ejemplo**: Simulaciones de ataques de ransomware o pruebas de vulnerabilidades en la infraestructura de servidores.

7.3 Herramientas y Recursos de Monitoreo y Auditoría

Componentes clave:

1. **Sistema de Gestión de Seguridad de la Información (SGSI):**
   - **Descripción:** Implementación de un SGSI basado en estándares internacionales como ISO 27001 o NIST.
   - **Función:** Asegurar que todas las actividades de monitoreo y auditoría estén centralizadas, gestionadas y documentadas correctamente.
2. **Sistemas de Monitoreo y Alerta:**
   - **Descripción:** Uso de plataformas de monitoreo continuo (SIEM, IDS/IPS, soluciones de UTM) para la detección temprana de incidentes y generación de alertas.
   - **Ejemplo:** Splunk, SolarWinds, o sistemas similares que permiten monitorear tráfico, accesos y eventos en tiempo real.
3. **Software de Auditoría:**
   - **Descripción:** Herramientas que permiten auditar el acceso a sistemas y la gestión de usuarios, así como generar informes detallados sobre las actividades de seguridad.
   - **Ejemplo:** Tools como Nessus, OpenVAS o Wireshark para auditorías de vulnerabilidad y de redes.

7.4 Respuesta ante Incidentes Detectados

El monitoreo y la auditoría deben estar estrechamente relacionados con la respuesta ante incidentes de seguridad, asegurando una acción rápida y efectiva.

Acciones a seguir:

1. **Generación de alertas:**
   - **Descripción:** Establecer un sistema de alertas automáticas para notificar de inmediato cuando se detecten accesos no autorizados o actividades sospechosas.
   - **Frecuencia:** En tiempo real.

- **Responsables:** Equipo de seguridad informática.

2. **Análisis y mitigación de incidentes:**
   - **Descripción:** Una vez detectado un incidente, realizar un análisis forense para determinar el alcance del mismo y tomar acciones correctivas inmediatas.
   - **Acciones:**
     - **Aislar el sistema comprometido.**
     - **Realizar una investigación forense para entender el origen del incidente.**
     - **Implementar medidas correctivas (actualización de parches, cambios en credenciales de acceso, etc.).**
3. **Informe de incidentes:**
   - **Descripción:** Documentar todos los incidentes de seguridad y las acciones tomadas, para generar un informe detallado que se use como base para mejorar las políticas de seguridad.
   - **Frecuencia:** Después de cada incidente.
   - **Responsables:** Equipo de seguridad.

7.5 Cumplimiento y Mejora Continua

El monitoreo y la auditoría no solo deben evaluar el cumplimiento, sino también permitir la mejora continua de los controles de seguridad.

Acciones clave:

1. **Revisión de informes de auditoría:**
   - **Descripción:** Revisar los informes generados a partir de auditorías y monitoreos para determinar las áreas que requieren mejoras.
   - **Frecuencia:** Anual o cuando se identifiquen nuevas vulnerabilidades.
2. **Ajuste de medidas de seguridad:**
   - **Descripción**: A partir de los resultados de las auditorías, ajustar las políticas, procedimientos y controles de seguridad para mejorar la protección de la información.

- **Frecuencia**: Después de cada auditoría o incidente significativo.

8. Cumplimiento Normativo en Seguridad y Privacidad de la Información

El objetivo principal de este componente es garantizar que todas las actividades de tratamiento de datos y las medidas de seguridad implementadas en Empresas de Servicios Públicos de La Ceja E.S.P. cumplan con la normativa vigente en materia de protección de datos personales y seguridad de la información, como la Ley 1581 de 2012, la Ley 1266 de 2008 y las directrices establecidas por el MINTIC.

8.1 Normativa Aplicable

En esta sección, se debe listar y explicar las principales leyes y regulaciones que rigen el tratamiento de la información y la seguridad de los datos personales en Colombia, asegurando que todas las actividades cumplan con los requisitos legales.

Leyes y normativas clave:

1. **Ley 1581 de 2012 – Ley de Protección de Datos Personales:**
   - **Objetivo: Establecer las disposiciones generales para la protección de datos personales en Colombia.**
   - **Principios fundamentales:**
     - Principio de legalidad.
     - Principio de finalidad.
     - Principio de transparencia.
     - Principio de acceso y circulación restringida.
     - Principio de seguridad.
     - Principio de confidencialidad.
   - **Requisitos clave:**
     - Obtención del consentimiento expreso para el tratamiento de datos personales.
     - Implementación de medidas de seguridad para proteger los datos personales.

- Registro de bases de datos en el registro de bases de datos personales de la SIC (Superintendencia de Industria y Comercio).

