Modelo de Seguridad y Privacidad de la Información

1. Políticas y Directrices de Seguridad de la Información

La entidad cuenta con un conjunto de políticas diseñadas para gestionar de manera efectiva los riesgos de seguridad de la información:

- **Política de Control de Acceso:** Define los niveles de autorización necesarios para acceder a datos y sistemas críticos, mediante controles basados en roles y autenticación multifactorial.
- **Política de Gestión de Contraseñas:** Establece estándares de contraseñas seguras, rotación periódica y protección contra almacenamiento inseguro.
- **Política de Clasificación de la Información:** Define criterios para categorizar la información en función de su sensibilidad y criticidad, asegurando un manejo adecuado en cada nivel.

2. Gestión del Riesgo de Seguridad de la Información

La entidad lleva a cabo un proceso continuo de gestión de riesgos que incluye:

- **Identificación de Riesgos:** Análisis de amenazas y vulnerabilidades en sistemas y procesos clave.
- **Valoración y Tratamiento de Riesgos:** Definición de planes de acción para mitigar, transferir, aceptar o eliminar los riesgos identificados.
- **Monitoreo y Seguimiento:** Evaluaciones regulares para verificar la efectividad de las medidas implementadas.

3. Respaldo y Recuperación de Datos

El respaldo de la información es una prioridad estratégica, y para garantizar la disponibilidad y recuperación en caso de incidentes, la entidad utiliza:

- **Veeam Backup:** Solución especializada para realizar copias de seguridad de los datos y sistemas críticos.
- **Frecuencia y Verificación de Backups:** Respaldo diario y pruebas regulares de restauración para verificar la integridad de los datos respaldados.
- **Ubicaciones Redundantes:** Copias almacenadas en diferentes ubicaciones físicas para proteger contra desastres locales.

4. Seguridad de la Infraestructura de Red

La infraestructura tecnológica está protegida mediante:

- **Cortafuegos (Firewalls):** Restricción de tráfico no autorizado hacia los sistemas de la entidad.

- **Sistemas de Prevención y Detección de Intrusos (IDS/IPS):** Monitorización continua de actividades sospechosas y bloqueos automáticos de intentos de intrusión.
- **Segmentación de Red:** Separación de redes internas para limitar la propagación de posibles ataques.

5. Gestión de Incidentes de Seguridad

La entidad dispone de un **Plan de Respuesta a Incidentes**, que incluye:

- **Detección y Notificación:** Mecanismos para identificar y reportar incidentes de forma inmediata.
- **Análisis y Contención:** Evaluación del impacto y aplicación de medidas para contener el incidente.
- **Recuperación y Aprendizaje:** Restauración de operaciones y adopción de mejoras basadas en las lecciones aprendidas.

6. Cumplimiento Normativo

La entidad asegura el cumplimiento de normativas nacionales e internacionales, tales como:

- **Ley 1581 de 2012**: Protección de Datos Personales.
- **Decreto 1377 de 2013**: Reglamentación para la gestión de datos personales.
- **Resolución MinTIC 1591 de 2020**: Lineamientos para la gestión de la seguridad digital en entidades públicas.
- **ISO/IEC 27001:** Estándar internacional para la gestión de la seguridad de la información.

7. Capacitación y Concientización

Para fomentar una cultura organizacional de seguridad, se realizan:

- **Talleres y Capacitaciones:** Formación continua para el personal sobre buenas prácticas de seguridad.
- **Simulacros de Incidentes:** Ejercicios prácticos para preparar a los equipos en la gestión de incidentes.

8. Auditorías y Evaluaciones de Cumplimiento

Se realizan auditorías periódicas para evaluar el estado de la seguridad y verificar el cumplimiento de las políticas y normativas aplicables. Estas auditorías incluyen:

- **Revisión de Controles de Seguridad:** Evaluación de la efectividad de las medidas implementadas.
- **Pruebas de Penetración:** Simulaciones de ataques para identificar vulnerabilidades.