- ❖ Coordinar con los propietarios de los procesos y activos de información, la alineación con la seguridad de la información definida por la institución pública.
- ❖ Asegurarse que la implementación de los controles de seguridad de la información es coordinada en toda la institución pública.
- ❖ Verificar la falta o superposición de controles en seguridad de la información.
- ❖ Desarrollar métricas y métodos que permiten monitorear las actividades de seguridad de la información y verificar la eficiencia y eficacia de los controles.
- ❖ Promover el cumplimiento con la normativa y legislación vigente en relación con aspectos de seguridad de la información.
- ❖ Promover el cumplimiento de las políticas y documentos relacionados del Sistema de Gestión de Seguridad de la información.
- ❖ Identificar cambios significativos en las amenazas y la exposición de la información y de las instalaciones de procesamiento de la información a las amenazas.
- ❖ Evaluar la información recibida de los seguimientos y revisiones de los incidentes de seguridad de la información y las acciones recomendadas en respuesta a los mismos.
- ❖ Colaborar con el Centro de Gestión de Incidentes Informáticos de la AGETIC en cuanto a notificación, evaluación, tratamiento y solución de incidentes se refiere.
- ❖ Colaborar con el equipo responsable por la definición e implementación del Plan de Continuidad del Negocio.

• BS 7799-3:2006: Proporciona una guía para soportar los requisitos establecidos por ISO/IEC 27001:2005 con respecto a todos los aspectos que debe cubrir el ciclo de análisis y gestión del riesgo en la construcción de un sistema de gestión de la seguridad de la información (SGSI).

• NTC 27001:2006: Sistema de Gestión de Seguridad de la Información (SGSI). En 2005, con más de 1700 empresas certificadas en BS7799-2, ISO publicó este esquema como estándar ISO 27001, al tiempo que se revisó y actualizó ISO 17799 y esta última norma se denomina ISO 27002:2005 el 1 de julio de 2007, manteniendo el contenido así como el año de publicación formal de revisión.

• ISO 27002:2005: Esta norma proporciona recomendaciones de las mejores prácticas en la gestión de la seguridad de la información a todos los interesados y responsables en iniciar e implantar o mantener sistemas de gestión de la seguridad de la información. En el siguiente esquema se pretende abordar los principales contenidos de la norma

• ISO/IEC 27001:2005: Es la evolución certificable del código de buenas prácticas ISO 17799. Define cómo organizar la seguridad de la información en cualquier tipo de organización, con o sin fines de lucro, privada o pública, pequeña o grande. Es posible afirmar que esta norma constituye la base para la gestión de la seguridad de la información

• ISO/IEC TR 18044:2004: Ofrece asesoramiento y orientación sobre la seguridad de la información de gestión de incidencias para los administradores de seguridad de la información y de los administradores de sistemas de información.

6. ADVERTENCIA

Cualquier usuario de los recursos de TIC del FONDESIF que se encuentre realizando actividades que vayan en contra del Manual de Normas y Políticas de Seguridad Informática, da lugar a que la Entidad realice las investigaciones disciplinarias pertinentes y reportar a los entes de control de la institución cuando haya lugar.

7. DEFINICIONES

ACTIVO: Se refiere a cualquier información o sistema relacionado con el tratamiento de la misma que tenga valor para la organización.

APLICACIONES CRITICAS: Son las aplicaciones o sistemas de información que reciben este término porque previamente se encuentran clasificados como vital o necesarias para el buen funcionamiento de los procesos y procedimientos misionales.

BASE DE DATOS: Se define una base de datos como una serie de datos organizados y relacionados entre sí, los cuales son recolectados y explotados por los sistemas de información.

BRECHA: Término que se utiliza para denominar la diferencia que se observa entre el mecanismo de seguridad que existe y la situación ideal para evitar que germinen vulnerabilidades que impacten el negocio de la Entidad.

BUENAS PRACTICAS: Son lineamientos que contiene los principios básicos y generales para el desarrollo de los productos o servicios de la organización para la satisfacción al cliente.

CICLO DE VIDA DE LA INFORMACIÓN DIGITAL: Se refiere a la clasificación y almacenamiento de la información; siendo necesario tener en cuenta los requisitos técnicos y legales; así como tener claro los conceptos de disponibilidad y velocidad que depende de la misma clasificación que varía conforme su valor con el tiempo.

CLASIFICACION DE LAS APLICACIONES: Las aplicaciones se clasifican conforme los procesos de la entidad.

CLASIFICACION DE LA INFORMACIÓN: Proceso formal que se utiliza para ubicar el nivel a la información de la Entidad con el fin de protegerla; previa estructura de valoración en atención al riesgo que se presume existe si hay una divulgación no autorizada. Generalmente la información debería clasificarse en relación a su valor, requisitos legales, sensibilidad y criticidad para la Organización.

CLIENTES: Persona natural o usuario que recibe un producto Institucional. El cliente puede ser interno o externo a la organización.

CONTINGENCIA: Es la consecuencia de acciones o imprevistos, que puede poner en peligro la integridad, disponibilidad y confiabilidad de la información.

CONFIDENCIALIDAD: Acceso a la información por parte únicamente de quienes esté autorizados.