2. **Ley 1266 de 2008 – Ley de Habeas Data:**
   - **Objetivo:** Regula el manejo de la información personal en el ámbito financiero, comercial, y crediticio.
   - **Requisitos clave:**
     - Garantizar la veracidad, exactitud y actualización de los datos personales.
     - Derecho de los titulares de los datos a acceder, rectificar y actualizar su información.
3. **Reglamento General de Protección de Datos (GDPR, por sus siglas en inglés) – Si la empresa tiene interacción con datos personales de ciudadanos europeos, debe considerar las implicaciones del GDPR.**
   - **Requisitos clave:**
     - Consentimiento explícito para la recolección de datos.
     - Derecho al olvido.
     - Evaluaciones de impacto en la protección de datos.
4. **Directrices del Ministerio de Tecnologías de la Información y las Comunicaciones (MINTIC):**
   - **Objetivo:** Proveer un marco regulador para la gestión de la seguridad y privacidad de la información en el ámbito colombiano.
   - **Requisitos clave:**
     - Alineación con las políticas de seguridad de la información y la ciberseguridad del país.
     - Cumplimiento con el marco normativo para la protección de la infraestructura crítica de la información.
     - Aplicación de las normas de seguridad en el tratamiento de la información.

Calle 20 #22-05, La Ceja (Ant)
NIT 811.009.329-0
553 77 88
www.eeppdelaceja.gov.co
esplaceja@eeppdelaceja.gov.co

8.2 Políticas Internas de Cumplimiento

Las políticas internas deben reflejar el cumplimiento de las leyes y normas vigentes en cuanto al tratamiento y protección de la información.

Componentes clave:

1. **Política de Protección de Datos Personales:**
    - **Descripción:** Definir los principios, procedimientos y medidas que garantizarán el cumplimiento de la Ley 1581 de 2012 y el respeto a los derechos de los titulares de datos personales.
    - **Elementos clave:**
        - Definición de los fines para los cuales se recolectan y procesan los datos.
        - Procedimientos para obtener el consentimiento expreso de los titulares.
        - Medidas para garantizar la confidencialidad, integridad y disponibilidad de los datos.
        - Protocolos de respuesta ante incidentes de seguridad que involucren datos personales.
2. **Política de Seguridad de la Información:**
    - **Descripción:** Garantizar que las medidas de seguridad implementadas sean adecuadas para proteger la información de acuerdo con las exigencias de la normatividad vigente.
    - **Elementos clave:**
        - Definición de roles y responsabilidades en la gestión de la seguridad.
        - Procedimientos para la protección de la infraestructura tecnológica.
        - Plan de respuesta ante incidentes de seguridad.
        - Capacitación continua a los empleados sobre buenas prácticas de seguridad.

3. **Política de Control de Accesos:**
    - **Descripción:** Establecer controles de acceso a la información, asegurando que solo las personas autorizadas puedan acceder a la información sensible.
    - **Elementos clave:**
        - Definición de niveles de acceso.
        - Procedimientos para la creación, modificación y eliminación de cuentas de usuario.
        - Auditoría y monitoreo de los accesos a sistemas críticos.

8.3 Evaluación de Cumplimiento

El cumplimiento normativo debe ser evaluado de manera continua a través de auditorías y revisiones periódicas, con el fin de garantizar que se mantengan los estándares de seguridad y privacidad establecidos por la legislación.

Actividades clave:

1. **Auditorías internas de cumplimiento:**
    - **Frecuencia:** Anual o tras la implementación de nuevos sistemas o servicios.
    - **Objetivo**: Evaluar el cumplimiento de las políticas internas con la legislación vigente.
    - Áreas a revisar:
        - Protección de datos personales.
        - Gestión de accesos y privilegios.
        - Protección de la infraestructura tecnológica.
        - Cumplimiento con las normativas del MINTIC.
2. **Revisión de documentos de cumplimiento:**
    - **Descripción:** Revisión de los registros de tratamiento de datos, consentimientos, y auditorías de seguridad.
    - **Frecuencia:** Anual o tras cualquier cambio en la legislación.

- **Responsables**: Departamento de Seguridad Informática y/o equipo legal.

3. **Evaluación de riesgos:**
   - **Descripción:** Realización de evaluaciones periódicas de riesgos para identificar nuevas amenazas que puedan comprometer la seguridad de la información y la privacidad de los datos.
   - **Frecuencia**: Anual o en caso de cambios importantes en la infraestructura tecnológica o procesos.

8.4 Medidas Correctivas y Preventivas

En caso de que se detecten incumplimientos durante las auditorías o evaluaciones de riesgos, deben tomarse medidas correctivas y preventivas para rectificar cualquier irregularidad y evitar futuros incidentes.

Acciones clave:

1. **Medidas correctivas:**
   - **Descripción:** Implementación de acciones para rectificar los incumplimientos detectados.
   - **Ejemplos:** Actualización de políticas, implementación de nuevas tecnologías de seguridad, ajuste en los procesos de tratamiento de datos.
2. **Medidas preventivas:**
   - **Descripción:** Implementación de acciones para prevenir la ocurrencia de riesgos futuros.
   - **Ejemplos:** Mejora en la formación y concienciación de los empleados, fortalecimiento de controles de acceso, implementación de nuevas medidas de encriptación de datos.

8.5 responsables del Cumplimiento Normativo

Es importante definir los roles y responsabilidades dentro de la organización para garantizar que el cumplimiento normativo sea gestionado de manera efectiva.

Responsables:

- **Comité de Cumplimiento:** Responsables de la supervisión y gestión de la implementación de políticas y procesos de cumplimiento.

- **Oficial de Protección de Datos (DPO):** Responsable de garantizar el cumplimiento de la Ley 1581 de 2012 y otras normativas relacionadas con la protección de datos personales.
- **Departamento Legal:** Asegura que todas las actividades de tratamiento de información estén alineadas con las leyes vigentes.
- **Departamento de Seguridad Informática:** Responsable de la implementación de medidas de seguridad para proteger la información conforme a la normativa.

9. Revisión y Actualización del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información

El objetivo de este componente es garantizar que el Plan de Tratamiento de Riesgos se mantenga actualizado, pertinente y efectivo frente a los riesgos cambiantes, las amenazas emergentes y cualquier modificación significativa en la estructura de la organización, la normativa o los sistemas tecnológicos. La revisión periódica y la actualización de este plan asegurarán que la empresa esté siempre preparada para proteger la información de acuerdo con las mejores prácticas y los requisitos legales.

9.1 Actividades de Revisión y Actualización

Este componente describe las acciones y procedimientos para revisar y actualizar el plan, asegurando su pertinencia y eficacia a lo largo del tiempo.

1. **Revisión Anual del Plan:**
    - **Descripción:** El Comité de Seguridad realizará una revisión anual del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información para evaluar su efectividad en la mitigación de los riesgos identificados, detectar posibles áreas de mejora y garantizar que se mantenga alineado con los cambios en el entorno de amenazas y los objetivos organizacionales.
    - **Frecuencia:** Anual.
    - **Responsables:** Comité de Seguridad.
    - **Acciones:**
        - Evaluar si los riesgos identificados han cambiado o si han surgido nuevos riesgos.

- Revisar el cumplimiento de las políticas y medidas de seguridad.
- Confirmar que el plan sigue alineado con las normativas locales e internacionales.

2. **Actualización en Caso de Cambios Significativos:**
   - **Descripción**: Si se presentan cambios significativos en el entorno de amenazas (por ejemplo, la aparición de nuevas ciberamenazas, vulnerabilidades tecnológicas o cambios regulatorios), el plan será actualizado de inmediato para incorporar nuevas medidas y estrategias de mitigación de riesgos.
   - **Frecuencia:** Según sea necesario, cuando se identifiquen cambios significativos en el entorno.
   - **Ejemplos de cambios significativos:**
     - Nuevas amenazas de seguridad cibernética (como el aumento de ataques de ransomware o vulnerabilidades en software utilizado).
     - Modificaciones en la legislación relacionada con la protección de datos personales (por ejemplo, cambios en la Ley 1581 de 2012 o nuevas regulaciones del MINTIC).
     - Implementación de nuevas tecnologías o sistemas dentro de la organización que puedan implicar nuevos riesgos.
   - **Responsables**: Comité de Seguridad, junto con el equipo de TI y de cumplimiento normativo.
3. **Revisión de Resultados de Auditorías y Monitoreos:**
   - **Descripción**: Tras cada auditoría interna, evaluación de riesgos o monitoreo de seguridad, se revisarán los resultados para identificar lecciones aprendidas y aplicar ajustes al plan de tratamiento de riesgos.
   - **Frecuencia:** Después de cada auditoría o monitoreo relevante.
   - **Responsables:** Comité de Seguridad, equipo de auditoría interna.

4. **Revisión de Impacto de Incidentes de Seguridad:**
    - **Descripción:** En caso de incidentes de seguridad (por ejemplo, brechas de datos, ciberataques o fallos tecnológicos) se llevará a cabo una revisión post-incidente para identificar áreas de mejora en el plan y actualizar las estrategias de prevención y mitigación de riesgos.
    - **Frecuencia:** Después de cada incidente significativo.
    - **Responsables:** Comité de Seguridad, equipo de respuesta a incidentes de seguridad.

9.2 Componente de Comité de Seguridad

El Comité de Seguridad tiene un papel central en la revisión y actualización del plan, ya que son los encargados de garantizar que las medidas implementadas sean adecuadas y efectivas frente a los riesgos cambiantes.

Composición del Comité de Seguridad:

1. **Responsable de Seguridad Informática:**
    - **Rol:** Dirige las actividades relacionadas con la protección de la infraestructura tecnológica y la gestión de incidentes de seguridad.
    - **Responsabilidad:** Liderar la implementación de medidas de protección cibernética y las actualizaciones del plan ante nuevos riesgos tecnológicos.
2. **Responsable de Cumplimiento Normativo:**
    - **Rol:** Asegura que el plan se ajuste a las normativas legales y regulaciones locales e internacionales sobre protección de datos y privacidad de la información.
    - **Responsabilidad:** Revisar la conformidad con la Ley 1581 de 2012, la Ley 1266 de 2008, las disposiciones del MINTIC y otras regulaciones pertinentes.
3. **Responsable de Riesgos y Auditoría:**
    - **Rol:** Evaluar los riesgos a los que se enfrenta la organización y auditar el cumplimiento del plan de seguridad.
    - **Responsabilidad:** Supervisar las auditorías internas y externas de seguridad, y coordinar la revisión de los riesgos identificados.

4. **Responsable de Infraestructura y Tecnología:**
    - **Rol:** Dirige la implementación y mantenimiento de los sistemas tecnológicos que apoyan la seguridad de la información.
    - **Responsabilidad:** Asegurar que la infraestructura tecnológica esté actualizada y sea capaz de enfrentar las amenazas emergentes.
5. **Responsable de Capacitación y Concienciación:**
    - **Rol:** Encargado de diseñar e implementar programas de capacitación para empleados en materia de seguridad de la información.
    - **Responsabilidad:** Coordinar las actividades de formación continua y garantizar que todos los miembros de la organización estén al tanto de las actualizaciones en políticas de seguridad.
6. **Responsable de Comunicación y Gestión de Incidentes:**
    - **Rol:** Maneja la comunicación interna y externa relacionada con incidentes de seguridad.
    - **Responsabilidad:** Garantizar una respuesta eficaz ante incidentes y la correcta comunicación de los mismos a las partes interesadas.

Frecuencia de Reuniones del Comité de Seguridad:

- El Comité de Seguridad se reunirá al menos una vez al trimestre para revisar el estado del plan de tratamiento de riesgos y evaluar los resultados de las auditorías, incidentes y cambios relevantes en la infraestructura o la legislación. Además, se realizará una reunión extraordinaria en caso de que se identifiquen cambios significativos que requieran una actualización urgente del plan.

9.3 Procedimiento de Actualización del Plan

El procedimiento de actualización debe seguir una serie de pasos estructurados para garantizar que cualquier cambio en el plan sea realizado de manera efectiva y con la participación de todas las partes responsables.

1. **Identificación de la Necesidad de Actualización:**
    - A través de auditorías, incidentes de seguridad, evaluaciones de riesgos, cambios en la legislación, o la revisión anual del plan, se identificarán las áreas que necesitan ser actualizadas.

2. **Evaluación del Impacto del Cambio:**
    - Una vez identificado el cambio necesario, se evaluará el impacto que tendrá en la organización y en los riesgos que se están gestionando.
3. **Revisión de Contenido del Plan:**
    - El Comité de Seguridad revisará el contenido del plan y las políticas relacionadas para asegurarse de que todas las áreas afectadas sean modificadas de acuerdo con el cambio identificado.
4. **Implementación de la Actualización:**
    - Se implementarán las actualizaciones y se comunicarán a todos los miembros de la organización, especialmente aquellos responsables de las áreas afectadas.
5. **Documentación de la Actualización:**
    - Se actualizarán todos los documentos relacionados con el plan, y se archivarán los registros correspondientes de la revisión y los cambios implementados.
6. **Comunicación de Cambios:**
    - Los cambios en el plan serán comunicados a todos los empleados y partes interesadas para asegurar que estén informados y preparados para aplicar las nuevas medidas.

9.4 Medición de la Eficacia del Plan Actualizado

Una vez realizado el proceso de revisión y actualización, es importante medir la eficacia del plan actualizado:

1. **Evaluación Post-Implementación:**
    - **Descripción:** Tras la implementación de las actualizaciones, se realizará una evaluación de los resultados para asegurarse de que las modificaciones mejoraron la eficacia del plan y no generaron nuevos riesgos.
    - **Frecuencia**: Después de la actualización.
    - **Responsables:** Comité de Seguridad, equipo de auditoría.

10. Conclusión

Finalmente, el plan debe concluir con un compromiso por parte de la alta dirección y un llamado a la acción para todos los empleados, destacando la importancia de cumplir con las políticas y procedimientos establecidos.

La alta dirección de Empresas de Servicios Públicos de La Ceja E.S.P. reafirma su compromiso con la protección de la seguridad y la privacidad de la información, y se espera que todos los empleados colaboren activamente en la implementación de este Plan de Tratamiento de Riesgos.

Elaboro:
María Carolina Noreña Sosa
Profesional Universitaria de las TIC